

bradscholars

Vulnerability in online social network profiles. A Framework for Measuring Consequences of Information Disclosure in Online Social Networks

Item Type	Thesis
Authors	Alim, Sophia
Rights	<p>
The University of Bradford theses are licenced under a Creative Commons Licence.</p>
Download date	2026-06-13 00:39:29
Link to Item	https://bradscholars.brad.ac.uk/handle/10454/5507.2



University of Bradford eThesis

This thesis is hosted in [Bradford Scholars](#) – The University of Bradford Open Access repository. Visit the repository for full metadata or to contact the repository team



© University of Bradford. This work is licenced for reuse under a [Creative Commons Licence](#).

VULNERABILITY IN ONLINE SOCIAL NETWORK PROFILES

A Framework for Measuring Consequences of Information
Disclosure in Online Social Networks

Sophia ALIM

submitted for the degree
of Doctor of Philosophy

Department of Computing
School of Computing, Informatics and Media

University of Bradford

2011

Sophia Alim

Vulnerability in Online Social Network Profiles

Keywords: personal information disclosure; data retrieval; vulnerability measurement; privacy and personal details in OSNs.

Abstract

The increase in online social network (OSN) usage has led to personal details known as attributes being readily displayed in OSN profiles. This can lead to the profile owners being vulnerable to privacy and social engineering attacks which include identity theft, stalking and re identification by linking.

Due to a need to address privacy in OSNs, this thesis presents a framework to quantify the vulnerability of a user's OSN profile. Vulnerability is defined as the likelihood that the personal details displayed on an OSN profile will spread due to the actions of the profile owner and their friends in regards to information disclosure.

The vulnerability measure consists of three components. The individual vulnerability is calculated by allocating weights to profile attribute values disclosed and neighbourhood features which may contribute towards the personal vulnerability of the profile user. The relative vulnerability is the collective vulnerability of the profiles' friends. The absolute vulnerability is the overall profile vulnerability which considers the individual and relative vulnerabilities.

The first part of the framework details a data retrieval approach to extract MySpace profile data to test the vulnerability algorithm using real cases. The profile structure presented significant extraction problems because of the dynamic nature of the OSN. Issues of the usability of a standard dataset including ethical concerns are discussed. Application of the vulnerability measure on extracted data emphasised how so called 'private profiles' are not immune to vulnerability issues. This is because some profile details can still be displayed on private profiles.

The second part of the framework presents the normalisation of the measure, in the context of a formal approach which includes the development of axioms and validation of the measure but with a larger dataset of profiles. The axioms highlight that changes in the presented list of profile attributes, and the attributes' weights in making the profile vulnerable, affect the individual vulnerability of a profile.

Validation of the measure showed that vulnerability involving OSN profiles does occur and this provides a good basis for other researchers to build on the measure further. The novelty of this vulnerability measure is that it takes into account not just the attributes presented on each individual profile but features of the profiles' neighbourhood.

Acknowledgements

I would firstly like to offer a special thank you and appreciation to my supervisors Dr Daniel Neagu and Mr Mick Ridley for their advice, encouragement and contributions throughout the research. Also I would like to thank my colleague and research papers co-author Ruqayya AbdulRahman for all her help in the collaborative research that we carried out together and Dr James Caverlee for allowing access to his MySpace dataset. Finally I would like to thank my family and friends for their continued support throughout the PhD.

Publications and Presentations Associated With Thesis

Publications

Alim, S., Neagu, D. and Ridley, M. (2011). A Vulnerability Evaluation Framework for Online Social Network Profiles: Axioms and Propositions. Inderscience, *Int. J. Internet Technology and Secured Transactions* (In Press).

AbdulRahman, R., Alim, S., Neagu, D., Holton, D.R.W. and Ridley, M.J. (2011). Multi Agents System Approach for Vulnerability Analysis of Online Social Network Profiles over Time. Inderscience, *Int. J. Knowledge and Web Intelligence* (In press).

Alim, S., Neagu, D. and Ridley, M. (2011). Axioms for Vulnerability Measurement of Online Social Network Profiles. IEEE. International Conference in Information Society. In: *Proceedings of the International Conference in Information Society (i-Society) 2011, 27th-29th June 2011, London, UK*, pp. 241-247.

Alim, S., Abdul-Rahman, R., Neagu, D. and Ridley, M. (2011). Online social network profile data extraction for vulnerability analysis. Inderscience, *Int. J. Internet Technology and Secured Transactions* , 3(2), pp. 194-209

AbdulRahman, R., Alim, S., Neagu, D. and Ridley, M. (2010). Algorithms for Data Retrieval from Online Social Network Graphs. IEEE. International IEEE Conference on Computer and Information Technology. In: *Proceedings of the 10th International IEEE Conference on Computer and Information Technology (CIT 2010), 29th June-1st July 2010, Bradford, UK*, (pp.1660-1666), IEEE CS.

Alim, S., Abdul-Rahman, R., Neagu, D. and Ridley, M. (2009). Data retrieval from online social networking profiles for social engineering applications. IEEE. International Conference for Internet Technology and Secured Transactions. In: *Proceedings of the 4th International Conference for Internet Technology and Secured Transactions ICITST-2009, 9th-12th November 2009, London, UK*, (pp.207-211).

Presentations

2011- The International Conference on Information Society (i-Society 2011):
Axioms for Vulnerability Measurement of Online Social Network Profiles

2010- The Institution of Engineering and Technology (IET) invited talk:
Algorithms for Social Engineering in Online Social Network (with Sophia Alim,
Daniel Neagu, Ruqayya Abdulrahman and Mick Ridley)

2010- The 10th IEEE International Conference on Computer and Information
Technology (CIT-10): Algorithms for Data Retrieval from Online Social Network
Graphs

2010-Open Day: Automated Data Retrieval from Online Social Network Profiles

2010-AI Research Seminar: Node Vulnerability in Online Social Network
Graphs

2009-Presentation at FAIRS 2009 in Cambridge University (UK) which is the
third annual forum for AI research students: Automated Data Retrieval from
Online Social Network Profiles

2009-Presentation and Demonstration to students from Bradford Grammar
School: Automated Data Extraction from Online Social Network Profiles

2009-Presentation to Teachers: Node Vulnerability in Social Network Graphs

2008-Research Seminar: Social Networking and Node Vulnerability

Table of Contents

Abstract	ii
Acknowledgements	iv
Publications and Presentations Associated With Thesis	iv
Publications	iv
Presentations	v
List of Figures.....	x
List of Tables.....	xi
CHAPTER 1: INTRODUCTION	1
1.1-Research Background	1
1.2-Motivation.....	3
1.3-Aims and Objectives	4
1.4-Methodology	5
1.5-Scope	5
1.6-Thesis Structure.....	6
CHAPTER 2: BACKGROUND AND RELATED WORK.....	8
2.1-Offline Social Networks	8
2.1.1-What Constitutes an Online Social Network.....	9
2.2-History of Online Social Networks	10
2.3-Developments in Social Networking Field	15
2.3.1-Inference.....	16
2.3.2-Information Disclosure Measures	17
2.3.3-Social Network Analysis.....	18
2.3.4-Media Stories	18
2.4-Six Degrees of Separation	19
2.4.1-Small World Effect.....	22
2.5-Privacy Attacks associated with Personal Details.....	25
2.6-Privacy Attitudes and Age	28
2.6.1-Children.....	29
2.6.2-Adolescents.....	32
2.6.3-Young Adults and Adults.....	34
2.6.4-Older Adults	36
2.7-Introduction into Graph Theory associated with an Online Social Network	38

2.7.1-Characteristic Measures for Complex Network Classification	42
2.8-Social Network Analysis Measures	44
2.8.1-Centrality Measures	44
2.8.2-Other Measures	47
2.8.3-Vulnerability Definitions	50
2.9-Conclusions	52
CHAPTER 3: VULNERABILITY MEASURE	53
3.1-Initial Vulnerability Concept.....	53
3.2-Vulnerability Formalism and Explanation	55
3.2.1-Vulnerability Measure Assumptions	57
3.2.2-Individual Vulnerability.....	57
3.2.3-Relative Vulnerability	61
3.2.4-Absolute Vulnerability	63
3.3-Vulnerability Measure Algorithm	64
3.4-Vulnerability Measure Application.....	66
3.5-Vulnerability Algorithm Issues	67
3.5.1-Attribute Weights	67
3.5.2-Choice of Attributes.....	77
3.5.3-Relationship Strength	77
3.5.4-Analysing different parts of the profile	84
3.6-Conclusions	84
CHAPTER 4: ONLINE SOCIAL NETWORK DATA EXTRACTION AND GRAPH PROCESSING	86
4.1-Data Extraction Methodologies in Social Networking.....	86
4.2-Our Data Extraction Approach	87
4.2.1-Breadth First Search.....	91
4.3-Data Extraction Findings	92
4.4-Online Social Network Graph Processing	94
4.5-Elements of an Online Social Network Graph that can affect Vulnerability	99
4.6-Ethical Issues associated with Extraction.....	101
4.7-Conclusions	103

CHAPTER 5: EXPERIMENTAL WORK ASSOCIATED WITH DATA EXTRACTION.....	105
5.1-Data Extraction Findings	105
5.2-Online Social Network Graph Findings	106
5.3-Case studies and Validation	108
5.4-Levels in Online Social Networks.....	111
5.5-Improvements	117
5.6-Conclusions	118
 CHAPTER 6: MODELLING OPERATORS FOR INDIVIDUAL VULNERABILITY	120
6.1-Improved Individual Vulnerability Calculation and Meaning	120
6.2-Normalisation	122
6.3-Modelling Criteria.....	123
6.4-Types of Functions and their Behaviours	126
6.5-Function Case Studies.....	128
6.6-Results	129
6.7-Validation of Case Studies.....	132
6.8-Improvements	134
6.9-Conclusions	134
 CHAPTER 7: AXIOMS, PROPOSITIONS AND VULNERABILITY MEASURE PROPERTIES	136
7.1-Vulnerability Measure Properties	136
7.2-Axioms.....	138
7.2.1- A Sample of Axioms Application.....	142
7.3-Propositions.....	144
7.4- Experimental Work and Findings Regarding Application of Propositions	162
7.5-Discussion	164
7.6-Conclusions	167
 CHAPTER 8: ADDITIONAL EXPERIMENTAL WORK VALIDATION.....	168
8.1-Vulnerability Measure Validation.....	168
8.1.1-Experiment 1: Vulnerability due to the Disclosure of the attribute values by the Neighbours.	169
8.1.2-Experiment 2: Vulnerability due to the Disclosure of the attribute values by the Friends of Friends.....	177

8.1.3-Experiment 3: Vulnerability of Larger Dataset due to the Disclosure of the attribute values by the Friends of Friends.....	181
8.2-Privacy Levels	186
8.2.1-Privacy levels and Vulnerability	191
8.3-Case Studies for Attribute Disclosure	197
8.4-Alternative Ways of Calculating Relative and Absolute Vulnerability.....	200
8.5-Challenges with Data Extraction	203
8.5-Conclusions	205
 CHAPTER 9: CONCLUSIONS AND FUTURE WORK.....	 208
9.1-Research Summary and Conclusions.....	208
9.2-Contributions to the Field of Online Social Networks	214
9.3-Future work.....	216
 References	 219
 Appendices.....	 231
Appendix I.....	231

List of Figures

Figure 1-A Directed Weighted Multigraph	39
Figure 2-A Directed Graph to Illustrate The Concept Of Paths	41
Figure 3-Kite Network from Krackhardt (1990).....	45
Figure 4-Reachability Matrix Example from (Tan 2007)	49
Figure 5-Unnormalised Vulnerability Measure Algorithm	64
Figure 6-Unnormalised Vulnerability Measure Application.....	67
Figure 7-Attribute Importance Classification	75
Figure 8-Data Extraction Approach for OSN Profiles	89
Figure 9-A Graph to illustrate Breadth First Search.....	92
Figure 10-OSN Graph for Top Friends Extraction	94
Figure 11-Indegree Distribution for Top Friends Extraction	96
Figure 12-Outdegree Distribution for Top Friends Extraction	97
Figure 13-The Concept of Indegree and Outdegree for a node in an OSN.....	100
Figure 14-Indegree Distribution for All Friends Extraction.....	107
Figure 15-Outdegree Distribution for All Friends Extraction.....	108
Figure 16-Levels of Friends and Vulnerability in an OSN.....	112
Figure 17-Graph of Mathematical Function Behaviours	127
Figure 18-OSN Graph and Table of Weights.....	142
Figure 19-Terminology for Experiments 1 to 3	169
Figure 20-Correlation between High Relative Vulnerability Profiles and Attribute Disclosure by Profiles' Neighbourhood.....	175
Figure 21-Correlation between High Relative Vulnerability Profiles and Attribute Disclosure by Profiles' Friends of Friends for a Small Profile Sample.....	180
Figure 22-Correlation between High Relative Vulnerability Profiles and Attribute Disclosure by Profiles' Friends of Friends for Bigger Profile Sample	184
Figure 23-Correlation between Neighbours with Various Relative Vulnerabilities and Neighbours' Personal Details Disclosure.....	193
Figure 24-Correlation between Neighbours with High Relative Vulnerability and Neighbours' Personal Detail Disclosure	195

List of Tables

Table 1-Privacy Risks Associated with Personal Details	25
Table 2- Different Extraction Methods from OSNs	87
Table 3-Case Studies for Unnormalised Vulnerability Measure	109
Table 4-Case Study Details for Various Users and their Profile Characteristics	129
Table 5-Vulnerability Values for the Case Studies where β is 0.5.....	129
Table 6-Statistics regarding Application of Different Operators	163
Table 7-Percentage of Disclosure of Attributes Viewable to the Start Profile..	188
Table 8-Vulnerability and Disclosure Details for Case Studies	198
Table 9-Vulnerability Results for Operator Combinations	201

CHAPTER 1: INTRODUCTION

1.1-Research Background

The World Wide Web (WWW) has played a part in the communication of humans for a number of years. Around 10-13 years ago though, internet usage was very different in terms of the activities carried out by the user. This is illustrated by a survey done by the U.S. Department of Commerce, into the access of technology tools in the years 1998 and 2000 (U.S Department of Commerce. 2000).

Their results indicated that there were many activities carried out online. Some of the most popular included searching for news and information, but the most popular activity was checking emails. Life before the online social networking revolution had very different characteristics (e.g. more face to face conversations between users and children were playing outside more rather than staying in and playing on the computer). Also people were not as open about themselves online (Kalamdani 2009). The introduction of online social networks (OSNs) and Web 2.0 changed those characteristics.

One of fastest growing phenomena has been the availability of social network sites on the WWW. Nielsen (2009) emphasised this by highlighting the fact that OSN sites have been overtaking email usage. A survey carried out in 2009 by Nielsen (2009) showed that 65.1% of web users used email but 66.8% were using OSN sites. Also in 2010 Nielsen (2010b) carried out a survey which found that Americans spent 22.7% of their time using OSNs in contrast to 8.3% of their time checking emails. This highlights that OSN usage for some users is becoming part of their daily life.

OSNs have been adopted by users of all different ages, varying from young children to older adults. They encourage vast amounts of different types of

Chapter 1-Introduction

information to flow around the WWW everyday and this is the area in which concern is starting to grow. With the freedom and innovation of OSNs comes the price of privacy. Unlike the past, people are more open with each other online and this encourages personal details to be shared. The disclosure of personal details on OSN profiles can cause problems for users of information systems which require personal details to authenticate the user. If a stranger gets hold of your personal details they can impersonate you and commit identity fraud.

Facebook, the most popular OSN, which in 2010 reached 500 million active users (Facebook 2010), has quite an interesting and controversial history regarding privacy.

For example, a significant event, which highlighted privacy breaches for Facebook users in November 2007, was the use of Beacon (the advertising system that monitored Facebook users), when users went shopping online, Facebook shared the data of what they bought with the users' friends and other businesses (BBC News 2007). This event is similar to a company called Phorm who in 2008 wished to target online advertisements based on users' online browsing behavior which in some peoples' eyes breached customer privacy (BBC News 2008b).

In July 2010, the security consultant Rob Bowes highlighted publically available profiles on Facebook by extracting personal details from them and publishing the data online. The extraction occurred from 100 million profiles that were open and publically available. Bowe's motivation for this action was to highlight the privacy issues associated with Facebook (Emery 2010). In 2011, two doctoral students at Indiana University had discovered a security vulnerability in Facebook, which allowed malicious websites to access the real name and the

Chapter 1-Introduction

private profile data of the visitor. Also the malicious websites could post bogus messages on the visitor's wall (Indiana University 2011).

Other OSNs besides Facebook have had issues regarding privacy. In 2010 it was found that in addition to Facebook, MySpace, LiveJournal, Twitter, Hi5, Xanga and Digg had been sending data to advertising companies. The data can be used to find out the personal details and names of users. This happened despite privacy policies of the OSNs claiming that they do not share user data without getting consent. When a user clicked on an advertisement, the user names and ID numbers of the personal profiles that were being viewed by the user were sent to the advertising companies. The companies can use the user names and ID numbers to go to find the profiles and view the public data available on there. Depending on the OSN site, the public data can include age, full real name of the user, occupation and hometown (Steel and Vascellaro 2010).

These events have highlighted the issue of privacy in OSNs and how personal details can spread into the wrong hands. This can make users vulnerable to privacy and social engineering attacks. An example of a privacy attack is reidentification by linking (Sweeney 1997) which would enable people to extract some personal details from an OSN profile and use external sources to investigate that person's identity. Social engineering attacks can also occur. One example is phishing where fraudsters get users to give their personal details to them via scams. Then they use the given details to look for profiles of that user on the WWW.

1.2-Motivation

The motivation for this research emerges from the need to address privacy in OSNs by establishing a measure which quantifies how vulnerable an OSN user

Chapter 1-Introduction

is to social engineering attacks and the spreading of personal details, because of the users own personal information disclosure and that of their friends network. OSN networks can be represented by graphs and the use of graphs will aid the calculation of vulnerability. At present in the social networks analysis field there is a lack of vulnerability measures based on graph theory which quantifies vulnerability and takes the information disclosure of the OSN user and its friends into account. In graph theory, an OSN graph consists of a node which represents an OSN profile which is used to by the OSN user to present their personal details and an edge which represents a friendship connection between two OSN profiles.

1.3-Aims and Objectives

The aim of this research is to design and implement an approach to measure how vulnerable an OSN profile is to privacy and social engineering attacks and the spreading of personal details through relationships represented using graph theory in this work.

The objectives of the research are:

1. Analysis of various OSN profiles and connections in order to define the concept of vulnerability.
2. Apply probability algorithms in order to establish a vulnerability measure which will enable the identification of vulnerable nodes.
3. Design and implement a data extraction approach for OSN profiles which will provide real life case studies for the vulnerability measure to be applied to. This will be part of the experimental work in order to analyse the effects of the vulnerability measure on different cases.
4. Investigate structural factors based in the OSN representation which can affect the vulnerability value of a profile.

1.4-Methodology

The methodology is a combination of several aspects of the research. Firstly a data retrieval approach is developed with graph algorithms in order to extract real life cases from an OSN in order to test the vulnerability algorithm on real data. The extracted data is subsequently placed into a repository and forms the basis for an OSN graph to be generated and the vulnerability algorithm for the vulnerability measure to be applied. The vulnerability measure uses the OSN graph in the calculations.

The vulnerability measure involves a mathematical operator between the vulnerability of a profile and the vulnerability of the profile's friends. A mathematical operator is defined by a mathematical function and various mathematical functions can be studied to investigate the properties and how they influence the vulnerability value of a profile.

There are two versions of the vulnerability measure which includes the unnormalised and normalised. The unnormalised version is covered in chapter 3 and used in the experimental work which is detailed in chapters 4 and 5. The normalised version of the vulnerability measure which was developed as a consequence of experimental findings is used in chapters 6-8.

The axioms and propositions which are presented in chapter 7 form the formal approach for the measure. They were formed after substantial experimental work which involved investigating how the vulnerability measure works and normalising the measure to a value between 0 and 1. The validation of the vulnerability measure with regard to variety of situations is detailed in chapter 8.

1.5-Scope

In terms of assumptions, the vulnerability measure assumes that only immediate friends of a profile can make it vulnerable. The friends of a friend or

Chapter 1-Introduction

external users are not taken into account. Also the strength of relationship between a profile and its friend is not incorporated in the measure. The strength of relationship between two profiles can be defined by the level of interaction which includes the writing of profile comments and the tagging of photos. If the two profiles do not interact as much then the personal details may or may not be leaked. The effect of presenting vulnerable attributes on OSN profiles is the same regardless of the type profile owner.

1.6-Thesis Structure

The rest of the thesis is organised as follows:

Following this introduction, chapter 2 surveys relevant literature in the OSN field by exploring the history of OSNs, as well as detailing several aspects that the concept of vulnerability is built upon. These aspects include privacy risks, graph theory as applied to OSNs and social network analysis measures.

Chapter 3 details the proposed vulnerability measure in its unnormalised form, based on the vulnerability concept alongside the algorithm and the issues associated with the algorithm.

Chapter 4 details our proposed OSN profile data extraction approach based on a *top friends* network and the processing of the OSN graph which is derived from the extraction. Also the findings associated with the extraction and the ethical issues associated with extracting OSN profiles are presented.

Chapter 5 extends the work done in chapter 4 by focusing on the graph findings and the validation of the vulnerability case studies based on extracting *all friends* from an OSN profile. Also an additional experiment is presented which examines the concept of levels in an OSN and how this can affect the vulnerability of a profile.

Chapter 1-Introduction

Chapter 6 explores the modeling of the individual vulnerability of a profile based on the privacy attitudes of the profile owner and how this affects the overall vulnerability of the profile.

Chapter 7 presents the axioms and propositions which forms the formal approach of the vulnerability measure.

Chapter 8 details the experiments to validate the vulnerability measure on a larger scale and show that the vulnerability concept is a valid one.

Chapter 9 presents the overall conclusions to the thesis, ideas for future research as well as detailing our contribution to the field of social network analysis.

CHAPTER 2: BACKGROUND AND RELATED WORK

The aim of this chapter is to provide an overview of background work as well as related work in other fields associated with vulnerability. Section 2.1 introduces the concept of offline social networks which leads on to a look into the features which make up an OSN and what sort of OSNs will be used in this thesis. Section 2.2 covers the history of OSNs. Section 2.3 explores current research developments in the OSN field which relate to the field of vulnerability.

Section 2.4 investigates the six degrees of separation which forms the basis for the experimental work on the concept for OSN levels which is detailed in section 5.4. Sections 2.5-2.6 present privacy attacks which can occur with information disclosure of personal details. This contributes towards the motivation for proposing a vulnerability measure. Also detailed are the various attitudes of different types of OSN users towards information disclosure.

Section 2.7 introduces important concepts of graph theory which can be applied to OSN graphs and are used in social network analysis measures to analyse an OSN. The graph will aid the calculation of the vulnerability of a profile. Section 2.8 centers on the current social network analysis measures and why there needs to be more measures associated with privacy and especially vulnerability. Section 2.8.2 investigates the various vulnerability definitions in regards to graph theory and this work provides more motivation for the proposed vulnerability measure. Section 2.9 concludes for this chapter.

2.1-Offline Social Networks

In general offline social network definitions cover the same concept in different ways. Downes (2005) describes an offline social network as a collection of individuals that are linked together by a set of relations. This definition illustrates that a variety of relations can link two individuals together e.g. sexual

Chapter 2-Background And Related Work

relationships, transactions and common interests but the most popular type of relation which is going to be used in this thesis is friendship. Van Tilburg's (1995) definition is similar to Downes (2005) but unlike Downes, emphasises that the relationships between individuals are interdependent which shows that there is a dependency upon each other and implies that the relationship is bidirectional.

2.1.1-What Constitutes an Online Social Network

Online social networks (OSNs) in comparison to offline social networks are web based sites e.g. Facebook¹ and MySpace². In this thesis, we consider web based OSNs but not email based OSNs. Email based OSNs are social networks based on email communications between users (Juszczyszyn and Musial 2009).

Boyd and Ellison (2008) describe the three ingredients of OSNs which include:

- Allowing a user to make a public or semi public profile inside a system which is bounded.
- Bringing together a list of other users in which they share a connection with and allowing the user to view.
- Travelling along their set of connections and the connections made by other users within the system.

This definition is interesting because it compares a user's online social network (OSN) to a bounded system which illustrates that the OSN is a network of interdependent user profiles which interact with one another. Like Downes (2005) and Van Tilburg (1995), Boyd and Ellison (2008) do state that what constitutes a relationship between two individuals can vary between different

¹ <http://www.facebook.com/>

² <http://www.myspace.com/>

Chapter 2-Background And Related Work

OSNs. All the authors though, fail to mention relationships that can happen between two individuals which are not interdependent.

An example of a non-interdependent relationship is the concept of *top friends* where the user can class the friends which they have a strong relationship with as a *top friend*. An example being node *A* may class node *B* as a *top friend* but node *B* may not class node *A* as a *top friend*. This implies that the relationship is not bidirectional. In saying that, some OSN sites (e.g. Facebook) require both individuals to agree to a bidirectional relationship by the accepting of a friend's request.

Boyd and Ellison (2008) highlight the use of public or semi public profiles by users. An OSN profile contains personal details, any interactions between a user and other users they are connected to and a list of these other users. These other users may be friends, acquaintances or even strangers. Having a public profile implies that that the contents of that profile is not hidden from the other users therefore they can see everything. At present some OSNs (e.g. MySpace) even allow external users to view the contents of public profiles. An external user in the case of MySpace is a user which does not have a MySpace account or a connection to profiles of MySpace users. In comparison a semi public profile implies that some of the profile contents are hidden from other users even if an online connection exists between the profile owner and other users.

2.2-History of Online Social Networks

Between the years 1997, when the first OSN (SixDegrees.com) was recognised, to the present day, there have been a variety of different OSNs

Chapter 2-Background And Related Work

which have catered to various users. SixDegrees.com³ was the first OSN site to combine features that were already present on dating sites and Classmates.com (a site that allowed users to connect to their school friends). These features highlighted by (Nickson 2009) were the following:

- Create user profiles which contain personal details about the user (e.g. name, age etc).
- Have the ability to view other users' profiles.
- Invite friends, list friends and have the ability to surf the lists of the friends.

The name of the first OSN was based upon '*6 degrees of separation*' theory made famous by Milgram (1967) , where one person is separated by no more than six degrees (steps) from another. Each step is linked by a *friend of a friend* relationship. This theory is explained and debated in more detail in section 2.4.

Unfortunately due to the lack of stability as a business and the trend of WWW users at that time, SixDegrees.com closed in the year 2000 with an estimated 1,000,000 registered members. Boyd and Ellison (2008) claim the OSN demise was due to the lack of activities to do on the site after accepting friends' requests and there were people who did not have a network of friends that were online. The features of SixDegrees.com formed the basis for the development of other OSNs with additional features (e.g. the classification of top friends as illustrated by Facebook and different OSNs presenting different personal details).

As well as SixDegrees.com, around the last few years of the 20th century there were other OSN sites including MiGente⁴ (targeted at the Hispanic community),

³ <http://www.sixdegrees.com/>

⁴ <http://www.migente.com/>

Chapter 2-Background And Related Work

AsianAvenue⁵ (targeted at the Asian American community) and Blackplanet⁶ (targeted at the African American community) which started a trend of having one directional connection between friends. This is because users could make connections with other users without seeking their approval. LiveJournal⁷ which is an online community where users can keep blogs or journals, was established around the same time in 1999 and they adopted the one direction connection (Boyd and Ellison 2008); (Nickson 2009). The aspect of one directional connection is taken into account in the proposed vulnerability measure.

In 2002, Friendster⁸ was launched and designed to encourage the friendship between friends of friends. An example being that if user *B* is friends with users *A* and *C* but *A* and *C* are not friends. This illustrates the concept of transitivity between profiles and what a mutual friend is. If user *A* wants to find out information about user *C*, then user *A* can view user *B*'s profile. Consequently the identity of user *C* could be built up and cause the privacy of user *C* to be compromised. User *B* is a mutual friend of users *A* and *C*.

As the popularity of Friendster grew, the site began to encounter technical issues which caused the site to become problematic. Friendster lost users because of their policy towards fake profiles. Fake profiles were profiles which represented celebrities, fictional characters who were icons or people who did not exist. The background to this policy stemmed from the design of the site not allowing users to view profiles that were four or more degrees away from them. To get around this problem, users started to become power users who were

⁵ <http://www.asianave.com/>

⁶ <http://www.blackplanet.com/>

⁷ <http://www.livejournal.com/>

⁸ <http://www.friendster.com/>

Chapter 2-Background And Related Work

users that send/accept friends requests with acquaintances or even strangers to demonstrate their popularity (Boyd and Ellison 2008).

The company did not like the use of the fake profiles, so they actively started to delete them. This action went down badly with the users and they started to leave Friendster because of the technical issues, they did not trust the company anymore and most users enjoyed browsing fake profiles (Boyd and Ellison 2008). Despite this, Friendster at present has over 115 million registered users and is a popular OSN site in Southeast Asia (Alexa 2010).

In 2003, MySpace was launched and started to compete with Friendster. MySpace was aimed at adolescents (teenagers) and young adults. The site offered an environment which was driven by music and the idea of customizing your profile to reflect your identity and stand out from everyone else. It was MySpace's ability to listen to their users and implement the functionalities that the users wanted, that made MySpace more popular than Friendster (Boyd and Ellison 2008).

In 2008, MySpace beat another OSN competitor called Facebook to become a leading OSN but Facebook managed to get a wider variety of users to join. This action led to a decline in the number of registered users of MySpace. Facebook beat MySpace because of what the OSN was offering to the user. Facebook centers on the connections and interactions between people in a person's life. In comparison MySpace is presented more as a "*hangout for teenagers*" as McWilliams (2009) illustrates, which is not what some users want. As of 2010 MySpace has more than 100 million users worldwide (MySpace 2010a).

Chapter 2-Background And Related Work

The introduction of Facebook encouraged the expansion of niche communities (e.g. LinkedIn⁹ and Ryze¹⁰ business networking). This is illustrated because in 2004, Thefacebook as it was initially called was introduced but only as an OSN site for Harvard University. In order to become a Thefacebook member the user had to have a Harvard University email address and this is what made the network a private OSN. It was not until 2005 that Facebook, which was its new name, started to expand to accept members from high schools, other universities i.e. Yale and corporate business networks. Eventually Facebook membership was open up to everyone but access could not be gained to closed networks without approval from the administrator or having a relevant email address (Boyd and Ellison 2008). Closed network are networks that require authentication from its members in order to view the contents of the network.

What made Facebook different back in 2005 was that a user could not make their profile public to all users of Facebook. This is no longer the case because users' profiles that are fully public can be searched for via the WWW or the user profile search function in Facebook. This can lead to an increased risk of the personal details of a user spreading throughout the OSN and beyond.

Also what made Facebook different to other OSNs in 2005, was that developers had the ability to build applications that users could install in order to add personality and gaming to their profiles. Applications, if added to a users' profile can allow third parties access to the users' personal details and this also causes spreading of personal information. Section 3.3.4 discusses the privacy issues regarding applications in more detail.

⁹ <http://www.linkedin.com/>

¹⁰ <http://www.ryze.com/>

Chapter 2-Background And Related Work

Facebook has grown to become the leader in OSNs as of 2011 by expanding its functionality to include various services (e.g. Facebook chat ¹¹ which allows users to chat with one another and Facebook places ¹² which allow a user to share their location at a given time with their friends, using a mobile). In 2010 Facebook had more than 500 million active users (Facebook 2010).

The number of users for both Facebook and MySpace have illustrated that OSNs are still popular. The increase in the functionalities of both OSNs will provide more opportunities for personal details of users to spread.

Looking at the future of OSNs, Twitter has become a rival to MySpace and Facebook when it comes to OSN sites used on mobile phones. Twitter ¹³ which is a micro blogging site grew 500% in 2010 in the USA alone (Nielsen 2010a). A micro blogging site is a web service which allows users to use blogs to write small message to other users. The future of OSN sites poses privacy issues especially with OSN data being accessible not just by the WWW but by various other means (e.g. mobile networks, different WWW browsers and applications).

2.3-Developments in Social Networking Field

In the past, the research field of offline and online social networks has covered topics ranging from data mining by the use of information retrieval as illustrated in Bird et al. (2006) and Chau and Xu (2006) right through to exploring privacy concerns amongst the student population. This is also illustrated in studies described in Gross and Acquistli (2005) and Gibson (2007).

In the last few years, offline and online social networking research has focused on privacy concerns and information disclosure due to the introduction and popularity of OSNs as illustrated in section 2.2.

¹¹ <http://www.facebook.com/sitetour/chat.php>

¹² <http://www.facebook.com/places/>

¹³ <http://twitter.com/>

Chapter 2-Background And Related Work

In recent studies involving examining personal details known as attributes on OSN profiles, Strater and Richter (2007), Gibson (2007), Hinduja and Patchin (2008) and Nosko et al. (2010) mainly looked at the data from the viewpoint of trends rather than devising a quantitative measure for privacy aspects. There has been research carried out in to various aspects of privacy. One of which has been inference.

2.3.1-Inference

The inference of personal details from OSN profiles via has become an interesting topic in regards to privacy but the thesis work into vulnerability and quantifying vulnerability does not head into the area of inference.

Lindamood and Kantarcioglu (2008) have looked at inferring private information using OSNs. Their approach talked about the use of machine learning algorithms to predict undisclosed information that was private. The area of machine learning concentrates on studying the design of computer programs in order to derive patterns and rules from past experiences. The computer program which acts as a learner, processes the data which represents past experiences and develops *“an appropriate response to future data, or describe in some meaningful way the data seen”* (Vucetic 2007). However Lindamood and Kantarcioglu (2008) did not look at the disclosure of personal details in terms of the vulnerability of profiles.

In contrast, Becker and Chen (2009) analysed privacy risks through the development of a tool to measure privacy risks and to advise users how to reduce the privacy risks. The aim of the tool was to investigate whether the personal details of a user could be inferred from their friends. This methodology used a threat model approach and the concept of frequency to try and infer the attribute values. In their experiment 93 participants installed the tool and the tool

Chapter 2-Background And Related Work

had a 60 % accuracy rate. This is due to 1673 attributes being inferred, 918 being verifiable inferences and 546 attributes being correctly inferred. This experiment focuses more on deriving the value of the attribute based on the attribute values stated by the friends rather than the spread of an attribute value in an OSN via the interactions made by a profile with its friends and friends of friends.

The spreading of attribute values is important for this research because it allows an investigation into whether an OSN profile displaying attributes that contribute towards privacy and social engineering attacks readily and publically, results in friends of the profile spreading the attribute values through the OSN network, via profile comments written to their friends.

2.3.2-Information Disclosure Measures

Quantifiable measures for information disclosure and vulnerability have started being proposed. This is illustrated by research done by Gundecha et al. (2011) and Schrammel et al. (2009). Gundecha et al. (2011) work focuses on the identification of vulnerable friends and how they impact on the user. A vulnerable friend in regards to a user is defined as a friend whose privacy and security settings will not protect the user or the user's network of friends. A combination of measures is proposed to help identify vulnerable friends. Schrammel et al. (2009) is mainly qualitative and involves investigating the accessibility of personal detail on OSNs to different levels of users (friends and unknown people) by the use of a questionnaire.

Two information disclosure measures were proposed, based on the questionnaire responses to measure for each questionnaire participant, the participants' information disclosure to its friends and information disclosure to unknown strangers.

2.3.3-Social Network Analysis

Graphs can be used to represent and analyse OSNs as illustrated by Wilson and Nicholas (2008). The study of OSN graphs which is introduced in section 2.7 can help to emphasise and understand how privacy is breached in an OSN, through information disclosure using the attributes inside the node rather than just the edges and nodes alone. The personal details on a profile are known as attributes and the node represents a profile in an OSN. Social network analysis measures can also be applied to graphs to explore the behavior of nodes in a social network.

Most of the work on social network analysis measures was undertaken in a pre Web 2.0 era by authors including Freeman (1979) and Wasserman and Faust (1994). In 2008 privacy became a main issue due to the increase of various types of spam attacks that can happen in OSNs (e.g. context aware spam as illustrated by Brown et al (2008)).

Since privacy issues have become more prevalent to end users especially, there is room for measures to consider privacy. Current social network analysis measures which are detailed in section 2.8 can be applied to an OSN graph but concentrate on the node environment (profile network of the OSN user) and fail to take the node contents (what is displayed on the OSN user's profile) into consideration as well. The vulnerability measure detailed in this thesis, takes both the node contents and the node environment into account.

2.3.4-Media Stories

Interesting issues in OSN research even became media stories. One of these issues was the maximum number of friends a human can handle on an OSN profile which is based on Dunbar's number (Dunbar 1992). This concept is illustrated in research done by an anthropologist called Robin Dunbar.

Chapter 2-Background And Related Work

The number of friends a person has can influence their vulnerability. The concept of power users emphasises the competition to have as many friends as possible (Bialik 2007; BBC News 2009). The issue with this is that the person may add strangers to their friend's list. Letting people you do not know view your personal details is risky and increases your chance of identity fraud and stalking. This in turn can increase your vulnerability.

In regards to privacy, work in the social networking field has been done into the analysis of user interactions on an OSN by Yun et al. (2010); Wilson et al. (2009); Viswanath et al. (2009) who look into the various types of user interaction. Interactions between two users, presented on a public profile can cause the loss of personal details and indicate the strength of relationship between the two users. The issue regarding about the strength of relationship between two profiles are presented in section 3.5.3.

Overall, the field of social network analysis measures is where the proposed vulnerability measure (detailed in chapter 3) which focuses on the spread of personal details would be beneficial.

2.4-Six Degrees of Separation

The concept of the six degrees of separation was made famous by Stanley Milgram in 1967. The concept revolves around the idea that one person is separated by no more than six degrees (steps) from another. Each step is linked by a *friend of a friend* relationship.

The aim of Milgram's experiment in OSN graph terms was to measure the average path length (average number of steps) between two nodes which were randomly chosen. The two selected nodes may or may not have known each other. If the two nodes did know each other in OSN graph terms there would be

Chapter 2-Background And Related Work

an edge directly connecting the two nodes together. The experiment (Milgram 1967) involved the following procedure:

1. Information packets were randomly sent by Milgram to people in Nebraska and Kansas in the USA. The information packets contain letters which gave details about the study and about the target person in Boston. Also included were business reply cards that were addressed to Harvard and a roster in which they could write their own name. This was so the researchers at Harvard could track the progress of the experiment and deal with any arising problems. Boston was chosen as the target destination because of the large geographical distance between it and Nebraska and Kansas.
2. If the person agreed to participate, the person was asked if they personally knew (on first name terms) the target person in Boston. If they did, then the person had to forward the letter directly to the target person. If the person did not know the target person, then they had to think of a relative or friend who is more likely to know the target person. If this was the case then the person had to sign the relative or friends name on the roster and forward the information packet to that person. A postcard was also sent to Harvard so they could track the packet's progression towards its target destination.
3. When the information packet did arrive at Boston, the roster was analysed to see how many people the packet had been forwarded to. Also the researchers at Harvard could use the postcards to investigate the packets which did not reach their target destination.

The results from the experiment (Travers and Milgram 1969) stated that out of the 296 information packets sent out, 64 (29%) of the packets actually reached

Chapter 2-Background And Related Work

their target destination. The average path length of these chains was 5.5 which was rounded up to 6 and consequently Travers and Milgram (1969) concluded that people in the USA are separated by an average of six people.

There have been several criticisms regarding the methodology and findings from the experiment. Kleinfield (2002) in particular questioned the reason why there was a low completion rate in regards to the information packets reaching their target destination. Another issue was the fact that Milgram had stated that the information packets had been sent to random people. What Kleinfield (2002) discovered was that there was an advertisement for recruiting for this study but the advertisement was written in such a way to attract social people. Social people probably had bigger circles of friends and would be able to get over class barriers.

James (2006) like Kleinfield (2002) highlights that the failure to participate in the experiment was a major factor towards the low success rate. Milgram's study showed that for whatever reasons, the participants failed to pass the information packets on to people they knew and so social connections were not completed. Therefore the results showed a failure in the small world theory. More research needed to be done into why the participants failed to pass the information packets even though they agreed to take part in the experiment. The participants could have been at any stage of establishing a chain.

In 2001, Duncan Watts repeated Milgram's experiment but used an email message rather than an information packet, as the package that needed to be delivered. There were 48,000 senders and 19 targets in 157 countries. The analysis of the results showed that the average path length was around 6 (Watts et al. 2002). Volunteers who took part in this experiment were given an individual's identity and were asked to email a message to someone who they

Chapter 2-Background And Related Work

thought would know the target individual. This process was repeated until the message reached the target individuals inbox. Like Milgram (1967) experiment, the completion rate was very small. Only 3% of the email chains reached the inboxes of the target individuals.

Leskove and Horvitz (2007) study involved analysing 30 billion MSN Messenger conversations amongst 240 million people. A communication graph was produced from the data gathered which contained 180 million nodes and 1.3 billion undirected edges. The structural features of the communication graph, (e.g. clustering, diameter of the graph and average path length) were analysed and it was found that the average path length of the graph was 6.6. The structural features are explained in section 2.7.

The two studies by Watts and Leskovec and Horvitz have helped to validate that the concept of the six degrees of separation does exist in modern times but is subject to changes in the future. This will come with more work done into OSNs and the degrees of separation.

2.4.1-Small World Effect

The theory of the small world effect was devised by Duncan Watts and Steven Strogatz in 1998 and centers around the concept of the six degrees of separation (Milgram 1967), which states that one person can be linked to another person in no more than six steps. The six degrees concept is important when investigating a profiles' vulnerability in regards to levels in an OSN. An OSN consists of levels of friends which help to build up your network. For a given profile, the levels of friends are as follows:

1. The first level consists of the **friends** of the profile. These friends have a direct friendship link to the profile.

Chapter 2-Background And Related Work

2. The second level of friends is the **friends of friends** of the profile. The friends of friends are friends of the profile's friends. The friends of friends do not have a direct friendship link to the profile but they may know about the existence of the profile by searching the friends list from the OSN profile of the profile's friends.

An OSN consists of dynamic components which are linked together. The use of shortcuts between a small number of the components in the network can turn the network into a small world network and bring users in an OSN closer together.

Small world networks can be identified by the following three characteristics which correspond to the OSN graph G of the network. More details about the characteristics are discussed in section 2.7.1 :

High Average Clustering Coefficient value of OSN graph G :

The clustering coefficient of a node (Watts and Strogatz 1998) reflects how well connected the node's friends are to each other. The coefficient value is between 0 and 1. A value of 0 means that the friend are not connected to each other and therefore do not know each other. A value of 1 indicates that the friends all know each other and therefore are connected to each other in graph G . This is commonly known as a clique. The average clustering coefficient of graph G is the average of all the clustering coefficients of the nodes in graph G .

A small world network is classed as having a high average clustering coefficient value because of the increase in the number of cliques in the network. This means that some of the nodes have highly connected neighbourhoods which will have a high individual clustering coefficient value.

Small average shortest path length for graph G

In graph G , a path length between two nodes is the number of edges between the two nodes. The shortest path length known as the geodesic distance is the minimum number of edges between two nodes. The average shortest path length for graph G is the average of all the shortest path lengths for each pair of nodes.

A small average path length indicates that a pair of nodes in graph G will have a short distance between them. This is where the small world effect concept is derived from. In this case, it is about bringing people closer together via the use of OSNs.

Degree distribution of graph G fits power law distribution

The degree is the total number of edges that are connected to a node. For a directed graph, the indegree and the outdegree distributions are analysed separately (Barabási and Oltvai 2004). The indegree of a node is the number of edges heading towards the node and the outdegree is the number of edges heading away from the node.

A power law distribution is a probability distribution which focuses on the frequency of the degree values for all of the nodes. Most of the nodes will have a low degree value and fewer nodes have a high degree value. The tail of the distribution will be long.

In a small world network, there are an increased number of nodes that have a high degree value (known as hubs). This forms the basis for the shorter path lengths between the nodes.

The indegree and outdegree distributions are important for analysis because they allow outliers to be identified which could prove significant when accessing

Chapter 2-Background And Related Work

the vulnerability of a profile. A neighbour of a node with a high outdegree could contribute towards spreading of the node's personal details deep into the OSN.

2.5-Privacy Attacks associated with Personal Details

Personal details presented and available online, raise social engineering issues as they can be used for identity fraud as emphasised by Narayanan and Shamatikov (2010). Personal details (e.g. first name and date of birth) are considered as '*personal identifiable information*' which can be used to identify ones individual data (Krishnamurthy and Wills 2009).

Since many web systems use personal details to authenticate users (e.g. online banking and payment), an individual is making themselves vulnerable to various privacy and social engineering attacks by being open about their lives online. This is a change from the past where people had more face to face conversations and did not disclose their personal details so readily. Some privacy risks involving personal details are illustrated in Table 1.

Table 1-Privacy Risks Associated with Personal Details

Risk	Risk Description	Case	References
Online Identity Loss	Personal details displayed on online social network profiles and other public resources can be used to hack into online systems such as email and bank accounts.	Sarah Palin	BBC News (2008a)
Phishing via online social networks	The retrieval of the personal details of a user through the art of deception via online social networks.	MySpace Phishing	Kirk (2006)
Phishing via instant messaging program	The retrieval of the personal details of a user through the art of deception via internet messaging programs.	MySpace Messaging Phishing	Kirk (2006)
Identity Theft via online social networks	Criminals steal your personal details to use them to carry out offline activities using your identity e.g. open a bank account or get a driving license.	Bryan Rutberg	Sutter and Carroll (2009) Schneier (2009)
Re-identification by linking	Anonymous data can be linked to external sources to derive the actual identity of a human	Hospital Discharge Records.	Sweeney (1997)

Chapter 2-Background And Related Work

The details of the example cases in Table 1 are described below

1. **The Sarah Palin case:** David Kernell used Mrs Palin's postcode, date of birth and other details to reset the password of her Yahoo email account. Mrs Palin's personal details were found on Wikipedia.
2. **MySpace phishing:** in late 2006 a phishing attack targeted MySpace users, tricking them into submitting personal details to a web page that looked like MySpace. These personal details were then sent to a hacker.
3. **MySpace messaging phishing:** is similar to the phishing attack detailed above but involves instant messaging. The user is sent a link to view some photos on MySpace. The link was sent via the instant messaging program from someone in their contact list. The user clicks the link which actually leads to a MySpace like login page. The login page looks very similar but actually is a fraudulent version of the login page. Once the authentication details are entered, the user is logged into the web pages of the real MySpace. The hacker can use the authentication details recorded in this way to extract the personal details from that account (Kirk 2006).
4. **Bryan Rutberg's case:** involved stealing his identity via his Facebook login details. The hackers then changed the Facebook pages to make it appear that Bryan was in trouble and sent emails asking for financial help.
5. **Hospital discharge records:** which included patient details were used to identify humans by linking their common demographic attributes to a database of details of public voters from Massachusetts in the USA. This can happen with OSN data due to attributes (e.g. date of birth, *gender* and location) being presented (Sweeney 1997).

Chapter 2-Background And Related Work

These cases illustrate how careful people have to be when submitting details online. The Bryan Rutberg identity fraud case highlighted the importance of knowing your friends thoroughly. The hackers in this case played with peoples' emotions regarding friendship. If a friend seems to be in trouble the first thing you want to do is help but it also is useful to know how your friend reacts in a real case.

There are also some other privacy risks that can occur especially if the OSN is careless about keeping some attributes (e.g. email address) private. These are illustrated by Balduzzi et al. (2010) and Jagatic et al. (2007).

If the email addresses of users were made public then spammers can crawl the OSNs and collect email addresses and who they belong to from user profiles. Then this information could be used to construct phishing emails or targeted spam by using personal details which could include real names and names of friends. This act is known as social phishing (Jagatic et al. 2007).

By allowing users, including outside users, to search through OSNs for profiles by name or email address, this can play into the hands of the spammers. Spammers can use the profile search (querying the OSN) to validate if the emails collected through their crawl belong to profiles in which the profile owners are real people as opposed to fake profiles of fake people. Also the spammers can track the amount of personal detail that is displayed on a profile because some users display their personal details in a very public way to the extent that outside users can view the details.

The technique of querying the OSN can be carried out by the spammer to also explore a company in terms of its employees and any details about the company especially if the company has an OSN profile page.

Chapter 2-Background And Related Work

Namestnikov (2010) highlights the popularity of OSNs to spammers because of the networks' ability to exchange information. One case that is presented is the Brazilian bank case, where emails were used to spread Trojan horse viruses which targeted online banking services but now OSNs are predominately being used to spread the viruses. One of the main reasons for this is the speed in which the attack can take hold (e.g. over 2000 users followed a link sent by spammers on Twitter within one hour).

The privacy risks mentioned in this section have highlighted how important it is to keep personal details hidden under control and the consequences of spreading personal details. This forms the motivation for wanting to construct a vulnerability measure which quantifies the likelihood than an OSN profile is subject to the spreading of the personal details which may lead to social engineering attacks. The next section explores how users of different ages react to the issue of privacy. The findings in this section will be important when modeling the vulnerability of different user types.

2.6-Privacy Attitudes and Age

The types of users who have profiles on OSN sites vary in age from children to older adults. A couple of years ago there was a common misconception that the only types of users that used OSNs were students. This was due to a increase in significant notable studies including Gross and Acquisti (2005), Gibson (2007), Hinduja and Patchin (2008), Govani and Pashley (2005) and Dwyer et al. (2007) who all concentrated on surveying students and their attitudes towards privacy. Since then, there have been social networking studies done which explore the attitudes to privacy of children and teenagers (De Souza and Dick 2009), adults (Lenhart et al. 2010) and older adults (Lehtinen et al. 2009).

Chapter 2-Background And Related Work

Different age categories display different behaviours when it comes to disclosing personal details on OSNs and this affects their attitudes towards privacy. One issue that has resulted from previous research is that there is no clear group of age bands. Different studies define age bands in different ways so the age bands are very roughly defined when discussing age bands and privacy below. An example is in the De Souza and Dick (2009) study where high school children are used to analyse the details they present on MySpace profiles. The age range of the children is between 12 to 18 years old. In comparison Hinduja and Patchin's (2008) study is concerned with adolescent (teenager) personal information disclosure on MySpace, classifies adolescents as 17 years old or younger. This study was carried out in 2006 and a user had to be 14 years old or over to have a MySpace profile so adolescent classification is technically between 14-17 years old. At present in 2011, the minimum age for MySpace users is 13 (MySpace 2011).

Underage users are a problem for OSNs because there is no system to validate a users' age. Lenhart et al. (2010) research found that nearly half of 12 year old in the United States use OSNs and this is despite the minimum age for Facebook as well as MySpace being 13 (Facebook 2011a).

In the sections below, various age bands and their attitude towards privacy are presented and discussed.

2.6.1-Children

For children, disclosing personal details on an OSN can lead to bullying, stalking and meeting with up strangers which could result in more serious consequences. This is illustrated by the Ashleigh Hall case. A 33 year old man called Peter Chapman who was known to the police as a sex offender, used Facebook in order to set up a profile where he posed as an adolescent boy. He

Chapter 2-Background And Related Work

befriended an adolescent girl called Ashleigh Hall who was 17 years old. They organised to meet one another, Chapman suffocated her and dumped her body in a field (BBC News 2010b). This case highlighted how important it was not to add people you do not know as your OSN profile friends because the details of OSN profiles can hide the truth in regards to identity.

Unlike older users, children have less awareness about the ramifications of their actions. De Souza and Dick (2009) highlighted several factors that influenced the disclosure of personal details by children and adolescents which included **peer pressure, website interface design** and **signaling**.

Peer pressure is when a child sees that their friends disclose personal details using their OSN profile and decide that in order to fit in, they have to do the same. The child does not want to feel left out of conversations that their friends may be having. The ability to **have independent thinking** has not quite developed yet. In childhood, children go through phases of wanting the latest items (e.g. certain toys or gadgets). Social networking is no different and this is emphasised by Boyd (2006) who discusses the concept of adolescents migrating to MySpace because their friends were there and the pressure to stand out through the personalisation of profiles.

Website interface design of OSNs is another factor in influencing information disclosure. MySpace and Facebook require members to register to get an OSN profile, which causes the disclosure of personal details. The fields on the registration forms normally have attribute fields (e.g. *name, date of birth and location*) which have to be filled in. This is forcing children to disclose their personal details at the earliest stage. These details ultimately appear on the profile by default until the child changes the privacy settings (De Souza and Dick 2009).

Chapter 2-Background And Related Work

Signaling is the art of presenting yourself in a positive light or to be seen in a certain way by providing information (Donath and Boyd 2004). This concept causes concerns for privacy, because to make people see you in a certain way, a lot of personal details have to be disclosed (e.g. *gender, age, profile picture, likes and hobbies*).

De Souza and Dick (2009) research study involved developing and distributing a privacy questionnaire to high school children to uncover what personal details they disclosed on their MySpace profiles. Their analysis and findings indicated that children who were very private in the offline world applied the same theory in the online world and this resulted in them being less likely to disclose as many personal details on their profile. The worrying finding was that the younger children i.e. those under 15 years old were showing signs of disclosing more personal details therefore highlighting that peer pressure could be a major driver in information disclosure especially for younger children.

This finding has been justified in Livingstone et al (2011) research which involved an online survey of 9-16 year old WWW users in 25 European Union countries. The research findings highlighted that younger children are more likely to have public profiles than older children. Also the address and phone number is displayed twice as often by children with public profiles as it is for children with private profiles.

Public concern over the safety of children using OSNs has led to pressure to educate children about OSN profiles and the disclosure of personal details. An example response is the 'Click Clever Click Safe' campaign by the UK Council for Child Internet Safety (2010).

2.6.2-Adolescents

Besides work done by De Souza and Dick (2009) on children, there have been various other studies (Boyd 2006, Pierce 2007, Lenhart et al 2010 and Patchin and Hinduja 2010) that have focused on adolescents and the characteristics of the way they use their social networking profiles. Lenhart and Madden (2007) and Patchin and Hinduja (2010) studies in particular, have provided significant findings on adolescent personal detail disclosure and privacy issues.

Lenhart and Madden (2007) study involved telephone interviews in 2006 with 935 adolescents who were aged between 12 to 17 and their parents. The findings showed that the issue of privacy is starting to become an issue that adolescents think about. This is in contrast to younger children who are more likely to disclosure personal details without thinking about the issues about privacy, therefore affecting their levels of vulnerability. In this study 66% of the teenagers limit access to their profiles so that the profile is not visible to all WWW users. This is important as some OSN profiles, if left absolutely public can be searched for through the WWW. Some profiles are very public and so can, by the use of a search engine, but also there are profiles that are public to the OSN but can't be searched for via a search engine. This issue has be implemented in the Facebook privacy controls. Facebook has a privacy option which allows everyone including external users access to view your profile.

This finding is justified by Patchin and Hinduja (2010) who analysed 1403 MySpace profiles in 2009 and found that 58.3% of the adolescents who used their profiles, often had made them private. The study carried out in 2009 is a continuation of a study carried out in 2006 (Hinduja and Patchin 2008) in which 2423 profiles were analysed and only 38.6% were private profiles.

Chapter 2-Background And Related Work

Regarding personal details disclosed in the Lenhart and Madden (2007) and Patchin and Hinduja (2010) study, *first and full names* seems to be disclosed readily. The name accompanied with other details can help to establish the identity of someone. This is stated by Patchin and Hinduja (2010) who claim that having several details of the adolescent (e.g. name, current city, profile picture and school) is all that is needed to locate the individual. Based on the age of the person, different items of personal details are required to extract the person's identity. To investigate an adults' identity, details about their workplace and current location may be required alongside the more common details which include name, profile picture and date of birth.

The major issue regarding private profiles which is not highlighted by Patchin and Hinduja (2010) is that making a profile private in MySpace does not make your OSN profile totally private. Personal details (e.g. *name, profile picture* and *age*) can still be presented on a private profile. A private profile in MySpace does not show the list of friends or interactions between the profile user and their friends. If a user with a private profile has friends who have public profiles then the friendship between the user and the friend can be inferred. Also if the public profile has their interactions displayed, then personal details of the user could be leaked in those interactions.

The most important personal detail that will distinguish an adolescent from an adult is the name of the school. In Lenhart and Madden (2007) study, 49% of the adolescents displayed the school name and educational details. Unlike De Souza and Dick (2009) comment, that younger children disclose more information than older children, ironically older adolescents (15-17 years old) too, share their photos and school name on their OSN profiles.

2.6.3-Young Adults and Adults

OSN sites are just as popular with young adults as they are with adolescents or older adults. This is justified by Lenhart et al (2010) who did a survey of 2253 young adults, 18 or over, in 2009 and found that 72% of the young adults (18-29 years old) used OSN sites. Significantly more young adults use OSN sites than older adults (30+ years old) which are stated at 40% (Lenhart et al 2010). This may be the case because for young adults, they are part of a technology generation.

Gross and Acquisti (2005) is the most cited study into the disclosure of personal details by younger adults. Gross and Acquisti (2005) survey of 4000 university students who used Facebook found that 90.8% of the students surveyed disclose a *profile picture* online, 50.8% display their *current home address*, 87.8% display their *birthday* and 39.9 % display their *phone number* on their profile. These personal details along with their *full name* can be used to extract someone's identity. From these statistics, the trend of information disclosure does not change in terms of comparing adolescents to young adults. Young adults seem to disclose their personal details readily but you would think that as you grow up in the technology age you become more aware of privacy issues.

Tuunainen et al (2009) justifies Gross and Acquisti (2005) findings because of his investigation, where 210 people responded to a web questionnaire about their Facebook usage in terms of their privacy and information disclosure. 88% of the people were aged between 18-30 years old and the results indicated that there was a severe amount of information disclosure and a lack of knowledge about the visibility of their profiles and the content of the Facebook privacy policy.

Chapter 2-Background And Related Work

The Facebook privacy policy concentrates on certain key areas. The first area details what Facebook do with the information that is submitted to their site. Examples of what Facebook do with the information include to maintain a service, contact you, to serve social ads and to help you find friends. Also detailed is the information that is collected when you interact with Facebook. Some of the information collected includes site activity information and cookie information.

The second area details how the information that is presented on profiles can be shared and public to other users but only if you set your privacy settings to do so. Also detailed is information that is shared with third parties if you add (e.g. an application). The third area focuses on how Facebook keeps the information from users secure (Facebook 2011b).

In regards to the information disclosure of the subjects on Facebook regarding Tuunainen et al (2009) study, 99% displayed *real name*, 98% displayed *profile picture*, 89% displayed *birthday*, 89% displayed *hometown*, 83% displayed *email address* and 80% displayed *education information*. These results alone illustrate the readiness of personal detail disclosure even if the sample size is very small.

In comparison to Tuunainen et al (2009) and Gross and Acquisti (2005) studies, Lampe et al (2007) analysed the information disclosure of a larger group of profiles on Facebook. In total 38,407 profiles were analysed and the results were quite similar in that 83.8% of the subjects display their *birthday*, 83.3% displayed their *hometown*, 45.1% displayed their *current address*, 92.3% displayed their *email address* and 93.8% displayed their *gender*.

A reason for the readiness to disclose personal details was emphasized by Govani and Pashley (2005) who pointed out that students in particular seem to

Chapter 2-Background And Related Work

.be aware about the privacy issues associated with OSNs but despite this, still feel comfortable with displaying the personal details. There is a false feeling of trust because they think that Facebook will protect their details when in fact their details being displayed on profiles are their responsibility. Govani and Pashley (2005) study involved conducting a pilot survey with 50 students from Carnegie Mellor University in the USA. The survey investigated the students' awareness of privacy concerns and available privacy protection supplied by Facebook.

Their survey results showed that *real name, profile picture, birthday, home town, email address* and *education information* were the top six attributes disclosed on profiles which correspond to the top six attributes displayed in the Tuunainen et al. (2009) study.

In terms of adult usage of OSNs, even though there has been a lack of studies carried out on what personal details adults disclose, there has been some work carried out into their trends regarding social media. Lenhart et al (2010) study uncovered some interesting trends on adults and OSN profiles. In general adults like to have multiple profiles. This brings up the question about how much an adult takes privacy issues into consideration if they are willing to spread their personal details across multiple profiles. Adults may choose to have multiple profiles because they sometimes want to keep their work and family life separate.

2.6.4-Older Adults

Of all the age bands, the older adults seem to be the most reluctance to use OSN sites. Despite this, there is a specific market for OSNs for older adults which include Eons¹⁴ and Saga Zone¹⁵. There are several reasons why older

¹⁴ <http://www.eons.com/homepage>

¹⁵ <http://www.sagazone.co.uk/>

Chapter 2-Background And Related Work

adults do not share the same enthusiasm as younger adults and teenagers do towards social networking technology.

One reason emphasised by Lehtinen et al. (2009) is that older adults are conscious that they will show too much of their identity if they display their personal details. They like to keep themselves private and there is a hesitation to post items such as media or photos on OSN profiles.

Gibson et al. (2010) highlighted a major reason why older adults may be reluctant to present personal details online which is a feeling of vulnerability. This is largely down to the media highlighting stories about identity theft that happens online. On a positive note, this proves that the use of the media can be used to highlight the dangers of disclosing personal details on OSN profiles.

Overall in analysing different age groups and their perceptions of privacy, there needs to be more done to emphasise privacy to children, adolescents and young adults because of their increased desire to display their personal details on OSN profiles. As you grow older, you would expect the user to understand the repercussions of displaying their personal details on an OSN profile. This trend is not always the case when it comes to younger adults. More research needs to be done also into what adults disclose online.

In 2009 the case of Sir John Sawers highlighted how even adults need to be more careful in regards to the privacy of OSN profiles. The wife of Sir John Sawers who was the next head of MI6, displayed personal family details on a Facebook profile. The profile was open and very public to 200 million users in an open access London network. The personal details included the location of the couple's flat and the location of their three children (Evans 2009).

There are some signs that privacy issues have been taken into account but with the increase in OSNs coming up with applications to use the personal data stored in their systems, controlling personal data usage will be harder than ever.

2.7-Introduction into Graph Theory associated with an Online Social Network

An OSN graph is a representation of an OSN at a specific time. The representation consists of nodes which represent the profiles of the users in the OSN and edges which in this case are the friendship relationships between two profiles. The edges can represent various types of relationships. A formal way of describing the representation of an OSN graph G is $G = (V, E)$ where V is the set of nodes and E is the set of edges that connect the nodes together. Each edge $e \in E$ consists of two nodes (e.g. $e_1 = \{a, b\}$).

In terms of the edges between the nodes, there are two representations. An undirected graph indicates that the edge between two nodes is symmetric and therefore has no direction (unordered pair). An example being that in a graph G , edges $\{a, b\} = \{b, a\}$. This indicates that the edge linking nodes a to b is the same as the edge linking nodes b to a .

In comparison, a directed graph indicates that the edge consists of an ordered pair of nodes (e.g. edge $e = \{a, b\}$ is not the same as edge $e = \{b, a\}$ unless $a=b$) which can imply a self loop where a node is connected to itself. The edges are known as directed edges and edge $e = \{b, a\}$ shows that there is a directed edge from node b to node a where node b is the tail and node a is the head.

A directed graph is ideal to model an OSN because it allows the flow of information to be seen. To analyse the edges between two nodes in more detail, a directed multigraph is more appropriate. A directed weighted multigraph which is illustrated in Figure 1 and denoted as $G = (V, E)$ allows

Chapter 2-Background And Related Work

parallel edges between the nodes where V is a set of vertices and E is a set of edges that is represented by the function: $f : E \rightarrow \{\{u, v\} : u, v \in V \wedge u \neq v\}$

The parallel edges between the nodes, allows a more in depth analysis of the relationships and allows relationships from OSNs to be accurately depicted. For modeling OSNs in this thesis, there are no self loops in a directed weighted multigraph so a node cannot be friends with itself. The weights between the edges can represent the level of interaction (e.g. number of emails exchanged between two nodes). Figure 1 illustrates a directed weighted multigraph as explained above.

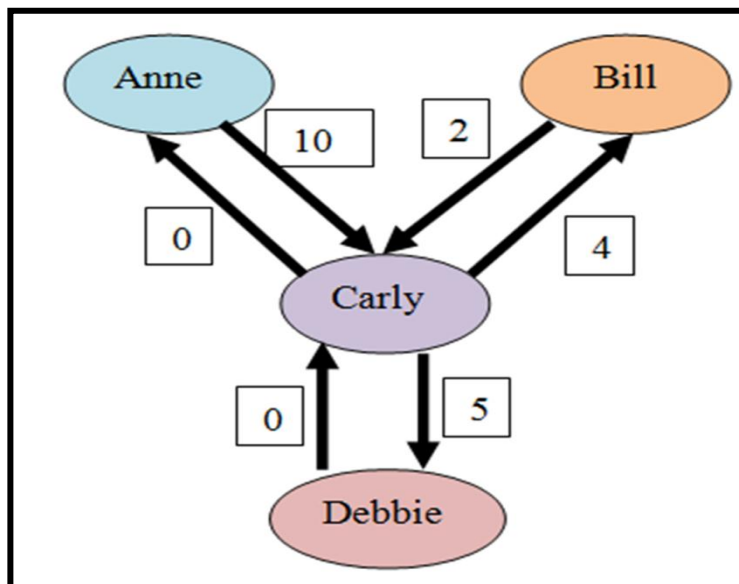


Figure 1-A Directed Weighted Multigraph

A formal representation of the OSN which is represented by the directed weighted multigraph G in Figure 1 is as follows:

Using Naji et al. (2011) notation, graph G can be denoted by $G = (V, E, W)$ where V is the set of nodes which represent actors in the network, E is the set of edges which connect the nodes together to signify friendship and W is a matrix of $|V| \times |V|$ which consist of values which represent the edge weights between the $|V|$ nodes. In the case of graph G , the edge weights represent the number of emails exchange between one node and another. Set $E \subseteq (V \times V)$ and each e_i

Chapter 2-Background And Related Work

$\in E$ where i is the $|E|$ in graph G , is an ordered pair so edge $e_i = \{a, b\} \neq$ edge $e_j = \{b, a\}$. This means that the edge weight for the edge e_i may not be the same as the edge for e_j .

Figure 1 illustrates that Carly is the most connected node with connections to three other nodes. In terms of the amount of emails, Carly receives more emails (12 emails) then she sends out (9 emails).

The indegree of node n is the number of directed edges that have node n as the head of the edge. The indegree of a node which is explained in more detail in section 4.5 signifies how popular a node is within a network. This is important in terms of information flow because the indegree can indicate how many friends trust the node and as a result leak personal details to the node. The outdegree of node n is the number of directed edges that have node n as the tail of the edge. In terms of information flow, the outdegree of a node can represent the spreading of personal details from the node to its friends.

A subgraph of $G = (V, E)$ is another graph $H = (A, B)$ where $A \subseteq V$ and $B \subseteq E$. A subgraph of a node can give information about the node's connection to other nodes. The other nodes are known as the neighbours of a node. In an OSN the neighbours would be the friends of the profile owner.

Using Figure 1, the subgraph of the node named Bill would just include the node named Carly because none of the other nodes are connected to Bill. Carly is the neighbour of Bill. If a node contains neighbours in which all the neighbours are connected to each other then this is known as a clique. In terms of information flow, information may spread more quickly around a clique due to the nature of the nodes knowing each other. A clique can signify a strong friendship group.

Chapter 2-Background And Related Work

The clustering coefficient value (Watts and Strogatz 1998) of a node illustrates how well connected the neighbours are and is a value between 0 and 1. The higher the clustering coefficient value, the more connectivity there is between the neighbours. More details of the calculation of the clustering coefficient value for a node is detailed in section 2.71.

Two nodes that are connected by an edge can be commonly known as adjacent nodes. A path is a sequence of nodes such that each node is adjacent to the next. In a path, each edge can be only traveled along once. The length of the path is the number of edges in that path. The same principle of paths applies to directed graph as well as undirected graphs but the difference is that the path for directed graphs must go in the direction of the arrows. An example of a path using a directed graph is illustrated in Figure 2.

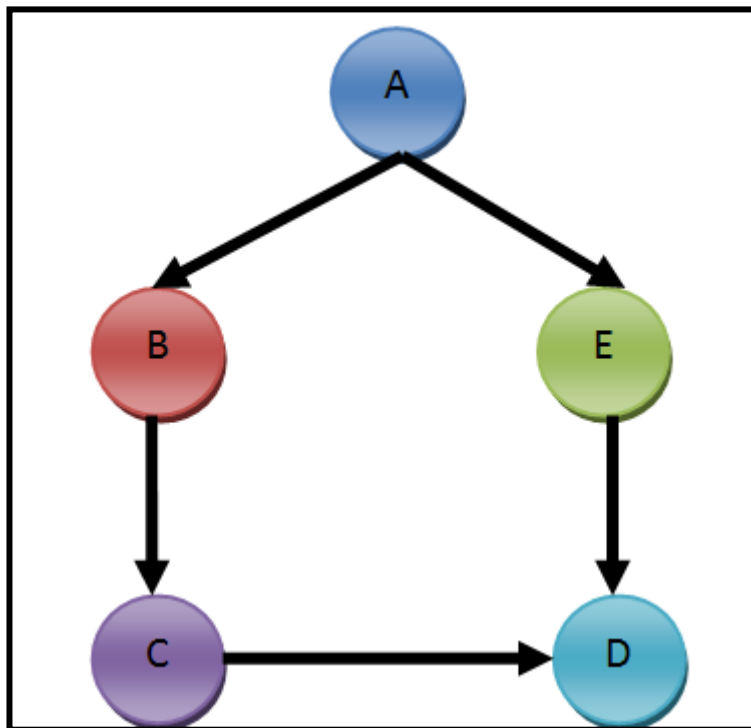


Figure 2-A Directed Graph to Illustrate The Concept Of Paths

Using Figure 2, an example of a path is from node A to node D which has a path length of 3 ($A \rightarrow B \rightarrow C \rightarrow D$). The geodesic distance (shortest path) between two nodes is the minimum path length (e.g. the geodesic distance between

Chapter 2-Background And Related Work

nodes A and D is 2 ($A \rightarrow E \rightarrow D$). The geodesic distances between all pairs of nodes in the graph can be used to help calculate the diameter of the graph which is the longest geodesic distance between any two nodes in the graph.

In the case of Figure 2, the diameter of the graph is 2 which is a small value for a graph diameter. If each of the nodes in Figure 2 represents an OSN profile, then the small diameter indicates a very compact network. A node is no more than 2 steps away from any other node (Hannerman and Riddle 2005).

The geodesic distance between two nodes is used to work out the average shortest path distance of a network using an OSN graph. This measure is detailed in section 2.7.1.

Overall this section has introduced the components of what makes an OSN graph and some concepts of graph theory which will be used to help explain the vulnerability concept in section 2.7.2 and 3.1. Also the small world effect in section 2.4.1.

There are various types of networks that a graph can represent (e.g. road networks, flight networks and electrical networks). An OSN is an example of a complex network and there are various types of complex networks which include small world (Watts and Strogatz 1998), scale free (Barabási and Albert 1999) and random (Erdős and Rényi 1960). The small world model is the most relevant to the OSNs because of its characteristics which are stated and discussed in section 2.4.1.

2.7.1-Characteristic Measures for Complex Network Classification

Wilson and Nicholas (2008) highlighted that there are three particular characteristics of a network that are used in classifying the type of network. The three characteristics are **clustering coefficient** of each node, **average path length** across the network and **degree distribution** of the nodes.

Chapter 2-Background And Related Work

The clustering coefficient of a node defines how well connected the neighbours are to each other. Since directed graphs are used in this thesis, the clustering coefficient of node n using Watts and Strogatz's (1998) equation will be:

$$C_i = \frac{e_i}{(k_i(k_i - 1))} \quad (1)$$

where e_i is the number of edges that exist between the neighbours of node i and k_i is the number of neighbours of node i . If the value of the clustering coefficient which is denoted as C_i is heading towards 1, then most of the neighbours of a node are connected to each other. On the other hand, if the coefficient value is near 0 then the neighbours are not connected to each other at all.

Examining the average clustering coefficient for all the nodes in the OSN graph G , calculated using Watts and Strogatz (1998) metric in equation 2, can define how well connected or not the nodes in the graph are to each other:

$$\bar{C}_G = \frac{1}{n} \sum_{i=1}^n C_i \quad (2)$$

where n is the number of nodes and C_i is the clustering coefficient for each node in OSN graph G .

The average path length of graph G which represents an OSN network is the average number of edges along the shortest path (geodesic distance) between two nodes for all pairs of nodes in graph G .

Let graph G have a set of nodes V . The notation for the shortest (geodesic) distance between two nodes is $d(v_1, v_2)$ where v_1 and $v_2 \in V$. The equation for the average path length of graph G would be:

$$p_G = \frac{1}{n * (n-1)} \sum_{a,b} d(v_a, v_b) \quad (3)$$

where n is the number of nodes in the OSN graph G and $d(v_a, v_b)$ is the shortest distance between two nodes. The higher the average shortest path length, the harder it is for information to flow across a network. Milgram's (1967) experiments which involved the 6 degrees of separation and the analysis of the average path length made the concept of the small world famous.

With the degree distribution of a network, the analysis of the distributions can be divided into indegree distribution and outdegree distribution. The indegree distribution involves studying how many edges are heading towards the node for every node in graph G , and then plotting the distribution. The outdegree distribution involves studying how many edges are heading away from the node for every node in graph G , and then plotting the distribution.

2.8-Social Network Analysis Measures

Social network analysis measures are more specifically used to analyse and evaluate an OSN through the use of a graph. This section will explain some of the more commonly used measures in social network analysis.

2.8.1-Centrality Measures

The most popular set of measures are the centrality measures by Freeman (1979) which concentrate on the structure (edges) around the node. The measures include degree centrality, betweenness centrality and closeness centrality.

Degree Centrality of a node is the number of edges attached to the node. This concept utilises the concept of degree in graph theory which has been

Chapter 2-Background And Related Work

explained in section 2.4. The normalised degree centrality for an undirected graph $G = (V, E)$ containing node v is shown in equation 4:

$$C_D(v) = \frac{\text{deg}(v)}{n-1} \quad (4)$$

where $\text{deg}(v)$ is the number of edges attached to node v and n is the number of nodes based in the graph. For a directed graph, the degree centrality is the outdegree of the node. The outdegree is the number of edges going away from the node.

The concepts for the other centrality measures i.e betweenness centrality and closeness centrality will be explained using a commonly used example which is a kite network from Krackhardt (1990) that is shown in Figure 3. The kite network is an undirected graph which consists of 10 nodes and 18 edges.

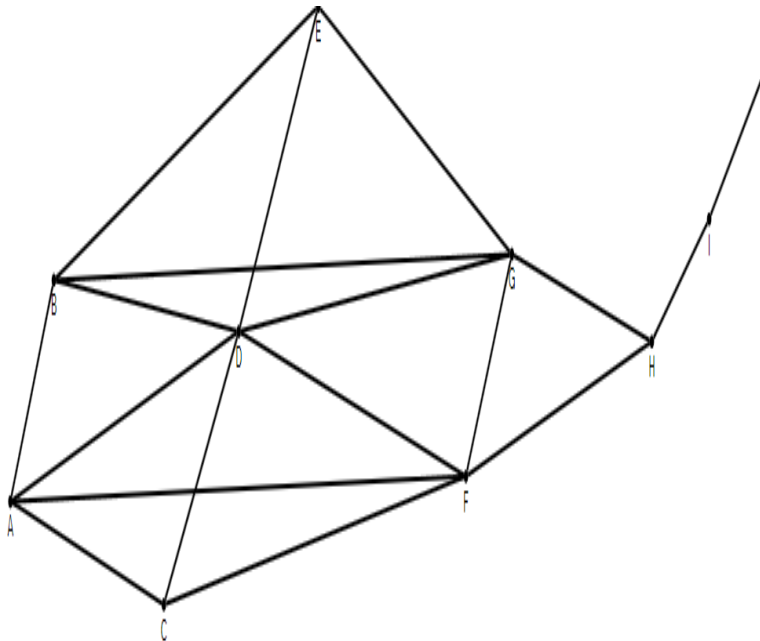


Figure 3-Kite Network from Krackhardt (1990)

Betweenness centrality pinpoints the node that has the highest control when it comes to the information flow in the network. A node with a high betweenness centrality indicates that they have more control over the information flow of the

Chapter 2-Background And Related Work

network. They act like brokers to control the passage of information. This gives the node a sense of power over the other nodes. The betweenness centrality of node p is calculated using Equation 5:

$$C_B(p) = \sum_{a < b} \frac{geo_{ab}(p)}{geo_{ab}} \quad (5)$$

where geo_{ab} is the number of shortest paths between nodes a to b and $geo_{ab}(p)$ is the number of shortest paths that pass through node p . Equation 5 can be used for a directed graph but the value has to be normalized by dividing by the number of pairs of nodes that do not include p as demonstrated in equation 6 where n is the number of nodes in the network.

$$C_{B'}(p) = \frac{\sum_{a < b} \frac{geo_{ab}(p)}{geo_{ab}}}{(n-1)(n-2)} \quad (6)$$

Analysing the kite network in Figure 3, node H has the highest betweenness centrality value. Even though node H is only related to 3 other nodes, the node acts as a bridge which connects nodes I and J (indirectly) to the rest of the network. This indicates that node H is important in the network because if node H was removed then nodes I and J would not be able to communicate with the rest of the network therefore node H is vital for information flow. In comparison nodes E , C and J have the lowest betweenness centrality values because if they are removed from the network, everyone in the network is still connected together and there would be no change in the information flow (Hansen et al. 2009)

Closeness centrality measures the average shortest distance (geodesic distance) from one node to every other node. The closeness centrality of node a

Chapter 2-Background And Related Work

based on an undirected graph $G = (V, E)$ is the inverse of the sum of shortest paths to all the other nodes of node a . This is indicated in equation 7:

$$C_c(a) = \left[\sum_{b=1}^N d(a,b) \right]^{-1} \quad (7)$$

where $\sum_{b=1}^N d(a,b)$ represents the sum of all the shortest distances between node a and all the other nodes in the network which are represented by b . The notation N represents the number of nodes in the network. A low closeness centrality value indicates that the node plays a central role in the network i.e. these nodes would be able to spread information to all the other nodes in the network because of their short path lengths. Equation 7 can still be used for a directed graph but the direction of the edges has to be taken into account.

Using the kite network in Figure 3, nodes F and G have the lowest closeness centrality values so they play a more central role in the network and act as efficient information disseminators (Hansen et al 2009). The next section describes some other measures in the social network analysis field.

2.8.2-Other Measures

Density describes how well the nodes are connected to each other. The density for an undirected graph G which is calculated using equation 8 is the ratio of edges present against the maximum number of potential edges. The density value is a number between 0 and 1 and the higher the number the denser the graph is.

$$Den_G = \frac{|E|}{(n(n-1)/2)} \quad (8)$$

Chapter 2-Background And Related Work

where $|E|$ is the number of edges and n is the number of nodes present in graph G . Using the kite network in Figure 3, the density of the kite network would

equal $\frac{18}{(10(10-1)/2)} = \frac{18}{45} = 0.4$, which shows that the network is not dense. To

increase the density of the graph, there would have to be more edges between the nodes. In comparison, for a directed graph the density is calculated as $|E|/(n(n-1))$.

Degree prestige (Knoke and Burt 1983) concentrates on the indegree of the node. The context of a network can dictate what an indegree edge actually represents. The most prestigious node in a network would be seen as the most popular person in the network. The degree prestige of (e.g. node Z) is calculated using equation 9:

$$P_D(Z) = \frac{d_m(Z)}{(n-1)} \quad (9)$$

where $d_m(Z)$ is the indegree of node Z and n is the number of nodes in the network.

Proximity prestige (Knoke and Burt 1983) improves on degree prestige by using the concept of reachability. Reachability is where one node can reach another via a sequence of nodes which are linked together (adjacent nodes). A reachability matrix can be produced where if a node is reachable from another then a number 1 is placed in the matrix, otherwise if the node is not reachable from another than a number 0 is placed.

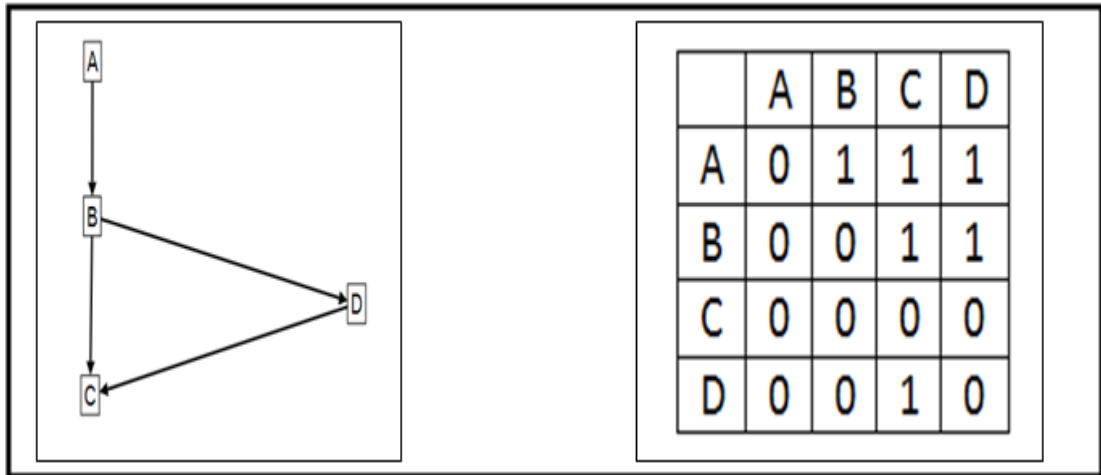


Figure 4-Reachability Matrix Example from (Tan 2007)

Figure 4 illustrates that even though (e.g. node A is not directly linked to node D), there is a path of adjacent nodes from (A→B→D) and that is why there is a 1 in row A column D in the reachability matrix. The proximity prestige of node v_i is calculated using equation 10.

$$P_p(v_i) = \frac{(|Reach(v_i)|)/(n-1)}{\sum d(v_j, v_i)/|Reach(v_i)|} \quad (10)$$

where $|Reach(v_i)|$ is the number of nodes that can reach node v_i , n is the number of nodes in the network, $\sum d(v_j, v_i)$ is the average distance between the nodes that can reach v_i and node v_i .

The advantage of having a directed graph is that it allows you to analyse prestige as well as centrality. Both prestige and centrality measure the importance of a node but the centrality of a node in a directed graph focuses on the outdegree of the node whereas degree prestige of a node focuses on the indegree of the node.

Sections 2.8.1 and 2.8.2 have explained a variety of common measures that are used in social network analysis. With the introduction of OSNs and the increased use of the WWW, there needs to be more social network analysis

Chapter 2-Background And Related Work

measures for privacy. As demonstrated by the measures explained above, many of them involve the analysis of edges but fail to take the contents of the node into account. This is important for a privacy measure because the contents of a node (in this case an OSN profile) can dictate what the privacy attitude of the user is and therefore influence their disclosure of personal details. This forms part of the motivation in wanting to contribute a privacy measure for the social network analysis field that takes the node and its structure into account.

Section 2.8.3 explores the concept of vulnerability which forms the basis for the proposed vulnerability measure which is detailed in chapter 3 and the contribution to the area of privacy measures in the field of social network analysis measures.

2.8.3-Vulnerability Definitions

In different fields the term vulnerability can imply different concepts. For example, in computer networks, attack vulnerability (Holme et al. 2002) is linked to the reduction of network performance, due to the loss of network nodes and connections. This definition highlights the use of graph theory but provides limited information about the node contents.

This is further justified by some common definitions for vulnerability in the area of graph theory which can be applied to OSN graphs as well. The definitions include:

1. **Cutpoint:** is the weakest node or nodes of the OSN graph. If the node was removed then the OSN graph would be divided into clusters that were unconnected. This would make the OSN graph vulnerable because it exploits the weak points of the graph. In doing this the attacker will

know that if they attack the node which is the cutpoint they can stop the network from functioning properly (Hannerman and Riddle 2005).

2. **Vulnerable Bridges:** (Lambda sets and Bridges) Lambda sets involve ranking the relationships in terms of how much flow there is between each edge that links the nodes together. Lambda sets then identify sets of relationships which, if disconnected, would greatly disrupt the flow among all of the nodes (Hannerman and Riddle 2005).
3. **Outer Nodes only connected to one other node:** The outer nodes which are only connected to the main node (node with the highest number of relationships with the nodes) in the OSN are vulnerable because if the main node disappears they are no longer part of the social network therefore they are connected to no one. You could argue that the rest of the network is vulnerable because these outer nodes as long as they are attached to the main node could be watching how the network grows and changes. The outer nodes could be the possible network attackers.
4. **Clustering Coefficient:** The nodes which have a high clustering coefficient will have a neighbourhood where most or all of the neighbours are connected to each other. In terms of privacy the neighbours would make the main node vulnerable because of the good flow of information between them. The relationship between the nodes would be so information rich that if a new node joined a highly clustered community they would learn a lot about the community. This could be what an attacker may do if you want to learn more about a network. A high clustering coefficient of a node can lead to information spreading throughout the OSN if the node's neighbours display their profiles so

publically. The information can also leak into other sub networks based in the OSN.

2.9-Conclusions

With the increase in OSN usage and the disclosure of personal details via OSN profiles, the field of social networking and privacy has bought up some major issues. Displaying personal details so publicly using OSN profiles can make OSN users vulnerable to privacy and social engineering attacks. OSN usage attracts a lot of different age groups and each age group has their own attitudes towards the disclosure of personal details on OSN profiles. The older adults seem to be more wary of disclosing personal details online where as children, adolescents and young adults have peer pressure to contend with as well as a willingness to trust the OSN with their details. More needs to be done to educate these age groups about the dangers of displaying personal details so publicly.

The representation of an OSN by a graph can help to investigate and analyse how privacy attacks can affect users. The analysis of OSN graph through the use of graph theory concepts and social network analysis measures can help to identify where personal details can flow more freely. In terms of the concept of vulnerability, the common definitions associated with graph theory talk about the structure surrounding the node and fail to acknowledge the contents of the node. This observation forms the basis for our proposed vulnerability definition.

With the social network analysis measures, there needs to be more measures associated with privacy and our proposed vulnerability measure, which is explained in section 3, will fit in to this area.

CHAPTER 3: VULNERABILITY MEASURE

The aim of this chapter is to explore the vulnerability concept as well as detail the three components (individual vulnerability, relative vulnerability and absolute vulnerability) which make up the vulnerability measure. The measure explained in this chapter is in its unnormalised form. Chapter 6 will explain how the measure is normalized. The individual vulnerability calculates the vulnerability of an individual node which represents an OSN profile. The relative vulnerability calculates the overall vulnerability of the neighbourhood which contains the neighbours of the node and the absolute vulnerability of the node is a result of a mathematical operation between the individual and relative vulnerability values of the node. Also highlighted in this chapter are the issues which are associated with the algorithm developed for measuring vulnerability.

3.1-Initial Vulnerability Concept

With the observation that there needed to be, vulnerability definitions that took both the structure around the node and the node contents into consideration as illustrated in section 2.8.2, a vulnerability definition was proposed to take into consideration the structure around the nodes in an OSN graph, as well as the node contents (AbdulRahman et al. 2010).

A directed multigraph was used to model the OSN because the direction of relationship would allow investigation, to see from which node the flow of personal details were coming from. A multigraph represents an accurate representation of an OSN used for this research because the edge connecting node *A* and node *B* is not the same as the edge connecting node *B* to node *A*. This allows a more detailed analysis of the strength of relationship between two nodes based on the online social interaction. The strength of relationship can be different depending on the actions of the node (e.g. Node *A* may interact more

Chapter 3-Vulnerability Measure

with Node *B* by writing profile comments on Node *B*'s OSN profile, but node *B* may be more reserved and not write anything on Node *A*'s OSN profile).

Our initial definition (AbdulRahman et al. 2010) for a vulnerable node in an OSN is stated below:

Definition: the vulnerable node in a social network graph is the node that contains attributes to breach privacy and provide grounds for a social engineering attack. For such a node a highly connected neighbourhood in which the neighbours display the attributes readily will increase the risk of vulnerability, as detailed below.

An OSN profile consists of personal details, a list of friends of the user and interaction elements (e.g. a wall where the user and their friends can exchange comments with each other). The friends of the user, who owns the profile, form the node's neighbourhood which can be analysed using an OSN graph.

If you have a public profile and friends who are highly connected and who also have very public profiles where they display a lot of personal details, then your personal details may spread easier and this may increase your chances of being vulnerable to social engineering attacks.

Also vulnerability is about the loss of control of personal details. The more public you make yourself then the less likely you are to have total control of your personal details. A very public profile which can be accessed via web searches allows personal details to be gained by social engineering attackers, sexual predators, hackers, etc. The aim is to make your profile and personal details less accessible to unknown users. This can be done by using privacy settings, being careful what personal details are displayed or by displaying false data.

Chapter 3-Vulnerability Measure

A concept of vulnerability was proposed by Gundecha et al. (2011) but this concept unlike ours focuses a lot more on the privacy and security settings of the friends of the OSN user and the identification of vulnerable friends. A user will have a vulnerable friend if the friend's privacy and security settings do not protect the user or the user's network of friends.

In comparison, our research concentrates more on the propagation of the personal details of the user through the OSN network because of the behavior of the user and its friends in terms of information disclosure. Also our vulnerability measure emphasises the potential for the user to be vulnerable to social engineering attacks.

3.2-Vulnerability Formalism and Explanation

Given an OSN $s_i \in \mathcal{S} = \{s_i, i \in \mathbb{N}^*\}$ where \mathcal{S} is a set of OSNs, each social network s_i consists of a set of profiles $P_{ij}, j \in \mathbb{N}^*$ where i represents the OSN (e.g. 3) for example Facebook and j represents the profile number (e.g. 2). Each profile has a different username and is associated with a individual email address (making it uniquely identifiable). There are two types of users: external users and members where a member has a profile $p_j \in \mathcal{P}_i$. An external user denoted as $U_k \in \mathcal{U}, k \in \mathbb{N}^*$ where the set of all types of users for social network $s_i \in \mathcal{S}$. An external user can view some if not all the information of many $p_j \in \mathcal{P}_i$ which is the set of profiles for social network $s_i \in \mathcal{S}$, as long as the profile is publicly available via a search engine.

A member denoted as $m_{ij} \in \mathcal{U}$ owns a profile $p_j \in s_i$ which corresponds to a specific username, email address and social network. In a social network $s_i \in \mathcal{S}$, member m_{ij} can have many profiles $p_j \in \mathcal{P}_i$ though based on different email addresses. Members can have many profiles $p_j \in \mathcal{P}_i$ with the same or different

Chapter 3-Vulnerability Measure

usernames which spread over many online social networks $s_i \in \mathcal{S}$. Each profile is defined by a tuple of attributes $\mathcal{A} = \langle a_1, a_2, \dots, a_i, \dots, a_n \rangle$. The attributes can be personal details or social network attributes (e.g. news feeds).

For each profile $P_j = \langle a_{1j}, a_{2j}, \dots, a_{ij}, \dots, a_{nj} \rangle$. For each attribute $a_i \in \mathcal{A}$ in profile p_j a vulnerability score was allocated. If an attribute $a_i \in \mathcal{A}$ is classed as vulnerable then the attribute a_i is allocated a weight $w_i \in \mathcal{W}$. For each profile p_j $VP_j = \langle w_{1j}, w_{2j}, \dots, w_{ij}, \dots, w_{nj} \rangle$ where VP_j represents the individual vulnerability of profile P_j . Each w_i value is between $[0, 1]$. The combination of these weights is used in the calculation of the individual vulnerability of the profile p_j . One attribute of a profile p_j is the list of friends which act as neighbours $n_i \in \mathcal{N}$ whereas the other attributes are atomic (e.g. name). Each neighbour $n_i \in \mathcal{N}$ is also a profile $p_j \in \mathcal{P}_i$.

In each social network $s_i = P_{ij}, j = 1, \dots, N_i$ where N_i is the total number of users in s_i , $P_{ij} = \langle a_{1ij}, a_{2ij}, \dots, a_{kij}, \dots, a_{nij} \rangle$ where n is the number of attributes defining each profile in s_i . For each profile P_{ij} its individual vulnerability $V_{I_{ij}} \in [0, 1]$, relative vulnerability $V_{R_{ij}} \in [0, 1]$ and absolute vulnerability which is an operation between V_I and V_R and denoted by $V_{A_{ij}} \in [0, 1]$ are calculated.

Even though an external user $U_k \in \mathcal{U}$ does not own a profile $p_j \in s_i$ external user $U_k \in \mathcal{U}$ can make members $m_{ij} \in \mathcal{U}$ vulnerable by spreading the members' personal details on other webpages. The vulnerability measure at present does not take this into account.

Chapter 3-Vulnerability Measure

The vulnerability measure proposed to quantify vulnerability is based on an OSN graph $G=(V, E)$ which is a directed multigraph. Each node $(N_a \in N, a \in \mathbb{N}^*)$ where N is a set of nodes, represents an OSN profile and the edge defines the connection between two profiles. A vulnerability value is associated with each node and the vulnerability value is defined by three components which include the individual vulnerability, relative vulnerability and absolute vulnerability.

3.2.1-Vulnerability Measure Assumptions

There are some assumptions made by us before the vulnerability measure is implemented. One of the main assumptions is that the profile data is correct. If the resources were available, the profile data could be analysed against external resources to double check the details matched. With the vulnerability measure the assumption is that only the immediate friends contribute towards the vulnerability of a node. The measure does not take into consideration that a friend of a friend or an external user could pose a threat. The idea has been explored but the technical concept has not been implemented. Also the measure at this stage has not taken into account the interaction of the node (e.g. how many comments are displayed on a profile wall and does the content contain any personal information about other users). In regards to the weights, the assumption made is that the presence of attributes that lead to vulnerability, cause the same effect for all the users.

3.2.2-Individual Vulnerability

The individual vulnerability (V_i) is the vulnerability created by the self disclosure of personal details. It is calculated based on examining each profile for the presence of attributes that contribute towards vulnerability to social engineering attack.

Chapter 3-Vulnerability Measure

An initial set of attributes contributing to possible vulnerability included:

1. Full Name
2. Gender
3. Age
4. Profile Photo
5. Current Location
6. Zodiac Sign

The attributes above were selected because research highlighted their significance in breaching privacy and leading to social engineering attacks, which can cause loss of identity. The research is explained below. Krishnamurthy and Wills (2009) and McCallister et al. (2009) emphasised that some of the attributes that were selected (e.g. *full name, current address, and date of birth*) were “*Personally identifiable information*” which can be used to “*distinguish or trace an individual’s identity*”. If friends of a profile user were to help to leak personal information by being talkative on an OSN then this could compromise the identity of the person in the offline and online world.

The attribute selection is also acknowledged by other works: Irani et al. (2011) emphasises that the attributes which include *name, location, gender, hometown* and birthdate can be used in a password recovery attack to recover passwords to accounts such as email accounts. These attributes can be answers to *secret questions* which are asked to ascertain the identity of the user and makes sure it matches the identity of the account user. An example of this attack is the Sarah Palin case which is described in section 2.5.

In Social Media University Global (2008) the authors state that you should not display family information (e.g. the maiden *name* of your mother or the *name* of

Chapter 3-Vulnerability Measure

your pet). These attributes are common security questions, as stated by Furnell (2010), when the user has forgotten to reset their passwords. Banks also use these questions as illustrated by Kelly (2008). Federal Trade Commission (2006) and Social Media University Global (2008) highlighted that displaying personal details (e.g. *full name, date of birth and contact number*) can help attackers steal your identity.

Nosko et al. (2010) justified this further by stating that displaying too many personal details (e.g. *full name, phone number, address and date of birth*) can increase identity theft concerns. These details can also be extracted by using the reverse telephone directory in combination with some of the personal details displayed on a profile. A reverse telephone directory allows users to search by telephone number in order to find the details of the person or service they require.

Date of birth is a commonly used attribute when associated with identity (e.g. in the National Health Service) in the UK and in the USA where 87 % of Americans can be uniquely identified from a combination of the date of birth, *gender* and the five digit zip code (Miceli and Kim 2010). Irani et al (2011) extends this further by highlighting that OSNs use the attribute *location* more widely than *zip code*.

This shows the importance of not disclosing personal details anywhere. If the *date of birth* is not present on the profile then the *age* and *zodiac* sign can be used in an attempt to infer the date. Also profile comments mentioning the words happy birthday may help to validate the inferred *date of birth*.

With the introduction of Foursquare which is a opt in social networking tool that transmits your location , keeping parts of your current address a secret may have just got harder and also there is an increased possibility of being stalked

Chapter 3-Vulnerability Measure

as demonstrated by (Hickman 2010). The disclosure of current address or hometown can lead to real world stalking where users' movements are tracked. (Schrammel et al. 2009).

Even photos on OSN profiles can cause information disclosure and loss of identity through the art of photo tagging. Photos can be used to validate a person's *age* or who members of their family and friends are. This is validated by Gross and Acquisti (2005) who found in their study that 61% of the profile pictures that were disclosed were suitable for identification purposes.

Digital cameras which are used to take photos, store extra data for each image in an EXIF (exchangeable image file format) that is embedded in each file. The extra data can come in useful if a photo is cropped because the original photo can sometimes remain in the digital file itself. Mobile devices that are used to take photos, can store a wider variety of data because the image file incorporates GPS (Global Positioning System) data. The data can include the date and the time in which the photo was taken and also the exact position of the photographer (Vamosi 2011).

Future work for the vulnerability measure involves research being done to highlight other attributes which can contribute towards vulnerability. The type of user that the attributes belong to will be a contributing factor to the attributes chosen and their respective weights.

The conditions of individual vulnerability (V_i) are that $V_i \in \{ V_{I1}, V_{I2}, \dots, V_{In} \mid V_{Ii} \in [0,1], i = 1, \dots, n \}$ where n is the number of nodes in the network. Each node represents a profile. The V_i value is based upon allocated weights to some of the attributes mentioned previously. The list of the attributes includes *name, profile picture, gender, age, current location and*

Chapter 3-Vulnerability Measure

zodiac. The weights were based on the relative frequency of the attributes in the dataset which was constructed using our extraction approach which is detailed in chapter 4. The relative frequency approach means that the total of the weights has to equal 1 and there is no need for normalisation to be applied.

If the contents of the node have any of these attributes then an attribute weight is allocated to the node. The total of the weights for the node is the V_i value. The calculation for the V_i value is illustrated using Lam et al. (2008) metric in equation 11. For simplicity V_{I_i} denotes the individual vulnerability of node i where $i=1, \dots, n$ and n is the number of nodes in the network. For each of the nodes:

$$V_{I_i} = \sum_{j=1}^m F_j * W_j \quad (11)$$

where m is the number of attributes, F_j is a binary value to show whether an attribute j has been displayed in the profile and W_j is the weight that has been allocated to the attribute if it is vulnerable. In this case the weights are the relative frequency of the attributes. The higher the V_i value, the increased chance that the node will become vulnerable to social engineering attacks.

3.2.3-Relative Vulnerability

The relative vulnerability value is the summation of the individual vulnerabilities of the neighbours of node i as illustrated in equation 12:

$$\begin{cases} V_{R_i} = \sum_{\substack{j=1 \\ j \neq i}}^n V_{I_j} & \text{if } n > 0 \\ 0 & \text{if } n = 0 \end{cases} \quad (12)$$

where n is the number of the neighbour and V_j is the individual vulnerability of the neighbour j . The reason that j is not equal to i is because a node cannot be

Chapter 3-Vulnerability Measure

neighbours with itself. Any $V_{R_i} \in \{V_{R_1}, V_{R_2}, \dots, V_{R_n}\}, i = 1, \dots, n$ where n is the number of nodes in the network. Equation 12 also illustrates that the relative vulnerability is calculated recursively. If node i has no neighbours then the relative vulnerability is 0.

The relative vulnerability of a node is important because it summaries the neighbourhood of the main node (node being analysed for vulnerability) i.e. if the relative vulnerability is high then it shows that the neighbours are willing to post their personal details online readily. This can cause the main node to be vulnerable because of the attitude towards privacy from the neighbours and the potential for personal details of the main node to be leaked via public interaction (e.g. profile comments). The attributes that are accessed for vulnerability are personal details which could lead to social engineering attack and the loss of control of personal information. If the personal details of a node are leaked because a neighbour who likes to talk mentions them in their own profile comments then this causes problems for the node if (e.g. a hacker views the neighbour's profile and extracts the personal details). The personal details can also leak through the network because of the neighbour's willingness to be open.

Peer pressure is one of the major factors which drives information disclosure on OSNs (De Souza and Dick 2009; Govani and Pashley 2005; Gross and Acquisti 2005; Cachia 2008; Boyd 2006). This is true especially with the younger age groups (e.g. children, adolescents and young adults) where they can be influenced by trends in technology. This is illustrated by the Digital Youth Project which found that for American teenagers, there was a strong peer pressure to join OSNs and this added to their anxiety of feeling left out if they did not join a network (Boyd and Buckingham 2008).

Chapter 3-Vulnerability Measure

This issue is what makes the concept of the relative vulnerability of a node important especially in networks which consist of young people. If a node is highly influenced (due to peer pressure) by its talkative friends, who presents vulnerable attributes readily on OSN profiles, then the node has an increased chance of self disclosing their own vulnerable attributes and this results in an increase of the individual vulnerability of the node. Consequently the absolute vulnerability of the node will rise due to the behaviour of the friends and the increased self disclosure of the node.

3.2.4-Absolute Vulnerability

The absolute vulnerability V_A which is calculated in equation 13, takes the individual vulnerability V_I and the relative vulnerability V_R into account. To these values, a mathematical operator is applied. This gives an absolute vulnerability value for each node.

$$V_{A_i} = V_{I_i} \bullet V_{R_i} \quad (13)$$

where $i=1, \dots, n$, n is the number of nodes and \bullet represents the MAX operator in this case which is the maximum value between the V_I and the V_R value. An example of the application of absolute vulnerability is presented below:

Node Z has a V_I value of 0.9 and has 2 neighbours which are B and C. B has a V_I value of 0.5 and C has a V_I value of 0.9. The V_R value is therefore 1.4 and shows that node C displayed their vulnerable attributes so readily and therefore contributed towards the vulnerability of node Z. This is because node C has shown signs that because they are public with the vulnerable attributes, they may leak the personal details of their neighbours via interactions which are displayed on node C's profile. If the profile of node C is publically available to external users then the personal details of the neighbours can leak even into

Chapter 3-Vulnerability Measure

unknown networks. The operator in the equation 13 is MAX so the V_A value is 1.4. Further research is done into operators and vulnerability and this is presented in chapter 6 and chapter 8.

3.3-Vulnerability Measure Algorithm

Figure 5 explains the algorithm for the unnormalised vulnerability measure which is used to calculate the individual, relative and absolute vulnerability values for each node $n \in N$ which is the set of nodes in the network. At the beginning of the algorithm, before the first for loop, the important components are defined which includes the list of vulnerable attributes and their respective weights. The values for the individual, relative and absolute vulnerability are set to 0 initially because no nodes have been analysed yet.

```
Input: List of nodes N
begin
Let Y = |N| be the number of nodes and i is a counter, i=1,...,Y
Let F be set of vulnerable attributes {First name, profile picture, gender, age, current address, zodiac}
Let B be set of all attributes in the node
Let W be the set of weights allocated to the node if vulnerable attribute is present. Weight is calculated by the relative frequency of the attribute.
Let WT be the total of the node's weight
Let Ni be the list of neighbouring nodes for each node N[i]
Let I be individual vulnerability of each N
Let R be relative vulnerability of each N
Let A be absolute vulnerability of each N
WT := 0
I := 0
R := 0
A := 0
for i = 1 to Y do
  Analyse B[i] to see what attributes are present
  while B[i] eF then
    Get W for vulnerable attribute F
    WT[i] =WT+W
    if B[i] eφ
      Keep going until there B[i]eF
      WT[i]=I
      Store I value for node i in repository
  i++
  else
    For each node i take its neighbours eNi
    For each neighbour Ni[j]
      Get I value from the repository
      j++
    endfor when j=φ
    Sum together the I values of the neighbours, calculate the average and allocate to R
    Store R value for node i in repository
  i++
  For each node i
    Get I value and R value from the repository
    Apply mathematical operator and allocate result to A
    Store A value in repository
  i++
Terminate algorithm when i=φ
```

Figure 5-Unnormalised Vulnerability Measure Algorithm

Chapter 3-Vulnerability Measure

Once all the variables are initialised, then counter i is incremented by 1 so this means that the OSN profile for node 1 is to be examined first. All the profile attributes of node 1 are stored in set B and are ready to be analysed. If any of the attributes presented on the profile match any of the vulnerable attributes from set F , then the vulnerable attribute weight for that particular attribute from set W is taken and added to the running weight total of node 1 (WT). This means that every time a new weight is added, the total weight of the node is updated. Once there are no more vulnerable attributes, the running weight total becomes the individual vulnerability (I) value of the node which is then stored in the repository. The counter i is then incremented by 1 and the individual vulnerability is calculated for node 2. This process happens until the counter reaches the end of the node list which is represented by Y .

The next stage involves calculating the relative vulnerability of each node. This stage begins with node 1 again. For node 1, the list of neighbours is derived and their corresponding individual vulnerability values are extracted from the repository, one neighbour at a time. Once there are no more neighbours for node 1, the individual vulnerability values for the neighbours are added together and the total becomes the relative vulnerability (R) value for node 1 which is stored in the repository. The relative vulnerability is then calculated for the rest of the nodes in the node list and placed into the repository.

After the relative vulnerability has been calculated for all the nodes in the node list, the final stage of the algorithm involves calculating the absolute vulnerability for each node. This stage begins at node 1 and the individual and relative vulnerability values for node 1 are extracted from the repository. A mathematical operator (e.g. product or MAX) is applied to the values and this result in the absolute vulnerability (A) value for node 1. The value is stored in the repository

Chapter 3-Vulnerability Measure

and then the absolute vulnerability values are calculated for the rest of the nodes in the node list and once the end of the node list has been reached the algorithm will terminate.

3.4-Vulnerability Measure Application

Figure 6 highlights how the vulnerability measure can be applied by using the OSN graph in conjunction with the vulnerability algorithm. This shows how the graph is used especially in the relative vulnerability calculation when the neighbours of the node have to be identified. In the following example which is illustrated in Figure 6, the attributes and their weights are just for the sake of the example.

Using Figure 6, let's consider an OSN graph consisting of MySpace profiles linked together by *top friends* relationship. The edges with dashed lines in Figure 6 show that there is no relationship between two nodes. An example is that node B is in node C's *top friends* list but node C is not in node B's *top friends* list. The OSN graph in Figure.6.highlights the fact that in some OSNs, (e.g. MySpace), the relationship between two people may be bidirectional, although not necessarily always.

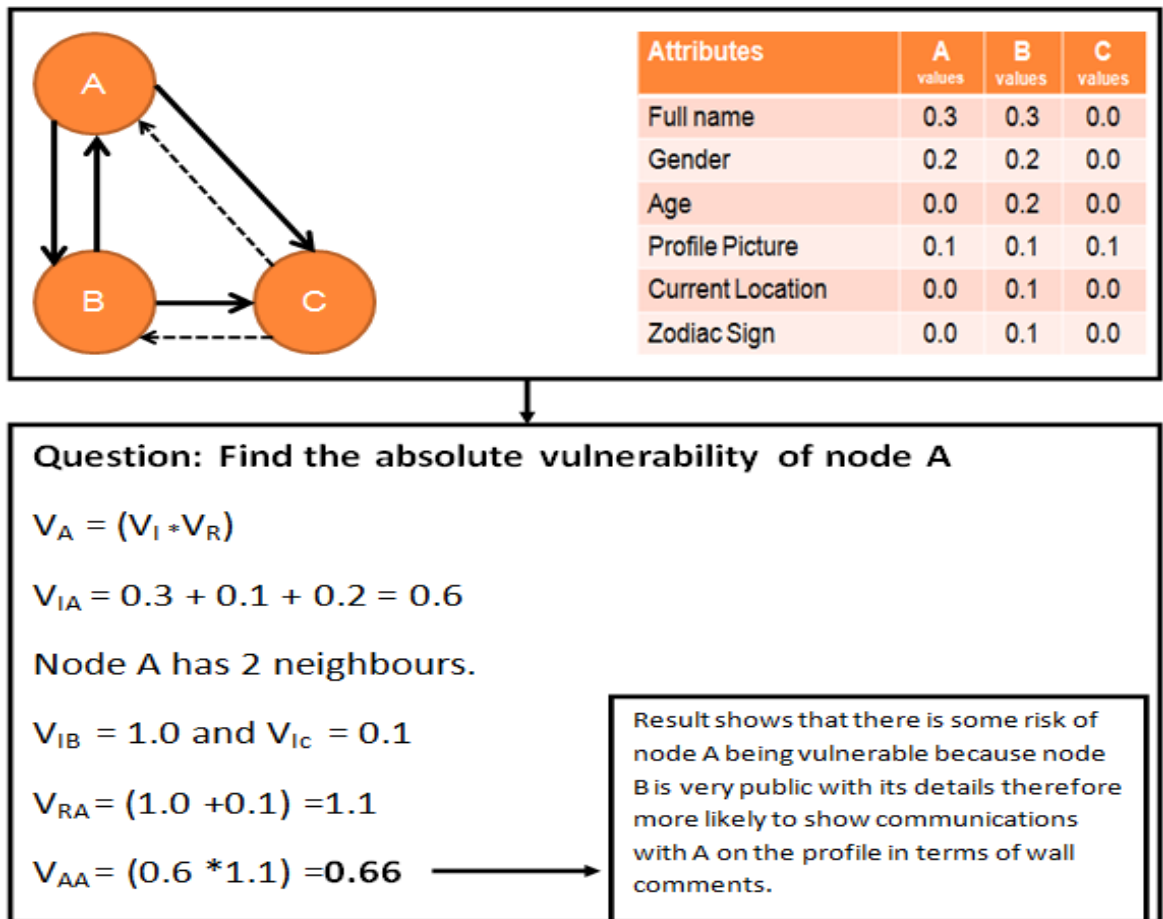


Figure 6-Unnormalised Vulnerability Measure Application

In the case illustrated in Figure 6 which uses the algorithm presented in Figure 5 , node B has the highest V_I and therefore contributes towards node A's vulnerability value The V_R value of node A is lowered because of the low V_I of node C.

3.5-Vulnerability Algorithm Issues

The algorithm has highlighted various aspects of the vulnerability measure which are detailed below, that can be altered or added, in order to accurately reflect a dynamic OSN network.

3.5.1-Attribute Weights

The weights of the attributes form a major part of the vulnerability measure. Even though for the weights the relative frequency of the attributes in the dataset can be taken, this approach does not indicate the importance of an

Chapter 3-Vulnerability Measure

attribute. As far as we know, there is a lack of research done into the importance of attributes (e.g. Does displaying a *name* on an OSN profile impact more than displaying your *age* on an OSN profile?) When hackers gain access to details, are they paid more for extracting certain user attributes? There is no established hierarchy of importance in regards to attributes. Stated below are two different approaches that can be used to investigate the importance of attributes

Information Theory Approach

The field of information theory is based around the concept of uncertainty and how to measure uncertainty. The more information there is available, the less uncertainty there is. This theory formed the basis for entropy (Shannon and Weaver 1949) which was used as a measure for uncertainty. The equation to measure the entropy of a random variable X is

$$H(X) = -\sum_{i=1}^n P(X_i) \log_2 P(X_i) \quad (14)$$

where n is the number of events and $P(X_i)$ is the probability of event i occurring. Entropy is measured in bits of information. The entropy measure can be used to measure the uncertainty of an OSN profile. In theory, the more personal details that are presented on the profile, the lower the amount of uncertainty and therefore a lower entropy value. Entropy can be a measure of surprise. The lower the probability of the event occurring, the more surprising it is.

Using equation 14, the events would be represented by the attributes of the profile and the probability of displaying the *name* is the number of nodes that display the *name* / total number of profiles in the network. There are some axioms which are associated with equation 14 i.e. the entropy is a non negative

Chapter 3-Vulnerability Measure

quantity and that if the probability of an event is 1 then there is no uncertainty. The function between probability and entropy should be continuous and monotonic. This means that small changes in the probability of an event should only result in small changes in the entropy value. In terms of vulnerability, the lower the vulnerability the higher the entropy.

Statistical Approach

Another type of approach which can produce attribute weights is using the results of a questionnaire to develop a statistical approach to derive the weights. To investigate the variety of weights that this approach would produce, we developed an online questionnaire.

Questionnaire Design

The specific aim of the questionnaire was to develop an approach for generating attribute weights based on peoples' responses to the questionnaire in terms of rank attributes according to importance in disclosing the identity of a person.

The questionnaire which is presented in Appendix I is comprised of two parts. The **first part** collected the gender and the age of the participants but this information was only used for statistical purposes.

The IP address and the name of the participant were not collected in the questionnaire, and no other particular information to identify the participant is used in the questionnaire.

The **second part** of the questionnaire required the participant to classify a list of 19 items of personal details known as attributes in terms of importance when it came to disclosing a persons' identity. The 19 items of personal details were

Chapter 3-Vulnerability Measure

selected because they were attributes that were available for users to fill in, on various OSN profiles.

The scale of importance in this questionnaire was a category scale which was ordinal because the orders of the categories are placed in terms of their magnitude. A category scale is a rating scale for closed ended questions where the response options (categories) are specific verbal descriptions (Zikmund et al 2010).

For the scale, the categories were not important, important and very important. Not important means that the participant feels there is no importance in the attribute contributing towards disclosing the identity of a person. Important indicates that the participant feels there is some importance that the attribute will contribute towards disclosing a person's identity. Very important means that when trying to disclose a person's identity, the participant feels this attribute has a significant contribution towards disclosure.

For the magnitude of the scale, very important has more magnitude than important which has more magnitude than not important. The magnitude of the categories contributes towards the statistical approach which is detailed in the section entitled questionnaire results.

The category scale only consists of three categories because the main aim of the questionnaire was to help generate attribute weights and having this scale would remove uncertainty when classifying attributes. Having a larger category scale which consists of the categories: not at all important, not important, neutral, important and very Important, would impose some uncertainty. This is because the category neutral implies that the participant has no opinion on the question asked. Also the category not at all important sounds too similar to not important.

Chapter 3-Vulnerability Measure

The questionnaire was initially designed using SurveyMonkey¹⁶ which is a free online survey software and questionnaire tool which allows you to collect responses as well as analyse the results. It is a subscription based service where if you chose the 'basic' service you would pay nothing but only be able to collect and analyse the responses for 100 participants. This issue meant that the same questionnaire was also created using Survey Methods¹⁷ where the number of responses you can collect and analyse for free is 500.

Questionnaire Sampling

The objective of the questionnaire was to determine what people thought about a variety of attributes in terms of importance in contributing towards disclosing a persons' identity.

Before distributing the questionnaire to participants, the target population had to be defined. Burns (2000) defines a population as "*an entire group of people or objects or events which have at least one characteristic in common, and must be defined specifically and unambiguously*".

The issue of privacy affects a variety of people in various age ranges. For the questionnaire, in order to take this issue into account, the target population was defined as a population of people who study or work at higher education establishments in the U.K and abroad. Also the population included friends and family of the thesis author and some of her research colleagues.

Respondents to the questionnaire included staff from the institution where the thesis author was based, students from the department which the thesis author was based, staff and students from Saudi Arabia, United Arab Emirates, UK, Malaysia and US higher education institutions. Also respondents included

¹⁶ <http://www.surveymonkey.com/>

¹⁷ <http://www.surveymethods.com/>

Chapter 3-Vulnerability Measure

college students taking part in an open day associated with the department where the thesis author was based, friends and family of the thesis author and her research colleagues. The students from the higher education institutions include undergraduate and postgraduate.

The questionnaire participants did not necessarily have to posse an OSN profile. Non OSN users still have opinions on what attributes can contribute towards the disclosing of a person's identity.

Sampling Methods

A mixture of snowball sampling and convenience sampling were used to select the sample from the population. These sampling methods are non-probability sampling methods because the sample is selected based on the researcher's judgment rather than a random selection which is a probabilistic approach to sampling. Non probability sampling methods are also suitable for exploratory research which is the case for this research.

Exploratory research is when there is limited information or no information about earlier studies regarding the research problem. Consequently the research is more centered on building a theory (Palgrave 2008; Jupp 2006). The research in this thesis is about building a theory involving the vulnerability of OSN profiles and there has not been any previous studies based on the measurement of vulnerability of OSN profiles.

In terms of sampling methods, snowball sampling is when initial respondents are selected and then additional respondents are acquired by information that is passed on from the initial respondents (Zikmund et al 2010). The ways in which snowball sampling was used in regards to the distribution of the questionnaire are listed below:

Chapter 3-Vulnerability Measure

The thesis author emailed the questionnaire to known lectures in universities based in the U.K and abroad and asked them to pass on the questionnaire to people they know including colleagues, students and friends. The lecturers were known to the thesis author because of either being taught by them or being research contacts.

- The thesis author also emailed the questionnaire details and link to her friends to fill out the questionnaire and asked that the friends passed on the questionnaire details and link to their friends and family. .
- In order for the questionnaire to be distributed to staff and students at universities abroad, the thesis author asked research colleagues who were lecturers in their home countries, to email the details of the questionnaire including the questionnaire link to acquaintances as well as colleagues, students and family members back at their home countries.

The reasons why snowball sampling was used because it allowed a possibility to reach populations that are normally difficult to sample. In the case of this questionnaire, participants who were not known to the thesis author directly were reachable indirectly.

Another sampling method used to gather a sample was convenience sampling. Convenience sampling is defined as obtaining participants who are readily available to take part in the questionnaire and also who are accessible (Zikmund et al 2010).

The ways in which convenience sampling was used in regards to the distribution of the questionnaire are listed below:

Chapter 3-Vulnerability Measure

- Staff from University of Bradford: details and link to the questionnaire submitted to ‘Staff Briefing’ which is a weekly newsletter which is delivered to staff at the University of Bradford via email.
- Students from University of Bradford computing department: for research students known to the thesis author, an email was sent out explaining and providing a link to the questionnaire. For undergraduate and postgraduate students, the head of the computing department distributed an email containing the details of the questionnaire and a link to the questionnaire to the relevant mailing lists.
- An open day took place at Bradford University with college students and the thesis author took part in a presentation of the vulnerability research. In the presentation, the questionnaire details and link to the questionnaire were mentioned to the college students.

Convenience sampling was used because it is a method which allows a researcher to use a less expensive approach in order to gain an approximation of the truth. Also Zikmund et al (2010) highlights that “*convenience samples are best used for exploratory research when additional research will subsequently be conducted with a probability sample*”. The research in this thesis is exploratory but in the future probability sampling methods can be used to gain a very large sample of participants who use OSNs or the WWW.

Questionnaire Results

The questionnaire was created in January 2010 and was available for participants to fill in from January 2010 to May 2010.

There were 275 people who responded to the questionnaire. In the respondents to the questionnaire, 51.2% were male, 48.3% were female and 0.36% chose not to specify their *gender*. The age ranges of the respondents varied. 3.2%

Chapter 3-Vulnerability Measure

were under 18, 41.4% were 18-24 years old, 44.7 % were 25-34 years old, 5.8% were 35-44 and 4.72% were 45 or over. Figure 7 illustrates how the attributes were classed in terms of importance when it comes to disclosing a persons' identity. There was a small percentage of respondents who filled out the first part of the questionnaire but then did not classify the attributes and that is why the percentages may not add up to 100.

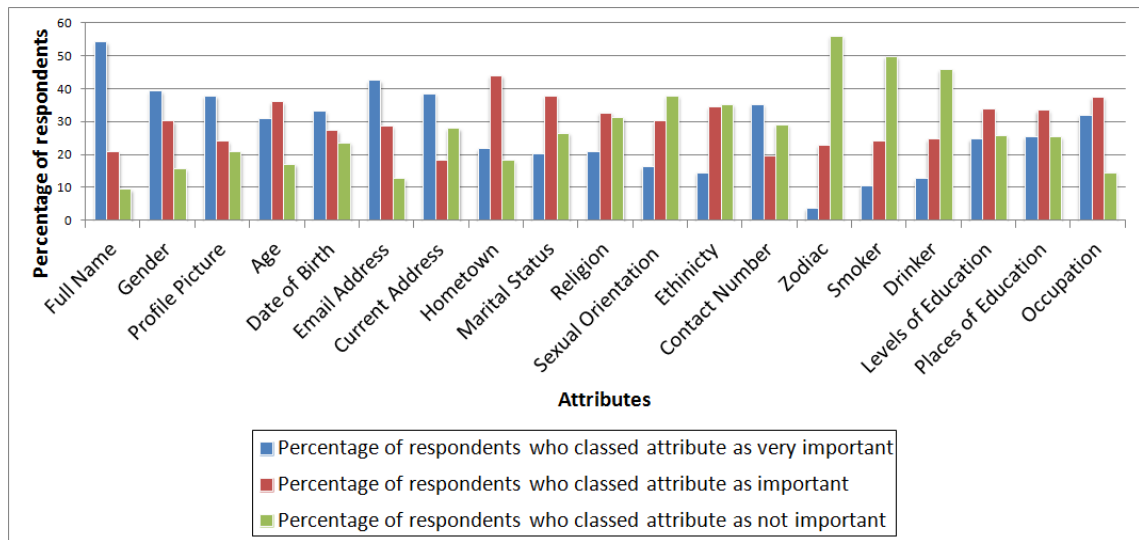


Figure 7-Attribute Importance Classification

From the online questionnaire results in Figure 7, the attributes were then placed into the class with the highest percentage of respondents. The attributes that were classed as the very important when it comes to identifying a person included *full name, gender, profile picture, date of birth, email address, current address and contact number*. These results justify our choice of some of the attributes for the vulnerability measure. Some of the attributes which were classed as important (e.g. places and levels of education) maybe classed as very important if the attributes are being used to identify children.

A statistical approach can be established from the results of the questionnaire. To allocate more significance to attributes that were considered as very important, they were given twice the weight then attributes that were classed as

Chapter 3-Vulnerability Measure

importance. This was because if the very important classed attributes were display on an OSN profile, those attributes would contribute more towards increasing the profile owner's chances of their identity being disclosed according to the results from questionnaires and the literature in the field.

Attributes classed as very important were given twice the weight. This factor of 2 was an initial setting and more research in the future into attribute importance involving OSN profiles, will provide a more accurate factor value.

A scenario which is illustrated below shows how the weights are derived.

An OSN user profile $p_j \in P$ is defined by a tuple of attributes $\mathcal{A} = \langle a_1, a_2, \dots, a_i, \dots, a_n \rangle$. The attributes can be personal details or social network attributes (e.g. news feeds). In the case of the OSN profile in Figure 6, the profile has displayed 6 attributes that have been classed as attributes that contribute towards a profile being vulnerable. One of these attributes (*Age*) is classed as important and four of the attributes (*Full name, gender, profile picture and current address*) are classed as being very importance. The attribute zodiac sign is classed as not important. The sum of the attribute weights has to be equal to 1 i.e. $\sum_{k \in A'} S_{j_k} + \sum_{k \in A''} 2 * S_{j_k} = S_j, \forall j$ where A_i is the set of attributes that contribute towards profile i being vulnerable; S_j is the total weight of the attributes that contribute towards vulnerability and S_{j_k} is the weight of the vulnerable attributes which are classed as important. The notation A' is the set of attributes that are classed as important and A'' is the set of attributes that are classed as very important.

Applying the approach detailed above to derive the weights, four attributes were classed as very important and one attribute was classed as important. This

Chapter 3-Vulnerability Measure

meant that the weight $1/9=0.111$ for important attributes and $2/9=0.222$ for very important attributes.

Overall the two approaches (entropy and statistical) are different in that entropy is based on the attributes presence in the profiles in the network whereas the statistical approach is based around a questionnaire which would produce subjective weights. The entropy approach which is factually based, focuses on the actual actions of the user. This gives a more accurate picture in comparison to the statistical approach which is subjective. The subjective approach is more associated with users' thoughts. There is also the issue of whether users' thoughts will translate in to actions carried out by the user.

3.5.2-Choice of Attributes

The attributes stated in section 3.11 that are used in the vulnerability measure, are not the definitive set of attributes. The types of attributes presented and the impact they have on vulnerability depends on the context of the OSN and the type of user. Different OSNs like to display different attributes of the user (e.g. Facebook) displays the *date of birth* where as with MySpace the *age* is displayed.

3.5.3-Relationship Strength

The one factor which needs to be incorporated into the vulnerability measure in the future is the strength of the relationship between two nodes. A node which has a poor relationship with another node will not interact as much with the node and therefore there is a reduced chance of leaking personal details via profile interactions. The concept of friendship in OSNs is a very interesting issue.

The notion of '*friendship*' has a variety of meanings . Boyd (2006) describes the relationship of a friend as one that requires a degree of admiration and mutual

Chapter 3-Vulnerability Measure

love. This definition is on a basic level and can be applied to a offline friendship i.e. communication without the use of computers (e.g. writing letters, talking to each other on the phone, a face to face conversation).

With the rise in social media usage, online friendship has become very popular and has led to a trend in using OSNs to track the activities and news of their family members rather than having a face to face conversation with them. This is illustrated in a survey carried out on 3000 British people by the company Flip Video at Cisco. 1 in 5 of the people surveyed admitted that they use OSNs to keep track of what their family members are doing rather than talking to them or phoning them (Cisco 2010). Having a friendship on an OSN (e.g. Facebook) can be different to having a friendship offline in regards to the number of friends you have. People can have 100 online friends on their profile but how many of those friends are real friends and how many are acquaintances or even strangers (Zinoviev and Duong 2009)?

Thelwall (2008) attempts to answer this question by presenting a friend mechanism for MySpace. The friend mechanism analyses the total number of friends that the person has on their profile and applies the following classification:

- Having 0 or 1 friends is classed as having no friends because Tom is automatically a friend when you create a profile on MySpace. This category is for people who have just joined MySpace and therefore have no friends yet.
- Between 2 to 9 friends is classed as close friends. These friends may be your offline friends who can be persuaded into joining the OSN or you have just a small close set of friends. This situation indicates that maybe this person is privacy conscious.

Chapter 3-Vulnerability Measure

- Between 10-90 friends is classed as acquaintances who are people you know but do not class them as friends. This category may include (e.g. work colleagues or old class friends).
- 90 or above friends indicates that there is a possibility that strangers have been added as friends. This can increase the vulnerability of the person and can lead to (e.g. cases of harassment, risk of pedophilia or identity fraud).

There are several reasons why people have many friends in their profiles. Boyd (2006) mentions the issue of popularity where there is a trend to see who can get as many friends as possible. If the owner of the profile is a child or a teenager then this sort of behaviour can lead to trouble. Lenhart and Madden (2007) carried out a telephone interview with 935 teenagers aged 12-17 and their parents in the United States. Their survey found that 31% of the teenagers that use OSNs have friends in their profiles that they have never met. A major disadvantage of having online friends is that if you do not know them then they can pretend to be someone totally different in terms of identity. This can lead to cases of harassment, stalking and bullying. Meeting a friend face to face takes some of the mystery out of their identity and what they present on their social networking profiles.

Another reason why people may have many friends is because the OSNs encourage them to do so. Wilkinson and Thelwall (2010) emphasises the fact that MySpace, like Facebook has ways to invite more friends to join the network. MySpace has the MySpace automated friend finder. The friend finder can work in different ways. It can search through your email accounts and flag contacts who have registered on the same social network as you, but neither of you have *friended* each other yet. The Facebook friend finder will also

Chapter 3-Vulnerability Measure

recommend people who you may know based on your friends' friends and similar attributes you may share i.e. being in the same year group at the same school. The use of the friend finder has highlighted that there needs to be more awareness on OSNs about online friends and the dangers in adding strangers.

A significant reason that is not mentioned by Wilkinson and Thelwall (2010) is very often associated with the simplicity and convenience of forming online friendships on OSNs. With making friends online, all it takes is one mouse click on the '*add as a friend button*' and a confirmation of the friendship with the friend you want to add. In the offline world, more work is needed to make and maintain a friendship via engaging in conversation and finding out about the person's personality, identity, likes and dislikes. Unlike the online world where the identity of the person is not always presented correctly, a face to face conversation allows validation of some of the features of the person's identity.

In terms of the likelihood of a friendship occurring, two people are more likely to establish an online friendship connection on an OSN if there are attributes that they both share in common (e.g. the same hobbies, going to the same school or having the same group of friends). Also their backgrounds may be similar. These attributes could be faked in order to establish a relationship with a user. With OSN profiles, validating a users' identity is difficult and because you can't see the users' face. Therefore, attributes such as age can't be validated.

This concept of friending people who are similar to you is known as homophily. In graph theory the concept of triadic closure can be applied to this model, where if two people share a common friend then there is an increased possibility that they will become friends themselves at some point (Simmel and Wolff 1950).

Chapter 3-Vulnerability Measure

Homophily can be called into question because of Granovetter's (1973) theory that if you want to find a job it is better to speak to someone outside your circle of friends. You may not have any attributes in common with the people outside your circle of friends but you may learn valuable job information. Granovetter's (1973) theory centers on the concept of strong and weak ties. Strong ties are people that you have strong bonds with (e.g. friends and family) whereas weak ties are people that you do not share a strong bond with (e.g. friend of a friend or an acquaintance). However with weak ties, they provide the chance to acquire new ideas or information. Also the weak ties are effective at spreading ideas because acquaintances and friend of a friend will have their own set of friends.

One element which has a significant effect on friendship in OSNs is the strength of the relationship between two people. This is known as '*tie strength*'. If the two people are presented by nodes in an OSN graph then the 'tie' is the edge which connects the two nodes together. In the field of OSN analysis, tie strength plays an important part when proposing measures which involve the analysis of relationships between two people. Tie strength was first characterised by Granovetter (1973). Granovetter's concept was that tie strength could be characterised by a "*combination of the amount of time, the emotional intensity, intimacy and reciprocal services*".

At present, in some OSNs (e.g. LiveJournal) the idea of tie strength being characterised by reciprocal services cannot always be applied. This is because the friendship between two people is not always bidirectional due to the fact that in the case of LiveJournal, permission does not have to be granted to add someone as a friend. This is in contrast to Facebook where to become a friend with a user they have to accept the friend request. Another example is the concept of *top friends* which are defined as close friends. Alice is in John's *top*

Chapter 3-Vulnerability Measure

friends list but John is not in Alice's *top friends* list. Research done after Granovetter (1973) by other authors has increased the list of factors of tie strength including Structural Factors and network topology (Burt 1995), Emotional support (Wellman and Wortley 1990) and Social Distance (Lin et al. 1981).

Structural Factors and network topology focuses on the network that two users that are friends have in common. The factors include the number of mutual friends, groups in common and the number of overlapping networks. Emotional support, analyses profile wall comments and inbox messages between the two users for the presence of positive and negative emotion words. Positive emotion words include sweetheart, congrats and birthday. Negative emotion words include hate, dump and useless. The social distance between two users can measure the age differences (in days) between two users, differences between the educations of the two users (degrees), number of occupations differences between the two users and the political differences of the two users Gilbert and Karahalios (2009).

As the world of social media has grown so has the list of factors that contribute towards tie strength. Gilbert and Karahalios (2009) highlighted this by explaining that in reality, tie strength has seven dimensions and many alternatives. The factors which have become more prevalent in recent years have revolved around the frequency of communication and interaction between the users. Singla and Richardson (2008), Yun et al. (2010) and Xiang et al. (2009) analysed how user interaction played a part in calculating the tie strength of two users.

There are various types of user interactions on OSNs that take place between two people including the viewing of each other's profiles, establishing a

Chapter 3-Vulnerability Measure

connection via the acceptance of the friend's request and the tagging of pictures (Xiang et al. 2009). Two users have a strong relationship on an OSN when there is regular user interaction between both parties. Singla and Richardson (2008) demonstrated this by emphasising that people who spend a lot of time talking via instant messaging are more likely to share their personal attributes and interests. This makes the relationship stronger but is it bad news for privacy issues and vulnerability especially if both the people display their profiles in a very public way.

The various types of user interactions can be classed into public and private. Public interaction such as writing comments on the person's profile or photo tagging whereas a private interaction is sending a private message to the person. Yun et al. (2010) makes an interesting point that private interactions should be given more weight when calculating the tie strength between two people. Their investigation involved analysing the user interactions of Twitter and me2DAY which is a Korean website similar to Twitter. They found that private interactions were rare online. Private interactions in the case of Yun et al. (2010) research study were direct messages, short messages by phone and sharing gifts.

Private interactions are harder to quantify inside a network in comparison to public interactions inside a network. Inside an OSN, say Facebook, users have access only to their own private interactions but Facebook can crawl and mine the private interactions for all the Facebook users.

Overall, tie strength is a multidimensional area which encompasses computer science, sociology and psychology in order to investigate the strength of relationship between two people. The fact that there has been emphasis on user interactions reflects the modern day use of OSN sites.

3.5.4-Analysing different parts of the profile

In OSN profiles there are various ways in which a user can leak their personal details (e.g. comment walls or tagging photos), but there are some OSN users who use blogs to interact with their friends. Blogs can be used to keep a reader up to date on a certain topic or as a personal diary containing (e.g. the inner most thoughts and emotions of a person). Blogs can contain music or video clips.

Another aspect which can leak personal details in a more obvious way is quizzes. Browner (2010) work emphasises how a relative harmless quiz can lead to big consequences for the user in terms of their identity. A multiple choice quiz that was an application that could be added to a Facebook profile asked questions like how long is your password? and is your password your *name* with some other numbers or somebody in the family? The answers given to these types of questions can lead to identity fraud, especially if the hacker manages to guess your password from the answers given in this quiz. Also because this quiz was a Facebook application, once the user agrees to run the application then the application has access to the user's Facebook profile and its contents. Personality quizzes can leak personal information(e.g. *gender, age, date of birth, email*) as well as likes and dislikes. The details that should never be given in quizzes includes personal identifiable information , password details, banking details and mother's maiden *name*.

3.6-Conclusions

The increase in use of OSN profiles to display personal details on profiles had provided a need for a vulnerability measure. The vulnerability measure is concerned with how the displaying of personal details can make you vulnerable to privacy or social engineering attacks. The vulnerability measure consists of

Chapter 3-Vulnerability Measure

three components which include the individual vulnerability which focuses on the vulnerability of a profile, relative vulnerability which highlights the collective vulnerability of the profile's neighbours and the absolute vulnerability which takes into consideration the individual and relative vulnerabilities. The algorithm which is stated in this chapter does present some significant issues which can form the basis for future work (e.g. the weights and the choice of the attributes). The vulnerability measure forms the foundations for the other work presented in this thesis

CHAPTER 4: ONLINE SOCIAL NETWORK DATA EXTRACTION AND GRAPH PROCESSING

The aim of this chapter is to present our data extraction approach for OSN profiles which is detailed in the papers: Alim et al. (2009) and Alim et al. (2011b). The data extraction allows for personal details and a list of friends to be extracted from OSN profiles, in this case MySpace, in order for an OSN graph to be generated. This OSN graph is analysed in this chapter for structural factors which can affect the vulnerability of a profile.

4.1-Data Extraction Methodologies in Social Networking

The field of data extraction in OSNs has come a long way since Gross and Acquisti (2005) who used a questionnaire to ask people about their views on privacy. Extraction methodologies can be split into two separate types which are non automated and automated. Non automated approaches through the use of surveys and interviews are used in research done by Gibson (2007), Govani and Pashley (2005), Dwyer et al. (2007) and Strater and Richter (2007). On the other hand, in the past couple of years there has been more analysis done on data produced from automated extraction approaches. Automated approaches include web crawlers and some examples of studies which use web crawlers include Arjan et al. (2008) and Caverlee and Webb (2008).

Table 2 illustrates some of the data extraction techniques in more detail which are used to extract attributes from OSN profiles. It shows some data extraction methods ranging from manual through to automated methods.

Chapter 4-Online Social Network Data Extraction and Graph Processing

Table 2- Different Extraction Methods from OSNs

Method	Research Study	Ref
Developed an automated web crawler using the Ruby programming language. The crawler would visit profile pages based on a randomly generated list of id numbers using the RAND function of Microsoft excel. Regular expressions were used to collect the relevant bits of data.	Age Differences in online social networking	Arjan et al (2008)
Wrote two crawlers that were MySpace specific based on " <i>Perl's LWP User agent and HTML parser modules</i> ". They gathered 2 datasets. One was collected using random sampling and the other one with relationship based sampling.	A large scale study of MySpace Observations and Implications for Online Social Networks	Caverlee and Webb (2008)
Downloaded MySpace profiles randomly.	Social Networks, Gender and Friending: An Analysis of MySpace Member Profile	Thelwall (2008)
Used a random number generator to decide which profiles to analyse. Analysis of the profiles took place by manually analysing the profiles and using a data collection form to record their findings	Personal Information of adolescents on the Internet. A quantitative content analysis of MySpace	Hinduja and Patchin (2008)

The first two approaches in Table 2 are automated crawlers which allow a vast amount of data to be extracted within a short period of time. However any changes to the source of extraction (e.g. structure changes to the webpage) may require some adjustments to the crawler. On the other hand, the bottom two approaches which are not automated, requires a lot of time to collect a substantial sample of data.

4.2-Our Data Extraction Approach

The overall aim of developing our data extraction approach (Alim et al. 2009; Alim et al. 2010; AbdulRahman et al. 2010) is to extract OSN profiles from MySpace in order to construct an OSN graph which would help us to measure the vulnerability of OSN profiles. Also the extracted profiles would provide real life cases for the vulnerability measure to be applied to. MySpace was chosen as an OSN because it allows a rich source of data to be derived from profiles without the need to be a member of MySpace.

Chapter 4-Online Social Network Data Extraction and Graph Processing

This chapter will focus on our initial experiment (Alim et al. 2009) which involved developing and running our data extraction approach algorithm 500 times and extracting attributes and *top friends* from 298 profiles because the rest of the profiles were private, musicians or bands. An OSN graph was produced and analysed to identify structural features that could contribute to and affect the vulnerability of a profile.

Chapter 5 will detail the second experiment which involved running the algorithm 250 times but instead of *top friends*, all the friends and relevant attributes were extracted from 163 profiles because the rest were musicians or band profiles. For the second experiment private profiles were also extracted as well because users still display personal details on private profiles. With private profiles the list of friends is not displayed on the profile but some personal details can be displayed. An OSN graph was constructed from the repository and the vulnerability measure was applied to the extracted profiles. Some of these profiles formed the basis for case studies which were used for validation purposes.

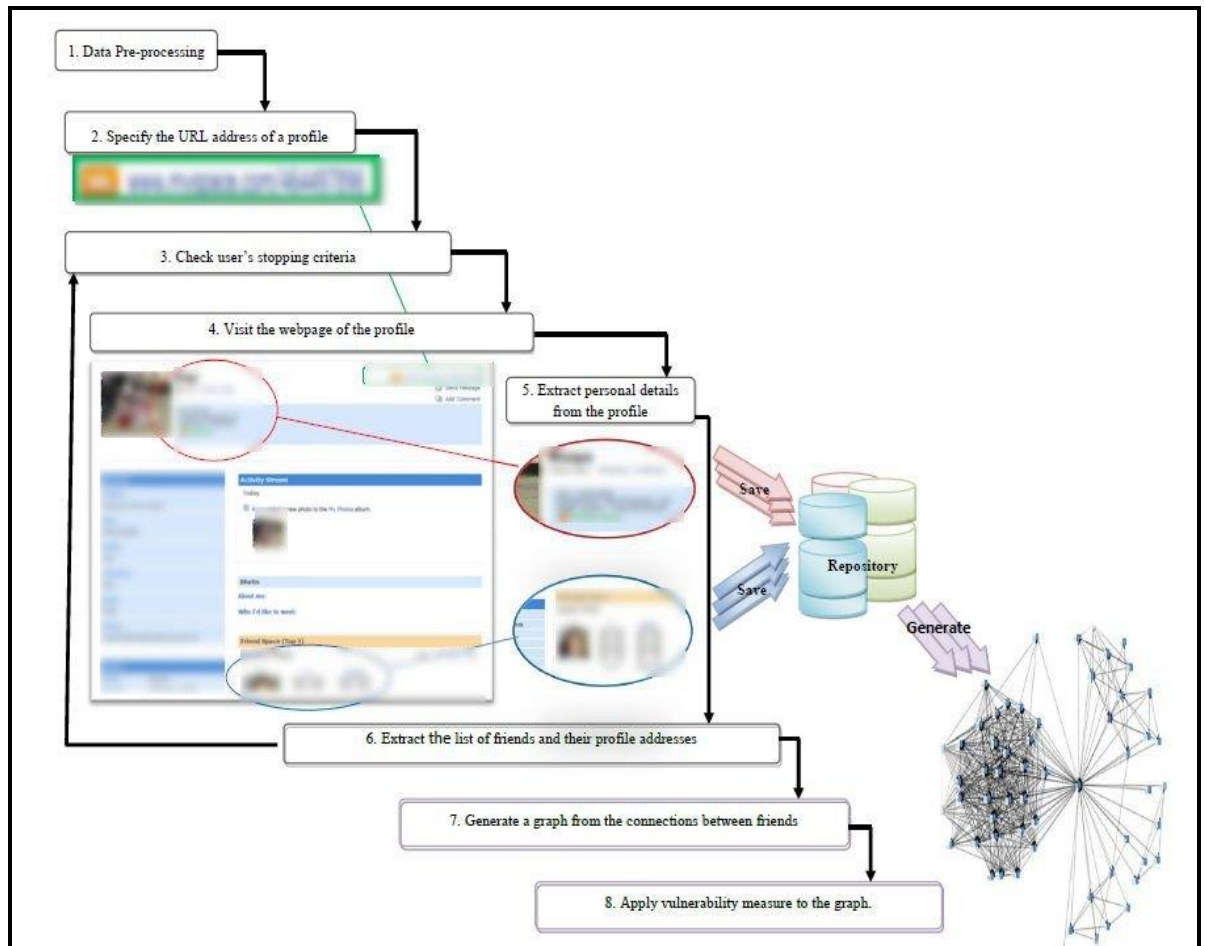


Figure 8-Data Extraction Approach for OSN Profiles

Our general data extraction approach for extracting from OSN profiles is comprised of eight stages:

Step1. **Data pre-processing** involves analysis of a given profile's HTML structure. The HTML content is parsed and a vector of tokens is produced. The extracted tokens help in the design of the tables in the repository and to determine the different types of structures of MySpace profiles. Different structures mean different tokens. We created our own MySpace profiles to help investigate the different possible structures and attributes associated with them.

Step2. **Specify the URL address of a profile.** All OSN profiles come with a unique profile URL address. The algorithm for the extraction of the personal details involved developing and expanding the library which

Chapter 4-Online Social Network Data Extraction and Graph Processing

was provided by Haines(1999). The Java code was developed to be applied to OSN profiles and the URL of the OSN profile was used as a parameter. Then Java IO methods would be used to extract the HTML of the profile's webpage and store it as a character array. The *parsePage* method which we defined would remove all the HTML tags from the string, split the remaining text in tokens and place the tokens into a vector. This method proved the most important when extracting the personal details and the list of *top friends* from the profile because the tokens would dictate the structure of the web page. In the case of Figure 8, the URL address, personal details and list of *top friends* have been blurred out for privacy reasons.

Step3. ***Check the stopping criteria.*** The extraction can be stopped by specifying the number of friends to be extracted (e.g., the first 100 friends) or by the level (e.g., level 1 is just the *top friends* of the specified profile extracted whereas level 2 is the *top friends* of the *top friends* of the profile extracted).

Step4. ***Visit the specified profile webpage*** after checking that it has not been visited before. Breadth First Search has been used for our applications to travel the OSN network as explained later.

Step5. ***Extract the relevant personal details from the profile*** and insert them into the repository, ready for OSN graph construction and the application of vulnerability measure. The repository that we used was PostgreSQL 8.1.4. The repository structure has to be designed for the Breadth First Search algorithm.

Step6. ***Extract list of the profile's friends and their profile addresses*** then insert them into the repository if they have not been stored in there

before. The extracted friends' lists can consist of the *top friends* of a profile or *all friends* of a profile. The data in the repository can be used for data mining purposes in the future to find patterns.

Step7. ***Automatically generates an OSN graph.*** The graph is generated from the extracted list of *top friend* or *all friends* of each profile. The various structural features of the graph will be analysed to see how they contribute towards the vulnerability of a profile (which is represented by a node in the graph).

Step8. ***Apply vulnerability measure to the OSN graph.*** The vulnerability of a profile which is represented by a node in an OSN graph is calculated by investigating the presence of vulnerable attributes on the profile and the profile's neighbours which are the profile's *top friends* or *all friends*.

4.2.1-Breadth First Search

Breadth First Search was used to travel across the OSN because for the vulnerability measure, profiles and their immediate friends were needed for the calculation. The scenario illustrating Breadth First Search in Figure 9 shows that profiles 2, 3 and 4 are the three *top friends* of profile 1. Profile 2 also has three *top friends* which are profiles 1, 3 and 5. Profile 3 is the top friend of profiles 1 and 2 where as profile 4 is the top friend of profiles 1 and 5. Entrance to the repository is implemented as a queue system. The arrows that the relationship represents are the '*is a top friend of*' relationship. An example is that profile 3 is a *top friend* of profile 1.

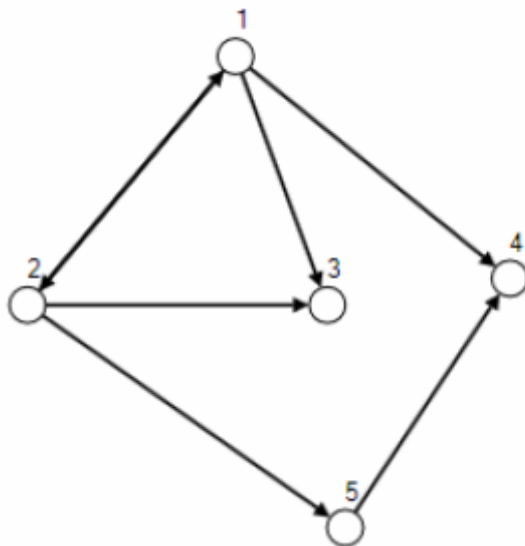


Figure 9-A Graph to illustrate Breadth First Search

The bidirectional arrows show that the relationship between the friends applies both ways. An example is that profile 2 is a friend of profile 1 and profile 1 is a friend of profile 2. Using Breadth First Search in this case follows the following steps:

1. Add profile 1's attributes and *top friends* list into the front of the queue ready to go into the repository.
2. Loop:
 - a. Look at profile 1's friends and check to see if they already exist in the repository. In the first iteration, the friends are profiles 2, 3 and 4.
 - b. If the friends do not exist in the repository, add their attributes and list of *top friends* to the rear of the queue.
 - c. Look at the next profile at the front of the queue (in this case profile 2).
 - d. Repeat steps a and b.

4.3-Data Extraction Findings

From our experimental work (Alim et al. 2009), it allowed us to learn how to automatically extract data from an OSN profile using a Breadth First Search approach. The structure of MySpace profiles was found to differ depending on

Chapter 4-Online Social Network Data Extraction and Graph Processing

the type of profile and the users' preferences. This proved a challenge when implementing the code especially when over time, the developers of MySpace have the ability to change the structure of the profile and therefore change the HTML structure. We identify this as a problem for data extraction from OSNs.

Analysis of web structures of various OSN profiles revealed that there was a standard format. Even though some of the profiles were private profiles, some attributes, (e.g., *nickname, gender, age and location* could still be extracted).

Data that is placed in the repository can be mined and analysed offline to recognise patterns and trends about the OSN in which the profiles are based. The repository is password protected and stored on a university computer for added security.

The profile data can also be used to identify which profile attributes and values make the person vulnerable to social engineering attacks. The meaning of vulnerability is associated with the disclosure of personal details. The more details you disclose the more vulnerable you can potentially make yourself.

Vulnerability can be inferred by the attributes presented, (e.g. if the *age* and horoscope signs are present on a profile then it is possible to guess when the birthday of the profile owner is). If there are comments which have happy birthday messages from friends present on the profile as well you may be able to tell the exact date of birth.

Displaying personal details in OSN profiles can make you more vulnerable to consequences in society. One example is whether the profile owner declares of there are a drinker and/or a smoker. Personal details present on OSN profiles can be of particular interest to employers when it comes to hiring employees. Profile details that can cause concern includes any mention of alcohol or drug

use and information that implies that the person has been linked to criminal activity (Havenstein, 2008).

4.4-Online Social Network Graph Processing

An OSN graph was then generated from the repository data. The repository data included the personal details and the friends' lists of all the OSN profiles that were crawled using the approach outlined in section 4.2. The graph was generated so we could analyse the graph for characteristics which could influence vulnerability via the spread of personal details in OSN profiles. The graph analysis took place using NodeXL¹⁸ and is illustrated in Figure 10.

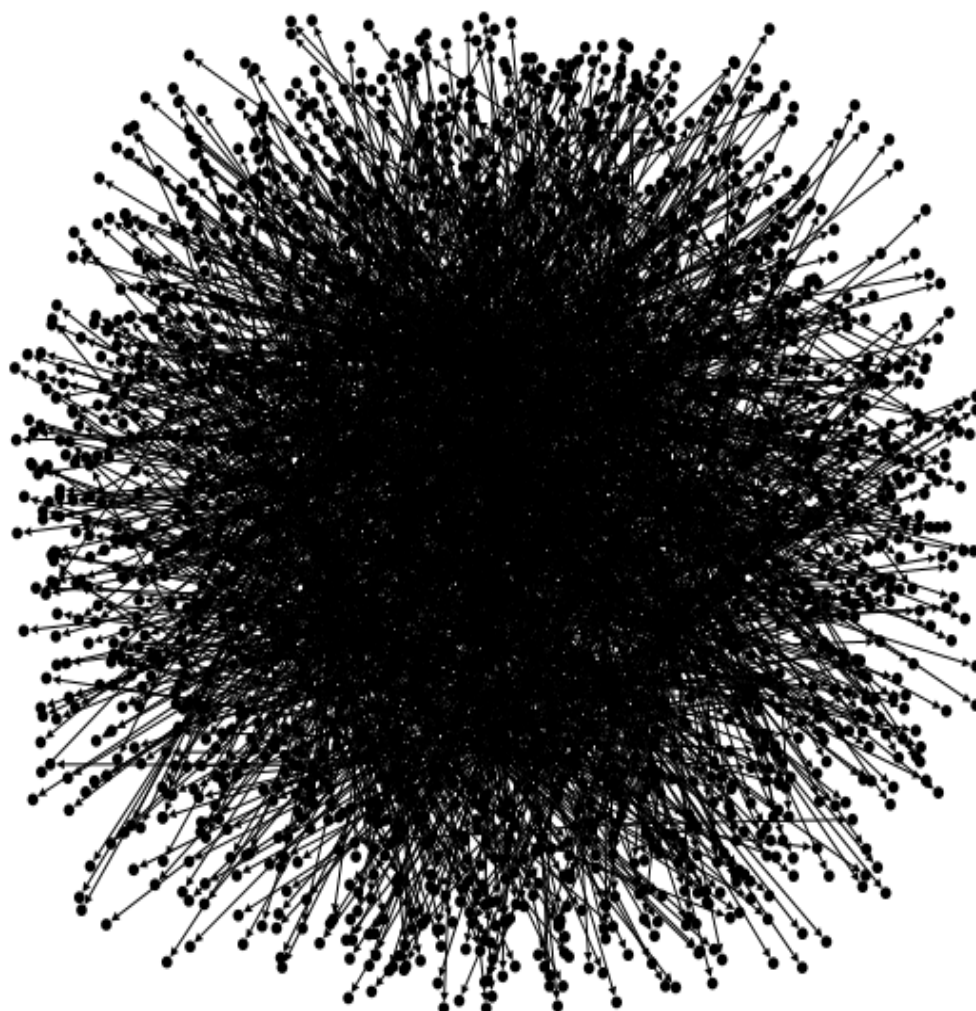


Figure 10-OSN Graph for Top Friends Extraction

The OSN graph G is modelled as a directed multigraph $G = (V, E)$. V is the set of nodes that represent the profiles of users on the OSN which has been

¹⁸ <http://nodexl.codeplex.com/>

Chapter 4-Online Social Network Data Extraction and Graph Processing

extracted from. E is the set of edges which links the profiles together. The relationship which is represented by the edges is a *top friend* relationship. *Top friends* are not bidirectional, (e.g., node 1 can be a *top friend* of node 2 but node 2 may not be on node 1's *top friends* list but may be a friend of node 1). Graph G is a directed multigraph because we want to analyse the flow of information so direction is required. Also the multigraph aspect gives an extra dimension to the analysis stage especially with the information flow being bidirectional.

There are many measures that can be applied when studying OSN graphs. Many authors including Wilson and Nicholas (2008), Wang and Chen (2003) and Xu and Chen (2008) have highlighted that there are three particular characteristics of a network graph that are used in classifying the type of network (i.e. small world, scale free or random). These characteristics include the average clustering coefficient, average path length and degree distributions.

Graph G in Figure 10 has $|V| = 2,197$ and $|E| = 2,747$. Graph G contains 1 connected component in which the maximum number of nodes in the component is 2197 and the maximum number of edges is 2747. The diameter of the graph is 10, which indicates that graph G represents a wide OSN network where there is a lack of small shortest path lengths between the nodes. An explanation for this being that graph G represents *top friend* relationships between nodes and there may be no relationship between a set of (e.g. node A 's *top friends* and node B 's *top friends*). This is further justified by the average geodesic (shortest path length) distance of graph G being 6 which corresponds to Milgram's (1967) 6 degrees of separation theory.

In terms of degree distribution of the directed graph G , the indegree distribution has a strong power law characteristic as illustrated in Figure 11. This indicates that most nodes have a low indegree and few nodes have a high indegree.

Chapter 4-Online Social Network Data Extraction and Graph Processing

Most nodes will only be classed by a few friends in the network as a *top friend* but there will be a few nodes that will be classed by many friends in the network as a *top friend*.

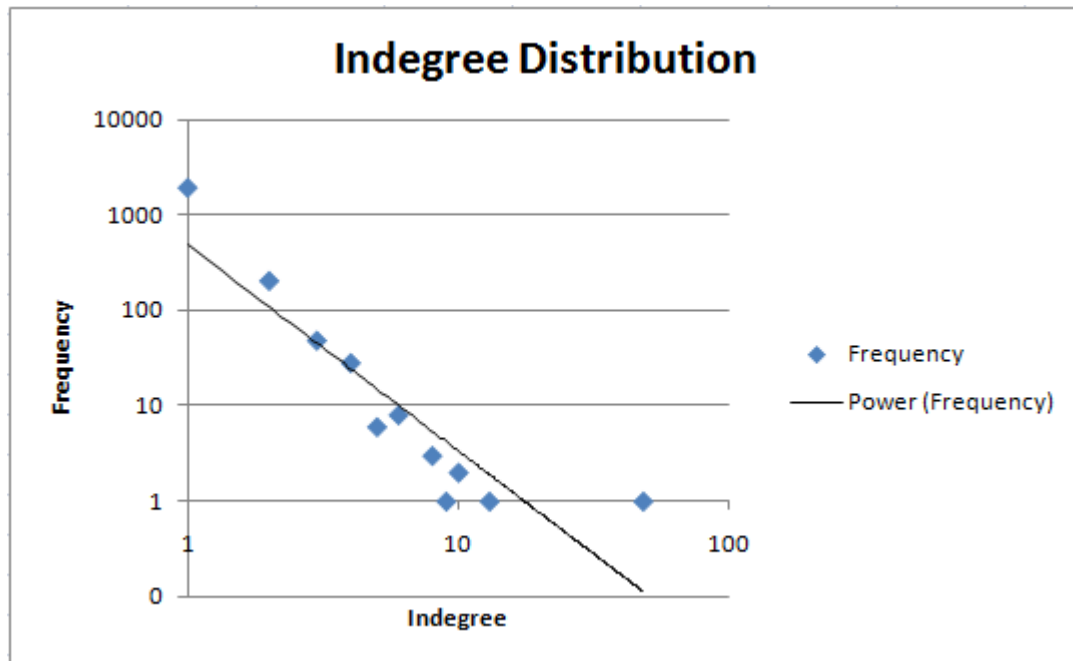


Figure 11-Indegree Distribution for Top Friends Extraction

The degree distribution graphs in Figure 11 and Figure 12 are plotted on a log log scale which means that a power law distribution will be represented by a straight line.

There are many activities in computing which follow a power law distribution (e.g. the visiting of websites or the viewing of social media). Power law distribution focuses more on the smaller values in the scale rather than the large values. The logarithmic scales only accept positive values i.e. 0, therefore nodes that had an indegree or outdegree of 0 were not taken into account.

The graph in Figure 11 uses a log log scale and follows a power law distribution. This is proven by the R^2 value which is 0.8175. The R^2 value denotes the reliability of the trend and is a value between 0 and 1. As the value heads towards 1 the trend is more reliable. Following a power law distribution in

Chapter 4-Online Social Network Data Extraction and Graph Processing

this case means that a lot of nodes will have low indegree values and a few nodes will have high indegree values.

Figure 11 illustrates that there are some nodes that have high indegree values. The highest indegree value is 48 and the average indegree value is 1.250. The node that has an indegree of 48 is the most popular node in the network because 48 other nodes have included this node as a *top friend*.

In comparison, the outdegree distribution which is illustrated in Figure 12 indicates that this distribution does not follow power law and this is shown by the R^2 value which is 0.1805. This may be because the number of *top friends* a node has is down to personal preference. Some nodes choose to have a low number of *top friends* because they know who their closest friends are. Other nodes may not be able to class *top friends* as easily, so they include a large number of *top friends* on their profile.

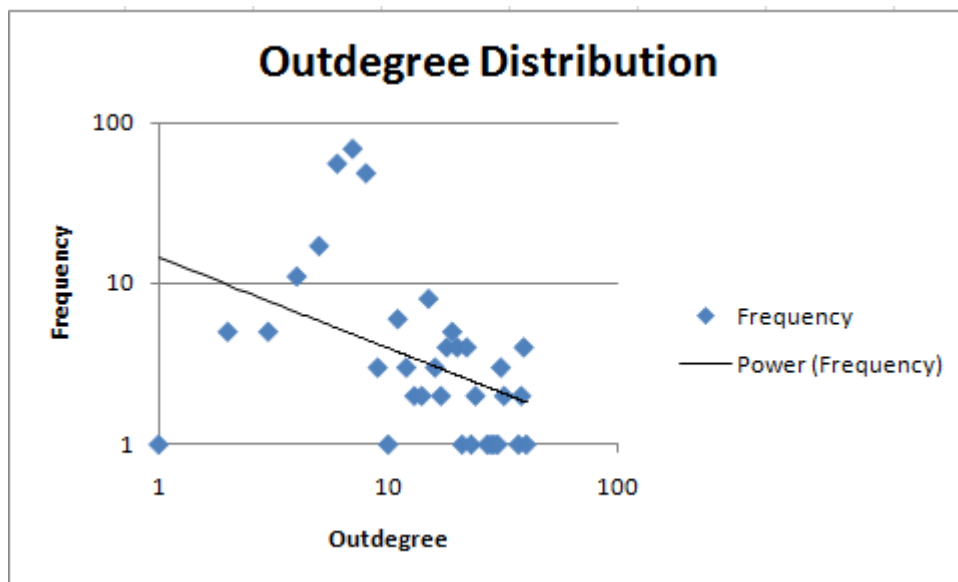


Figure 12-Outdegree Distribution for Top Friends Extraction

The maximum outdegree value is 40 with the average outdegree being 1.250. Also our data extraction approach will have influenced the outdegree value of some nodes because only the *top friends* of 250 nodes were extracted.

Chapter 4-Online Social Network Data Extraction and Graph Processing

In terms of clustering coefficient, the average clustering coefficient for graph G is 0.031 which highlights that this is not a highly clustered network and a low proportion of each node's neighbours are connected to each other. 36 nodes have an individual clustering coefficient of 1.000. These nodes contain a neighbourhood of 2 or 3 indegree nodes but no outdegree nodes. This means that the friends that classed this node as a *top friend* know each other and are connected to each other. This results in a highly connected neighbourhood.

Using social network analysis measures, the node with the highest betweenness centrality value has the highest indegree value of network which is 48 but has an outdegree of 0. This node can act like a broker to the information flow around the network because of its connections with other nodes. All the nodes in graph G have a closeness centrality of 0 because the *top friends* are not connected to each other.

Another measure that NodeXL includes in its graph analysis is PageRank (Brin and Page 1998) PageRank is an algorithm which was developed to help search engine Google rank their web pages in terms of importance. The theory of Page Rank is that the importance of a webpage can be justified by the number of hyperlinks pointing to it from other webpages. The importance of a webpage can be calculated using equation 15

$$PR(A) = (1 - d) + d(PR(T_1)/C(T_1) + \dots + PR(T_n)/C(T_n)) \quad (15)$$

where $PR(A)$ is the PageRank of a page A , $PR(T_i)$ is the PageRank of page T_i , $C(T_1)$ is the number of links going out from page T_1 and d is a damping factor in the range of 0 to 1 but it is normally set to 0.85. The damping factor is based around a random web surfer who is given a webpage at random and starts to

Chapter 4-Online Social Network Data Extraction and Graph Processing

click the links and then gets bored and goes to find another random page. The PageRank is the probability that the random web surfer visits a webpage.

The PageRank score for a webpage is dependent on the PageRank values for each of the webpages p it is linked to, divided by the outgoing links of each p . To get a high PageRank value, there have to be many incoming links from other pages (e.g. a link from webpage $D \rightarrow$ webpage A) would increase the importance of webpage A and therefore increase the PageRank value of A . Also if some of the incoming webpages have high PageRank values themselves, then this can increase the PageRank value of A . Another factor which affects the PageRank value of webpage A is the number of outgoing links of the webpages linked to A . The more outgoing links a webpage has, the less benefit it will offer webpage A and the lower the PageRank value.

With the concept of PageRank analysing incoming and outgoing edges, PageRank can be applied to OSN graphs. In graph G , illustrated in Figure 10, the node with the highest PageRank value of 18.527 has 1 indegree edge and 40 outdegree edges. This node has the highest PageRank score because of the value of the links. What PageRank has illustrated is how the use of indegree and outdegree can be used to measure the importance of in this case webpages. This helps to justify the modeling of an OSN using a directed multigraph and emphasizing the importance of edges whether indegree or outdegree.

4.5-Elements of an Online Social Network Graph that can affect Vulnerability

When analysing OSN graphs, there are many graph characteristics that can be examined as illustrated in section 4.4. Analysing the node as an individual entity in terms of structure is important when discussing vulnerability. This analysis

Chapter 4-Online Social Network Data Extraction and Graph Processing

gives us more information about the state of the node and the immediate neighbourhood. The three main characteristics (Alim et al. 2011b) to explore in the directed multigraph $G=(V, E)$ include the indegree, outdegree and clustering coefficient of a node. The indegree of node n which can signify trustworthiness is the number of edges coming towards node n . The indegree of node n is denoted by i_n . The outdegree of node n is the number of edges going away from node n . The outdegree of node n which can signify sociability is denoted by o_n . Figure 13 shows the subgraph of a node which in this case is denoted as node 14 and illustrates the indegree and outdegree concept. Node 14 has an indegree of 2 and an outdegree of 8.

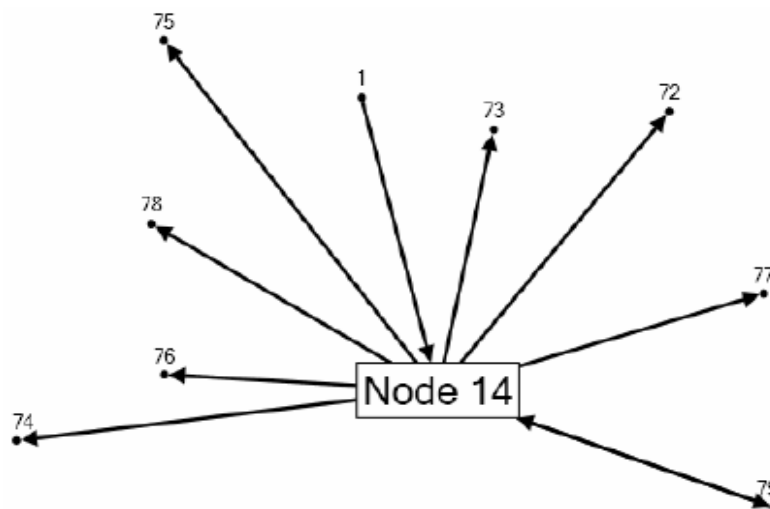


Figure 13-The Concept of Indegree and Outdegree for a node in an OSN

An indegree of node $n(i_n)$ in the case of node 14 specifies that this profile is a friend of someone and is in his/her *top friends* list. The number of indegree edges shows how much other people have an interest in that node. If there are many indegree edges, the node is highly interesting and trustworthy.

In terms of personal details, the fact that node n is classed as a *top friend* means that there is a flow of personal details coming towards it. There is the ability for node n to act like a broker and spread the personal details via its own

Chapter 4-Online Social Network Data Extraction and Graph Processing

top friends. The spreading of the personal details can be dependent on the number of *top friends* that node n has and how public or private the profile of node n and the neighbours are. If the profile is public then the interactions between node n , its *top friends* and all node n 's other friends could be public to all node n 's network. Interactions (e.g. photo tagging and writing profile comments) can leak personal details about node n 's *top friends* as well.

An outdegree (o_n) represents how many friends the node has in his/her *top friends* list. If a node has many outdegree edges this shows that the node has many friends on their profile they can pass information onto. Also the node can make itself vulnerable to attack from its own friends if its profile is very public.

A feature that plays an integral part in assessing the vulnerability of a node is its clustering coefficient. A node with a high clustering coefficient will have a neighbourhood where information will flow easily, due to nodes knowing each other. In terms of vulnerability, a node with a clique where all the nodes in the neighbourhood know each other will have a greater vulnerability value due to the increased possibility that the information can spread further through the network.

Another important factor that can contribute to the vulnerability of the node is the number of neighbours the node has and whether the neighbours choose to display their profiles publically or privately. With multigraphs allowing parallel edges, you have to be careful that the neighbours are not counted twice. This had to be taken into consideration when implementing the vulnerability measure.

4.6-Ethical Issues associated with Extraction

Due to the nature of the personal data presented on OSN profiles, crawling data from publically available OSN profiles in (e.g. MySpace) can raise various

Chapter 4-Online Social Network Data Extraction and Graph Processing

ethical issues due to the public personal details which can be used to identify a human being.

One view of crawling and extracting data from public OSN profiles that is discussed by (Thelwall and Stuart 2006) is that the OSN profile is in the public domain and an invasion of privacy occurs if the data from the OSN profile is used in certain ways. An example is extracting the email addresses from OSN profiles in order to construct a spam list. This type of attack was investigated by Balduzzi et al. (2010).

The other view states that crawling and storing of the OSN profile data breaks a number of ethical criteria and the terms of service of the OSN. Grier et al. (2010) presents a scenario where a researcher wants to investigate the use of access control restrictions in MySpace and so for publically available profiles, the profile data is extracted and stored for research that investigates the presence of publically identifiable data.

In terms of the Common Rule which is a set of medical ethical rules governing human research in the United States, the accessing and storing of personal data is seen as research which involves human subjects. The interpretation of public versus private data, decides whether this research qualifies for an exemption. One side of the case is that the researcher is extracting data that is clearly personal identifiable data, but the data is publically available to anybody and therefore cannot be classed as human subjects research (Grier et al. 2010).The other side of the case is that the personal identifiable data could pose a risk to the profile owner and so consent from the owner may be required. There can be double standards between OSNs and reality, because some OSNs (e.g. MySpace) don't allow profile data of other users to be downloaded, extracted via automation or scraped, but they do allow public profiles of

Chapter 4-Online Social Network Data Extraction and Graph Processing

personal identifiable information to be accessible to even external users. When using publically available data, researchers should be careful not to allow the identities of the profile owners to be discovered .

For our research, only public profile data has been extracted and used to calculate the vulnerability measure and generate an OSN graph. Unauthorized access was never used to gain access to profile data.

4.7-Conclusions

Our data extraction approach which is detailed in this chapter has allowed the personal details and list of *top friends* to be extracted from MySpace OSN profiles in order to be used for OSN graph generation and in chapter 5 for the application of the vulnerability measurement. The challenges involved in the extraction of MySpace profiles was that the profiles have a variety of formats depending on the type of profile and so decisions had to be made on the types of profiles to extract from. In this particular experiment certain profile types i.e. band, musician, comedy and private profiles were ignored.

In terms of vulnerability and the factors that affected it, analysing the indegree, outdegree and the clustering coefficient of node using the generated OSN graph can give an idea about how personal details can be spread around an OSN. A node with a high indegree indicates that this node is popular and there is a stream of information flowing towards it. Depending on the number of *top friends* and whether the node is private or public, the node can make the profiles that have classed it as a *top friend* vulnerable. A node with a high outdegree can be made vulnerable by its own *top friends* especially if the node itself is public. The data extraction of personal data from OSN profiles can raise various ethical issues depending on the interpretation of public available data.

Chapter 4-Online Social Network Data Extraction and Graph Processing

Overall this experiment formed a good basis for the vulnerability measure to be applied.

CHAPTER 5: EXPERIMENTAL WORK ASSOCIATED WITH DATA EXTRACTION

The aim of this chapter is to extend the work presented in the previous chapter by detailing and discussing the second experiment which involved the extraction of personal details and a list of *all friends* from a MySpace profile as well the application of the vulnerability measure application. The experimental work is detailed in the AbdulRahman et al. (2010) paper.

This is in contrast to the first experiment (Alim et al. 2009) which involved just extracting the *top friends* from a profile. The data extracted is used for an OSN graph analysis and forms the basis for a case study based approach into the vulnerability of profiles and a brief experiment into validation of the vulnerability measure using case studies. Also the 'degrees of separation issue' is investigated via the use of a case study to see how the vulnerability of a profile links in with the concept of levels in an OSN network.

5.1-Data Extraction Findings

This experiment involved running our data extraction approach (explained in the chapter 4) 250 times. The data extraction approach was implemented to extract *all friends* from an OSN profile rather than just *top friends*. Relevant attributes were extracted from 163 profiles because the rest were musicians or bands. Out of 163 profiles, 96 of them were private so their list of *all friends* could not be extracted.

For this experiment private profiles were also extracted from as well because private profiles can still contribute towards their vulnerability. Apart from extraction findings from the first experiment i.e. the various profile structures for this experiment, some of the users that have deleted their accounts still have their profiles present. This makes extraction harder and technically MySpace

should have deleted the profiles. Also in order to view the friends of some profiles you have to be a member of MySpace. This is a new technique which OSN members are using to protect their privacy. The various profile structures in MySpace is a vast contrast to Facebook where there is one standard profile structure. The problem with Facebook is that you have to be a Facebook account member to extract from profiles whereas with MySpace you can view and extract from full profiles that are publically available without being a MySpace account member.

5.2-Online Social Network Graph Findings

An OSN graph G was generated from the repository data. Graph G is a directed multigraph $G=(V, E)$ where $|V|=10,196$ and $|E|=17,223$. The graph just consists of one connected component in which the maximum number of nodes is 10,196 and the maximum number of edges is 17,223. The diameter of graph G is 5 which is smaller than the diameter of the OSN graph generated in the first experiment which was 10. A smaller diameter illustrates that the network is more connected. The average path length is 3 and that highlights that information flows more freely due to the short path lengths between the nodes.

The average clustering coefficient for graph G is 0.035 which is quite low and highlights that most of the neighbourhoods of the nodes are not well connected together. Any small sample may or may not be characteristic of the OSN overall.

In a small world network, the clustering coefficient value is normally high. The average path length is 3 which is small and shows one of the characteristics of a small world network. For the degree distribution, since the graph is a directed graph the indegree and outdegree distributions have to be analysed separately. The indegree distribution is heading towards a power law characteristic as

Chapter 5-Experimental Work Associated With Data Extraction

illustrated in Figure 14. This shows that most nodes have a lower indegree value and fewer nodes have a higher indegree value.

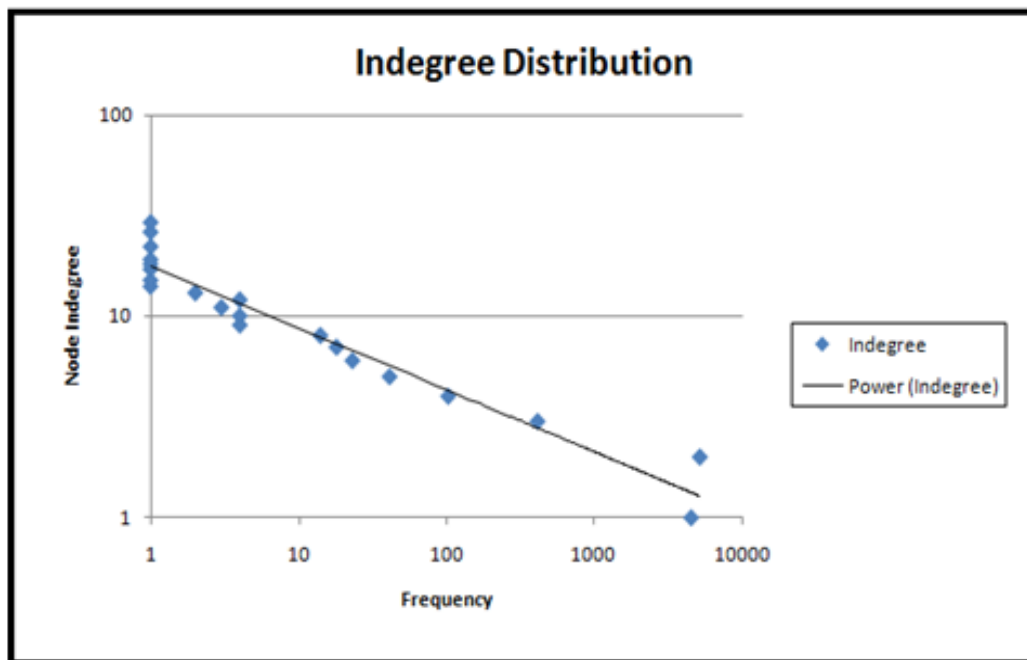


Figure 14-Indegree Distribution for All Friends Extraction

Most nodes are contained in someone's friend list but the surprising thing is that the outdegree distribution does not have a power law characteristic as illustrated in Figure 15. Some of the nodes in this network are private and we were not able to gain access to their friends' lists so this is probably a factor when calculating degree distribution. In saying that, if a private profile's friends had public profiles then we could extract their friends list and build up the friends list of the private profile.

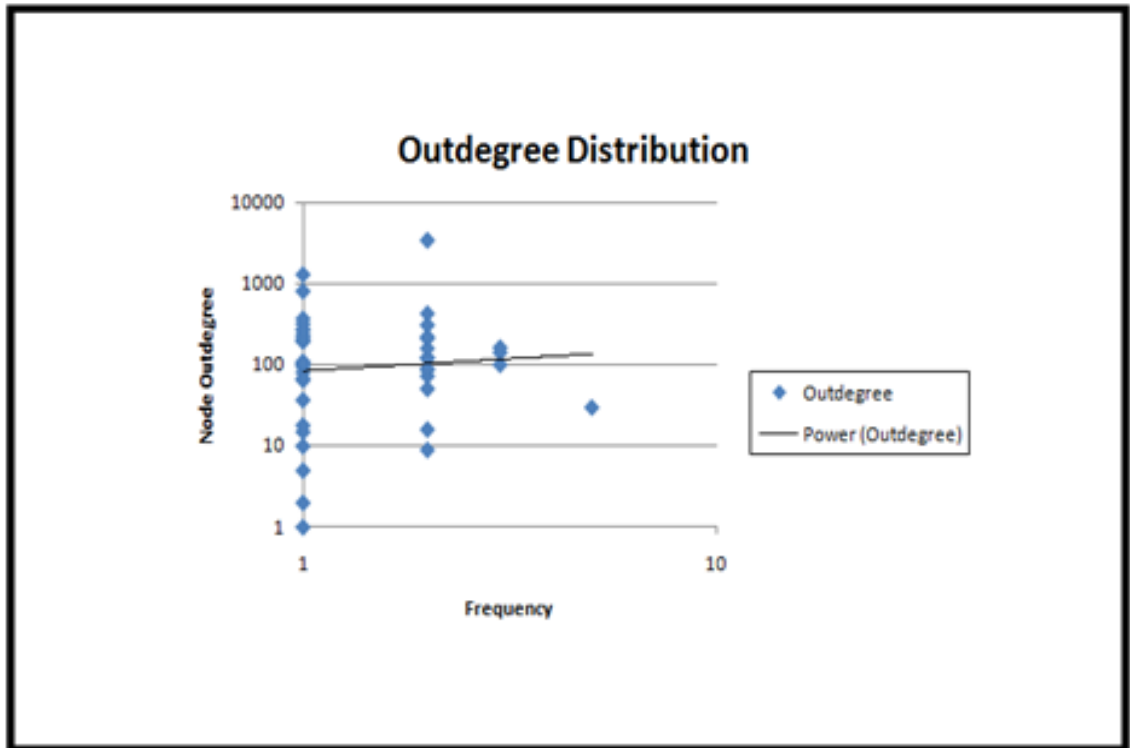


Figure 15-Outdegree Distribution for All Friends Extraction

5.3-Case studies and Validation

The vulnerability measure which is detailed in chapter 3 is applied using equations 11-13 to the repository data in order to help validate the measure. As far as we know there is no benchmark data to compare the results of the vulnerability measure so a case study based approach was adopted. In Table 3, for the validation of the measure, the characteristics of the node (e.g. the number of vulnerable attributes displayed) were analysed for three case studies. To give an overall picture about the node, the graph structure (e.g. indegree and outdegree of the node) was also included in the validation.

With using a directed multigraph to model the OSN, the indegree and outdegree values in Table 3 may have counted the neighbours twice especially if the relationship between the node and its neighbours is bidirectional. That is why the sum of the number of private and public neighbours will not match the sum of the indegree and outdegree.

Chapter 5-Experimental Work Associated With Data Extraction

Table 3-Case Studies for Unnormalised Vulnerability Measure

Cases	Profile Type	No. of Vulnerable Attributes	V_I	Metric Components				Graph Structure			Justification
				Public Neighbours	Private Neighbours	V_R	V_A	In-degree Value	Out-degree Value	Clustering Coefficient	
Highest Absolute Vulnerability	Public	6 out of the 6	1	85	78	145.87	145.87	29	230	0.015	This node is very vulnerable because of the size of its neighbourhood and the number of neighbours who display all their vulnerable attributes.
Medium Absolute Vulnerability	Public	6 out of the 6	1	7	2	8.81	8.81	3	65	0.005	This node is moderately vulnerable because of the number of neighbours and the fact that the node is not in very many friends' lists.
Lowest Absolute Vulnerability	Private	5 out of the 6	0.905	1	-	1	1	0	1	0.000	This node has a low vulnerability because of the lack of neighbours and it is not displayed in any ones friends' lists.

For the absolute vulnerability (V_A) calculation the MAX operator was used instead of the product operator shown in equation 13. The MAX operator selects the maximum value out of the individual vulnerability (V_I) and the relative vulnerability (V_R). The cases in Table 3 highlight that there are various factors which can influence the absolute vulnerability (V_A) of a node and these are detailed below:

1. **The number of neighbours and the neighbours' profile type:** the highest absolute vulnerability case highlights how the V_R (vulnerability value of the neighbours) significantly increases if there are a large number of neighbours. The problem with MySpace is that even private profiles will still display some personal details even though the friends list or interactions can't be seen. Therefore private profiles can still contribute towards the vulnerability of a node. In the highest absolute vulnerability case, the main node has a high V_A value caused by the neighbours displaying all their vulnerable attributes, they are indicating

that they may not take privacy as seriously and by displaying these attributes they are opening themselves up to social engineering attacks.

2. **Absolute vulnerability operator:** The effects of using the MAX operator are evident by the lowest absolute vulnerability case in Table 3. Even though the main node is private and the neighbour has got the highest individual vulnerability (V_i) of 1, the absolute vulnerability is 1. The MAX operator highlights the highest vulnerability component. In this case the neighbour makes the main node (the node being analysed for vulnerability) vulnerable and that is why the absolute vulnerability of the main node is 1. More research is done in chapter 6 and chapter 8 into various operators and how they impact on the vulnerability value.

In terms of justification, the node with the highest absolute vulnerability has a large number of neighbours which contributes towards a high V_A value. Also this node is contained in quite a few friends' lists so this spreads the information further. The node with a moderate absolute vulnerability has fewer neighbours than the node with the highest absolute vulnerability hence the lower absolute vulnerability value. The node with the lowest absolute vulnerability has its profile not displayed in the neighbour's friend list so the information cannot flow far in the network. Also the node is private so its friends list cannot be viewed by browsing the profile. The OSN graph is needed to analyse public profiles which may be friends with the node. Public profiles display a list of who they are friends with.

There are several factors which can influence the V_A value of the node, which are not taken into account but can form the basis for future research. The factors are the strength of relationship between two nodes and the amount of interaction that takes place between them. If two nodes have a strong online

Chapter 5-Experimental Work Associated With Data Extraction

relationship, they may divulge their personal details via their interactions (e.g. profile comments). The amount of interaction can tell a lot about the strength of relationship. A high amount of interaction between two nodes may indicate a close online relationship between them.

5.4-Levels in Online Social Networks

Carrying out an experiment investigating levels of friends on a larger dataset, would allow us to observe how the factors mentioned in Section 5.3 link in with the levels of friends and their vulnerability values. The aim of this experiment is to investigate how the vulnerability of a node which represents an OSN profile is affected by levels in its social network i.e. a node's neighbours and their sub networks (friend of a friend of the node). In reality OSN sites (e.g. Facebook) have in built user controls so the user can dictate (e.g. how much of the profile a friend of a friend may see) and this concept is explored in chapter 8.

To briefly explore the levels of friends, one node, its *top friends* and their sub networks were selected as a case from the Caverlee and Webb (2008) dataset. Caverlee and Webb (2008) used Breadth First Search algorithm to travel across the network and extract the *top friends* and personal details from the profiles in 2006.

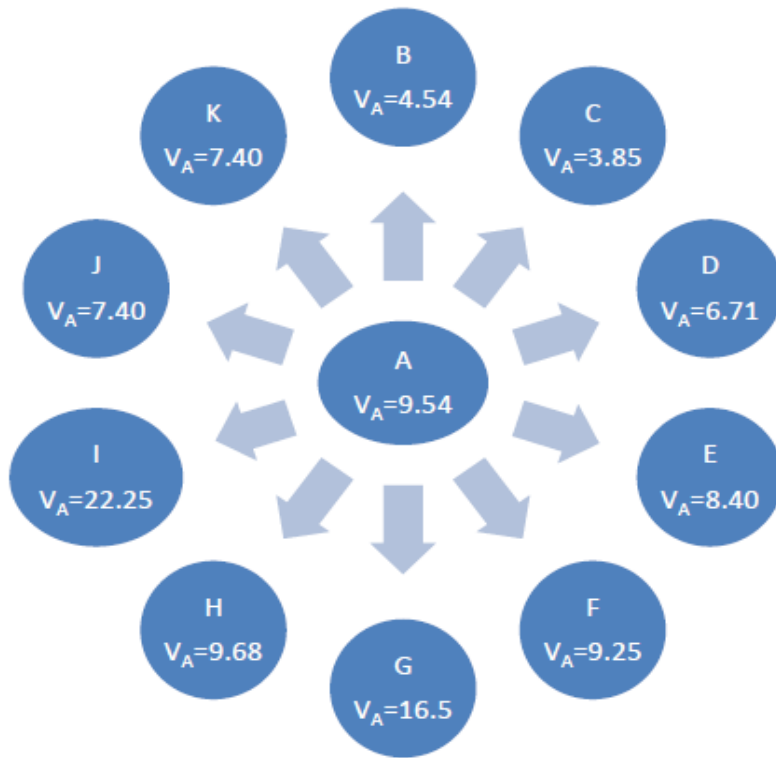


Figure 16-Levels of Friends and Vulnerability in an OSN

Figure 16 illustrates how the V_A (absolute vulnerability) of each of the top friends varies with the V_A value of the main node which in Figure 16 is node A. The V_A values in Figure 16 are not normalized between 0 and 1 at this stage but the issue of normalization is discussed at the end of the chapter. Node A, which is the main node, has 10 *top friends* that are labelled B to K. Each one of these *top friends* has its own *top friends* and this produces the levels aspect of the OSN. The V_A value is the absolute vulnerability of the node which takes into account the vulnerability of the node itself and its neighbours. The measure to calculate the V_A value uses the MAX operator. For example the V_A value of node B will take into account the V_I (individual vulnerability of B) and the V_R (relative vulnerability of B).

The results from Figure 16 show that some of node A's *top friends* have higher V_A values than node A itself. This is due to the node A having a lower number of *top friends* than some of the other nodes and the willingness or not for the top

Chapter 5-Experimental Work Associated With Data Extraction

friends of node *A* and their *top friends* to display their personal details especially the vulnerable attributes readily.

This illustrates that the number of neighbours and the amount they disclose is a factor in vulnerability. A lower number of *top friends* may indicate that the personal details flow will not cover as much of the network compared to other nodes especially where the *top friends* are all public and self disclose vulnerable attributes readily.

Node *A* has 8 *top friends* and so node *A*'s personal details will be seen by these *top friends*. Excluding the *top friends* who have private profiles, any interactions (e.g. photo comments and profile comments made from Node *A* to any of the 6 *top friends* e.g. node *B*), will be seen by the *top friends*/friends or even external users of node *B*. This is because the *top friends* of node *B* can see *B*'s profile in MySpace. These interactions will be present in the news feed, profile wall or photos section. At present, it is now possible in Facebook for *top friends* friends of node *A*, to see the first line of any profile comments made from Node *A* to any of its *top friends*/friends. This can increase the vulnerability of node *A* or its top friend/friend if those comments contain any type of personal information which can be used in social engineering attacks. In terms of Figure 16, Nodes *G* and *H* are private so the interactions from their *top friends* to them can't be seen by anyone who is not in node *G* or *H* *top friends*/friends list.

With an external user, the fact that node *A* is public and presents the *top friends* list on the profile would make *G* and *H* vulnerable because the user would then know that (e.g. node *A* is *top friend*). Also the external user can look at node *A*'s interactions which include profile comments to build up the identity of nodes *G* and *H*. For an attacker, what will make it harder is that (e.g. node *G* does not

Chapter 5-Experimental Work Associated With Data Extraction

display their *name* on the profile) so the neighbourhood of node *G* will have to be built up and analysed in order to extract an identity.

Node *I* in comparison is a public profile, which has the highest V_A values and has 23 *top friends*. This node has the highest V_A value because of the potential of its neighbours to spread details around the network because they display their vulnerable attributes so readily.

Analysis suggests that node *I* may be the biggest threat to node *A* because any of node *A*'s personal details that appears on node *I*'s profile via interactions will be seen by node *I*'s neighbourhood and therefore increases the possibility of spreading the personal details through the neighbourhood. Also *top friend* friendship may lead to frequent public interactions on the profile so this increases the chances of personal details being contained in those interactions. It is not just interactions that the neighbourhood can see. One of the current issues in social networking is what an external user who is based outside a node's immediate network can see. This is illustrated by a scenario below involving Facebook profiles.

In Facebook for example node *X* is friends with node *Y* and node *Z* is friends with node *Y*, but node *X* and *Z* are not friends. One day node *X* is looking through node *Y*'s friends list and clicks on profile link for node *Z*. The profile link consists of the *name* of node *Z* and a *profile picture*. These two details alone have already contributed towards the vulnerability of node *Z* because the details can be used in social engineering attacks. Once the profile link is clicked, even though node *X* can't see the whole profile, node *X* can find out about node *Z* in terms of *gender*, employment history, education details, marriage details and list of friends through its friendship with node *Y*. Now, node *X* is a threat to making node *Z* vulnerable in terms of losing control of its personal details. This scenario

Chapter 5-Experimental Work Associated With Data Extraction

highlights that a user has to be careful in what personal information is displayed and how the privacy controls of the profile are set. In Facebook there are privacy controls that only allow friends of the profile to see the profile contents.

In terms of the rate at which personal details will spread, factors that can affect it include the connections between the neighbours, how the neighbours display their personal details and how talkative the neighbours are in terms of disclosing personal details.

A talkative neighbour can be defined as a node which interacts a lot with other nodes through the use of profile comments, emails and wall postings on OSNs. In terms of graph structure of the interaction network, a talkative neighbour may have a high outdegree and indegree.

A high outdegree indicates that the talkative neighbour has the potential to interact with a lot of its friends. Also the interactions that the neighbours of the talkative neighbour have with the '*friend of friend*' of the talkative neighbour may help to propagate the personal details of the talkative neighbour. A high indegree indicates there is potential for a lot of neighbours to write comments on the talkative neighbour's profile wall.

A relationship with a high outdegree node will allow for profile details to be spread to many people. A high indegree node indicates that there is lots of interest in the node. If interactions between the talkative neighbour and its friends are all displayed on the profile and the profile is public to outside users and accessible, the personal details of the friends will spread quite widely and into networks unknown to the profile owner. This will allow more outer levels of the social network to potentially view the personal details.

Chapter 5-Experimental Work Associated With Data Extraction

Analysing the graphical structure of the network is very important when accessing vulnerability especially when the two nodes have the same vulnerability value. In Figure 16 this is shown by nodes *J* and *K* which have the same V_A value for a number of reasons. Both nodes have the same number of neighbours which is 8 but the structure of the neighborhood is different. Node *J* has an indegree of 7 and an outdegree of 1 where as node *K* has an indegree of 8 and an outdegree of 0. The structure of both nodes indicates that there is a lot of interest in both nodes which is shown by the indegree value but these nodes are more wary about selecting who their *top friends* are.

Both nodes *J* and *K* have 63% of their neighbourhoods containing nodes that have an individual vulnerability of 1 which shows that these nodes are willing to make themselves vulnerable by displaying their personal details.

In conclusion this brief investigation into the levels of friends and vulnerability has highlighted that the node's neighbours actions i.e. what vulnerable attributes they decide to display, impacts on the vulnerability of the node. If the neighbours of (e.g. node *C*) display their profiles very publicly, then other profiles which are in other levels (e.g. friend of one of node *C* neighbours) can view the neighbour's profile and find about about node *C*.

Also if the interactions of the neighbour and node *C* are displayed on the neighbour's profile and personal details of node *C* are leaked then this will be used when building up a profile of node *C*. If a node's neighbourhood contains talkative neighbours then this will increase the chances of allowing the personal details to cover more of the network. A talkative neighbour will be a node that has many friends who they interact with. Most of this interaction may be public and presented using profile comments therefore increasing the

vulnerability of a node connected to a talkative neighbour or even the talkative neighbour itself.

5.5-Improvements

The results from the experiments done in this section highlighted areas of the vulnerability measure that need to be improved. Some of the graph structures associated with the spreading of the personal details needs to be incorporated into the vulnerability measure, ideally the individual vulnerability measurement. The graph structures include the clustering coefficient and the number of friends. The clustering coefficient of a node will indicate how easily or not the personal details will flow. The number of friends a node has will highlight the depth and breadth in which the personal details will flow in the OSN. The vulnerability measure has to be applied to a larger OSN network with many nodes. This will allow for a wider variety of cases to be analysed. One major issue in regards to the vulnerability measure is the normalization of the V_R and V_A values.

Even though Min Max normalization which is illustrated in equation 16 can be used for normalisation, the maximum value is never set because an OSN is a dynamic object where profile details and list of friends change all the time. As a consequence, the vulnerability values for the node will change over time.

$$V_R' = \frac{v - \min_A}{\max_A - \min_A} (\text{new } \max_A - \text{new } \min_A) + \text{new } \min_A \quad (16)$$

where v is the value to be normalised, \min_A and \max_A are the minimum and maximum V_R values of the dataset of nodes. The new \max_A and new \min_A represent the maximum and minimum values of the scale the values are to be normalized to. In this case the $\text{new } \max_A = 1$ and $\text{new } \min_A = 0$.

Chapter 5-Experimental Work Associated With Data Extraction

By normalising the V_R and V_A values it will allow for relative and absolute vulnerability values for the nodes to be more comparable as well as emphasise that the vulnerability measure is based on a probabilistic approach. Also an in-depth validation will allow us to explore whether friends of the profile owner do leak personal details about the profile owner throughout the network.

5.6-Conclusions

The first experiment highlighted that extracting *all friends* from MySpace profiles can bring difficulties. The main one being the profile structure. Profile structure can change instantly depending on what the user wants to present or what the developer wants to improve in terms of site functionality.

The application of the vulnerability measure and the graph have illustrated that when both are applied together a lot of information about the node contents and the structure can be derived. The vulnerability of a node depends on the node contents as well as the environment of the node which can be analysed by the use of a graph. Factors that affect vulnerability include the number of neighbours, the clustering coefficient of the node as well as the number of public and private profiled neighbours and the operator used in the calculation of the absolute vulnerability. Private profiles in MySpace still display vulnerable attributes and therefore are taken into account when working out vulnerability.

The second investigation into the levels of friends in an OSN and vulnerability highlighted that the node's neighbours actions i.e. what vulnerable attributes they decide to display can have a significant impact. From the interaction on the neighbours profiles (e.g. profile comments), the other levels of the OSN (e.g. a friend of a neighbour) can infer details about the node by examining the profile comments.

Chapter 5-Experimental Work Associated With Data Extraction

Overall to improve the vulnerability measure, graph characteristics i.e. the number of friends and the clustering coefficient has to be incorporated into the measure as well as normalising the V_R and V_A values. Also an indepth validation of the measure and the especially the concept of vulnerability has to take place.

CHAPTER 6: MODELLING OPERATORS FOR INDIVIDUAL VULNERABILITY

The aim of this chapter is to address the issue of normalisation of the vulnerability measure as well as carrying out experimental work, to explore the effect of modeling the individual vulnerability of a profile using different mathematical operators. The experimental work is tested on an established OSN dataset which is Caverlee and Webb (2008). This is in order to model the profile owners various attitudes towards privacy. The effect of the different mathematical operators to model the individual vulnerability will impact on the relative and absolute vulnerability values of the profiles. Normalisation of the vulnerability measure will focus on normalising the relative vulnerability, to a value between 0 and 1.

6.1-Improved Individual Vulnerability Calculation and Meaning

The neighbourhood of a profile (the profile's friends) plays a big part in the theory of vulnerability which is detailed in this thesis. In the theory, a profile with a high V_R value increases the chances that one or more neighbourhood profiles will disclose personal details about the main profile (the profile at the center of the neighbourhood) via interactions (e.g. writing profile comments or tagging photos). The experimental work which aims to validate the vulnerability theory is detailed in chapter 8.

To reflect the importance of the neighbourhood in spreading the personal details of the profile, the neighbourhood features: *the total number of friends* and *clustering coefficient* of the profile which is illustrated in equation 1 were converted into attributes and added to the list of existing attributes to analyse for each main profile and its corresponding neighbourhoods.

Chapter 6- Modeling Operators for Individual Vulnerability

In terms of the attributes, *number of friends* and *clustering coefficient*, a weight was allocated if the profiles met certain criteria. The criteria were if the profile had 150 or fewer friends or had a *clustering coefficient* greater than 0.5.

Having 150 or fewer friends increases the chances of the personal details of the profile spreading across the network through interaction between a profile and its friends that makes up the neighbourhood. This value originates from Dunbar's (1992) theory: 150 is the maximum number of humans a person can have a stable and interactive relationship with.

A profile which has a *clustering coefficient* greater than 0.5 is allocated a weight because more of the friends which make up the neighbourhood are connected to each other and this may increase the spread of personal details. The *clustering coefficient* of a profile does not focus on the number of friends a profile has but how well connected the friends are to one another.

The weights that are allocated for the two features are calculated using the relative frequency approach (e.g. the number of profiles that have *150 or less friends* and the number of profiles that have a *clustering coefficient* of 0.5 or above) in regards to a dataset.

Gundecha (2011) validates the thinking behind the vulnerability theory by highlighting that a profile user can have a breach of privacy and security if the user's friends abuse their trust and have poor privacy and security settings themselves.

An improved definition of a vulnerable node (Alim et al. 2011) which is stated below, takes into consideration the issue of the spread of personal details via interactions. This is in comparison with the initial definition in section 3.2.

Chapter 6- Modeling Operators for Individual Vulnerability

An improved definition of a vulnerable node (Alim et al. 2011) is a node that contains attributes and neighbourhood features that breach privacy and provide grounds for a social engineering attack and the opportunity for the attribute values to spread through the network. For such a node a highly connected neighbourhood in which the neighbours display the attributes readily may increase the risk of vulnerability.

6.2-Normalisation

Normalisation is important because it allows for the vulnerability of profiles to be compared to one another. An example being that if you wanted to compare the relative vulnerability of two profiles, it is easier to see the difference between the relative vulnerability values, if the values are in the same scale. In this case the scale is [0,1]. Also with values that are between 0 and 1, probabilistic approaches can be used.

Min Max normalization is not an appropriate method to use for normalisation because the OSN is dynamic and can change over time. Therefore the maximum value for the relative vulnerability can never be attained and consequently the vulnerability measure can't be normalised.

In order to make the absolute vulnerability a value between 0 and 1, the relative vulnerability had to be normalised first to be a value between 0 and 1. To achieve this, instead of calculating the relative vulnerability using a summation of the individual vulnerabilities of a profile's neighbours as illustrated in equation 12, the geometric mean and the arithmetical mean of the profile's neighbours' individual vulnerability values can be applied instead. Equation 17 shows the calculation for the geometric mean of the profile's neighbours of profile i

$$V_{R_i} = \sqrt[n]{\prod_{\substack{j=1 \\ j \neq i}}^n V_{I_j}} \quad (17)$$

where n is the number of the profile neighbours and V_{I_j} is the individual vulnerability of the neighbour j . For simplicity V_{R_i} denotes the relative vulnerability of profile i where $i = 1, \dots, n$ and n is the number of profiles in the network. The reason that j is not equal to i is because a profile cannot be neighbours with itself. The relative vulnerability (V_R) has the condition $V_R \in \{V_{R1}, V_{R2}, \dots, V_{Rn} \mid V_R \in [0,1]$ where n is the number of nodes in the network

The arithmetical mean of the profile neighbours of node i which is calculated using Equation 18 will also produce a value between 0 and 1 for the relative vulnerability

$$V_{R_i} = \frac{1}{n} \sum_{\substack{j=1 \\ j \neq i}}^n V_{I_j} \quad (18)$$

where n is the number of the profile neighbours and V_{I_j} is the individual vulnerability of the neighbour j . For simplicity V_{R_i} denotes the relative vulnerability of profile i where $i = 1, \dots, n$ and n is the number of nodes in the network. Chapter 7 will detail the formal background of the vulnerability measure which includes the effect of the geometric and arithmetical mean on the relative vulnerability and how this can affect the absolute vulnerability of a profile.

6.3-Modelling Criteria

Mathematical functions were used in the modeling of the individual vulnerability of a profile. The vulnerability measure was based on the total weight of the

Chapter 6- Modeling Operators for Individual Vulnerability

profile. In the modeling process, this is referred to as the variable x : the total weight of the profile is the summation of the weights of the attributes which are present in the profile and this is illustrated in equation 11. The aim of this experiment was to improve the calculation of individual vulnerability to take into consideration the type of network user (e.g. child, adolescent, adult) and what sort of network they belong to (e.g. a network consisting of OSN profiles of children). The types of users and their behavior towards privacy are discussed in section 2.6.

Therefore we modeled the individual vulnerability of the profile with a function applied to the total weight of the profile which is represented by x . Individual vulnerability can be described in terms of information disclosure. A high individual vulnerability value indicates a high amount of information disclosure which can increase the likelihood of social engineering attacks especially if the profile is very public. When selecting the types of functions to model with, the following initial criteria were applied:

- C1. Function $f: x \rightarrow y$ is a bijective mapping $f: [0, 1] \rightarrow [0, 1]$, where x is the total weight of the profile and y is the individual vulnerability of the profile. Function f is bijective because for every profile, the total weight of the profile is mapped with exactly one unique individual vulnerability value. Also for every individual vulnerability value of a profile, there is a unique total weight of the profile.
- C2. For $\forall x_1, x_2, x_1 \leq x_2 \Rightarrow f(x_1) \leq f(x_2)$. This implies that the function is monotonically increasing which states that as the total weight of the profile x increases, then the amount of disclosure $y=f(x)$ increases as well and therefore makes the profile with weight x_1 at least as vulnerable to attack as a profile with the weight x_2 .

Chapter 6- Modeling Operators for Individual Vulnerability

- C3. $f(1) \leq 1$: when the total weight of the profile $x = 1$ then the profile disclosure $f = f(x)$ tends towards 1. $f(x) = 1$ is the maximum amount of disclosure possible for an individual profile which means that the profile owner displays all the attributes that contribute towards vulnerability on the profile and has maximum values for the structural factors (e.g. clustering coefficient and number of total profile friends).
- C4. $f(0) \geq 0$: therefore $f(x)$ may or may not go through the point $(0, 0)$ and this can influence the disclosure value when the total weight of the profile is 0. A profile with a total weight of 0 will not display any attributes that contribute towards vulnerability and also have no friends, which may be an ideal case
- C5. Function f is a continuous function. Continuity for (e.g. point a) for function f implies that there is no drastic change between the values of function f when it is near a in comparison to the values when it is at a . This means that as x approaches a , then the value of $f(x)$ has to be approaching $f(a)$ and this can be represented by the notation $\lim_{x \rightarrow a} f(x) = f(a)$. There are three criteria which have to be satisfied in order for function f to be classed as continuous, a has to be in the domain of f $[0,1]$. Also $\lim_{x \rightarrow a} f(x)$ has to exist and $\lim_{x \rightarrow a} f(x) = f(a) \in [0,1]$. A continuous function fits the theory that as a profile displays more attributes or features that contribute towards vulnerability, the total weight of the profile increases and the individual vulnerability consequently increases.
- C6. Function $f(x)$ has to be non negative therefore $f(x) \geq 0$. Consequently the domain of function f is $[0,1]$. The total weight of a profile is a non negative number because in the case of this vulnerability

Chapter 6- Modeling Operators for Individual Vulnerability

measure, displaying attributes on a profile does not reduce the likelihood of contributing towards the vulnerability of a profile.

The domain of function f will enable probabilistic approaches to be used to assess the privacy risks of profiles. Also the normalisation of the vulnerability values will allow comparisons to be made with profiles in other OSNs.

6.4-Types of Functions and their Behaviours

Parameters i.e. network characteristics for example the number of profiles in the network who have friends that have public profiles or the collective level of interaction, can be incorporated into function f as a β value (e.g. $\beta f(x)$). The β value can represent a manner of network characteristics (more examples include the average number of friends in the network and its surrounding levels, the amount of communication between age bands and the age range of the network).

β has to be a value between 0 and 1 so the values have to be normalised. This implies that function f in conjunction with β has to be a value between 0 and 1. Also the limit of function f with β has to tend towards 1 or hit 1 exactly. At present the research is not concerned with the value of β but further research will be required to assign values to β based on the statistical analysis of the network.

For the modeling of the individual vulnerability of a profile we selected a limited number of function models as illustrated in Figure.17 which met the modelling criteria C1-C6, some of the functions having a generalised form by the introduction of a parameter.

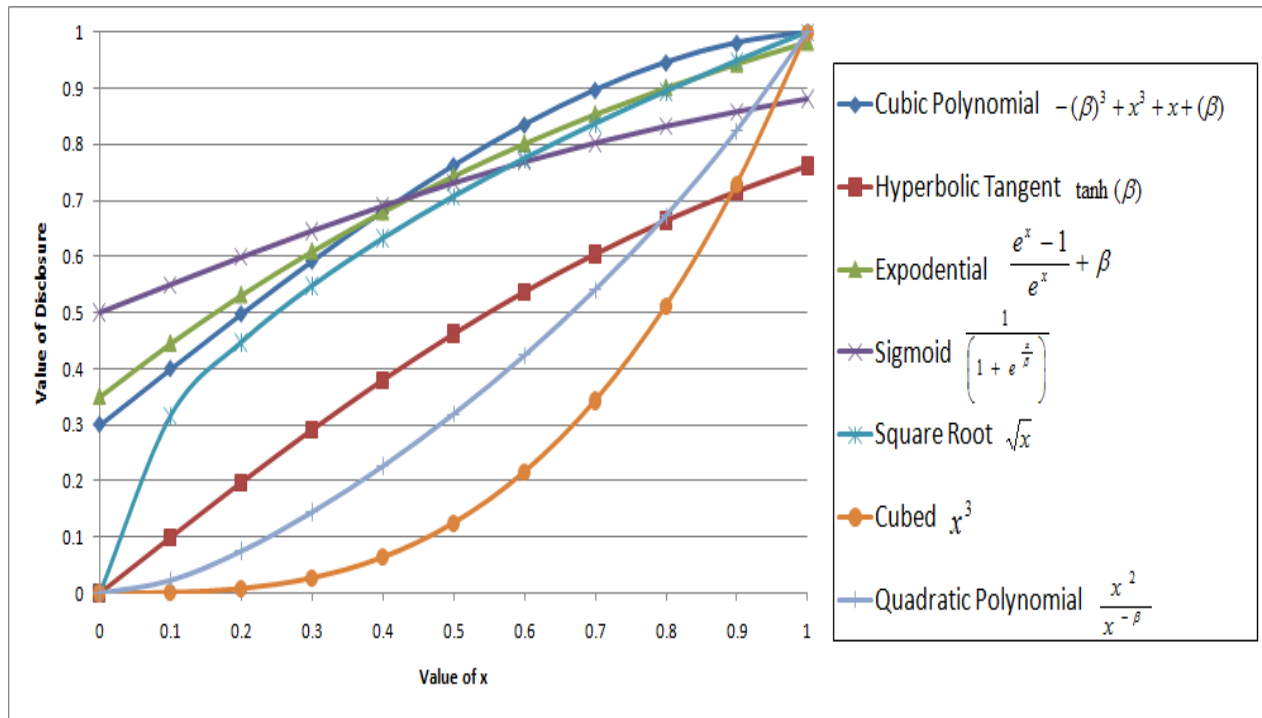


Figure 17-Graph of Mathematical Function Behaviours

These functions were chosen to see how the functions behaved in accordance to the modelling criteria. Some of the functions had β parameter values already specified to investigate the effects of the parameter especially when the disclosure value hit 1 or was near 1. The cubic polynomial function had a β value of 0.3, the exponential function β value was 0.35, the sigmoid had a β value of 0.5 and the quadratic polynomial had a β value of 0.9. The β values of the functions are different, in order to investigate what β values are required so the functions tends to or hits 1.

All of the functions fitted some of the modelling criteria specified but the quadratic polynomial function fitted the modeling criteria strictly. Three functions were chosen to apply and validate against the real life cases from the Caverlee and Webb (2008) dataset and these functions included:

$$x^{\left(\frac{1}{\beta}\right)} \tag{19}$$

$$x^{(3 + \beta)} \tag{20}$$

$$\tanh(x*(1+\beta)) \quad (21)$$

The functions were chosen because they would provide a variety of different case results to analyse and they fitted the modelling criteria with the β value incorporated into the function. The functions that were not chosen either started off too slow and only gained momentum until the very end (e.g. cubed) or started off at a high rate of disclosure and did not increase very far (e.g. sigmoid). Some of the functions when incorporated with the addition of a provisional β parameter gave results that were outside the 0-1 range.

6.5-Function Case Studies

Three profiles from the Caverlee and Webb (2008) dataset with varying features and neighbourhood environments were selected as case studies in order to examine how well the different functions modeled the various cases. Each case represents a different type of user (e.g. adolescent, young adult and older adult) and so this will allow an investigation into whether the functions can model reality.

Table 4 presents the details of the case studies in regards to vulnerability. The number of attributes that contribute towards vulnerability, total number of friends and clustering coefficient are analysed for each profile in order to calculate the total weight of the profile. Since a directed multigraph was used to model the OSN network, the number of immediate neighbours of a profile is the *top friends* of the profile and the friends that specify the profile as a *top friend*. The clustering coefficient of the case study profiles is low because *top friends* of a profile may not know each other. The neighbours' behaviour is very important when calculating the overall vulnerability of the profile because of the increased chance that they may leak the profile's personal details via interactions which can include profile comments or photo tagging. The vulnerability measure in its

Chapter 6- Modeling Operators for Individual Vulnerability

present form does not directly incorporate the interactions aspect of the OSN in the calculation but this will be incorporated into the calculation of the relative vulnerability in the future.

Table 4-Case Study Details for Various Users and their Profile Characteristics

Cases	Individual Profile Environment			Total Weight of the Profile	Profile's Neighbourhood Environment		Explanation
	No. of vulnerable attributes	Total number of friends quoted on profile	Clustering Coefficient		No of immediate neighbours	Neighbours' Behaviour	
Young Adult User	6	47	0.157	0.9982	1	The profile's neighbours display all the vulnerable attributes and the number of friends is a factor but the potential clustering coefficient is not.	Both the profile and its neighbour are very public in terms of displaying their attributes. Also the number of total friends is a factor that has to be taken into consideration. The number of total friends is lower than 150 for both the profile and its neighbour.
Adult User	4	0	0.075	0.6433	18	5 neighbours of the profile have an extremely high V_i value and the rest of the neighbours have slightly lower vulnerability values.	The profile has not displayed the some attributes as well as the total number of friends on the profile. 5 neighbours of the profile are very public and this can increase the overall vulnerability of the profile but the other neighbours have slightly lower values but are still considered vulnerable
Adolescent User	6	67	0.050	0.9982	4	2 neighbours of the profile have high vulnerabilities and the rest are more private and have vulnerability values that are significantly lower.	The profile is public but the neighbours of the profile are more private about what personal details they display on their profiles. This can lower the overall vulnerability value of the profile.

6.6-Results

Table 5 below presents the results of the application of the functions on the case studies. With the functions, x represents the total weight of the profile and an initial β value of 0.5 which is a neutral value, was used.

Table 5-Vulnerability Values for the Case Studies where β is 0.5

Cases	$x^{\left(\frac{1}{\beta}\right)}$			$x^{(3 + \beta)}$			$\tanh(x * (1 + \beta))$		
	V_i	V_R	V_A	V_i	V_R	V_A	V_i	V_R	V_A
Young Adult User	0.9965	0.9965	0.9930	0.9939	0.9939	0.9878	0.9046	0.9046	0.8183
Adult User	0.4139	0.8692	0.3597	0.2136	0.7913	0.1690	0.7465	0.8825	0.6587
Adolescent User	0.9965	0.3421	0.3409	0.9939	0.2333	0.2318	0.9046	0.5593	0.5059

Chapter 6- Modeling Operators for Individual Vulnerability

The individual vulnerability modeling impacts on the relative and absolute vulnerability of a profile. The arithmetical mean operator in equation 17 was used to calculate the relative vulnerability and the product operator which is illustrated in equation 13 was used to calculate the absolute vulnerability. The $x^{\frac{1}{\beta}}$ function and the $\tanh(x*(1+\beta))$ function results in Table 5 shows validation between the results and the profile details listed in Table 4. Apart from the $x^{(3+\beta)}$ function, the absolute vulnerability of the profile decreases as the behaviour of the profiles' neighbours' decreases.

A profile with a high absolute vulnerability indicates that there is an increased chance of the profile losing control of its personal details due to its own self disclosure and/or its neighbours disclosure. This is illustrated because the high individual vulnerability profile which is the young adult user mentioned in Table 5 itself, is very public with its attributes and the number of friends is a factor that contributes towards its vulnerability because it has less than 150 friends. This profile's neighbour displays the same behaviour as the profile.

On the other hand, the function $x^{(3+\beta)}$ shows some interesting results especially with the profiles representing the adult user and the adolescent user. This is because the rate of the $x^{(3+\beta)}$ function is very slow until the value of x reaches 0.6 then there are significant increases in the individual vulnerability values of the profiles.

The reason why the profile representing the adult user has a lower V_A value in comparison to the profile representing the adolescent user is because of the individual and relative values. The profile representing the adult user has a lower individual vulnerability value of 0.2136 in comparison to the profile representing the adolescent user which has an individual vulnerability value of

Chapter 6- Modeling Operators for Individual Vulnerability

0.9939. Another reason is due to the reduction effect of the product operator which is used to calculate the absolute vulnerability. If one of the components has a high vulnerability and one of them has a low vulnerability then the reduction effect occurs (e.g. the adult user and the $x^{(3+\beta)}$ function). The individual vulnerability is low but the relative vulnerability is high. Theoretically the absolute vulnerability should reflect that the profile itself is private in terms of self disclosure but there is still the likelihood for the profile's personal details to spread due to the high relative vulnerability.

Out of all the function values in Table 5, the behaviour of the $\tanh(x*(1+\beta))$ function in general makes it harder to highlight which profiles are very vulnerable and need further analysis. This is because the function increases from the very beginning in terms of individual vulnerability value. Even with a small value of x , there is an individual vulnerability which is significantly bigger than the other two functions. This function $\tanh(x*(1+\beta))$ which is a convex function could model an alarmist approach to vulnerability. An example being if a child disclosed a small amount of personal information then there would be a lot of concern regarding the disclosure and its contribution towards the privacy and welfare of the child. Therefore the child would have a high individual vulnerability value.

The other two functions which are concave, display behaviour where the value of x has to be high to produce a significant individual vulnerability value. This approach would be used to model an adult or older adult who is more aware about the consequences of privacy and its impact on their life. A younger adult may have a function which is both concave and convex in order to reflect the fact that they may be more privacy aware but have peer pressure to disclose their personal details.

Chapter 6- Modeling Operators for Individual Vulnerability

Overall what Table 5 does show is that the behaviour of the profile alone does not dictate the vulnerability of the profile. The profiles that have a high absolute vulnerability and low absolute vulnerability both have high individual vulnerability values but the profiles' neighbours act in different ways in terms of disclosure. Another stage of the research will involve carrying out an investigation into modeling the overall characteristics of the OSN and incorporating this into the functions via the β value.

6.7-Validation of Case Studies

The aim of the validation is to explore whether a profile with high relative vulnerability contains neighbours who leak some of the profile's personal details via interactions (e.g. profile comments). For the three case studies which are detailed in Table 4, where each case represents a seed profile, the profile comments of the profile's neighbours immediate friends were examined to see if the comments written by any of the profile's neighbours leaked any personal details about the profile.

With the Caverlee and Webb (2008) dataset, the neighbours represent the *top friends* of the node and since a multigraph was used to model the OSN, the neighbours also included the *top friends* that class the profile as a *top friend*. Caverlee and Webb (2008) extracted only the first page of profile comments from OSN profiles which contains the most up to date comments.

For the profile representing a young adult user, only three comments disclosing the *name* of the of the profile owner were present in the profile's neighbours' interactions.

For the profile representing an adult user, the profile's neighbours do not disclose any personal details about the profile in their interactions. This is probably because the profile never really interacted with the neighbours.

Chapter 6- Modeling Operators for Individual Vulnerability

However the neighbours friends do disclose some of the personal details of the neighbours (e.g. *surname*).

With the profile representing the adolescent user, two of the neighbours leak the current state of *education* of the profile owner and the relationship status of the profile owner in their interactions with their other friends. The neighbourhood contains neighbours which are interactive with one another and this is shown by the number of comments they exchange with one another.

From the results in Table 5, it seems that the young adult user has the highest possibility of being vulnerable due to the high individual and relative vulnerability value, which demonstrate that both the profile and its neighbours display their personal details publically. However the validation results highlight that out of the three case studies, the profile representing the adolescent user is more vulnerable because the neighbours disclose more personal details about the profile in their interactions. This increases the chance of the neighbours' friends and other users viewing the personal details of the profile and spreading the personal details through the network. What the results do highlight is that other personal details can contribute towards vulnerability (e.g. *education*).

The analysis of the neighbours' profile interactions for disclosure of the profile's personal details and whether the profile interacts with the neighbours, can tell you information about the relationship strength between a profile and its neighbours. These case studies have highlighted various degrees of strength of relationships. An example being that a profile has a weak relationship with its neighbours because the profile does not interact with the neighbours, but the neighbours still disclose personal details about the profile.

6.8-Improvements

The validation of this experiment has highlighted that a profile with a high relative vulnerability doesn't necessarily mean that the profile's neighbours will leak personal details about the profile in their interactions with other friends.

The vulnerability values have to match the amount of disclosure of the profile by the neighbours. The collective amount of disclosure by each neighbour of the profiles's personal details can be converted into a coefficient with a value between 0 and 1 and incorporated into relative vulnerability calculation. This will help to reflect the behaviour of the profile's neighbours in terms of privacy as well as their contribution in making the profile vulnerable to social engineering attacks. A neighbour with a high individual vulnerability increases the effect of details spreading especially if the neighbours' interactions are public.

Also different operators associated with the absolute vulnerability calculation need to be validated to reflect the nature of the OSN profile and its neighbourhood in terms of disclosure.

6.9-Conclusions

The modeling of the individual vulnerability of profiles via different mathematical functions has highlighted how the type of mathematical function used can also link to the vulnerability approach adopted because of the users' attitudes towards privacy.

An example being that with a convex function a small amount of personal detail disclosure can lead to a higher individual vulnerability value straight away ,resulting in an alarmist approach to vulnerability. This approach is more suitable to model an OSN profile of a child, adolescent or young adults.

A concave function on the other hand would require a bigger disclosure to be made before vulnerability was significant. This would lead to a conservative

Chapter 6- Modeling Operators for Individual Vulnerability

approach on vulnerability, which may be applied to adults or older adults OSN profiles. The modeling of the individual vulnerability can affect the relative and absolute vulnerability values of the profiles.

The validation of the vulnerability measure in the three case studies showed that in this particular set of cases, even if a profile has a very high relative vulnerability value, this does not necessarily imply that the amount of disclosure of the profile's personal details by the profiles' neighbours is high as well. To account for this, the amount of personal details that the neighbours disclose about the profile has to be incorporated into the relative vulnerability of vulnerability measure as a coefficient.

CHAPTER 7: AXIOMS, PROPOSITIONS AND VULNERABILITY MEASURE PROPERTIES

The aim of this chapter is to present the formal aspects of the vulnerability measure. The formal aspects include the properties of the vulnerability measure, initial axiom regarding the individual vulnerability of the profiles and propositions which concentrate on the relative vulnerability and absolute vulnerability. The axioms are detailed in the (Alim et al. 2011a). The propositions and experimental work regarding the propositions are detailed in (Alim et al. 2011c).

7.1-Vulnerability Measure Properties

Our definitions of absolute vulnerability, individual and relative vulnerability for an OSN user in the context of the OSN users (friends, friends of friends, general users etc) center around the concept that these value are normalized to value between 0 and 1. Within this context, the properties of the algebraic structure $G = ([0,1], \bullet)$ associated with our vulnerability measure are introduced below. In this example, the operator \bullet can be represented by the MAX operator.

The properties of the algebraic structure $G = ([0,1], \bullet)$ include:

1. *Closure*: $\forall V_1, V_2 \in [0,1], V_1 \bullet V_2 \in [0,1]$ this property implies that when applying the operator for the vulnerability measure, all the components needed are contained in the same domain of $[0,1]$. This is because the measure utilises the concept of probability. If a profile has a high absolute vulnerability value, then there is a chance of this profile being vulnerable to social engineering attacks due to the behavior of itself and its neighbours in regards to privacy.

2. *Associativity*: $(V_1 \bullet V_2) \bullet V_3 = V_1 \bullet (V_2 \bullet V_3)$. By saying that the measure is associative we are acknowledging that the grouping order of the friends' contribution in the calculation of vulnerability is not important. The value of the relative vulnerability of the profile is still the same This is emphasized by the permutation mapping illustrated by Calvo and Dercon (2005) in their measure to measure vulnerability in regards to poverty and assures us that changes in the way the friends of a OSN profile are browsed does not affect the value of the vulnerability measured in the OSN graph for a particular user profile (OSN graph node).
3. *Identity Element*: the element V_e from G defined in the interval $[0,1]$ such that for any element V_a from G : $V_a \bullet V_e = V_e \bullet V_a = V_a$. Applying the MAX operator into the relationship above implies that such an identity element satisfies $\text{MAX}(V_a, V_e) = V_a$. for any V_a . This implies that $V_e = 0$. In reality to get registered a profile on an OSN, some at least minimal (vulnerable) attributes have to be disclosed (e.g. *name, gender, date of birth or age*). Therefore the vulnerability of the individual profile cannot be 0 in practical terms, but of course may have at least a theoretical chance.
4. *Inverse Element*: For every V_a from G there is an element called V_a^{-1} such as $V_a \bullet V_a^{-1} = V_e$ (identity element) and $V_a^{-1} \bullet V_a = V_e$. This property cannot be applied to the vulnerability measure because if you are fully vulnerable, then your friend's good behaviour will not make you less vulnerable, in other terms if V_a is any non-zero value having the identity element null for the MAX operator it is not possible to find an inverse element to satisfy this property.

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

5. *Commutativity: For every V_1 and V_2 from G , $V_1 \bullet V_2 = V_2 \bullet V_1$.* By saying that our measure is commutative we acknowledge that the order of the friends' contribution in the calculation of vulnerability is not important.

In conclusion the vulnerability model properties mentioned above relative to the MAX operator define an algebraic structure of a commutative monoid (commutative because the operator MAX is commutative for any value in the interval $[0,1]$). The measure is a monoid because it meets the requirements of being commutative, associative and has an identity element.

7.2-Axioms

The proposed axioms (Alim et al. 2011a) which were established after much experimental work, are based up on the work done by (Calvo and Dercon 2005) into individual vulnerability, but the difference being that their measurement of vulnerability is associated with poverty. In comparison, our vulnerability axioms are based around the self disclosure of personal details in an OSN profile.

Definition 1: Let the individual vulnerability for an OSN profile be defined by the tuple $V=(z,A,P)$, where z can be used to illustrate a vulnerability threshold that indicates the total amount of self disclosure attributes needed for a profile to be labeled as highly vulnerable. The set of attribute values for the i -th OSN profile is denoted by a_i . The probabilities set $P_i=(p_{i1}, p_{i2}, \dots, p_{ij}, \dots, p_{im})$ where m represents the number of attributes, contains the likelihoods p_{ij} , which measure if the presence of the j -th attribute will cause the i -th profile to be vulnerable to social engineering or privacy attacks. Consequently p_{ij} delivers the value for W_j in equation 11 in section 3.2.2. The weighted total of the probabilities p_{ij} is the individual vulnerability of the i -th profile: according to equation 11, V_i is a positive value less or equal to 1, and this meets the closure property of the

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

vulnerability model since our model components (V_I, V_R, V_A) have to be in the domain $[0, 1]$.

In this thesis, we are not concerned with the value of z (vulnerability threshold) in the tuple V or its use. However this vulnerability threshold will be used in the future for highlighting the degree of vulnerability a profile may have. Definition 1 illustrates that our individual vulnerability measure takes initially into consideration attributes that contribute towards vulnerability. There is an issue about whether a profile which does not disclose any personal details or has any friends is classed as having any sort of vulnerability.

If a user would like to apply for an OSN profile he or she is encouraged to record personal details in the registration process. The only way to not display the personal details publically is after getting the profile, change the privacy setting to hide the details or give false personal details in the registration process. The latter reason seems the more realistic scenario of the two because currently, for example for Facebook users, attributes like *name* can't be removed from an OSN profile; they can only be change. Three axioms were proposed for the probability dependent effect of OSN profile attributes, for the probability change and for the addition of attributes onto the profile definition:

Axiom 1 (Probability Dependent Effect of Attributes) Given two OSN profiles characterized by the vulnerabilities $V=(z,A,P)$ and $V'=(z,A',P')$ respectively, for any change $d>0$ in one attribute value:

$$\left\{ \begin{array}{l} V(z,(a_1,a_2,\dots,a_m),(p_1,p_2,\dots,p_m)) - V(z,(a_1+d,a_2,\dots,a_m),(p_1,p_2,\dots,p_m)) = \\ V(z,(a_1,a'_2,\dots,a'_m),(p_1,p'_2,\dots,p'_m)) - V(z,(a_1+d,a'_2,\dots,a'_m),(p_1,p'_2,\dots,p'_m)) \end{array} \right\} (22)$$

$$\left\{ \begin{array}{l} V(z,(a_1,a_2,\dots,a_m),(p_1,p_2,\dots,p_m)) - V(z,(a_1+d,a_2,\dots,a_m),(p_1,p_2,\dots,p_m)) \neq \\ V(z,(a_1,a_2,\dots,a_m),(p_1,p_2,\dots,p_m)) - V(z,(a_1+d,a_2,\dots,a_m),(p_1'',p_2'',\dots,p_m'')) \end{array} \right\} (23)$$

where V is the profile's individual vulnerability, A is its set of attributes and P is its set of probabilities. The change in attribute value is denoted by d .

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

A constraint of Axiom 1 is that the attributes have to be independent of one another. This is so the probability of each attribute contributing to vulnerability does not depend on the presence of another attribute. An example of an independent relationship between attributes is *age* and *zodiac* because people of different ages can have different zodiac signs. In comparison the relationship between the date of birth and *age* is dependent because the date of birth is used to calculate the *age*.

Equation 22 describes the case when two OSN profiles have the same profile attributes and these attributes have the same probability values. This consequently gives the profiles the same individual vulnerability value. For example both profiles have the number of friends as an attribute a_1 and the probability that this leads to the profile being vulnerable is p_1 .

Over time (e.g. a few days later) the number of friends has increased from a_1 to a_1+d for both profiles. In equation 22, this change in the number of friends is represented by d . The consequent effect on individual vulnerability is that the change with the same increment in the same attribute values for both profiles is reflected similarly in the vulnerability of both profiles under the circumstances that both profiles have the same probability $p_1=p_1'$ associated with the information disclosure because of the attribute a_1 .

On the other side, in equation 23 if the two OSN profiles have the same attributes but the probability of the attributes contributing towards the individual vulnerability of each profile differs, as illustrated by the probability notations p' and p'' , the changes in the individual vulnerability values for both profiles are not the same. This situation may arise when, for example, one profile belongs to an adolescent and the other one to an adult. The probability of, let's say, the attribute education information causing vulnerability is higher for a child or

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

adolescent than an adult. This is backed by Hinduja and Patchin (2008) who claims that having several details of the adolescent (e.g. *name, current city, profile picture and school*) is all that is needed to locate the individual and trace their identity.

Axiom.2: (Probability Change): For every $V=(z,A,P)$, the probability change $e \in [0,1]$ and $p_i + e \leq 1$.

$$V(z, (a_1, a_2, \dots, a_m), (p_1, p_2, \dots, p_m)) \leq V(z, (a_1, a_2, \dots, a_m), (p_1 + e, p_2, \dots, p_m)) \quad (24)$$

$$V(z, (a_1, a_2, \dots, a_m), (p_1, p_2, \dots, p_m)) \geq V(z, (a_1, a_2, \dots, a_m), (p_1 - e, p_2, \dots, p_m)) \quad (25)$$

Equation 24 presents a scenario where there are two users with OSN profiles. Unlike the first profile, the first attribute a_1 in the second profile has a higher probability value of making the profile vulnerable. This means that the individual vulnerability of profile one is the same or smaller than the individual vulnerability value of the second profile. In equation 25 represents the same scenario with two OSN profiles but this time attribute a_1 in the second profile has a lower probability value. Consequently, the first profile will have the same or a higher individual vulnerability value.

Axiom.3: (Addition of Attributes): For every $V=(z,A,P)$, $V'=(z',A',P')$, $A'=(a_1, a_2, \dots, a_m, a_{m+1}, a_{m+2}, \dots)$ where $A=(a_1, a_2, \dots, a_m)$, z' and P' are the vulnerability threshold and the probability values of the OSN profile with the addition of new attributes. This changes the individual vulnerability value denoted as V' . The new set including additional independent attributes is denoted as A' . However, if additional independent attributes are added to an OSN profile, then they may or may not contribute towards an increase in the individual vulnerability of a profile. The attributes' effect on the individual vulnerability will depend on the attributes already present in the profile and their

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

probability values. Also the importance of the attribute in social engineering attacks will be a significant factor but more work is required in this area.

7.2.1- A Sample of Axioms Application

The directed multigraph to model the OSN in Figure 18 can be used alongside the table of attributes and neighbourhood features present in the profiles and their respective weights, to demonstrate the vulnerability calculation by applying the axiom notation previously mentioned. In Figure 18, there are three profiles which are represented by nodes *A*, *B* and *C*. The solid lines represent a top friend link between two profiles, (e.g. profile *C* is a *top friend* of profile *A* but profile *A* is not a *top friend* of profile *C*).

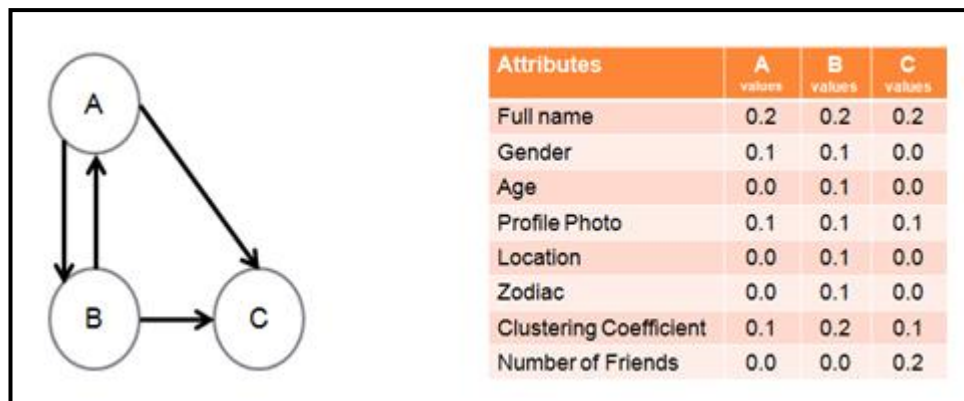


Figure 18-OSN Graph and Table of Weights

To calculate the absolute vulnerability of node *A*, the first step is to calculate the individual vulnerability V_I of node *A*. Node *A*'s profile is represented by the tuple $V(z, (fullname, gender, age, profilephoto, location, zodiac, clustering_coefficient, number_of_friends), (0.2, 0.1, 0.0, 0.1, 0.0, 0.0, 0.1, 0.0))$. According to equation 11 in section 3.2.2, $V_{IA} = 0.5$. The attribute/neighbourhood feature weights represent the probability values which state the likelihood that the presence of the attribute or neighbourhood feature will contribute towards the vulnerability of the profile. In this case the probability values are chosen values between $[0,1]$ which add up to 1. The attribute *fullname* and neighbourhood feature

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

number_of_friends are given higher weights because fullname is a common attribute which is used in identity theft. Having lower than 150 friends may cause information to spread quickly across a network due to the increased chances of having a highly interactive relationship with some of the friends.

The relative vulnerability V_R of node A takes the individual vulnerability of the neighbours B and C into consideration. Profile B is represented by the tuple $V(z, (fullname, gender, age, profilephoto, location, zodiac, clustering_coefficient, number_of_friends), (0.2, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.0))$ has a V_I value of 0.8. Node C 's profile represented by the tuple $V(z, (fullname, gender, age, profilephoto, location, zodiac, clustering_coefficient, number_of_friends), (0.2, 0.0, 0.0, 0.0, 0.0, 0.0, 0.1, 0.2))$ has a V_I value of 0.5. According to equation 12 in section 3.3.3, V_{RA} value is 0.65. The V_{RA} value is high because of node B readily presenting its personal details as well as having a high clustering coefficient and node C only presenting one personal detail but having less than 150 friends and so there is an increased chance of having a interaction between friends.

Consequently according to equation 13 in section 3.2.4, the V_{AA} is 0.32 with the product operator. The product operator balances the vulnerability of the node and the collective vulnerability of the neighbours. The choice of operator used in equation 13 can influence the absolute vulnerability value.

Based on the vulnerability measure, the axioms presented have helped to investigate the impact of attribute and probability value change on the individual vulnerability of a profile. Axiom 1 highlights the issue of attributes and the probability that the attribute change can contribute towards the profile's vulnerability. In our vulnerability measure we make the assumption that an attribute's contribution towards the vulnerability of a profile is independent of the

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

type of user, as illustrated in equations 22 and 23. This assumption helps when modeling an OSN because different users have different attitudes towards privacy.

On the other hand, Axiom 2 illustrates the effect that a probability change can have on the individual vulnerability value of the profile. An increase in an attribute weight will increase the individual vulnerability of the profile. Since the weights of the attributes that contribute towards vulnerability have to add up to one, an increase in one attribute weight will lower the weights of the other attributes.

7.3-Propositions

The effect of different operators on the vulnerability model via new consistent findings forms the propositions stated below. They provide an insight into how changes to the vulnerability model components can impact on the overall vulnerability of a profile. The propositions depend on the operators used in equations 12 and 13. Propositions 1 and 2 are based on the axioms which are stated in section 7.2, whilst propositions 3-6 aim to explore in more detail other areas of the vulnerability model (e.g. relative and absolute vulnerability). The list of propositions that we have proposed include:

Proposition 1 states that in the context of using the product operator in equation 13, the absolute vulnerability value increases when there is an increase in the individual vulnerability value and the absolute vulnerability value decreases when there is a decrease in the individual vulnerability value.

In the context of using the MAX operator in equation 13, **proposition 2** emphasises that the absolute vulnerability value increases when the individual vulnerability value increases subject to the value being higher than the relative vulnerability value. On the other hand the absolute vulnerability value decreases

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

when the individual vulnerability value decreases subject to the individual vulnerability value being higher than the relative vulnerability value.

Proposition 3 explores the calculation of the relative vulnerability value by substituting the geometric mean operator into equation 12. The relative vulnerability value increases when the individual vulnerability value of the new neighbour added to the existing neighbourhood is higher or equal to the maximum individual vulnerability value of the existing neighbours. Whereas the relative vulnerability value calculated using the geometric mean operator can decrease when the individual vulnerability value of the new neighbour added to the existing neighbourhood, is lower than the minimum individual vulnerability value of the existing neighbours.

In **proposition 4**, the arithmetical mean operator is used to calculate using equation 12 the relative vulnerability value. There is an increase in the relative vulnerability value when the individual vulnerability value of the new neighbour added to the existing neighbourhood, is higher than the maximum individual vulnerability value of the existing neighbours. The relative vulnerability value calculated using the arithmetical mean operator can decrease when the individual vulnerability value of the new neighbour added to the existing neighbourhood, is lower than or equal to the minimum individual vulnerability value of the existing neighbours.

Proposition 5 focuses on the change to the absolute vulnerability value. The absolute vulnerability value which is calculated using equation 13 and the product operator, increases when the relative vulnerability which is calculated using geometric mean increases due to the addition of a neighbour (with a higher individual vulnerability value than the maximum value in the existing neighbourhood). The absolute vulnerability value decreases when the relative

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

vulnerability decreases due to the deletion of a neighbour (with a higher individual vulnerability value than the maximum value in the existing neighbourhood).

In **proposition 6** which centres on the absolute vulnerability value, the absolute vulnerability which is calculated using equation 13 and the product operator, increases when the relative vulnerability that is calculated using arithmetical mean, increases due to the addition of a neighbour (with a higher individual vulnerability value than the maximum value in the existing neighbourhood). The absolute vulnerability value decreases when the relative vulnerability decreases due to the deletion of a neighbour (with a higher individual vulnerability value than the maximum value in the existing neighbourhood).

The propositions are presented in more detail below:

Proposition 1: An increase or decrease in the individual vulnerability value determines an increase or decrease in the absolute vulnerability value, absolute vulnerability is calculated using the product operator, \bullet .

If $V_{A_i} = V_{I_i} \bullet V_{R_i}$ for profile i and \bullet is product, then a change in the V_I value will be reflected by a change in the V_A value. Proposition 1 is based on Axiom 2 regarding probability changes.

Proof

$V_{A_i} = V_{I_i} \bullet V_{R_i} \in [0,1]$ where \bullet indicates the product operator. According to Axiom

2:

$$V_{A_e} = V(z, (a_1, a_2, \dots, a_m), (p_1 + e, p_2, \dots, p_m)) \bullet V_{R_i} \geq V(z, (a_1, a_2, \dots, a_m), (p_1, p_2, \dots, p_m)) \bullet V_{R_i} = V_{A_i} \quad (26)$$

where the probability change $e \in [0,1]$, $p_i + e \leq 1$, V_{A_e} is the absolute vulnerability value of profile i as a result of the increase in probability value of the attributes

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

contributing towards vulnerability. V_{R_i} is the relative vulnerability of profile i and V_{A_i} is the absolute vulnerability of profile i without the probability change taken into account. In Equation 26, V_{R_i} is a constant calculated using the arithmetical mean. This proposition fits in with the concept that the individual vulnerability value of a profile monotonically increases with the absolute vulnerability value of a profile.

We can identify two cases regarding the change in the V_i value:

a) *Increase in Individual Vulnerability Value:*

Equation 27 highlights how the absolute vulnerability value increases when the individual vulnerability value of a profile increases due to a change in the probability of an attribute or what attributes the profile chooses to present.

$$V'_{I_i} > V_{I_i} \Rightarrow V'_{A_i} = V'_{I_i} \bullet V_{R_i} > V_{I_i} \bullet V_{R_i} = V_{A_i} \quad (27)$$

where V'_{I_i} represents the increased individual vulnerability value and the V'_{A_i} represents the increased absolute vulnerability value.

An example of this case is that profile A in Figure 18 decides to present the *location* attribute on their profile which has an attribute weight of 0.1. This increases the V_i value of profile A from 0.5 to 0.6. The change in V_i value (ΔV_i) is an increase of 0.1 due to the addition of the attribute weight for location. This consequently increases the V_A value for profile A from 0.325 to 0.390 with a difference of 0.065. This case links in with Axiom 3 which focuses on the addition of attributes and Axiom 2.

b) *Decrease in Individual Vulnerability Value:*

Equation 28 highlights the decrease in absolute vulnerability value when the individual vulnerability value of profile i decreases, due to a change in the

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

probability of an attribute or a deletion of a profile attribute that contributes towards vulnerability.

$$V'_{I_i} < V_{I_i} \Rightarrow V'_{A_i} = V'_{I_i} \bullet V_{R_i} < V_{I_i} \bullet V_{R_i} = V_{A_i} \quad (28)$$

where V'_{I_i} represents the decreased individual vulnerability value, the V'_{A_i} represents the decreased absolute vulnerability value and V_{R_i} is constant and calculated using the arithmetical mean.

An example of this case is that profile *B* in Figure 18 decides to delete the *Full name* attribute on their profile. This decreases the V_I of profile *B* from 0.8 to 0.6 with a ΔV_I decrease of 0.2. Consequently this decreases the V_A value for profile *B* from 0.400 to 0.300. This observation illustrates that with a ΔV_I decrease of 0.2 and a V_{R_i} value of 0.5, the V_A value decreases by 0.1. This case links in with equation 25 in Axiom 2 which focuses on probability change.

Proposition 2: An increase or decrease in the individual vulnerability value reflects an increase or decrease in the absolute vulnerability value, when absolute vulnerability is calculated using the MAX operator, \bullet and the individual vulnerability value is higher than the relative vulnerability value.

For profile *i* \bullet is MAX, then a change in the V_I value will be reflected by a change in the V_A value if and only if the $V_I \geq V_R$.

Proof

$$\left. \begin{cases} V_A = \text{MAX}(V_I, V_R) \\ V_I \geq V_R \end{cases} \right\} V_A = V_I \quad (29)$$

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

The proof highlights that in order for the V_I change to lead to a V_A change, the $V_I \geq V_R$. Subject to $V_I \geq V_R$ we have identified two cases of change for individual vulnerability:

a) *Increase in Individual Vulnerability:*

Equation 30 highlights the increase in absolute vulnerability value when the individual vulnerability value of profile i increases, due to a change in the probability of an attribute or what attributes the profile presents.

$$V'_{I_i} > V_{I_i} \Rightarrow V'_{A_i} = \text{MAX}(V'_{I_i}, V_{R_i}) > \text{MAX}(V_{I_i}, V_{R_i}) = V_{A_i} \mid V_{I_i} \geq V_{R_i} \quad (30)$$

where V'_{I_i} represents the increased individual vulnerability value and the V'_{A_i} represents the increased absolute vulnerability value.

An example of this case is that profile A in Figure 18 decides to present the *age* and *location* attributes on their profile. This increases the V_I of profile A from 0.5 to 0.7 with a ΔV_I of 0.2. Consequently the V_A for profile A increases because the updated V_I of profile A is larger than the V_R of profile A which is 0.65. The V_A value of profile A has increased from 0.65 to 0.70 and this shows that with the MAX operator, as long as the updated V_I value is lower than or equal to the V_R value, then the changes to profile A will not be reflected in the overall vulnerability. This case links in with equation 24 in Axiom 2 which centres on probability change.

b) *Decrease in Individual Vulnerability:*

Equation 31 highlights the decrease in absolute vulnerability value when the individual vulnerability of profile i decreases, due to a change in the probability of an attribute or a deletion of an attribute that contributes towards the vulnerability of a profile.

$$V'_{I_i} < V_{I_i} \Rightarrow V'_{A_i} = \text{MAX}(V'_{I_i}, V_{R_i}) < \text{MAX}(V_{I_i}, V_{R_i}) = V_{A_i} \quad | V_{I_i} \geq V_{R_i} \quad (31)$$

An example of this case is that profile *B* in Figure 18 decides to delete the attributes *Full Name* on their profile. This decreases the individual vulnerability value of profile *B* from 0.8 to 0.6 with a ΔV_I of 0.2.

Consequently the absolute vulnerability value for profile *B* decreases from 0.8 to 0.6. The change in absolute vulnerability (ΔV_A) = ΔV_I because the individual vulnerability before and after the attribute change for profile *B* was higher than the relative vulnerability value of profile *B* which is 0.5. However the decrease depends on the comparison between $(V_{I_i} - V_{R_i})$ and $(V'_{I_i} - V_{I_i})$.

In regards to how the absolute vulnerability is affected by the changes to the relative vulnerability of a profile, two operators were selected which can help calculate the relative vulnerability of a profile. One of these operators is the geometric mean, which is illustrated in equation 17.

Proposition 3: On the change in relative vulnerability value when relative vulnerability is calculated using the geometric mean operator.

Given that $V_{A_i} = V_{I_i} \bullet V_{R_i}$ and $V_{R_i} = \sqrt[n]{\prod_{\substack{j=1 \\ j \neq i}}^n V_{I_j}}$

If $V_{I_{n+1}} > V_{I_i}, \forall i = 1, \dots, n$ (\Rightarrow) $V_{I_{n+1}} \geq \text{MAX}_{i=1}^n V_{I_i}$ where MAX an operator which selects out the maximum individual vulnerability (V_{I_n}) from the neighbours, then $V_{R_{n+1}} > V_{R_n}$, where $V_{R_{n+1}}$ is the relative vulnerability value of neighbourhood with addition of new neighbour and V_{R_n} is the relative vulnerability of the existing neighbourhood.

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

As long as the V_i of the new neighbour ($V_{I_{n+1}}$) is equal to or higher than the maximum individual vulnerability value from the existing neighbours, then the relative vulnerability value will increase with the addition of a new neighbour and this is shown in the proof below where V'_{R_n} represents the new relative vulnerability value of the profile with the addition of the new neighbour into the existing neighbourhood. The proof which is explained below is based on the following additional calculations:

$$\begin{aligned}
 V_{R_i} &= \left(\prod_{\substack{i=1 \\ i \neq j}}^n V_{I_i} \right)^{\frac{1}{n}} \quad \left| \quad \frac{V_{R_i}}{V'_{R_i}} = \frac{\left(\prod_1^n V_{I_i} \right)^{\frac{1}{n}}}{\left(\prod_1^{n+1} V_{I_i} \right)^{\frac{1}{n+1}}} \right. \\
 V'_{R_i} &= \left(\prod_{\substack{i=1 \\ i \neq j}}^{n+1} V_{I_i} \right)^{\frac{1}{n+1}} \\
 \log \frac{V_{R_i}}{V'_{R_i}} &= \frac{1}{n} \log \prod_1^n V_{I_i} - \frac{1}{n+1} \log \prod_1^{n+1} V_{I_i} = \\
 &= \frac{(n+1) * \log \prod_1^n V_{I_i} - n * \log \prod_1^{n+1} V_{I_i}}{n(n+1)} = \\
 &= \frac{n * \log \prod_1^n V_{I_i} + \log \prod_1^n V_{I_i} - n * \log \left(\left(\prod_1^n V_{I_i} \right) * V_{I_{n+1}} \right)}{n(n+1)} = \\
 &= \frac{n * \log \prod_1^n V_{I_i} + \log \prod_1^n V_{I_i} - n * \log \prod_1^n V_{I_i} - n * \log V_{I_{n+1}}}{n(n+1)} = \\
 &= \frac{\log \prod_1^n V_{I_i} - \log V_{I_{n+1}}}{n(n+1)} = \frac{\log \prod_1^n \left(\frac{V_{I_i}}{V_{I_{n+1}}} \right)}{n(n+1)} \\
 V_{I_i} < V_{I_{n+1}} &\Rightarrow \frac{V_{I_i}}{V_{I_{n+1}}} < 1 \\
 \prod_1^n \frac{V_{I_i}}{V_{I_{n+1}}} &< 1 \\
 \log \prod_1^n \frac{V_{I_i}}{V_{I_{n+1}}} &< 0 \\
 \frac{V_{R_i}}{V'_{R_i}} < 1 &\Rightarrow V_{R_i} < V'_{R_i}
 \end{aligned}$$

Proof

$$V_{I_{n+1}} > V_{I_i}, \forall i = 1, ..n$$

$$\frac{V_{I_{n+1}}}{V_{I_i}} > 1, \forall i = 1, \dots, n$$

$$\text{then } \frac{V_{I_{n+1}}}{V_{I_i}} > 1, \forall i = 1, \dots, n$$

$$\text{then } \prod_{i=1}^n \frac{V_{I_{n+1}}}{V_{I_i}} > \log 1 = 0$$

$$\log \prod_{i=1}^n \frac{V_{I_{n+1}}}{V_{I_i}} > 0 \Rightarrow V'_{R_n} > V_{R_n}$$

An example of this case involves the neighbourhood of profile *A* in Figure 18. The highest individual vulnerability value of the neighbours in *A*'s neighbourhood is 0.8. If a new neighbour with an individual vulnerability of 0.85 joins the neighbourhood, then the relative vulnerability of profile *A* when calculated using the geometric mean operator will increase from 0.632 to 0.697 with a change of 0.065. Additionally, if the new neighbour had an individual vulnerability of 0.8, then the relative vulnerability of profile *A* would still increase from 0.632 to 0.683 with a change of 0.051.

The relative vulnerability value of profile *A* can decrease when the individual vulnerability value of the new neighbour is equal to or lower than the minimum individual vulnerability value in the existing neighbourhood, which in this case is 0.5. A new neighbour with an individual vulnerability value of 0.4 would decrease the relative vulnerability value of profile *A* from 0.632 to 0.542 with a change of 0.090.

Another operator which can be used to calculate the relative vulnerability of a profile is the arithmetical mean, which is illustrated in equation 18.

Proposition 4: On the change in relative vulnerability value when relative vulnerability is calculated using the arithmetical mean operator

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

Given that $V_{A_i} = V_{I_i} \bullet V_{R_i}$ and $V_{R_i} = \frac{1}{n} \sum_1^n V_{I_j}$

If $V_{I_{n+1}} > V_{I_i}, \forall i = 1, \dots, n$ (\Rightarrow) $V_{I_{n+1}} \geq \text{MAX}_{i=1}^n V_{I_i}$ where MAX is the operator which selects out the maximum individual vulnerability (V_{I_n}) from the neighbours, then $V_{R_{n+1}} > V_{R_n}$, where $V_{R_{n+1}}$ is the relative vulnerability value of neighbourhood with addition of new neighbour and V_{R_n} is the relative vulnerability of the existing neighbourhood.

As long as the individual vulnerability value of the new neighbour ($V_{I_{n+1}}$) is higher than or equal to the maximum individual vulnerability value from the existing neighbours, then the relative vulnerability value will increase with the addition of a new neighbour. This is shown in the proof below, where V'_{R_n} signifies the new relative vulnerability value of the profile with the addition of the new neighbour into the existing neighbourhood. The proof which is explained below is based on the following additional calculations:

$$V_{R_{n+1}} = \frac{1}{n+1} \sum_1^{n+1} V_{I_i}$$

$$V_{R_n} = \frac{1}{n} \sum_1^n V_{I_i}$$

$$V_{R_{n+1}} - V_{R_n} = \frac{1}{n+1} \sum_1^{n+1} V_{I_i} - \frac{1}{n} \sum_1^n V_{I_i} =$$

$$\frac{n * \sum_1^{n+1} V_{I_i} - (n+1) * \sum_1^n V_{I_i}}{(n+1) * n} =$$

$$\frac{n * (\sum_1^n V_{I_i} + V_{I_{n+1}}) - n * \sum_1^n V_{I_i} - \sum_1^n V_{I_i}}{n(n+1)} =$$

$$\frac{n * \sum_1^n V_{I_i} + n * V_{I_{n+1}} - n * \sum_1^n V_{I_i} - \sum_i^n V_{I_i}}{n(n+1)} =$$

$$\frac{n * V_{I_{n+1}} - \sum_1^n V_{I_i}}{n * (n+1)} =$$

$$\frac{\sum_1^n V_{I_{n+1}} - \sum_1^n V_{I_i}}{n * (n+1)} =$$

$$\frac{\sum_1^n V_{I_{n+1}} - V_{I_i}}{n * (n+1)}$$

$$V_{I_{n+1}} > V_{I_i}$$

$$\sum_1^n V_{I_{n+1}} > \sum_1^n V_{I_i} \Rightarrow \sum_1^n (V_{I_{n+1}} - V_{I_i}) > 0$$

$$\frac{\sum_1^n (V_{I_{n+1}} - V_{I_i})}{n(n+1)} > 0$$

$$V_{R_{n+1}} - V_{R_n} > 0$$

$$V_{R_{n+1}} > V_{R_n}$$

Proof

$$V_{I_{n+1}} > V_{I_i}, \forall i = i, \dots, n$$

$$\sum_1^n V_{I_{n+1}} > \sum_1^n V_{I_i} \mid \sum_1^n (V_{I_{n+1}} - V_{I_i}) > 0 \text{ and } \frac{\sum_1^n (V_{I_{n+1}} - V_{I_i})}{n(n+1)} > 0 \text{ and } V_{R_{n+1}} - V_{R_n} > 0$$

$$V_{R_{n+1}} > V_{R_n}$$

$$V'_{R_n} = V_{R_{n+1}} \Rightarrow V'_{R_n} > V_{R_n}$$

The proof illustrates that in order for $V_{R_{n+1}} > V_{R_n}$, the difference between $V_{I_{n+1}}$ and V_{I_i} has to be a positive number which is above 0.

An example of this case involves the neighbourhood of profile A in Figure 18.

The highest individual vulnerability value of the neighbours in A's

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

neighbourhood is 0.8. If a new neighbour joins the neighbourhood with an individual vulnerability value of 0.85, then the relative vulnerability of profile A when calculated using the arithmetical mean operator will increase from 0.650 to 0.716. Even if the individual vulnerability value of the new neighbour was 0.8, then the relative vulnerability of profile A would increase from 0.650 to 0.700.

The relative vulnerability value of profile A can decrease if the individual vulnerability value of the new neighbour was equal to or lower than the minimum individual vulnerability value in the existing neighbourhood, which in this case is 0.5. A new neighbour with an individual vulnerability value of 0.4 would decrease the relative vulnerability value of profile A from 0.650 to 0.566.

Proposition 5: On the change in absolute vulnerability due to addition or deletion of a neighbour when relative vulnerability is calculated using geometric mean operator and absolute vulnerability is calculated using the product operator, \bullet .

Given that $V_{A_i} = V_{I_i} \bullet V_{R_i}$ and $V_{R_i} = \sqrt[n]{\prod_{j=1}^n V_{I_j}}$ where n is the number of neighbours and V_{I_j} is the individual vulnerability of neighbour j . if \bullet is product, then a change (increase or decrease) in the relative vulnerability value (V_{R_i}) will be reflected by a change (increase or decrease) in the absolute vulnerability (V_{A_i}) if and only if $V_{R_{n+1}} > V_{R_i}$. $V_{R_{n+1}}$ is the relative vulnerability of profile i with the addition of a new neighbour and V_{R_i} is the relative vulnerability of profile i without the addition of a new neighbour.

Proof

$V_{A_i} = V_{I_i} \bullet V_{R_i} \in [0,1]$ for profile i where \bullet indicates a product operator.

$$V_{I_{n+1}} > V_{I_i}, \forall i = 1, \dots, n$$

$$\frac{V_{I_{n+1}}}{V_{I_i}} > 1, \forall i = 1, \dots, n$$

$$\text{then } \frac{V_{I_{n+1}}}{V_{I_i}} > 1, \forall i = 1, \dots, n$$

$$\text{then } \prod_{i=1}^n \frac{V_{I_{n+1}}}{V_{I_i}} > \log 1 = 0$$

$$\frac{1}{n(n+1)} * \log \prod_{i=1}^n \frac{V_{I_{n+1}}}{V_{I_i}} > 0 \Rightarrow V_{R_{n+1}} > V_{R_n}$$

$$V_{R_{n+1}} > V_{R_n} \Rightarrow V_{R_{n-1}} < V_{R_n}$$

The proof shows that when the relative vulnerability is calculated using the geometric mean operator, the addition of a new neighbour can increase the profile's relative vulnerability value. We have identified two cases regarding the increase in relative vulnerability value due to addition and deletion of a neighbour in the profile's neighbourhood:

a) *Increase in Relative Vulnerability through addition of a neighbour*

Equation 32 highlights an increase in the V_A when the V_R of profile i increases, due to the addition of a neighbour into the profile's neighbourhood.

$$V_{R_{n+1}} > V_{R_n} \Rightarrow V'_{A_i} = V_{I_i} \bullet V_{R_{n+1}} > V_{I_i} \bullet V_{R_n} = V_{A_i} \quad (32)$$

where $V_{R_{n+1}}$ is the relative vulnerability of profile i with the additional neighbour, V_{R_n} is the relative vulnerability of profile i without the neighbour, V'_{A_i} is the absolute vulnerability of profile i as a result of the addition of the neighbour and V_{A_i} is the absolute vulnerability of profile i without the addition of the neighbour.

An example of this case involves the neighbourhood of profile A in Figure 18. With the addition of a new neighbour with an individual vulnerability value of 0.9, the relative vulnerability value of profile A increases from 0.632 to 0.711 with an

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

increase change of 0.079. Consequently, the absolute vulnerability value increases from 0.316 to 0.355 with an increase of 0.039. An important observation between these results, is that the difference between V'_{A_i} and V_{A_i} is half the difference between $V_{R_{n+1}}$ and V_{R_n} .

b) *Decrease in Relative Vulnerability through the deletion of a neighbour*

Equation 33 states a decrease in the absolute vulnerability value of profile i when the relative vulnerability of profile i decreases, due to the deletion of a neighbour in the profile's neighbourhood.

$$V_{R_{n-1}} < V_{R_n} \Rightarrow V'_{A_i} = V_{I_i} \bullet V_{R_{n-1}} < V_{I_i} \bullet V_{R_n} = V_{A_i} \quad (33)$$

where $V_{R_{n-1}}$ is the relative vulnerability of profile i with a neighbour deleted, V_{R_n} is the relative vulnerability of profile i before the neighbour was deleted, V'_{A_i} is the absolute vulnerability of profile i as a result of the deletion of the neighbour and V_{A_i} is the absolute vulnerability of profile i before the neighbour was deleted.

Equation 33 highlights that deleting a neighbour in the neighbourhood with an individual vulnerability value that is higher than the maximum individual vulnerability value of the neighbourhood, decreases the relative vulnerability value of the profile and this results in a decrease in the absolute vulnerability value of the profile.

An example of this case involves the neighbourhood of profile A in Figure 18. If profile B which has the highest individual vulnerability value is removed from profile A 's neighbourhood, then the relative vulnerability value of profile A decreases from 0.632 to 0.500 with a difference of 0.132. Consequently the absolute vulnerability value decreases from 0.316 to 0.250, with a difference of

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

0.066. The difference between V'_{A_i} and V_{A_i} is half the difference between $V_{R_{n+1}}$ and V_{R_n} .

Proposition 6: On the change in absolute vulnerability due to addition or deletion of a neighbour when relative vulnerability is calculated using arithmetical mean operator and absolute vulnerability is calculated using the product operator, •.

Given that $V_{A_i} = V_{I_i} \bullet V_{R_i}$ and $V_{R_i} = \frac{1}{n} \sum_1^n V_{I_j}$ where n is the number of neighbours and V_{I_j} is the individual vulnerability of neighbour j . If • is product, then a change in the relative vulnerability (V_{R_i}) will be reflected by a change in the absolute vulnerability (V_{A_i}) if and only if the $V_{R_{n+1}} > V_{R_n}$ where $V_{R_{n+1}}$ is the relative vulnerability of profile i with the addition of a new neighbour and V_{R_n} is the relative vulnerability of profile i without the addition of a new neighbour.

Proof

$V_{A_i} = V_{I_i} \bullet V_{R_i} \in [0,1]$ for profile i where • indicates a change.

$$V_{I_{n+1}} > V_{I_i}, \forall i = i, \dots, n$$

$$\sum_1^n V_{I_{n+1}} > \sum_1^n V_{I_i} \mid \sum_1^n (V_{I_{n+1}} - V_{I_i}) > 0 \text{ and } \frac{\sum_1^n (V_{I_{n+1}} - V_{I_i})}{n(n+1)} > 0 \text{ and } V_{R_{n+1}} - V_{R_n} > 0$$

$$V_{R_{n+1}} > V_{R_n} \Rightarrow V_{R_{n+1}} < V_{R_n}$$

The proof shows that when the relative vulnerability is calculated using the arithmetical mean operator, the addition of a new neighbour in to the existing neighbourhood can increase the profile i relative vulnerability value if and only if the individual vulnerability value of the new neighbour is higher than the maximum individual vulnerability value of the existing neighbourhood.

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

This implies that the deletion of a neighbour will decrease the relative vulnerability value of the profile. In order for the relative vulnerability value to increase, the individual vulnerability value of the new neighbour has to be higher than the maximum individual vulnerability value of the existing neighbours in the neighbourhood.

There are two cases of change for relative vulnerability:

a) *Increase in Relative Vulnerability through addition of a neighbour*

Equation 34 highlights the increase in absolute vulnerability when the relative vulnerability value of a profile increases due to the addition of a neighbour into the profile's neighbourhood.

$$V_{R_{n+1}} > V_{R_n} \Rightarrow V'_{A_i} = V_{I_i} \bullet V_{R_{n+1}} > V_{I_i} \bullet V_{R_n} = V_{A_i} \quad (34)$$

where $V_{R_{n+1}}$ is the relative vulnerability of the profile with the additional neighbour, V_{R_n} is the relative vulnerability of the profile without the neighbour, V'_{A_i} is the absolute vulnerability of the profile as a result of the addition of the neighbour and V_{A_i} is the absolute vulnerability of the profile without the addition of the neighbour. Equation 34, illustrates that adding a neighbour with a higher individual vulnerability value to a neighbourhood, increases the relative vulnerability value of the profile and this results in an increase in the absolute vulnerability value of the profile.

An example of this case involves the neighbourhood of profile A in Figure 18. With the addition of a new neighbour with an individual vulnerability value of 0.9, the relative vulnerability value increases from 0.650 to 0.733 which is a difference of 0.083. Consequently the absolute vulnerability value of profile A increases from 0.320 to 0.366 with a difference of 0.046.

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

b) *Decrease in Relative Vulnerability through deletion of a neighbour*

Equation 35 highlights the decrease in absolute vulnerability when the relative vulnerability value of a profile decreases due to the deletion of a neighbour with the highest individual vulnerability value, in a profile's neighbourhood.

$$V_{R_{n-1}} < V_{R_n} \Rightarrow V'_{A_i} = V_{I_i} \bullet V_{R_{n-1}} < V_{I_i} \bullet V_{R_n} = V_{A_i} \quad (35)$$

where $V_{R_{n-1}}$ is the relative vulnerability of the profile with a neighbour deleted, V_{R_n} is the relative vulnerability of the profile before the neighbour was deleted, V'_{A_i} is the absolute vulnerability of the profile as a result of the deletion of the neighbour and V_{A_i} is the absolute vulnerability of the profile before the neighbour was deleted. Equation 35 illustrates that deleting a neighbour with the highest individual vulnerability value in the neighbourhood, decreases the relative vulnerability value of the profile and this results in a decrease in the absolute vulnerability of the profile.

An example of this case involves the neighbourhood of profile *A* in Figure 18. If profile *B* is removed from profile *A*'s neighbourhood, then the relative vulnerability value of profile *A*, decreases from 0.650 to 0.500 which is a difference of 0.150. Consequently the absolute vulnerability value of profile *A* decreases from 0.325 to 0.250 which is a difference of 0.075.

Overall this section has detailed several propositions, which focus on changes in the vulnerability model. What the propositions have demonstrated is that the changes in what a user present on their profile and the adding and deletion of friends into a neighbourhood, impacts on the overall profile vulnerability.

7.4- Experimental Work and Findings Regarding Application of Propositions

In order to explore how the operators from the propositions affect the vulnerability of real life cases, different operators for the relative and absolute vulnerabilities calculations were used. These calculations were tested on 76,263 profiles from the Caverlee and Webb (2008) dataset. For the 76,263, the average age of the profile owners is 25.6. 50.1% of the profile owners are male, 48.6% of the profile owners are female and 1.3% profile owners do not state their gender. 16.3% of the profiles are private profiles. Private profiles may present basic information (e.g. name, gender, profile picture and age) on their profiles but not the list of friends or interactions.

The different operators were used in the following ways: the relative vulnerability value of the cases in the dataset was calculated using the geometric and arithmetical mean. These operators are used in propositions 3-6. The absolute vulnerability value for the cases was calculated using the product and MAX operators used in propositions 1, 2, 5 and 6. The operators were applied to 76,263 cases with varying individual vulnerability values.

In terms of the relative vulnerability calculation, unlike some operators (e.g. MAX and MIN) which select just the maximum or minimum individual vulnerability value of the neighbourhood, the geometric and arithmetical mean takes into account all the individual vulnerability values of the neighbours in the calculation. With the arithmetical mean operator, 78.0% of the profiles had a relative vulnerability of 0.9 or above and with the geometric mean, 75.9% of the profiles had a relative vulnerability of 0.9 and above. The results highlight that most neighbours in profiles' neighbourhoods self disclose the attributes and display structural features, that contribute towards vulnerability readily.

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

The effect of the calculation of the relative vulnerability on the absolute vulnerability of profiles is covered in propositions 5 and 6. Table 6 presents statistics for the whole dataset, regarding different combinations of operators for the relative and absolute vulnerability calculations. The MAX operator is mainly used in proposition 2. In Table 6, the absolute vulnerability of profiles is denoted as V_A .

Table 6-Statistics regarding Application of Different Operators

Absolute Vulnerability Operators	Product		MAX	
Relative Vulnerability Operators	Geometric	Arithmetical	Geometric	Arithmetical
Features Corresponding to Whole Dataset				
% of profiles that have a V_A of 0.9 or above	47.4%	50.2%	99.1%	99.2%
Average V_A value	0.871	0.872	0.964	0.969
Standard Distribution of V_A values	0.134	0.132	0.034	0.034
Skewness	-3.386	-3.454	-2.455	-2.105

What Table 6 demonstrates, is the big difference between the effect of the product and MAX operator in regards to the absolute vulnerability of profiles. The product operator can act as a reducing effect. An example is that if a profile has friends which self disclose personal details readily (V_R value of 0.8), but the profile itself is very private (V_I value of 0.2), the overall vulnerability of the profile would be 0.16. This emphasises that there is a low likelihood of the profile's personal details spreading through the OSN.

On the other hand the MAX operator selects the higher value between the V_I and V_R . The high percentage of profiles that have an absolute vulnerability of 0.9 or above highlights that there are cases in which the profile's neighbours

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

many not collectively disclose many attributes that contribute towards vulnerability but the profile itself will and this causes the overall vulnerability of the profile to increase.

The average absolute vulnerability values of the dataset for the product and MAX operators demonstrate that the MAX operator may not be an effective operator for the calculation of absolute vulnerability. This is because it does not take into effect the meaning of both the individual and relative vulnerability values together and it would be hard to select the profiles which are truly vulnerable.

With the product operator, 15.5% of the profiles in which the relative vulnerability is calculated using arithmetical mean have an absolute vulnerability value which is less or equal to 0.8. Therefore the product operator is more realistic than the MAX operator in selecting vulnerable nodes. This is validated by the standard deviation for the V_A values calculated using the product operator. It illustrates that in this dataset there are a variety of cases with varying V_I and V_R values.

The negative skew for the product and MAX operators indicates that there is a long distribution tail to the left and consequently more profiles have a higher absolute vulnerability value. Overall what the statistics have shown is that the choice of operator especially for the calculation of absolute vulnerability can influence the number of profiles which are classed as having a high overall vulnerability (V_A of 0.9 or above).

7.5-Discussion

Based on the vulnerability model, the axioms and propositions presented have helped to investigate the impact of attribute and probability value change on the individual vulnerability of a profile. Axiom 1 highlights the issue of attributes and

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

the probability that the attribute change can contribute towards the profile's vulnerability. In our vulnerability model we make the assumption that an attribute's contribution towards the vulnerability of a profile is independent of the type of user, as illustrated in equations (22) and (23). This assumption helps when modelling an OSN because different users have different attitudes towards privacy.

On the other hand, Axiom 2 illustrates the effect that a probability change can have on the individual vulnerability value of the profile. An increase in an attribute weight will increase the individual vulnerability of the profile. Since the weights of the attributes that contribute towards vulnerability have to add up to one, an increase in one attribute weight will lower the weights of the other attributes. The generation of the weights is an issue which will require further investigation. Even though the relative frequency approach is stated in section 3.2.2, there are other approaches to generate weights. One approach is based on human perception and involves distributing a questionnaire which asks subjects about their willingness to share certain profile attributes. Another way is to use an information theory based approach to investigate how distinctive a profile attribute is.

The propositions focus on how changes in the individual and relative vulnerabilities of a profile, can impact on the overall (absolute) vulnerability of the profiles. The mathematical operators (geometric mean and arithmetical mean) used for the calculation of the relative vulnerability, highlighted the issue of a profile adding friends that have a high individual vulnerability. Propositions 3 and 4 show that if a new friend added to the neighbourhood has an individual vulnerability that is higher than or equal to the maximum individual vulnerability of the existing neighbourhood, then the relative vulnerability of the profile will

Chapter 7- Axioms, Propositions and Vulnerability Measure Properties

increase. This may increase the likelihood of the personal details of the profile spreading through the OSN.

In order for OSN users to lower their relative vulnerability, the user has to unfriend the friends who self disclose readily and have a high individual vulnerability. This finding is validated by Gundecha et al (2011) who carried out research into defining vulnerable friends and states that an *“individual is vulnerable if any friends in the network of friends has insufficient security and privacy settings to protect the entire network of friends”*.

Propositions 5 and 6 demonstrated that with the operators presented in the proposition, if the addition of a new neighbour causes the relative vulnerability to rise, then this will lead to an increase in the absolute vulnerability of the profile. The experimental work regarding the propositions highlight how important it is to use the right operators for the calculation of absolute vulnerability, in order to model the vulnerability of profiles in a realistic way. The choice of using simple weighted average functions (geometric and arithmetical means) for calculating relative vulnerability was used by Gundecha et al (2011) in their calculations which expanded their definition of vulnerable friend.

In terms of the MAX and product operators, even though product operator has a reduction effect, it is suitable in this case because the concept of vulnerability centers on the spreading of personal details of the profile through comments written by friends or friends of friends of the profile.

Concentrating on just an online relationship between a profile and its friends, if a profile is very private in terms of self disclosure and the friends are very public in terms of their disclosure, then the overall vulnerability will be quite low because there would not be many personal details to spread through the OSN

network. The MAX operator would just focus on the actions of one or more users regardless of what the other users are doing.

7.6-Conclusions

With the increase in the amount of personal details displayed on an OSN profile comes the privacy issue and the threat of social engineering attack which can make users vulnerable. Our proposed vulnerability model considers that the vulnerability of a profile can be quantified in such a way to also take into account how the behaviour of the profile's friends can impact on the vulnerability of a profile. The axioms presented have highlighted various areas that can be developed and implemented into the model in the future, to accurately reflect the vulnerability of a profile. One of the issues is incorporating the profile interaction into the model. Analysis of interactions has helped to validate that the personal details of a profile can be spread through the OSN network. This is shown by the profile's personal details being displayed in the neighbours' profile comments. Another open issue is the attribute weight and the reality of using OSNs.

The propositions which are based on the axioms, highlighted the changes in what a user present on their profile and the adding and deletion of friends into a neighbourhood which impacts on the overall profile vulnerability. The experimental work which involved investigating the effect of different operators on the overall vulnerability of a profile, demonstrated that the product operator in comparison to the MAX operator was the most effective in the absolute vulnerability calculation. This was because the product operator realistically modelled the concept of vulnerability.

CHAPTER 8: ADDITIONAL EXPERIMENTAL WORK VALIDATION

The aim of this chapter is to detail experiments used to validate the vulnerability measure, as well as investigate whether personal details of a profile, are spread through an OSN network because of the friends actions on the OSN and the implications of privacy options on the vulnerability of a profile. Facebook is an OSN which gives the profile owners the ability to set privacy options, to define which type of users (friends, friend of friend, external users) have access to different items of their personal details.

Also various mathematical operators used to calculate the relative vulnerability and absolute vulnerability will be applied to case studies, in order to explore the effects of the different operators on the relative and absolute vulnerability values.

8.1-Vulnerability Measure Validation

The concept of vulnerability in this thesis centers on the theory that an OSN profile with a high relative vulnerability will lead to an increased likelihood of the profile's friends leaking the profile's personal details. This can occur with comments that the profiles' friends write on the walls of the profile's friends of friends. The three experiments presented in sections 8.1.1-8.1.3, explore whether there is a correlation between profiles that have a high relative vulnerability and the number of comments written by the profiles' friends and the profiles' friends of friends, which disclose some of the profiles' personal details. Personal details are referred to as attributes.

8.1.1-Experiment 1: Vulnerability due to the Disclosure of the attribute values by the Neighbours.

The aim of experiment 1 is to investigate using profiles from Caverlee and Webb (2008) dataset, whether the neighbours (top *friends* and other friends that are not classed as top friends) of profiles do leak the profiles' personal details in comments **written to the profiles' top friends of top friends**. This experiment involved analysing the comments written by *top friends* and other friends (of 43,259 profiles which will act as *start profiles*) from the Caverlee and Webb (2008) dataset, to see if any of the *start profile's* personal details were disclosed. Figure 19 demonstrates some of the terminology for OSN levels that will be used to explain experiments 1,2 and 3.

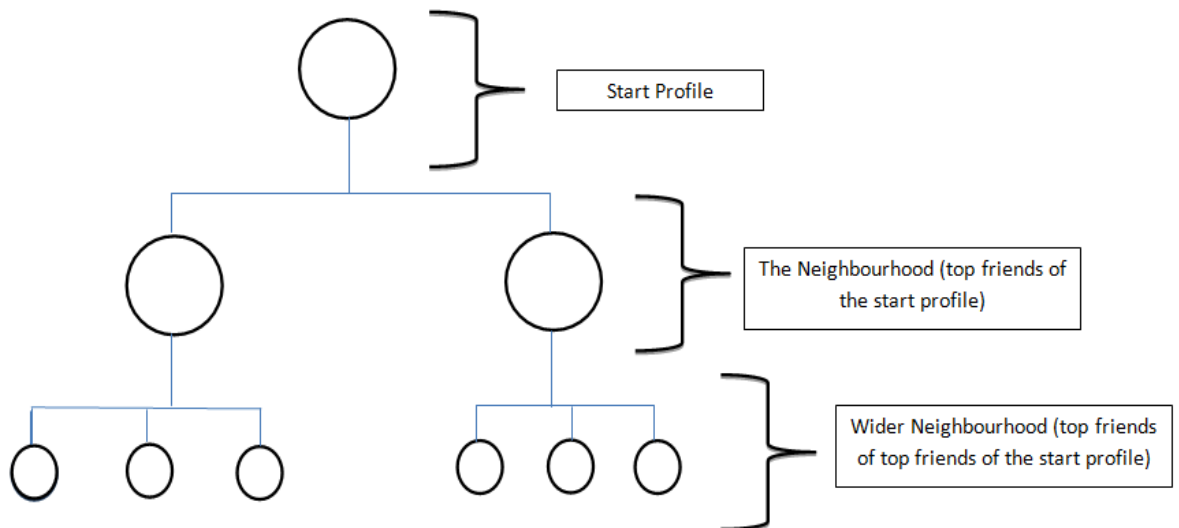


Figure 19-Terminology for Experiments 1 to 3

The **start profile** will refer to the profile whose sub network is being analysed for the leakage of its personal details by its *top friends*, other friends or wider neighbourhood. The **neighbourhood** is the friends that the *start profile* classifies as *top friends*. The **wider neighbourhood** contains the *top friends* of the neighbourhood.

Chapter 8-Additional Experimental Work Validation

For experiment 1, the focus is on the unidirectional relationship between a *start profile* and its *top friends* (the friends classed as *top friends* by the *start profile*). This is because the Caverlee and Webb (2008) dataset is a *top friends* network. When analysing the comments on the walls of the wider neighbourhood of the *start profiles*, comments made by other friends as well as top friends are examined as well. This is because it is not just *top friends* of a profile that can make the *start profile* vulnerable. Other friends of the *start profile* can write comments to the walls of the wider neighbourhood that can leak personal details of the *start profile*.

Only 43,259 profiles were used for this experiment because this was the number of *start profiles* that had their wider neighbourhoods extracted and present for analysis. Due to technical issues, the wider neighbourhoods of the rest of the profiles could not be extracted.

Also the correlation between high and heading towards high relative vulnerability profiles (0.8-1.0) and the number of comments that leak the *start profiles'* personal details is investigated to help to validate the vulnerability concept.

Unlike experiments which are explained in previous chapters, the relative vulnerability for experiment 1 is calculated using just the ***top friends of the start profile, not the friends who class the start profile as a top friend***. This is because the network is a network of *top friends* and this experiment focuses on the *top friends* that have a strong friendship with the *start profile*.

To calculate the individual vulnerability, the MySpace *start profiles* were analysed for the presence of personal information: *name, gender, profile picture, age, current location and zodiac* as well as neighbourhood features i.e. clustering coefficient and number of friends. The attribute weights which are

Chapter 8-Additional Experimental Work Validation

used in the individual vulnerability calculation were calculated based on the relative frequency of the attributes in the dataset. The relative vulnerability was calculated using the arithmetical mean operator which is illustrated in equation 17 in section 6.2 and the absolute vulnerability which was calculated using the product operator in equation 13 in section 3.2.4.

Also for the 43,259 MySpace *start profiles*, the comments from the walls of the wider neighbourhood of the *start profiles* were examined to see if any of the comments written by the *start profiles'* neighbourhood, leaked personal details of the *start profile* itself. This was done in an automated way by developing a program which analysed the comments that were written by the *start profiles'* neighbourhood and other friends on the walls in the wider neighbourhood. These comments were analysed for the presence of some of the *start profiles'* personal details.

Personal details that appear in comments on the walls in the wider neighbourhood can be seen by other users (friends of friends of the neighbourhood and external users if the OSN profiles in the wider neighbourhood are very public in terms of privacy.

If the *start profile's* personal details appear in the wider neighbourhood walls which are posted by the *start profiles'* neighbourhood , then this shows that the personal details of the *start profile* are propagating through the OSN network and can be seen by other users. Also it shows that vulnerability does exist regarding OSN profiles.

The results from experiment 1 indicated that some *start profiles* that had high relative vulnerabilities (0.9 or above), had leakage of personal details about the *start profiles*, in the comments written by the neighbourhoods . The comments appeared in walls of the wider neighbourhood of the *start profiles*. This showed

Chapter 8-Additional Experimental Work Validation

that as well as the top friends self disclosing their own details readily, some of them were talking about the *start profile*. Out of the 43,259 selected *start profiles*, 32.1% of the profiles had a high relative vulnerability (0.9-1.0). In terms of personal detail disclosure:

- 0% of the MySpace *start profiles* with high relative vulnerabilities contained profile neighbours (*top friends* including other friends) that had mentioned the *birthday* of the *start profile* owner, in the comments made to the wider neighbourhood. Out of these *start profiles*, the average number of comments disclosing the *birthday* was 0.
- 51.2% of the MySpace *start profiles* with high relative vulnerabilities contained profile neighbours (*top friends* including other friends) that had disclosed the *name* of the *start profile* owner, in the comments made to the wider neighbourhood. Out of these *start profiles*, the average number of comments disclosing the *name* was 10.2.
- 0% of the MySpace *start profiles* with high relative vulnerabilities contained profile neighbours (*top friends* including other friends) that had disclosed the *age* of the *start profile* owner, in the comments made to the wider neighbourhood. Out of these *start profiles*, the average number of comments disclosing the *age* was 0.
- 21.6% of the MySpace *start profiles* with high relative vulnerabilities contained profile neighbours (*top friends* including other friends) that had disclosed the *current location* of the *start profile* owner, in the comments made to the wider neighbourhood. Out of these *start profiles*, the average number of comments disclosing the *current location* was 23.5.
- 0.7% of the MySpace *start profiles* with high relative vulnerabilities contained profile neighbours (*top friends* including other friends) that had

Chapter 8-Additional Experimental Work Validation

disclosed the *education* of the *start profile* owner, in the comments made to the wider neighbourhood. Out of these *start profiles*, the average number of comments disclosing the *education* was 35.8.

- 8.8% of the MySpace *start profiles* with high relative vulnerabilities contained profile neighbours (top *friends* including other friends) that had disclosed the hometown of the *start profile* owner, in the comments made to the wider neighbourhood. Out of these profiles, the average number of comments disclosing the *hometown* was 4.46.
- 40.2% of the MySpace *start profiles* with high relative vulnerabilities contained profile neighbours (top *friends* including other friends) that disclosed no attributes (personal details) of the *start profile* owner in the comments made to the wider neighbourhood.

The results above illustrated that top *friends* including other friends of *start profiles* which have a high relative vulnerability (collective individual vulnerability of the top friends of the *start profile*), do leak the *start profiles'* personal details in the interactions with the wider neighbourhood. In this case the interactions comments are written on the walls based in the wider neighbourhoods.

These findings are validated by Ho et al. (2009) and Gundecha et al (2011) observations that profile users cannot prevent personal information about themselves from being uploaded and spread by their friends.

To investigate if there was a relationship between the number of comments written by the *start profiles'* neighbourhood, who leaked the *start profiles'* personal details and the relative vulnerability of the *start profiles* being analysed, statistical analysis was used to derive the correlation between the two variables. This was in order to test the following hypothesis:

Chapter 8-Additional Experimental Work Validation

H₁- The number of comments which appear on the walls of the wider neighbourhoods and disclose some of the personal details of the *start profiles* increases as the relative vulnerability of the *start profiles* increases.

whereas the null hypothesis is that:

H₀- There is no significant relationship between the number of comments which appear on the walls of the wider neighbourhoods and discloses some personal details of the *start profile* and the relative vulnerability of the *start profiles*.

To approve or disprove the hypothesis H₁, Spearman Rank which is illustrated in equation 36 was used to correlate *start profiles* that have a relative vulnerability greater than 0.8 against the number of comments present in the wider neighbourhood walls which disclose some personal details of the *start profiles*.

The value of 0.8 and above is used for correlation because there needs to be a suitable scale of increase in values of relative vulnerability. In this case, the scale covers *start profiles* which are heading towards having a high relative vulnerability (0.8) and having a high relative vulnerability (0.9 and above).

$$r = 1 - \frac{6 \sum_{i=1}^n d_i^2}{n^3 - n} \quad (36)$$

where r is the Spearman Rank coefficient, n is the set of observations for variables x and y , and d_i is the difference between the i -th rank of x and the i -th rank of y .

Chapter 8-Additional Experimental Work Validation

			Relative Vulnerability	No of comments that mention birthday	No of comments that disclose name	No of comments that disclose age	No of comments that disclose current location	No of comments that disclose education	No of comments that disclose hometown
Spearman's rho	Relative Vulnerability	Correlation Coefficient	1.000	.	.025**	.	.001	.004	-.010
		Sig. (2-tailed)	.	.	.001	.	.927	.633	.218
		N	16223	16223	16223	16223	16223	16223	16223
	No of comments that mention birthday	Correlation Coefficient
		Sig. (2-tailed)
		N	16223	16223	16223	16223	16223	16223	16223
	No of comments that disclose name	Correlation Coefficient	.025**	.	1.000	.	.028**	.003	.055**
		Sig. (2-tailed)	.001000	.722	.000
N		16223	16223	16223	16223	16223	16223	16223	
No of comments that disclose age	Correlation Coefficient	
	Sig. (2-tailed)	
	N	16223	16223	16223	16223	16223	16223	16223	
No of comments that disclose current location	Correlation Coefficient	.001	.	.028**	.	1.000	.050**	.362**	
	Sig. (2-tailed)	.927	.	.000	.	.	.000	.000	
	N	16223	16223	16223	16223	16223	16223	16223	
No of comments that disclose education	Correlation Coefficient	.004	.	.003	.	.050**	1.000	.063**	
	Sig. (2-tailed)	.633	.	.722	.	.000	.	.000	
	N	16223	16223	16223	16223	16223	16223	16223	
No of comments that disclose hometown	Correlation Coefficient	-.010	.	.055**	.	.362**	.063**	1.000	
	Sig. (2-tailed)	.218	.	.000	.	.000	.000	.	
	N	16223	16223	16223	16223	16223	16223	16223	

** . Correlation is significant at the 0.01 level (2-tailed).

Figure 20-Correlation between High Relative Vulnerability Profiles and Attribute Disclosure by Profiles' Neighbourhood

The results in Figure 20, show that the attributes *name*, *current location* and *education* have a weak positive relationship. A positive relationship signifies that as the relative vulnerability of the *start profiles* increases from 0.8 to 1.0 (full vulnerability), the amount of comments which disclose the personal details of the *start profile* increases. Even though the correlation is weak, the attribute *name* has a significant and meaningful correlation. The attribute *hometown* has a weak negative correlation which implies that as the relative vulnerability increases from 0.8 to 1.0, the amount of comments which disclose the *hometown* of the *start profile* decreases.

Overall in this experiment, the results have shown that there are instances where personal details of a *start profile* can be spread by the profiles' neighbours in their interactions. Therefore vulnerability does exist in OSN profiles.

Chapter 8-Additional Experimental Work Validation

Correlation has been shown even with initial data available because Caverlee and Webb (2008) only extracted the first page of comments. The Caverlee and Webb dataset is a well used and established dataset and has been used for studying of the characteristics of MySpace in terms of who uses the network and how the networks is being used. Also language models were constructed from the wall comments of MySpace users. Researchers who have referred to work carried out by Caverlee and Webb (2008) with their dataset have included Gauvin et al (2010) who extended Caverlee and Webb (2008) work on analysis of word frequencies from MySpace wall comments which were grouped by gender and age, by analysing patterns in other posted content i.e. images and hyperlinks.

The investigation into the relationship between the high relative vulnerability of some of the *start profiles* and number of comments disclosing certain personal details of the *start profiles*, showed that even though a weak positive relationship existed between the two variables, a relationship did exist. Top friends who self disclose readily can contribute towards an increase in information disclosure of some of the *start profiles* attributes.

Out of all the attributes, the *start profile* owners' *name* was the most popular attribute to be leaked. This attribute also had a significant weak positive correlation between the relative vulnerability of the *start profiles* and the number of comments that leaked the *name* of the *start profile* owner. The surprising finding was that the attributes *birthday* and *age* were not leaked at all.

The reason being that adolescents and young people like to talk about their social lives and this can include going to birthday parties. Another reason being that when the software was built to analyse the number of comments that disclosed certain personal details of the *start profile*, the *name* of the *start*

profile owner had to be present in the comment as well as the *age* or *birthday*.

This was in order to add meaning. If just the words happy birthday were extracted, it may not correspond to the start *profile*'s birthday.

8.1.2-Experiment 2: Vulnerability due to the Disclosure of the attribute values by the Friends of Friends

The aim of experiment 2 is to investigate if there is any correlation between high relative vulnerability *start profiles* and the amount of personal details of the *start profile* that are spread and appear on the walls in the neighbourhood rather than the wider neighbourhood. In this experiment, the neighbourhood of a *start profile*, consist of *top friends* that the *start profile* classes as *top friends* and the *top friends* that class the *start profile* as one of their *top friends*. For this experiment (Alim et al. 2011a) the individual, relative and absolute vulnerability were calculated for 100 random MySpace *start profiles* from the Caverlee and Webb (2008) dataset.

As in experiment 1, the MySpace *start profiles* were analysed for the presence of personal information: *name, gender, profile picture, age, current location and zodiac* as well as the neighbourhood features i.e. clustering coefficient and the number of friends. The weights in the individual vulnerability were calculated based on the relative frequency of the attributes in the dataset. The relative vulnerability was calculated using the arithmetical mean operator which is illustrated in equation 17 in section 6.2 and the absolute vulnerability was calculated using the product operator in equation 13 in section 3.2.4. Also for the 100 MySpace *start profiles*, the comments on the neighbourhood walls were examined manually, to see if any of the comments written by the *start profiles*' friends of friends leaked information about the *start profile* itself. Personal details of the *start profiles* which are leaked in the walls based in the neighbourhoods , can be seen by other users (friends of friends of the

Chapter 8-Additional Experimental Work Validation

neighbourhood and external users if the profiles in the neighbourhood are very public in terms of privacy). If the *start profile*'s personal details appear in the neighbours' wall comments, then this indicates that the personal details of the *start profile* are spreading through the OSN because the *friends of friends*, who may not have a friendship link with the *start profile*, have written the comments. Other reasons maybe that the wider neighbourhood and the *start profile* may have a stronger offline relationship.

The results from this experiment indicated that some neighbours from neighbourhoods, of *start profiles* that had high relative vulnerabilities (0.9 or above), had personal details about the *start profile* in their walls. Out of the 100 *start profiles* which were analysed manually, 47% of them had a high relative vulnerability (0.9-1.0) and there was interaction between the neighbours and the *start profile* considered. In terms of personal detail disclosure:

- 14.8% of the MySpace *start profiles* with high relative vulnerabilities contained neighbours that had mentioned, the *birthday* of the *start profile* owner in their comments. Out of these *start profiles*, the average number of comments disclosing the *birthday* was 1.14.
- 68% of the MySpace *start profiles* with high relative vulnerabilities contained neighbours that that had the *name* of the *start profile* owner displayed in their comments. Out of these *start profiles*, the average number of comments disclosing the *name* was 1.53.
- 4.25% of the MySpace *start profiles* with high relative vulnerabilities contained neighbours that had the *age* of the *start profile* owner in their comments. Out of these *start profiles*, the average number of comments disclosing the *age* was 1.

Chapter 8-Additional Experimental Work Validation

- 25.3% of the MySpace *start profiles* with high relative vulnerabilities contained neighbours that had the *current location* of the *start profile* owner in their comments. Out of these *start profiles*, the average number of comments disclosing the *current location* was 1.08.
- 17.0% of the MySpace *start profiles* with high relative vulnerabilities contained neighbours that had the *education* of the *start profile* owner displayed in their comments. Out of these *start profiles*, the average number of comments disclosing the *education* was 1.25.
- 8.51% of the MySpace *start profiles* with high relative vulnerabilities contained neighbours that had the *hometown* of the *start profile* owner displayed in their comments. Out of these *start profiles*, the average number of comments disclosing the *hometown* was 1.

To investigate if there is a relationship between the amount of information disclosure of the *start profiles*' personal details in the neighbours walls and the relative vulnerability of the *start profiles* being analysed, statistical analysis was used to derive the correlation between the two variables. To evaluate whether the *start profiles*' personal details spread through the network, for this experiment, the vulnerability theory is based around the following hypothesis:

H₁- The number of comments which appear on the neighbours' walls that leak the personal details of the *start profile* increases as the relative vulnerability of the *start profiles* increases.

whereas the null hypothesis is that:

H₀- There is no significant relationship between the number of comments which appear on the neighbours' walls that leak the *start profiles*' personal details and the relative vulnerability of the *start profiles*.

Chapter 8-Additional Experimental Work Validation

To approve or disprove the hypothesis H_1 , Spearman Rank which is illustrated in equation 36 was used to correlate *start profiles* that have a relative vulnerability greater than 0.8 to allow for a suitable increase of V_R against the amount of information disclosure for certain attributes in the comments present on the neighbours' wall.

			Relative	No of Name	No of Birthday	No of Age	No of Current Location	No of Education	No of hometown
Spearman's rho	Relative	Correlation Coefficient	1.000	.128	-.118	.032	.370*	.102	.089
		Sig. (2-tailed)		.392	.431	.833	.010	.497	.554
		N	47	47	47	47	47	47	47
No of Name	No of Name	Correlation Coefficient	.128	1.000	.083	-.088	.018	.134	.114
		Sig. (2-tailed)	.392		.579	.556	.907	.368	.447
		N	47	47	47	47	47	47	47
No of Birthday	No of Birthday	Correlation Coefficient	-.118	.083	1.000	-.127	.155	.081	.356*
		Sig. (2-tailed)	.431	.579		.395	.298	.589	.014
		N	47	47	47	47	47	47	47
No of Age	No of Age	Correlation Coefficient	.032	-.088	-.127	1.000	.113	-.095	-.064
		Sig. (2-tailed)	.833	.556	.395		.450	.525	.668
		N	47	47	47	47	47	47	47
No of Current Location	No of Current Location	Correlation Coefficient	.370*	.018	.155	.113	1.000	.121	.037
		Sig. (2-tailed)	.010	.907	.298	.450		.419	.805
		N	47	47	47	47	47	47	47
No of Education	No of Education	Correlation Coefficient	.102	.134	.081	-.095	.121	1.000	-.138
		Sig. (2-tailed)	.497	.368	.589	.525	.419		.356
		N	47	47	47	47	47	47	47
No of hometown	No of hometown	Correlation Coefficient	.089	.114	.356*	-.064	.037	-.138	1.000
		Sig. (2-tailed)	.554	.447	.014	.668	.805	.356	
		N	47	47	47	47	47	47	47

*. Correlation is significant at the 0.05 level (2-tailed).

Figure 21-Correlation between High Relative Vulnerability Profiles and Attribute Disclosure by Profiles' Friends of Friends for a Small Profile Sample

The results displayed in Figure 21 highlighted that the attributes: *name*, *age*, *education* and *hometown* have weak positive relationships. A positive relationship signifies that as the relative vulnerability of the *start profiles* increase, so does the amount of disclosure of the *start profiles'* personal details contained in the neighbourhood wall comments.

The relationships involving the attributes mentioned are not significant because the significance value is greater than .05. The attribute *current location* on the other hand has a significant medium positive relationship. This shows that as

Chapter 8-Additional Experimental Work Validation

the relative vulnerability of the *start profiles* increase, the number of neighbours' comments that the *current location* of the profile is disclosed in, increases as well. A higher relative vulnerability value for a *start profile* demonstrates that the profiles' neighbours display their personal details publically and this can increase the likelihood of the personal details of the profile spreading through the OSN and contributing towards privacy and social engineering attacks.

The attribute *birthday* has a weak negative relationship that shows that as the relative vulnerability of the *start profiles* increases, the number of times the *birthday* of the profile is mentioned in the neighbours' comments decreases.

The presence of a weak positive relationship for some of the attributes is a good outcome for this experiment to validate the spreading of profiles' personal details because it demonstrates that personal details can spread though an OSN and can be seen by other users.

8.1.3-Experiment 3: Vulnerability of Larger Dataset due to the Disclosure of the attribute values by the Friends of Friends

The aim of experiment 3 is to repeat experiment 2 but with a larger sample of *start profiles* and concentrating on the unidirectional relationship between a *start profile* and its *top friends*. The experiment was repeated with 76,662 random MySpace *start profiles* from the Caverlee and Webb (2008) dataset. Out of these profiles, 35,123 (45.8%) had a high relative vulnerability (0.9 and above) and the comments from the neighbours' walls were extracted and analysed in an automated way, in comparison to experiment 2 which was done manually. Also like experiment 1, only the *top friends* classed by the *start profile*, were analysed for their comments. From the high relative vulnerability profiles:

- 23.6% of the *start profiles* with high relative vulnerabilities contained neighbours that had mentioned, the *birthday* of the *start profile* owner in

Chapter 8-Additional Experimental Work Validation

their wall comments. Out of these *start profiles*, the average number of comments mentioning the *birthday* was 4.94.

- 8.9% of the *start profiles* with high relative vulnerabilities contained neighbours that had the *name* of the *start profile* owner in their wall comments. Out of these *start profiles*, the average number of comments disclosing the *name* was 3.04.
- 0% of the *start profiles* with high relative vulnerabilities contained neighbours that had the *age* of the *start profile* owner in their walls comments.
- 2.0% of the *start profiles* with high relative vulnerabilities contained neighbours that had the *current location* of the *start profile* owner in their wall comments. Out of these profiles, the average number of comments disclosing the *current location* was 11.5
- 1.1% of the *start profiles* with high relative vulnerabilities contained neighbours that had the *education* of the *start profile* owner in their wall comments. Out of these profiles, the average number of comments disclosing the *education* was 3.73.
- 0.13% of the *start profiles* with high relative vulnerabilities contained neighbours that had the *hometown* of the *start profile* owner in their wall comments. Out of these profiles that average number of comments disclosing *hometown* was 3.76.

The results contribute towards justifying that personal details about the *start profile* can spread via the comments that a friend of a friend writes on the *start profiles'*neighbours' wall.

An interesting aspect of this area is that in some OSNs (e.g. Facebook), each profile has an activity stream which records the interaction of the profile owner

Chapter 8-Additional Experimental Work Validation

(e.g. the contents of the comments that the profile owner writes in response to status changes, photo comments or profile comments on their neighbours' profiles). If these profiles were Facebook profiles then the personal details of the profiles could spread even further through the OSN network. This is because unlike MySpace, the interaction in Facebook appears on the activity stream. With Facebook, when a profile owner posts a status on their profile, they may react to any comments about the status made by their friends, on their own profile rather than posting a comment on their friends' profile. This means that a lot of interaction about the profile owner can take place on the profile owner's own profile.

For experiment 3, to correlate *start profiles* approaching high relative vulnerability and high relative vulnerability (V_R of 0.8 and above) against the amount of information disclosure of certain personal details of the *start profile* by the profile's '*friend of a friend*', Spearman Rank was again used. The results for this dataset which are illustrated in Figure 22, show that the attributes *birthday* and *name* have significant weak positive relationships.

Chapter 8-Additional Experimental Work Validation

			Relative Vulnerability	Birthday Disclosed	Name Disclosed	Age Disclosed	Current Location Disclosed	Education Disclosed	Hometown Disclosed
Spearman's rho	Relative_Vulnerability	Correlation Coefficient	1.000	.062**	.045**	.	.002	-.010*	-.010*
		Sig. (2-tailed)	.	.000	.000	.	.672	.030	.038
		N	45645	45645	45645	45645	45645	45645	45645
	Birthday_Disclosed	Correlation Coefficient	.062**	1.000	.102**	.	.015**	-.058**	-.020**
		Sig. (2-tailed)	.000	.	.000	.	.001	.000	.000
		N	45645	45645	45645	45645	45645	45645	45645
	Name_Disclosed	Correlation Coefficient	.045**	.102**	1.000	.	.025**	.018**	.020**
		Sig. (2-tailed)	.000	.000	.	.	.000	.000	.000
		N	45645	45645	45645	45645	45645	45645	45645
	Age_Disclosed	Correlation Coefficient	.	.	.	1.000	.	.	.
		Sig. (2-tailed)	1.000	.	.
		N	45645	45645	45645	45645	45645	45645	45645
	Current_Location_Disclosed	Correlation Coefficient	.002	.015**	.025**	.	1.000	-.009*	-.001
		Sig. (2-tailed)	.672	.001	.000	.	.	.047	.803
		N	45645	45645	45645	45645	45645	45645	45645
	Education_Disclosed	Correlation Coefficient	-.010*	-.058**	.018**	.	-.009*	1.000	.220**
		Sig. (2-tailed)	.030	.000	.000	.	.047	.	.000
		N	45645	45645	45645	45645	45645	45645	45645
	Hometown_Disclosed	Correlation Coefficient	-.010*	-.020**	.020**	.	-.001	.220**	1.000
		Sig. (2-tailed)	.038	.000	.000	.	.803	.000	.
		N	45645	45645	45645	45645	45645	45645	45645

** . Correlation is significant at the 0.01 level (2-tailed).

* . Correlation is significant at the 0.05 level (2-tailed).

Figure 22-Correlation between High Relative Vulnerability Profiles and Attribute Disclosure by Profiles' Friends of Friends for Bigger Profile Sample

The correlation between relative vulnerability and number of comments that disclose a *start profiles'* personal details may be weak because Caverlee and Web (2008) only extracted the first page of profile comments from each MySpace *start profile*, so there could have been comments that the profiles' personal details were leaked in. Also the fact that this experiment looks at the *friend of friend* relationship. The profile and the *friend of a friend* are not directly linked through friendship.

Some neighbours of *start profiles* can be privacy aware and know not to display personal details in comments written to other friends and so refer to their friends by using nick names. What the results do show is that as the *top friends* self disclose some of their personal details, the profiles' *'friends of friends'* can leak the *start profiles* personal details in interactions made with the start profiles' neighbourhood and if MySpace had activity streams then this would increase

Chapter 8-Additional Experimental Work Validation

the vulnerability of the *start profile*. Consequently the personal details of the *start profile* would spread through the network.

The *start profile* owners' *age* was not disclosed in any of the comments on the neighbours' walls but the *age* can be derived from the *birthday* of the *start profile* owner. Apart from *age*, the attribute *current location* was the only attribute to not have a significant positive or negative relationship with other attributes.

Overall the validation experiments have shown that the concept of the vulnerability theory has been born out of practice. There are signs that as the V_R of the *start profile* increases, the neighbours of the *start profiles* profile become more public with their disclosure of personal details and there can be an increase in the number of comments written by the neighbours of the *start profile*, which leak the personal details of the *start profile*.

Experiment 1 demonstrated the concept of vulnerability does exist and personal details can spread through the OSN due to the actions of the *start profiles'* neighbours. In the experiment, the attributes *age* and *birthday* were not leaked but the attributes *name*, *current location*, *education* and *hometown* were. In terms of the correlation between *start profiles* heading towards high relative vulnerability or high relative vulnerability (0.9+), and the number of comments that disclose certain attributes of the *start profile*, most of the attributes have a weak positive correlation. The attribute *name* displays a significant and meaningful weak correlation.

The reason behind a weak correlation may be that the vulnerability measure in its current state does not factor in the strength of psychology between the neighbours. Some neighbours who may display their personal details readily on a MySpace profile may not interact online regularly with the *start profile* and this

Chapter 8-Additional Experimental Work Validation

can be seen by a low number of profile comments written between them. They may have a stronger offline relationship with their friends. Also only the first page of comments for each profile was extracted by Caverlee and Webb (2008) and the network was a top friends network so only the individual vulnerabilities of these profiles were calculated for the relative vulnerability, rather than all the friends of the *start profile*.

Experiments 2 and 3 highlighted that a '*friend of friend*' of a *start profile* can make that profile vulnerable. Popular attributes leaked according to the statistical work included *name and current location*.

8.2-Privacy Levels

The levels of privacy play an important part in some OSNs and the control of personal details. In May 2010, Facebook introduced a set of simpler privacy controls which allowed profile owners to control who sees their personal details and give profile owners the ability to turn off applications, so their personal details can't be viewed without consent (BBC News 2010a). The three main categories for privacy controls are everyone, friends only and friends of friends. Also privacy controls can be customised according to the profile owner.

This section extends the work done in section 5.4 by incorporating the disclosure of the personal details into the concept of OSN levels. The aim of this first experiment is to investigate a small Facebook network to analyse the amount of a '*friend of a friend*' personal details, the start profile can view. An example to illustrate this concept is that profile X and profile Y are friends and so are profile Y and profile Z. The aim is to investigate how much of profile Z's personal details, profile X can view. Profile X and Z are not friends directly and this will give a better idea about the levels of privacy that profile owners have set their profiles to.

Chapter 8-Additional Experimental Work Validation

Any data that is extracted from Facebook (or any other OSN) whether manually or automated and used for analysis will be destroyed after the PhD has been finished. This is because, if the data was kept beyond the PhD then it can be perceived that we may be facilitating the spread of personal details of the profiles. Also it would contravene one of the Data Protection Act principles which states that data can be only kept for as long as needed.

For this experiment the following methodology was carried out to build up a Facebook network to experiment on:

1. A profile in a small Facebook network was selected. This acts as the *start profile*
2. The *start profile's* 70 neighbours (friends of the *start profile*) were selected.
3. For each of the neighbours, 10 of the neighbours' friends were randomly selected and were analysed for the personal details that were presented and viewable to the *start profile*. This means that 700 profiles were analysed altogether.

Also if the neighbours' friends' walls could be viewed by the *start profile*, then the comments in the wall made since January 2011 were analysed for presence of some of the neighbours' personal details. The wall for each profile in Facebook consists of an activity stream which contains the interaction regarding a profile (list of profiles' statues, what the profile owner wrote on their friends profile walls, who the profile owner added as a friend and what the friends wrote on the profile owner's wall).

The results based on what the *start profile* (who was not directly linked but who is friends with the neighbour) can view, regarding the attributes present in walls

Chapter 8-Additional Experimental Work Validation

in the wider neighbourhood (which in this case contains neighbours' friends), are presented below in Table 7.

Table 7-Percentage of Disclosure of Attributes Viewable to the Start Profile

Attribute	% of profiles whose attribute is viewable to the start profile
Full Name	100
Gender	78
Profile Picture	74.4
Date of Birth	15.4
Current Location	34.8
Hometown	25.1
Email Address	2.5
Education Details	22.2
List of friends	56.1
Profile Walls	11.4

Out of the 11.4 % of the neighbours' friends who had their walls public for the *start profile* to see:

- 191 comments disclosed the *name* of the neighbour .
- 2 comments disclosed a *photo* of the neighbour
- 2 comments disclosed the *birthday* of the neighbour.
- 10 comments disclosed the *current location* of the neighbour.
- 6 comments disclosed the *hometown* of the neighbour .
- 5 comments disclose *family information* of the neighbour .

The presence of the neighbours' details in the walls of the other friends demonstrates that the neighbours' personal details can spread through OSN levels due to the actions of some of the neighbours' friends, in making their profiles public. If the profiles are very public then external users or *friends of friends* of the neighbours can view the wall contents.

Schrammel et al. (2009) results from a study into information disclosure involving friends and unknown persons can be used to compare to the results presented in Table 7. Schrammel et al. (2009) study involved developing and

Chapter 8-Additional Experimental Work Validation

distributing an online questionnaire about information disclosure behaviour. 856 people answered the questionnaire and the results highlighted the following in terms of disclosure to an unknown person.

- 55.0% of the users reveal their *full name* to an unknown person when using OSNs
- 65.7% of the users reveal their *profile picture* to an unknown person when using OSNs
- 42.6% of the users reveal their *birthday* to an unknown person when using OSNs.
- 39.8% of the users reveal their *friends list* to an unknown person when using OSNs.
- 12.5 % of the users reveal their *email address* to an unknown person when using OSNs.
- 2.8% of the users reveal their current address to an unknown person when using OSNs.

In terms of the experiment involving the small Facebook network, the *start profile* can count as an unknown person because the *start profile's* wider neighbourhood does not know the *start profile* directly and no friendship link exists.

Even though the results from Schrammel et al. (2009) are from questionnaire responses in 2008 which focus OSNs in general, not just a specific OSN, there are some interesting comparisons. The disclosure of *full name* is higher in the results in Table 7 because the results just focus on Facebook in which most users readily disclose their real personal details. On the other hand Schrammel et al. (2009) results takes into account a variety of OSNs and is based on human responses rather than analysing the profile manually. With some OSNs

Chapter 8-Additional Experimental Work Validation

i.e. MySpace, some users commonly use nicknames as their main identity with their real names being mentioned in profile contents.

Facebook is different to MySpace when it comes to interaction and privacy. If a MySpace profile is private then the profile's interaction can't be viewed, where as a Facebook profile has more control over what can be shown on a profile. An example being that the profile owner may display only their *name* and their profile wall (which contains the interactions between them and their friends), but not any of their other personal details.

Schrammel et al. (2009) results for the users claimed to have disclosed birthday were higher because in 2008 some OSNs did not offer the users adequate privacy controls in terms of who could see what. Some OSNs (e.g. MySpace) displayed the *age* and *zodiac sign* rather than the *birthday*.

For the attribute *current location*, the results in Table 7 are higher and one of the reasons maybe due to the introduction of applications (e.g. Foursquare) which can transmit the *current location* of the user.

In terms of displaying the list of friends, the results in Table 7 are significantly higher because in Facebook even with the privacy controls, some users still want to be found and don't think that displaying the list of friends causes any privacy issues. Also with some OSNs (e.g. MySpace) where the user has defined their profile as private, the friends list cannot be seen. Some users may not like to admit in Schrammel et al. (2009) questionnaire that their networks of friends is available to unknown users and therefore lie to protect their privacy.

Schrammel et al. (2009) results have demonstrated that even back in 2008, profile owners claimed their profiles were open for unknown users to view their personal details. What the results in Table 7 have shown is despite the

Chapter 8-Additional Experimental Work Validation

introduction of privacy controls, there are still profiles that are publically open and available to view. This indicates that more responsibility needs to be taken by the OSNs to remind users about the privacy controls and the consequences of making your profiles too public.

Overall the results in this section have shown that in the case of this Facebook network, some of the profiles in the *start profile*'s wider neighbourhood have not used the privacy controls effectively. A *start profile* who does not have a friendship link to the wider neighbourhood can view some of the personal details of the wider neighbourhood including interactions made because of how public their OSN profiles including the walls are.

In this experiment the user who is able to view some of the public walls of the wider neighbourhood, is known to the neighbour but what if the user is not known to the neighbour or the wider neighbourhood i.e. an external user who is a Facebook user and has no friendship connections to the Facebook network used in this experiment.

8.2.1-Privacy levels and Vulnerability

The aim of this next experiment is to extend the experimental work using the small Facebook network detailed in section 8.2, by incorporating the vulnerability concept detailed in this thesis into the experiment and investigating if there is a relationship between the relative vulnerability value of the neighbours of the *start profile* and the amount of disclosure of the neighbours' personal details by the neighbours' friends, whose profiles are viewable to an external user.

An external user in the case of this experiment is a Facebook user (*Start profile*) who does not have any connections to the network used in this experiment. This is in contrast to the previous experiment in section 8.2 where there was a

Chapter 8-Additional Experimental Work Validation

link between the user and the neighbour but not between the user and the wider neighbourhood (friends of the neighbours). A fake Facebook profile which represents the external user was set up and the neighbours' friends' were visited using the fake profile.

In regards to this experiment, the vulnerability of the *start profile's* neighbours was calculated. The individual vulnerability calculated the vulnerability of each of the neighbours' profiles on their own whilst the relative vulnerability of the neighbours calculated the collective vulnerability of the neighbours' friends. The Facebook profiles representing the neighbours and the neighbours' friends were analysed for the presence of the attributes *name, gender, profile picture, date of birth, location, hometown, email address, education and the number of friends*.

The attribute weights for this experiment were calculated using the statistical approach derived from the results of the online questionnaire that is detailed in section 3.41. Using this approach for the calculation, the attributes *name, gender, profile picture, date of birth, current location, email address and number of friends* were classed as very important. *Hometown* and *education* were classed as important.

With the results of the vulnerability calculation, the highest relative vulnerability value of the neighbours' profiles was only 0.6125. This is because the individual vulnerability of the neighbours' friends varies in value as well as the weights of the attributes. Some of the friends are more private about their personal details than other friends. 11.4% of the neighbours have a relative vulnerability of 0.5 and above.

Out of all of the 70 neighbours regardless of the V_R value, 72.8% of the neighbours, contain 1 or more friends that have a wall which can be seen by an external user with no direct friendship connection with the neighbour or the

Chapter 8-Additional Experimental Work Validation

neighbours' friends. This result demonstrates how vulnerable the actions of a friend can make you.

It is these neighbours which were taken into account when correlating the relative vulnerability of the neighbours' against the amount of disclosure (number of comments) of the neighbours' personal details leaked on the walls in the wider neighbourhood, which are viewable and public to an external user. The walls contain the activity stream. Spearman Rank was used for the correlation.

			Relative Vulnerability
Spearman's rho	Relative Vulnerability	Correlation Coefficient Sig. (2-tailed) N	1.000 . 51
	No of name disclosed	Correlation Coefficient Sig. (2-tailed) N	.079 .580 51
	No of gender disclosed	Correlation Coefficient Sig. (2-tailed) N	. . 51
	No of profile picture/photos disclosed	Correlation Coefficient Sig. (2-tailed) N	-.183 .199 51
	No of date of birth disclosed	Correlation Coefficient Sig. (2-tailed) N	.052 .719 51
	No of location disclosed	Correlation Coefficient Sig. (2-tailed) N	.177 .214 51
	No of home disclosed	Correlation Coefficient Sig. (2-tailed) N	-.032 .823 51
	No of email disclosed	Correlation Coefficient Sig. (2-tailed) N	. . 51
	No of education disclosed	Correlation Coefficient Sig. (2-tailed) N	. . 51

Figure 23-Correlation between Neighbours with Various Relative Vulnerabilities and Neighbours' Personal Details Disclosure

Figure 23 shows correlation results for the *start profile's* neighbours that have various relative vulnerability values, which range from high to low. The results of

Chapter 8-Additional Experimental Work Validation

the correlation show that even though there are no significant relationships between the relative vulnerability of the *start profiles* neighbours and the number of comments present on public walls which leak some of the neighbours' attributes, some attributes (e.g. *name, date of birth and current location*) have a weak positive relationship as the relative vulnerability values increases.

The positive relationship indicates that as the neighbours' friends self disclose more attributes that contribute towards vulnerability (increase in relative vulnerability of the neighbours), there is an increase in the number of comments present on the walls of the neighbours' friends, which leak the neighbours' personal details and these walls can be viewed by an external user.

Reasons for the positive relationship being weak include the fact that only 10 of the neighbours' friends profiles were analysed for each neighbour but not all of the neighbours friends profile walls were publically available for the external user to view. Also only reciprocated friends for each neighbour were analysed. This means that both the neighbour and the friend consented to the friendship.

Figure 24 shows the correlation results but just for the neighbours with high relative vulnerabilities (0.5 and above) in this dataset. The analysis of neighbours with high relative vulnerabilities links in with the vulnerability concept detailed in this thesis. In terms of this experiment and vulnerability theory, higher relative vulnerability relates to an increased likelihood that one or more profiles in the wider neighbourhood of the *start profile*, will disclose personal details of the neighbours to its friends.

Regarding this experiment, the addition to the vulnerability theory involves the use of OSN levels, by analysing the amount of personal details of the neighbour which is leaked by the neighbour's friends and is viewable by an external user.

Chapter 8-Additional Experimental Work Validation

			Relative Vulnerability
Spearman's rho	Relative Vulnerability	Correlation Coefficient	1.000
		Sig. (2-tailed)	.
		N	6
	No of name disclosed	Correlation Coefficient	.103
		Sig. (2-tailed)	.846
		N	6
	No of gender disclosed	Correlation Coefficient	.
		Sig. (2-tailed)	.
		N	6
	No of profile picture/photos disclosed	Correlation Coefficient	.
	Sig. (2-tailed)	.	
	N	6	
No of date of birth disclosed	Correlation Coefficient	.	
	Sig. (2-tailed)	.	
	N	6	
No of location disclosed	Correlation Coefficient	.315	
	Sig. (2-tailed)	.543	
	N	6	
No of home disclosed	Correlation Coefficient	.	
	Sig. (2-tailed)	.	
	N	6	
No of email disclosed	Correlation Coefficient	.	
	Sig. (2-tailed)	.	
	N	6	
No of education disclosed	Correlation Coefficient	.	
	Sig. (2-tailed)	.	
	N	6	

Figure 24-Correlation between Neighbours with High Relative Vulnerability and Neighbours' Personal Detail Disclosure

The results in Figure 24 highlight there is a weak positive relationship for the attributes *name and location*. The relationship does exist between the amount of personal disclosure that the external user can view and the high relative vulnerability of the neighbours. This demonstrates that as the neighbours' friends become more public, there is a potential for them to leak the *name and location* of the neighbours in their interactions with other friends.

Overall what the findings in this section have illustrated is that you do not have to be the friend of someone directly in order to learn more about them in terms of their identity. The results in section 8.2 contributed towards validating this by highlighting the amount of personal detail, an external user who has no direct friendship link with its neighbour's friends but has direct links with the

Chapter 8-Additional Experimental Work Validation

neighbours, can view, despite privacy controls being available. Also some of the neighbours' friends made their walls public and these walls can leak personal details about a neighbour via the activity stream and therefore demonstrates that vulnerability exists. This finding forms the basis for the spreading of personal details and rallies up the issue of what if the user did not know the neighbours or the neighbours' friends in the network.

In terms of vulnerability and the different OSN levels, the correlations in the statistical work demonstrated the presence of a weak positive relationship (for the attributes *name* and *current location*) between the high relative vulnerability of the neighbours and the amount of personal details that were leaked in interactions made by the neighbours' friend and viewable by the external user. The findings in this section have shown that the vulnerability theory can be applied to external users because of the actions of the neighbours' friends and therefore the issue of OSN levels can be incorporated into the vulnerability measure.

Schrammel et al. (2009) measures for information disclosure to friends and unknown people can be incorporated into the relative vulnerability measure as highlighted in equation 37, in order to incorporate the issue of OSN levels. This is to emphasise the potential for the personal details of the profile to spread through the OSN and increase the profile owners' risk of being vulnerable to privacy attacks.

$$V_{R_i} = \frac{1}{n} \sum_{\substack{j=1 \\ j \neq i}}^n V_{I_j} * PF_j * PU_j \quad (37)$$

Chapter 8-Additional Experimental Work Validation

where n is the number of the profile neighbours and V_{I_i} is the individual vulnerability of the neighbour j . For simplicity V_{R_i} denotes the relative vulnerability of profile i where $i=1, \dots, n$ and n is the number of profiles in the network. The notation $PF_j \in [0,1]$ is the information disclosure to friends of neighbour j and is calculated using equation 38

$$PF_j = \frac{\# pdf_j}{\# pd_j} \quad (38)$$

where PF_j is the information disclosure to friends of neighbour j , $\#pdf_j$ is the number of personal details disclosed to friends and unknown people by neighbour j and $\#pd_j$ is the number of available items of personal details on neighbour j . The notation $PU_j \in [0,1]$ is the information disclosure to unknown people of neighbour j and is calculated in equation 39:

$$PU_j = \frac{\# pdu_j}{\# pd_j} \quad (39)$$

where PU_j is the information disclosure to unknown people of neighbour j , $\#pdu_j$ is the number of personal details disclosed by neighbour j and $\#pd_j$ is the number of available items of personal details on neighbour j .

8.3-Case Studies for Attribute Disclosure

The case studies in Table 8 highlight several OSN *start profiles* from the Caverlee and Webb (2008) dataset with varying individual and relative vulnerability values and how much the neighbours and other friends of the *start profile*, leak certain personal details (attributes) of the *start profile* in interactions with their *top friends*. The relative vulnerability is calculated using equation 12 and the absolute vulnerability is calculated using equation 13.

Chapter 8-Additional Experimental Work Validation

With the vulnerability theory in this thesis, the higher the relative vulnerability (V_R) of the *start profile*, the increased likelihood there is of the personal details of the *start profile* spreading due to the actions of its neighbours.

Table 8-Vulnerability and Disclosure Details for Case Studies

Case no	Vulnerability Details				Number of Comments which Discloses Attribute Values					
	V_I	V_R	Number of Profiles' Top Friends	V_A	Birthday	Name	Age	Current Location	Education	Hometown
1	0.9982	0.9661	12	0.9643	0	168	0	336	0	0
2	0.9340	0.8907	24	0.8319	0	72	0	0	0	0
3	0.9340	0.6659	8	0.6219	0	0	0	216	0	0
4	0.1298	0.9340	7	0.1212	0	40	0	0	0	0
5	0.8041	0	0	0	0	0	0	0	0	0
6	0.9982	0.9660	7	0.9642	0	30	0	0	38	24
7	0.9982	0.9340	12	0.9323	0	0	0	0	0	0

Table 8 highlights the common attribute values that can be leaked by the *start profiles'* neighbours and other friends. The number of *top friends* of a profile is the number of neighbours which the profile classes as *top friends*. In this experiment the comments were analysed just for the attribute values of the *start profiles*.

The number of comments that leak certain attributes is high in some of the case studies because quantifying the amount of attribute disclosure of a *start profile* by a *start profiles'* neighbours means analysing the walls of each one of the *top friends* of the neighbours.

Case number 2 in Table 8 highlights that an increased number of *top friends* for the *start profile* does not always result in a higher amount of leakage of the *start profile's* attributes. In case 2, a large proportion of the *top friends* of the *start profile* had private profiles so their interactions were not accessible. The

Chapter 8-Additional Experimental Work Validation

concept of a private profile for this experiment is illustrated in case number 5 because the *start profile* is private, the *top friends* list can't be viewed so the interactions can't be analysed. Consequently the V_R is 0 because this experiment focuses on unidirectional friendship.

In comparison case 7 demonstrates that there will be cases where *start profiles* which display their personal details publically and have *top friends* that do the same but, the *top friends* or other friends do not disclose any of the *start profile's* personal details in their interactions. In this particular case, the wider neighbourhood of the *start profile's* were mainly private profiles where the list of friends are not accessible and consequently the interactions between the profile's *top friends* and their *top friends* could not be analysed. This shows that most of the *top friends* of the *start profiles'* neighbours that have private profiles have privacy concerns. Although the *top friends* of the *start profiles'* neighbours still display personal details about themselves.

A few of the *top friends* of the *start profiles'* neighbours had public profiles so personal details of the profile can still be leaked even though there was no leakage in this case.

The issue of leakage is demonstrated in case 4, where the *start profile* has a low V_I value but the collective vulnerability of the *top friends* is very high and the *top friends* and other friends of the *start profile* leaked the *name* of the owner of the *start profile* in its interactions.

Case 6 highlights the various attributes that can be leaked by the *start profile's* *top friends* and other friends. The leakage of a profiles' *education* alongside *name and current location* can increase the chances of an adolescent being located and stalked (Patchin and Hinduja 2010).

Chapter 8-Additional Experimental Work Validation

Overall what Table 8 has shown is that the *top friends* as well as other friends of a *start profile* can leak the profiles' personal details through interactions with the wider neighbourhood. A *start profile* having a high number of *top friends* does not necessarily mean a greater amount of disclosure. This is because of the issue surrounding private profiles.

Private profiles will not allow access to a profile's list of *top friends* or any profile comments. One factor which is not incorporated into the vulnerability theory but does play a part in information disclosure is the psychology between the *start profiles' top friends* and the *start profiles* wider neighbourhood. Even though *top friends* indicates a strong relationship between one profile and another, the *top friends* of a profile may be privacy aware and choose not to disclose the profiles' personal details in interactions in order to respect the profile's privacy. This issue is touched upon by Gundecha et al. (2011) who states that when a new friend is accepted by the user, it is the user's responsibility to ensure that the new friend does not increase the security risk of the user's friend network.

8.4-Alternative Ways of Calculating Relative and Absolute Vulnerability

The calculation of the relative and absolute vulnerability values is affected by the operators used in both the calculations. In previous experiments the arithmetical mean and product operators have been used for the calculation of the relative and absolute vulnerability. The aim of this experiment is to investigate different combinations of operators and how they affect the vulnerability values. For this experiment, the multigraph aspect will be used to ascertain the neighbours of the *start profile* (*top friends* of the *start profile* and friends that class the *start profile* as a top friend). Three profiles were selected randomly from the Caverlee and Webb (2008) dataset and the vulnerability

Chapter 8-Additional Experimental Work Validation

values which were calculated using different operator combinations are stated in Table 9.

Table 9-Vulnerability Results for Operator Combinations

Case	V_I	Combination 1		Combination 2		Combination 3	
		V_R Operator MAX	V_A Operator Arithmetical Mean of (V_I, V_R)	V_R Operator Arithmetical Mean	V_A Operator $\frac{V_I * V_R}{V_I + V_R}$	V_R Operator Arithmetical Mean	V_A Operator $\frac{1}{\pi} \arctan(V_I + V_R) + \frac{1}{2}$
A	0.9340	0.9982	0.9661	0.9768	0.4774	0.976863	0.8465
B	0.8041	0.2909	0.5475	0.2909	0.2136	0.290906	0.7644
C	0.1298	0.9982	0.5640	0.9228	0.1138	0.922867	0.7581

In terms of the operators used to calculate the relative vulnerability (V_R) of the profile, case *B* is an example where when the profile has only one neighbour, so the MAX and arithmetical mean operators will generate the same value for the relative vulnerability.

The MAX operator in general will highlight the neighbour of the profile with the highest individual vulnerability (V_I) regardless of what the other neighbours individual vulnerabilities are, so an accurate picture of the neighbourhood vulnerability may not be given. On the other hand, the arithmetical mean operator takes the individual vulnerabilities of all the neighbours into account and gives a more accurate picture of the neighbourhoods' collective vulnerability.

For calculating the V_A , using the arithmetical mean operator takes into account both the V_I and the V_R value and this is reflected by the V_A values for cases *A*, *B* and *C* where case *C* has six neighbours and case *A* has 3 neighbours. Case *C* has the higher V_A value because even though the profile self disclosure is more private, the likelihood of the personal details spreading is very high compared

Chapter 8-Additional Experimental Work Validation

to case B where the V_I of the profile is fairly high but the likelihood of the profile's personal details spreading is quite low.

This is in comparison to the actions of the operators $\frac{V_I * V_R}{V_I + V_R}$ and

$\frac{1}{\pi} a \tan(V_I + V_R) + \frac{1}{2}$ for calculating the V_A value where case C has a lower V_A

value even though the profile has more chance of its personal details spreading.

The $\frac{V_I * V_R}{V_I + V_R}$ operator has a reduction effect and the V_A values are too small and

harder to distinguish which profiles have very high overall vulnerabilities. The

operator $\frac{1}{\pi} a \tan(V_I + V_R) + \frac{1}{2}$ and its behavior is similar to the arithmetical mean

operator but unlike the arithmetical mean operator, the $\frac{1}{\pi} a \tan(V_I + V_R) + \frac{1}{2}$

operator does not emphasise the importance of the V_R value. This is demonstrated by how close the V_A values of the cases are.

Ideally the best combination of functions would allow the V_A values not to be close together, so it is easier to identify the profiles that are very vulnerable overall.

Also the V_R values should be emphasised by the functions because the neighbours' behavior can contribute towards how far the personal details will spread. With these criteria, combination 1 is more suited towards an accurate calculation of the vulnerability of a profile with the exception of the calculation of the V_R . The V_R value needs to take all the neighbours' behaviours in to account and not just the maximum individual vulnerability value in the neighbourhood. There are other ways to calculate the V_R and an example is shown in equation

40

$$V_{R_i} = \frac{\underset{j \neq i}{\overset{j=1}{\text{MIN}}}(V_{I_j})}{\underset{j \neq i}{\overset{j=1}{\text{MAX}}}(V_{I_j})} \quad (40)$$

where n is the number of the profile neighbour and V_{I_i} is the individual vulnerability of the neighbour j . For simplicity V_{R_i} denotes the relative vulnerability of profile i where $i = 1, \dots, n$ and n is the number of profiles in the network. The reason that j is not equal to i is because a profile cannot be neighbours with itself. The notation MIN is the minimum individual vulnerability values of all j neighbours of profile i where as the notation MAX is the maximum individual vulnerability values of all j neighbours of profile i .

The problem with this operator is that if the MIN and MAX values are the same then the V_R value will be 1 regardless of whether the values are big or small.

This experiment has highlighted how the combination of different mathematical operators can affect the overall vulnerability and that it is important for the operator for the V_R calculation to emphasise the true value of the V_R .

8.5-Challenges with Data Extraction

At present, validating the vulnerability measure with a larger amount of OSN profiles, poses a variety of challenges. One example is with Facebook. With Facebook, data extraction from OSN profiles has brought about new challenges recently due to the tightening of privacy controls by Facebook. In the past it was acceptable to build a web crawler to extract a vast amount of data from a Facebook network. Now, in order to extract data, an application has to be built using an API (Application Programme Interface). An API as described by IBM (2005) is “a functional interface supplied by the operating system or a separately orderable licensed program that allows an application program

Chapter 8-Additional Experimental Work Validation

written in a high-level language.” In comparison to using a web crawler to extract data from Facebook profiles, with an API application, the profile owner has to grant permission to the application in order to extract from their profile and profiles of the immediate network of friends. The profile owner grants access to the application in order to know exactly what type of data the profile owner has authorised the application to access. For an application that wants to extract data, types of permissions that an application may require include:

- Access to the basic information of the profile owner
- The ability to post statues, messages, photos and videos on the profile owner’s behalf.
- Access messages in the profile owner’s inbox
- Access posts in the news feed (known as a wall) of the profile owner.
- Access the profile owner’s list of friends
- Access information that people share with the profile owner

Granting the list of permission mentioned above to the applications enables the extraction of useful and meaningful data but poses serious privacy concerns. One issue highlighted by the permissions is that the profile user is responsible for the privacy of their friends’ profiles as well. This can cause some ethical debate because Facebook’s stance on data extraction profiles is that you have to ask permission of the profile owner that you wish to extract from (BBC 2011). Applying this statement in a strict way would mean that permission has to be gathered by each of the friends of the profile owner for their data to be extracted as well. At present, the only way to extract data from Facebook is to use their API to build applications to extract and the API does not specify that you need the permission from the profile owners friends in order to extract data from their

Chapter 8-Additional Experimental Work Validation

pages. Several OSNs (e.g. Google+ and MySpace) have their own API's which use the same approach.

Using an API will increase the time needed to extract from Facebook profiles, due to the need to ask permission from the profile owner, but a lot of effort will be required to gather a large dataset. In the current climate where privacy and data leakage is a main concern for society, asking a vast amount of Facebook users (even if it is users you know) to grant an application access to extract their and their networks data for research purposes may lead with some resistance. Alternatives to automated extraction may have to be used (e.g. questionnaires and interviews).

8.5-Conclusions

The experiments detailed in this chapter have illustrated that the vulnerability concept in the thesis does exist in terms of the spread of a *start profile's* personal through the OSN.

Experiment 1 showed that there are neighbours of a *start profile* that will leak the *start profiles'* personal details in comments made to the *start profile's* wider neighbourhood. What the experiment did highlight was that, as there was an increase in relative vulnerability from 0.8 to 1, for most attributes, there was a weak correlation between the increase in relative vulnerability of the *start profiles* and the number of comments that were written by the *start profiles'* neighbourhood that leaked some of the *start profiles'* personal details. Out of the attributes, only *name* had a significant and meaningful correlation which highlights that *name* is a popular attribute to be leaked. There are other factors which affect whether profile friends with high individual vulnerabilities can leak information (e.g. psychology and relationship strength between the profile's friends and profile's friends of friends).

Chapter 8-Additional Experimental Work Validation

What the experiment did show is that there is a correlation even when only the front page of comments for each profile were extracted as the case was with the Caverlee and Webb (2008) dataset.

Experiments 2 and 3 highlighted that some profile attributes (personal details) had a weak positive correlation between the high V_R of the *start profile* and the number of comments made by the *start profile's* friends of friends, on the *start profile's* neighbourhood walls, that leaked the *start profile's* personal details. Attributes that had significant weak positive correlations included *current location, birthday and name*.

This demonstrated that the vulnerability concept can be applied not just to the comments made by the *start profile's* neighbours but also by the profile's '*friend of friends*'. Consequently, this can facilitate the spread of its personal details because depending on how public the *start profile's* neighbours or profile's friends of friends are, other users including external users, other friends of the *start profiles's* neighbours or neighbours of the *start profiles* who are not top friends, can view the comments.

In terms of privacy levels in OSNs, when investigating a small Facebook network, the available privacy controls do not deter users from making their profiles public to a friend of a friend or even an external user. This can facilitate the spread of personal details. Incorporating the vulnerability theory and privacy levels together showed that there is a weak positive correlation for two attributes (*name and current location*). The correlation involved high V_R profiles and the amount of the profile neighbours's personal details that are leaked and are viewable by the external user. This shows that vulnerability exists in a modern day OSN due to the actions of the profiles' neighbours' friends, the neighbours were made vulnerable because the external user could view some

Chapter 8-Additional Experimental Work Validation

of the neighbours' personal details and build up the identity of the neighbours' without having a friendship link with them.

The experimental work presented so far highlighted that two of the most popular attributes that were leaked were *name* and *current location* and this was illustrated in the case studies that were analysed. The case studies showed that not all profiles with high V_R values have neighbours that disclose their personal details via interactions with their friends. This shows that more research needs to be done into the psychology between profiles and this will inform the relationship strength. Consequently this can be incorporated into the vulnerability measure.

The experiment involving mathematical operators showed that finding the right operators to reflect the relative and absolute vulnerability of profiles is challenging. The best combination of operators for V_R and V_A , allows for emphasis to be placed on the neighbours of the nodes and the V_I value of all the nodes because of their role in spreading information. In terms of the V_A value, the nodes that are vulnerable should be easily identified.

Ideally the best combination of functions would allow the V_A values not to be close together so it is easier to identify the nodes that are very vulnerable overall. Also the V_R values should be emphasized by the functions because the neighbours' behavior can contribute towards how far the personal details will spread. With these criteria, combination 1 is more suited towards an accurate calculation of the vulnerability of a profile with the exception of the calculation of the V_R .

CHAPTER 9: CONCLUSIONS AND FUTURE WORK

9.1-Research Summary and Conclusions

The increase in the use of OSNs has resulted in a vast amount of personal details being displayed on OSN profiles. This can lead to social engineering and privacy attacks due to the spread of personal details.

OSNs can be modeled using graphs where a node represents an OSN profile and an edge defines a friendship link between two profiles. In the field of graph theory including social network analysis, the various definitions and concepts of vulnerability focused on the structure surrounding the node (friends of the profile) but not as much on the content of the node (what personal details are displayed on the profile itself).

This formed the motivation for the concept of vulnerability and a vulnerability measure. The definition of vulnerability was considered as the likelihood that the personal details displayed on an OSN profile will spread due to the actions of the friends of the profile in regards to information disclosure of the profile's personal details by the profile's friends via the interactions with their other friends.

The research in this thesis mainly focused on the design, implementation and development of the vulnerability measure as well as the data extraction approach for OSN profiles. This was in order to provide real life cases for the vulnerability measure to be applied to.

The first phase of the research involved designing a vulnerability measure algorithm (which is detailed in chapter 3) to quantify the vulnerability of an OSN profile. The measure consisted of three components: individual vulnerability, relative vulnerability and absolute vulnerability. At this stage, the measure was

Chapter 9-Conclusions and Future Work

unnormalised but the measure was normalised later on after significant experimental work. It was concluded after the initial design of the algorithm that there were several issues regarding the algorithm. The issues included:

- Attribute weights-allocating weights which emphasise the importance of the attribute's disclosure in contributing towards the vulnerability of a profile.
- Attributes that are classed as contributing towards vulnerability.
- Relationship strength between two profiles.
- Other features of the profile that can contribute towards vulnerability (e.g. the number of friends).

Some of these issues would be explored later on in the thesis.

The second phase of the research involved developing and implementing a data extraction approach for OSN profiles. This was in order to produce real data for the vulnerability measure to be applied to, as well as produce an OSN graph to aid investigations into structural features that can affect the vulnerability of a profile. After further investigation, the OSN graph which resulted from the data extraction approach was used in the calculations of the individual vulnerability of a profile.

The data extraction approach for *top friends* and *all friends* highlighted various issues (e.g. various profile structures and ethical debate) regarding the extraction. The profile structure presented significant problems because the profile structure can change instantly depending on what the user wants to present or what the OSN wants to improve in terms of site functionality. The program for data extraction depended a lot on the tokens and tags present in the profile structure so a change in profile structure caused extraction issues. It

Chapter 9-Conclusions and Future Work

was concluded that the data extraction approach would need to be improved to deal with the extraction issues.

Also in late 2011 MySpace, which was the OSN used in our data extraction approach, blocked parsers extracting from MySpace profiles. Therefore our parser could not be updated to reflect the new structure of MySpace profiles.

The research involving the analysis of the OSN graph produced from the *all friends* data extraction approach highlighted that the number of friends and the clustering coefficient were the main structural factors which can affect the vulnerability of a profile. These two factors were later taken and added to the list of attributes which could contribute towards the vulnerability of a profile.

The third phase of the research involved the development and implementation of the vulnerability measure to real life data. The real life data is based on profiles extracted as a result of our data extraction approach and profiles from Caverlee and Webb (2008) dataset. Further experimental work took place to explore the application of the vulnerability measure. To develop the measure, it had to be normalized in order to allow profiles to be compared on the same scale.

The experimental work in chapter 5 concluded that in order for the vulnerability measure to be normalized, the relative vulnerability could not be normalized using the Min Max method of normalization due to the dynamic nature of the OSN. This raised the issue regarding the calculation of the relative vulnerability to produce values between 0 and 1 and how to accurately reflect the OSN.

One issue when choosing the appropriate operator for normalization of the relative vulnerability value, is reflecting the vulnerability of the profiles' neighbours in an accurate way. Many different operators were considered to

Chapter 9-Conclusions and Future Work

normalize the relative vulnerability. Most of the operators (e.g. MAX) emphasized the actions of the profile with the highest individual vulnerability, regardless of what the other profiles in the neighbourhood do, or with (e.g. MIN/MAX) where if two profiles have an individual vulnerability of 0.2 then the relative vulnerability value will be 1 which is incorrect. On the other hand, the arithmetical mean operator was chosen for experiments from chapter 6 onwards because of its ability to take the individual vulnerabilities of all the neighbours into account when calculating the relative vulnerability.

Another aspect of the vulnerability measure implementation which was explored in chapter 6 was the attitudes of various users towards privacy. The modeling of the individual vulnerability of profiles via different mathematical functions highlighted how the type of mathematical function used to model the user, can also link to the vulnerability approach adopted because of the user's attitudes towards privacy. The experimental work in this chapter concluded that with a convex function a small amount of personal detail disclosure can lead to an individual vulnerability value straight away resulting in an alarmist approach to vulnerability. This function would suit children and adolescent users who are not so privacy aware and are more vulnerable to their personal details being leaked.

A concave function on the other hand requires a bigger disclosure to be made before the vulnerability value became significant. This would lead to a conservative approach on vulnerability. This function would suit aspects of adult or older adult users who understand the issues considering privacy. A younger adult user might need a function which displays both aspects of concave and convex behavior because even though they may be more privacy aware than a

Chapter 9-Conclusions and Future Work

child or an adolescent, they still receive peer pressure and this can lead to an increased chance of information disclosure.

The fourth phase of research involved establishing axioms and propositions based around the vulnerability measure to form a formal approach for the measure. The axioms and propositions were established after substantial experimental work into the vulnerability measure. The axioms and propositions took into account the dynamic nature of the OSNs and showed how the vulnerability of a profile can change because of this.

In conclusion, the axioms which focused on the individual vulnerability demonstrated, that changes in the list of profile attributes that are presented and the attributes' probabilities in making the profile vulnerable, affects the individual vulnerability of a profile. Also one main issue is that the disclosure of attributes can have different effects on the type of user. The propositions emphasized the dynamic nature of the OSN and how this affects the relative and absolute vulnerability of a profile. In the experimental work regarding the application of the propositions, the product operator was identified as the most effective operator in calculating the absolute vulnerability due to its accurate reflection of the meaning of vulnerability.

The fifth phase of the research focused on the validation of the measure. The first three experiments using profiles from the MySpace Caverlee and Webb (2008) dataset highlighted that vulnerability can occur in OSN profiles because of the comments written made by the profiles' neighbourhood and wider neighbourhood. This is despite the experiments only taking place on MySpace profiles where only the first page of comments was extracted. Popular attributes of the profile that were leaked by the profiles' neighbourhood or wider neighbourhood included *current location* and *name*.

Chapter 9-Conclusions and Future Work

In the analysis of the correlation between high relative vulnerability profiles and the number of comments written by the profiles' neighbourhood, that leaked certain personal details known as attributes of the profile, most of the attributes had a weak positive correlation with the attribute *name* having a weak positive correlation, in which the correlation is significant. What this finding concludes in the case of this experiment, is that as the neighbourhoods (top friends) of profiles self disclose their personal details more readily and display factors that contribute towards vulnerability, the amount of information disclosure of the profile's personal details in comments written by its neighbours does not necessarily increase. More work has to be done into the psychology between a profile and its friends in order to ascertain the true strength of relationship between the two in terms of interactions on the OSN and incorporate this into the vulnerability measure.

Also private profiles are a factor when validating whether a profiles' personal details are leaked by its friends. A private profile in MySpace or Facebook will not show the interaction elements (e.g. comments written on the profile's wall or in the case of Facebook, the activity stream of the profile). If a profile has friends that have private profiles, then the interactions between the profile's friends and the profile's wider neighbourhood can't be viewed. However if the wider neighbourhood of the profile is open to even external users, then the comments on the walls of the profile's wider neighbourhood can be seen .

To test if the vulnerability can occur in current Facebook OSN profiles, a small Facebook network was built up. Incorporating the vulnerability theory into the small Facebook network provided extra challenges due to use of privacy levels. In comparison to MySpace, Facebook contained an activity stream which displayed the details of the interactions that the OSN profile would carry out

Chapter 9-Conclusions and Future Work

(e.g. profile comments written to friends and the tagging of photos). Investigating the amount of personal details of OSN profiles that were leaked by the profiles friends (whose OSN profile and interactions could be viewed by an external user) highlighted how the consequences of vulnerability could extend far beyond the small Facebook network.

An external user was defined in this case as a user which had no connections to the small Facebook network used for the experiment. There were a variety of personal details that were leaked which included *name, profile picture, date of birth, hometown and location*. In conclusion what this experiment showed was that vulnerability does occur in an OSN even with a higher level of privacy control set by profile owner. All it takes is friends of the profile owner who set their profiles to be very public and therefore be available for anyone to view.

At present, one challenge which will affect the process of validation in the future is the automated extraction of data from OSNs (e.g. Facebook). This is due to the tightening of privacy. With the move towards the use of an API application to extract data due to privacy, permission has to be granted by the profile owner before data extraction can take place. This can increase the time it takes to automatically extract a big sample of data.

Overall what this thesis has presented is a vulnerability measure which illustrates that the actions of your friends can have an impact on your own privacy in terms of your personal details. In the age of systems which require personal details for authentication, any leakage of personal details can have major effects on our identity and consequently our everyday lives.

9.2-Contributions to the Field of Online Social Networks

This thesis proposes contributions into the fluid domain of OSNs, which has developed in the last 10 years and is a dynamically moving field.

Chapter 9-Conclusions and Future Work

To address the issue of privacy and personal detail disclosure that has arisen due to the use of OSNs, this thesis has introduced a framework for a quantifiable measure for the vulnerability of a user profile.

The contributions of this are as follows:

- A concept of vulnerability which takes into account the information disclosure of a OSN profile owner as well as the information disclosure of the profile owners friends. An OSN graph is used to aid the concept of vulnerability. Vulnerability concepts in the graph theory field (e.g. cutpoint, vulnerable bridges and clustering coefficient) only take into account the connections between a profile owner and its friends whereas our concept of vulnerability acknowledges the profile content as well as the connections. The vulnerability concept is explained in chapter 3 and in the papers AbdulRahman et al. (2010); Alim et al. (2011b) and Alim et al. (2011a).
- A normalised measure that will quantify the vulnerability of an OSN user's profile. The measure will quantify vulnerability by using a weights system to allocate weights to the profile if the profile displays attributes or features which contribute towards information disclosure. The normalization of the measure is explained in chapter 6 and in the papers AbdulRahman et al. (2011); Alim et al. (2011a) and Alim et al. (2011c). The weights based system is detailed in AbdulRahman et al. (2010); Alim et al. (2011b) ; Alim et al. (2011a) and Alim et al. (2011c).
- An extraction approach to retrieve personal data from OSN profiles was applied and the extracted friendship connections were used to produce a simple OSN graph. Features of the graph are used to aid the vulnerability calculation of a user's profile. The extraction approach and OSN graph

Chapter 9-Conclusions and Future Work

analysis are described in chapters 4 and 5 and detailed in the papers Alim et al. (2009); AbdulRahman et al. (2010) and Alim et al. (2011b).

- Different mathematical functions can be used to model the individual vulnerability of a profile user based on the type of user (e.g. children, adolescent, young adult and older adult). A variety of different users of different age groups use OSNs. Different types of users display different behaviours when disclosing personal details. Some choose to display a lot of their personal details whilst other users are more reserved about what they present on their profiles. The mathematical modeling is detailed in chapter 6.
- A set of notations, axioms and propositions which form a formal approach for the vulnerability measure. This is all detailed in chapter 7 and described in the papers Alim et al. (2011a) and Alim et al. (2011c). As the vulnerability measure develops, more notations, axioms and propositions can be added.
- Ways to validate the vulnerability measure to prove the concept that as the friends of a profile owner can spread the profile's personal details through interactions made with other users. The ways are detailed in chapter 8.

9.3-Future work

The development and implementation of an approach to measure the vulnerability of OSN profiles has opened up opportunities for future work to be carried out. The future work includes:

- Comparing the vulnerability of profile from various OSNs in order to investigate how the vulnerability measure works in terms of the personal details that are displayed by user and the user's friends.

Chapter 9-Conclusions and Future Work

- Further test the vulnerability measure by using another dataset which has all the comments from the profiles extracted rather than just the first page (e.g. Caverlee and Webb).
- Test the vulnerability of profiles across multiple OSNs to compare and contrast the vulnerability values of these profiles. To add complexity to the analysis, the OSN graphs of each of the profiles can be compared across the networks to explore the activity of the neighbourhood of a profile. Also one user's profile in multiple networks can be analysed to calculate if the user is more vocal on one network compared to the others or if the user discloses more personal details on a specific network than the others.
- Incorporate the strength of relationship between two OSN profiles that are friends into the relative vulnerability calculation. The strength of relationship between two friends can influence the amount of personal information disclosure of each of the friends and whether their attitude towards privacy, affects the profile's personal details being spread through the network.
- Expand the vulnerability measure to take into account that a profile's *friends of friends* can make the profile vulnerable. This can be incorporated into the relative vulnerability calculation of a profile.
- Link the attribute weights and the attributes classed as contributing towards vulnerability with different users. An example that an OSN consisting of childrens' profiles will have different vulnerable attributes and weights in comparison to an OSN consisting of profiles belonging to adults.

Chapter 9-Conclusions and Future Work

- Extract the data from OSN profiles over time in order to investigate how the vulnerability of profiles changes over time. We have made a start on this work and the results have been submitted to a journal in the paper entitled 'Multi Agents System Approach for Vulnerability Analysis of Online Social Network Profiles over Time'. The paper is currently under review.
- Extract the data from OSN profiles using an API application. This is in order to produce a larger dataset for validation purposes. Work has already started on this and an application has been sent for ethical approval.
- Investigate and apply different mathematical operators to model the various behaviors in regards to information disclosure of the profile owners and their friends.
- Propose and apply axioms for the relative and absolute vulnerability. This will lead to more propositions being designed to incorporate different aspects of the vulnerability model (e.g. strength between friends) alongside different operators to reflect the behavior of the friends.
- Investigating other approaches to calculate the attribute weights in the individual vulnerability calculations.
- The vulnerability values of profiles based in a *top friends* network and in an *all friends* network, can be compared along with the full walls of the profiles, to explore the true extent to which vulnerability occurs in profiles.
- Identify and analyse outliers in a variety of networks. Outliers can pose a danger to OSN users especially children and teenagers.

References

AbdulRahman, R., **Alim, S.**, Neagu, D., Holton, D.R.W. and Ridley, M.J. (2011). Multi Agents System Approach for Vulnerability Analysis of Online Social Network Profiles over Time. Inderscience, *Int. J. Knowledge and Web Intelligence* (Conditionally Accepted).

AbdulRahman, R., **Alim, S.**, Neagu, D. and Ridley, M. (2010). Algorithms for Data Retrieval from Online Social Network Graphs. IEEE. International IEEE Conference on Computer and Information Technology. In: *Proceedings of the 10th International IEEE Conference on Computer and Information Technology* (CIT 2010), 29th June-1st July 2010, Bradford, UK (pp.1660-1666), IEEE CS.

Alexa. (2010). Friendster.com site info. Available from: <<http://www.alex.com/siteinfo/friendster.com#>> Retrieved 24th December 2010

Alim, S., Neagu, D. and Ridley, M (2011a). Axioms for Vulnerability Measurement of Online Social Network Profiles, IEEE, International Conference in Information Society. In: *Proceedings of the International Conference in Information Society* (i-Society 2011), June 27th-29th, London, UK (pp.241-247) IEEE CS

Alim, S., Abdul-Rahman, R., Neagu, D. and Ridley, M. (2011b). Online social network profile data extraction for vulnerability analysis. Inderscience, *Int. J. Internet Technology and Secured Transactions*, Inderscience, 3 (2), pp. 194-209

Alim, S., Neagu, D. and Ridley, M. (2011c). A Vulnerability Evaluation Framework for Online Social Network Profiles: Axioms and Propositions. Inderscience, *Int. J. Internet Technology and Secured Transactions* (Under Review).

Alim, S., Abdul-Rahman, R., Neagu, D. and Ridley, M. (2009). Data retrieval from online social networking profiles for social engineering applications. IEEE. International Conference for Internet Technology and Secured Transactions. In: *Proceedings of the 4th International Conference for Internet Technology and Secured Transactions* (ICITST-2009), 9th-12th November 2009, London, UK, (pp.207-211) IEEE CS.

Arjan, R., Pfeil, U. and Zaphiris, P. (2008). Age difference in online social networking. In: *CHI'08 extended abstracts on the ACM Human factors in computer systems* (CHI'08), April 5th -10th 2008, Florence, Italy, (pp. 2739-2744). New York, NY: ACM Press.

Balduzzi, M., Platzer, C., Holz, T., Kirde, E., Balzarotti, D. and Kruegel, C. (2010). Abusing social networks for automated user profiling. 13th International Symposium on Recent Advances in Intrusion Detection (RAID). In: *Proceedings of Springer LNCS*, Volume 6307/2010, September 15th -17th 2010, Ottawa, Canada, (pp. 422-441).

Barabási, A.B. and Oltvai, Z.N (2004). Network Biology: Understanding the cell's functional organisation. *Nature Reviews*, 5(2004), pp.101-113

References

Barabási, A.L. and Albert, R. (1999). Emergence of Scaling in Random Networks. *Science*, 286, pp.509-512.

BBC News. (2011). Socialbots used by researchers to 'steal' Facebook data. Available from :< <http://www.bbc.co.uk/news/technology-15553192>> Retrieved 12th November 2011.

BBC News. (2010a). Facebook reveals simplified privacy measures. Available from :< <http://www.bbc.co.uk/news/10167143>> Retrieved 31st May 2011.

BBC News. (2010b). Police criticised over Facebook killer case referral. Available from:<<http://news.bbc.co.uk/1/hi/england/wear/8560008.stm>>Retrieved 28th December 2010.

BBC News. (2009). What's the ideal number of friends? .Available from: <<http://news.bbc.co.uk/1/hi/7920434.stm>> Retrieved 30th January 2010

BBC News. (2008a). Palin e-mail hack details emerge. Available from: <<http://news.bbc.co.uk/1/hi/technology/7624809.stm>>Retrieved 3rd July 2010

BBC News. (2008b). Phorm warned about web data rules. Available from: < <http://news.bbc.co.uk/1/hi/technology/7339263.stm>> Retrieved 9th May 2008

BBC News. (2007). Protests force Facebook to change. Available from:<<http://news.bbc.co.uk/1/hi/7120916.stm>> Retrieved 10th February 2011

Becker, J. and Chen, H. (2009). Measuring Privacy Risk in Online Social Networks. IEEE. IEEE Workshop on Web 2.0 Security and Privacy. California. USA. Available from: <<http://w2spconf.com/2009/papers/s2p2.pdf>>Retrieved 17th July 2010

Bialik, C. (2007). Sorry, you may have gone over your limit of network friends. *The Wall Street Journal*. Available from :< <http://online.wsj.com/article/SB119518271549595364.html>> Retrieved 30th January 2010.

Bird, C., Gourley, A., Devanbu, P., Gertz, M., and Swaminathan, A. (2006). Mining email social networks. ACM. *International Workshop on Mining Software Repositories*. In: *Proceedings of 2006 ACM International Workshop on Mining Software Repositories (MSR 2006)*, May 22nd-23rd 2006, Shanghai, China (pp.137-143).New York, NY: ACM Press.

Boyd, D. and Buckingham, D. (2008). Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life. *Youth, Identity, and Digital Media* (2008), pp. 119-142.

Boyd, D. M., and Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1), pp.210-230.

References

Boyd, D. (2006). Friends, Friendsters, and MySpace Top 8: Writing Community into Being on Social Network Sites. *First Monday*, 11(12). Available from:< http://www.firstmonday.org/issues/issue11_12/boyd/index.htm> Retrieved 31st October 2011.

Brin, S. and Page, L. (1998). The Anatomy of a Large-Scale Hypertextual Web Search Engine. *Computer Networks and ISDN Systems*, 30(1998), pp.107-117.

Brown, G., Howe, T., Ihbe, M., Prakash, A. and Borders, K. (2008). Social Networks and Context-Aware Spam. ACM. ACM conference on Computer Supported Cooperative Work. In: *Proceedings of 2008 ACM conference on Computer Supported Cooperative Work (CSCW 08)*, 8th -12th November, 2008, San-Diego, California, USA (pp.403-412).New York, NY: ACM Press.

Browner, J. (2010). Which Disney Princess are you. Available from:<http://www.sans.org/reading_room/whitepapers/privacy/disney-princess-you_33328>Retrieved 28th January 2011.

Burns, R. (2000). Introduction to Research Methods, Sage, London, U.K

Burt, R.S. (1995). Structural holes: The social structure of competition. Cambridge. Harvard University Press

Cachia, R. (2008). Social Computing: Study on the Use and Impact of Online Social Networking. Available from: <<http://ftp.jrc.es/EURdoc/JRC48650.pdf>> Retrieved 9th December 2010.

Calvo, C. and Dercon, S. (2005). Measuring Individual Vulnerability. Available from:<http://website1.wider.unu.edu/conference/conference-2005-3/conference-2005-3_papers/Calvo%20&%20Dercon.pdf>Retrieved 8th April 2011

Caverlee, J. and Webb, S. (2008). A Large-Scale Study of MySpace: Observations and Implications for Online Social Networks. AAAI. AAAI International Conference on Weblogs and Social Media. In: *Proceedings of the 2nd AAAI International Conference on Weblogs and Social Media (ICWSM 2008)*, March30th -April 2nd 2008, Seattle, USA (pp. 36-44). California CA: Association for the Advancement of Artificial Intelligence.

Chau, M. and Xu, J. (2006). Mining communities and their relationships in blogs: A study of online hate groups. Springer. *International Journal Human Computer Studies*. 65(2007). pp.57-70.

Cisco. (2010). Families sharing more than ever over social networks as a means of staying in touch. Available from: <http://www.theflip.com/engb/buzz/articles/uk/buzz_040810b.aspx>Retrieved 15th September 2010

De Souza, Z. and Dick, G.N. (2009). Disclosure of information by children in social networking: not just a case of 'you show me yours and I'll show you mine'. *International Journal of Information Management*, 29(4). pp.255-261.

References

- Donath, J., and Boyd, D. (2004). Public displays of connection. *BT Technology Journal*, 22. pp.71–82.
- Downes, S. (2005). Semantic networks and social networks. *The learning organization*, 12(5). pp.411-417.
- Dunbar, R.I.M. (1992). Neocortex size as a constraint on group size in primates. *Journal of Human Evolution*.22 (6). pp.469-493.
- Dwyer, C., Hiltz, S.R.and Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace". Americas Conference on Information Systems. In: *Proceedings of the Thirteenth Americas Conference on Information Systems (AMICS 2007)*, 9th -12th August, 2007, Colorado, USA.
- Evans, M. (2009). Wife of Sir John Sawers, the future head of MI6, in Facebook security alert. Available from:
<http://technology.timesonline.co.uk/tol/news/tech_and_web/article6644199.ece>Retrieved 8th July 2011.
- Emery, D. (2010). Details of 100m Facebook users collected and published. Available from :< <http://www.bbc.co.uk/news/technology-10796584>> Retrieved 10th February 2011.
- Erdős, P. and A. Rényi. (1960). On the Evolution of Random Graphs. *Publication of the Mathematical Institute of the Hungarian Academy of Sciences*, 5. pp.17-61.
- Facebook. (2011a). What is the minimum age required to sign up for Facebook. Available from:<<http://www.facebook.com/help/?faq=210644045634222>>Retrieved 8th July 2011.
- Facebook. (2011b). Privacy Policy. Available from:<<http://www.facebook.com/policy.php>>Retrieved 8th July 2011.
- Facebook. (2010). Press Room. Available from :< <http://www.facebook.com/press/info.php?statistics>> Retrieved 23rd December 2010.
- Federal Trade Commission. (2006). Facts for Consumers. Available from:
<<http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm>> Retrieved 13th September 2009.
- Freeman, L.C. (1979). Centrality in social networks: Conceptual clarification. Elsevier. *Social Networks*. 1(3). pp.215-239
- Furnell, S.M. (2010). Online identity: Giving it all away? Elsevier, *Information Security Technical Report*, 14th October 2010.
- Gauvin,W.,Riberio,B.,Towsley,D., Benyuan, L. and Jie,W. (2010). Measurement and gender-specific analysis of user publishing characteristics on MySpace

References

IEEE. IEEE Network: *The Magazine of Global Internetworking*, 24(5). pp 38-43, IEEE Press Piscataway, NJ, USA.

Gibson, L., Moncur, W., Forbes, P., Arnott, J., Martin, C., and Bhachu, A. S. (2010). Designing social networking sites for older adults. BCS. BCS Conference on Human-computer Interaction. In: *Proceedings of the 24th BCS Conference on Human-computer Interaction*, Dundee, September 2010.

Gibson, R. (2007). Who's really in your top 8: Network security in the Age of Social Networking. ACM. ACM SIGUCCS conference on User services. In: *Proceedings of the 35th annual ACM SIGUCCS conference on User services*, October 7th-10th, 2007, Orlando, Florida, USA (pp.131-134). New York, NY: ACM Press.

Gilbert, E. and Karahalios, K. (2009). Predicting tie strength with social media. ACM. Conference on Human Factors in Computing Systems. In: *Proceedings of the 27th international conference on Human factors in computing systems (CHI 2009)*, Boston, USA (pp.211-220). New York, NY: ACM Press.

Govani, T. and Pashley, H. (2005). Student Awareness of the Privacy Implications When Using Facebook. Available from :<<http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf>> Retrieved 19th September 2010.

Granovetter, M. (1973). The Strength of Weak Ties. *American Journal of Sociology*, 78(6), pp.1360–1380.

Grier, C., Kurt, A. and Nicol, D.M. (2010). Barriers to Security and Privacy Research in the Web Era. Workshop on Ethics in Computer Security Research. In: *Proceedings of the Workshop on Ethics in Computer Security Research (WECSR 2010)*, January 28th 2010, Tenerife, Canary Islands, Spain.

Gross, R. and Acquistli, A. (2005). Information Revelation and privacy in Online Social Networks. In: *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, November 7th 2005, Alexandria, Virginia, USA, (pp.71–80). New York, NY: ACM Press.

Gundecha, P., Barbier G. and Liu H. (2011). Exploiting vulnerability to secure user privacy on social networking site. ACM. Available from: <<http://engineering.asu.edu/sites/default/files/shared/ASUCIDSE-2011-001.pdf>> Retrieved 1st July 2011.

Haines, S. (1999). Java 2 from Scratch, QUE, Canada.

Hannerman, R.A and Riddle, M. (2005). Introduction to social network methods. Available from :<http://www.faculty.ucr.edu/~hanneman/nettext/C7_Connection.html#geodesic> Retrieved 29th December 2010.

Hansen, D., Shneiderman, B. and Smith, M. (2009). Analyzing Social Media Networks: Learning by Doing with NodeXL. Available from :<

References

- http://casci.umd.edu/images/4/46/NodeXL_tutorial_draft.pdf>Retrieved 3rd January 2011.
- Havenstein, H. (2008). One in five employers uses social networks in hiring process. Available from: <http://www.computerworld.com/s/article/9114560/One_in_five_employers_use_social_networks_in_hiring_process> Retrieved 11th March 2010.
- Hickman, L. (2010). How I became a Foursquare cyberstalker. Available from: <<http://www.guardian.co.uk/technology/2010/jul/23/foursquare>> Retrieved 26th November 2010.
- Hinduja, S. and Patchin, J. (2008). Personal Information of Adolescents on the Internet: A Quantitative Content Analysis of MySpace. Elsevier. *Journal of Adolescence*.31(1). pp.125-146.
- Ho, A., Maiga, A. and Aimeur, E. (2009). Privacy protection issues in social networking sites. IEEE, IEEE/ACS International Conference on Computer Systems and Applications. In: *Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications (AICSSA 2009)*, May 10th-13th, 2009, Rabat, (pp.271-278). IEEE CS.
- Holme, P., Kim, B.J., Yoon, C.N. and Han, S.K. (2002). Attack vulnerability of complex networks. *Physical Review*, E(65). pp.1-14
- IBM (2005). API concepts. Available from: <<http://publib.boulder.ibm.com/infocenter/series/v5r3/index.jsp?topic=%2Fapis%2Fconcept.htm>> Retrieved 12th November 2011
- Indiana University. (2011). Informatics students discover, alert Facebook to threat allowing access to private data, bogus messaging. Available from: <<http://newsinfo.iu.edu/news/page/normal/17192.html>>Retrieved 10th February 2011
- Irani, D., Webb, S., Kang, L., Pu, C. (2011). Modeling Unintended Personal Information Leakage from Multiple Online Social Networks.*IEEE Internet Computing*,3(15). pp.13-19.
- Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F. (2007). Social Phishing. *Communications of the ACM*, 50(10), pp.94–100
- James, K. (2006). Six degrees of information seeking: Stanley Milgram and the small world of the library. *The Journal of Academic Librarianship*, 32(5). pp.527-532.
- Jupp, V.(2006). The SAGE Dictionary of Social Research Methods, Sage, California, USA
- Juszczyszyn, K. and Musial, K., (2009). Structural Changes in an Email-based Social Network.Springer.3rd KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications. In: *Proceedings of the Third KES International Symposium on Agent and Multi-Agent Systems:*

References

Technologies and Applications (KES-AMSTA 2009)3th -5th June 2009, Uppsala, (pp.40-49).

Kalamdani, V. (2009). Top 10 Comparisons Between Life Before and After Social Networking.

Available from: <<http://socialnetworkbuzz.wordpress.com/2009/05/04/top-10-comparisons-between-life-before-and-after-social-networking/>>Retrieved 21st June 2011

Kelly, S. (2008). Identity at risk on Facebook. Available from:

<http://news.bbc.co.uk/1/hi/programmes/click_online/7375772.stm> Retrieved 13th September 2008.

Kirk, J. (2006). Phishing Scam Takes Aim at MySpace.com. Available from: <http://www.pcworld.com/article/125956/phishing_scam_takes_aim_at_myspace.com.html> Retrieved 25th June 2010

Kleinfield, J. (2002). Could it be a big world after all? The six degrees of separation myth. *Society*, 39(61).April 2002.

Knoke, D. and Burt, R.S. (1983). Prominence. In R S. Burt and M. J. Minor (eds.). *Applied Network Analysis*, pp.195-222. Newbury Park. CA: Sage.

Krackhardt, D. (1990). Assessing the Political Landscape: Structure, Cognition, and Power in Organizations. *Administrative Science Quarterly*, 35, pp.342-369

Krishnamurthy, B. and Wills, C.E. (2009). On the Leakage of Personally Identifiable information Via Online Social Networks.ACM. The 2nd ACM SIGCOMM Workshop on Online Social Networks (WOSN 2009), In: *Proceedings of the 2nd ACM workshop on Online social networks* (WOSN 2009), August 17th 2009, Barcelona, Spain, (pp. 7-12), New York, NY: ACM Press

Lam, I.F., Chen, K.T. and Chen, L.J. (2008). Involuntary Information Leakage in Social Network Services. Springer. Third International Workshop on Security. In: *Proceedings of the 3rd International Workshop on Security: Advances in Information and Computer Security (IWSEC 2008)*, November 25th -27th 2008, Kagawa, Japan (pp.167-183).

Lampe, C., Ellison, N. and Steinfield, C. (2007). A Familiar Face(book): Profile Elements as Signals in an Online Social Network. 25th ACM Conference on Human Factors in Computing Systems. In: *Proceedings of the 25th ACM Conference on Human Factors in Computing* (CHI 2007),28th April-3rd May.2007,(pp.435-444)San Jose, California:ACM Press.

Lehtinen, V., Näsänen, J. and Sarvas, R. (2009). A little silly and empty-headed: older adults' understandings of social networking sites.ACM.British HCI Group Annual Conference on People and Computers. In: *Proceedings of 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology* (BCS HCI 2009), September 1st -5th, Cambridge, UK (pp. 45-54).

References

Lenhart, A., Purcell, K., Smith, A., and Zickuhr, K. (2010). Social Media and young adults. A Pew Internet and American Life Project report. Available from :<<http://pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx?r=1>> Retrieved 19th September 2010.

Lenhart, A. and Madden, M. (2007). Teens, Privacy & Online Social Networks. Pew Internet and American Life Project. Available from :<http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Society_and_the_Internet/PIP_Teens_Privacy_SNS_Report_Final.pdf> Retrieved 17th September 2010.

Leskovec, J. and Horvitz, E. (2008). Planetary-scale views on a large instant-messaging network'. In: *Proceedings of the 17th International Conference on the World Wide Web (WWW 2008)*, April 21st -25th, Beijing, China, pp.21–25.

Lin, N., Ensel, W.M., et al. (1981). Social Resources and Strength of Ties: Structural Factors in Occupational Status Attainment, *American Sociological Review*, 52(1). pp.122-131

Lindamood, J., and Kantarcioglu, M. (2008). Inferring Private Information using Social Network Data. Available from: <<http://www.utdallas.edu/~mxk055100/publications/techreport-sn-privacy.pdf>> Retrieved 14th December 2008

Livingstone, S., Olafsson, K. and Staksrud, E. (2011). Social Networking, Age and Privacy. Available from :<<http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/ShortSNS.pdf>> Retrieved 1st May 2011.

McCallister, E., Grance, T., and Scanfore, K. (2009). Guide to protecting the confidentiality of personally identifiable information (PII). Available from:<<http://www.scribd.com/doc/10968241/NIST-Guide-to-Protecting-the-Confidentiality-of-PII>> Retrieved 14th November 2010

McWilliams, J. (2009). How Facebook beats MySpace. Available from : <<http://www.guardian.co.uk/commentisfree/cifamerica/2009/jun/23/facebook-myspace-social-networks>> Retrieved 23rd December 2010.

Miceli, D. and Kim, R. (2010). Identity fraud survey report: consumer version. Javelin Strategy and Research. February 2010. Available from: <https://www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveyConsumer.pdf> Retrieved 30th November 2010.

Milgram, S. (1967). The Small World Problem. *Psychology Today*, 2. pp.60-67

MySpace. (2011). Minimum age for MySpace. Available from:<http://myspace2.custhelp.com/app/answers/detail/a_id/237/kw/underage%20users> Retrieved 8th July 2011.

References

MySpace. (2010a). Factsheet. Available from :<<http://www.myspace.com/pressroom/fact-sheet/>> Retrieved 24th December 2010.

MySpace. (2010b). Terms and Conditions. Available from :<<http://www.myspace.com/help/terms>> Retrieved 9th January 2011.

Naji, G., Nagi, M., Elsheikh, A.M, Gao, S., Kianmehr, K., Özyer, T., Demetrick, D., Alhajj, R., Rokne, J., and Ridley, M. (2011). Effectiveness of Social Networks for Studying Biological Agents and Identifying Cancer Biomarkers. Springer. *Lecture Notes in Social Networks*, 2(2).pp.285-313.

Namestnikov, Y. (2010). Information Security Threats in the Second Quarter of 2010. Available from: <http://www.securelist.com/en/analysis/204792133/Information_Security_Threats_in_the_Second_Quarter_of_2010> Retrieved 12th December 2010.

Narayanan, A. and Shmatikov, V. (2010). Privacy and Security- Myths and Fallacies of 'Personally Identifiable Information'. *Communications of the ACM*, 53(6). pp.24-26

Nickson, C. (2009). The History of Social Networking. Available from : <<http://www.digitaltrends.com/features/the-history-of-social-networking/>> Retrieved 24th December 2010.

Nielsen. (2010a). 2010 Media Industry Fact Sheet. Available from:<<http://blog.nielsen.com/nielsenwire/press/nielsen-fact-sheet-2010.pdf>> Retrieved 24th December 2010.

Nielsen. (2010b). 2010 What Americans Do Online: Social Media and Games Dominate Activity. Available from :<http://blog.nielsen.com/nielsenwire/online_mobile/what-americans-do-online-social-media-and-games-dominate-activity/> Retrieved 22nd May 2011.

Nielsen. (2009). Global Faces and Networked Places: A Nielsen report on Social Networking's New Global Footprint. Available from: <http://blog.nielsen.com/nielsenwire/wpcontent/uploads/2009/03/nielsen_global_faces_mar09.pdf> Retrieved 30th January 2010

Nosko, A., Wood, E., and Molema, S. (2010). All about me: Disclosure in online social networking profiles: the case of FACEBOOK. *Computers in Human Behavior*, 26(3), pp.406-418.

Palgrave, (2008), Understand Research Available from: www.palgrave.com/business/collis/br/docs/sample.pdf. Retrieved 27th March 2012

Patchin, J.W. and Hinduja, S. (2010). Changes in adolescent online social networking behaviours from 2006 to 2009. *Computers in Human Behaviour*, 26(2010). pp.1818-1821.

References

Pierce, T. (2007). X-Posed on MySpace: A Content Analysis of "MySpace" Social Networking Sites. Available from :<http://www.calstatela.edu/faculty/sfisco/X-posed_on_%20MySpace.htm> Retrieved 28th December 2010.

Schneier, B. (2009). Schneier on Security: A blog covering security and security technology. Available from: <http://www.schneier.com/blog/archives/2009/04/social_networkki.html> Retrieved 25th June 2010.

Schrammel, J., Köffel, C. and Tscheligi, M.(2009).How much do you tell? Information disclosure behavior in different types of online communities. Fourth International Conference on Communities and Technologies. In: *Proceedings of the fourth international conference on Communities and technologies (C&T 09)*,June 25th-27th.2009,(pp.275-284)Pensylvania,Pa:ACM Press.

Shannon, C.E. and Weaver, W. W. (1949). The Mathematical Theory of Communication. University of Illinois Press, Urbana, IL

Simmel, G. and Wolff, K.H. (1950). The Sociology of George Simmel, Free Press, New York, USA.

Singla, P. and Richardson, M. (2008). Yes, There is a Correlation - From Social Networks to Personal Behavior on the Web.ACM.World Wide Web Conference. In: *Proceedings of the Seventeenth International World Wide Web Conference (WWW 2008)*, Beijing, China, (pp.655-664). New York, NY: ACM Press

Social Media University Global. (2008). 4 tips to prevent Facebook identity theft. Available from :< <http://social-mediauniversity-global.org/2007/10/16/4-tips-to-prevent-facebook-identity-theft/>> Retrieved 13th September 2008.

Steel, E. and Vascellaro, J.E. (2010). Facebook, MySpace Confront Privacy Loophole. *The Wall Street Journal*. Available from :< <http://online.wsj.com/article/SB10001424052748704513104575256701215465596.html>> Retrieved 23rd November 2011.

Strater, K. and Richter, H. (2007). Examining Privacy and Disclosure in a Social Networking Community. In: *Proceedings of the 3rd ACM symposium on Usable Privacy and Security (SOUPS 2007)*, July 18th -20th, 2007, Pittsburgh, USA (pp. 157-158) New York, NY: ACM Press.

Sutter, J. and Carroll, J. (2009). Fears of impostors increase on Facebook. Available from:<<http://edition.cnn.com/2009/TECH/02/05/facebook.impostors/index.html>> Retrieved 25th June 2010

Sweeney, L. (1997). Weaving technology and policy together to maintain confidentiality. *J. of Law, Medicine and Ethics*, 25. pp.98-110

Tan, Y. (2007). Social Networks: Theory and Applications. Available from:<http://faculty.washington.edu/ytan/Research/INFORMS_SNA.ppt>Retrieved 3rd January 2011.

References

- Thelwall, M. (2008). Social networks, gender and friending: an analysis of MySpace member profiles, *Journal of the American Society for Information Science and Technology*, 59(8). pp.1321–1330.
- Thelwall, M. and Stuart, D. (2006). Web crawling ethics revisited: Cost, privacy, and denial of service. *Journal of the American Society for Information Science and Technology*, 57(13),pp.1771-1779.
- Travers, Jeffrey and Milgram, S. (1969). An Experimental Study of the Small World Problem. *Sociometry*, 32(4), pp.425-443.
- Tuunainen, V.K, Pitkänen, O. and Hovi, M. (2009). Users' Awareness of Privacy on Online Social Networking sites – Case Facebook. Available from:<[http://www.bledconference.org/proceedings.nsf/0/9b675b5e811394f0c125760000390664/\\$FILE/1_Tuunainen.pdf](http://www.bledconference.org/proceedings.nsf/0/9b675b5e811394f0c125760000390664/$FILE/1_Tuunainen.pdf)> Retrieved 19th September 2010.
- UK Council for Child Internet Safety. (2010). Click Clever Click Safe. Available from: <<http://clickcleverclicksafe.direct.gov.uk/index.html>> Retrieved 4th December 2010.
- U.S Department of Commerce. (2000). Falling through the Net: Towards digital inclusion. Available from: <<http://www.ntia.doc.gov/ntiahome/fttn00/Falling.htm>> Retrieved 30th January 2010.
- Wang, X.F. and Chen, G. (2003). Complex Networks: Small-World, Scale-Free and Beyond.IEEE,*IEEE Circuits and Systems Magazine*,3(1).pp.6-20.
- Wasserman, S. and Faust, K. (1994). Social network analysis: Methods and applications. Cambridge University Press. Cambridge. UK
- Watts, D.J., Sheridan Dobbs, P. and Newman, M.E.J. (2002). Identity and Search in Social Networks. *Science*, 296(5571). pp.1302-1305.
- Watts, D.J. and Strogatz, S. (1998). Collective dynamics of small networks. *Nature*, 393. pp.440-442.
- Wilson, M. and Nicholas, C. (2008). Topological Analysis of an Online Social Network for Older Adults.ACM.ACM Conference on Information and Knowledge Management.In:*Proceedings of 2008 ACM workshop on Search in social media*, October 26th-30th 2008,Napa Valley, California, USA(pp.51-58).
- Wilson, C., Boe, B., Sala, A., Puttaswamy, K. P. N. and Zhao, B. Y. User Interactions in Social Networks and their Implications.ACM.Eurosys (2009) .In: *Proceedings of the 4th ACM European conference on Computer systems*, March 31st -3rd April,2009,Nuremerberg,Germany (pp. 205-218)New York,NY: ACM Press.
- Vamosi, R. (2011). When Technology betrays us. *Wired*. Jul. pp.140-143.
- Van Tilburg, T.G. (1995). Delineation of the social network and differences in network size. in C.P.M., Knipscheer, J. de Jong Gierveld., T.G. van Tilburg and

References

P.A. Dykstra (eds.) Living Arrangements and Social Networks of Older Adults, pp.83-96, VU University Press, Amsterdam

Viswanath, B., Mislove, A., Meeyoung, C. and Gummadi, K.P. (2009). On the Evolution of User Interaction in Facebook. ACM. ACM SIGCOMM 2009 workshop. In: *Proceedings of the 2nd ACM Workshop on Online Social Networks (WOSN 2009)*, August 17, 2009, Barcelona, Spain, (pp. 37-42) New York, NY: ACM Press.

Vucetic, S. (2007). Machine Learning. Available from :<<http://www.dabi.temple.edu/~vucetic/cis526fall2007/lecture1.pdf>> Retrieved 15th July 2011.

Wellman, B. and Wortley, S. (1990). Different Strokes from Different Folks: Community Ties and Social Support. *The American Journal of Sociology*, 96(3). pp.558-588

Wilkinson, D. and Thelwall, M. (2010). Social network site changes over time: The case of MySpace. *Journal of the American Society for Information Science and Technology*, 61(11).pp.2311-2323.

Xiang, R., Neville, J. and Rogati, M. (2009). Modelling Relationship Strength in Online Social Networks. ACM. World Wide Web Conference. In: *Proceedings of 19th international conference on World Wide Web (WWW'10)*, New York, USA, (pp.981-990) New York, NY: ACM Press.

Xu, J. And Chen, H. (2008). The topology of Dark Networks. ACM. *Communications of the ACM*. 51(10). pp.58-65.

Yun, S., Do, H. And Kim, H.G. (2010). Analysis of User Interactions in Online Social Networks. Available from:<<http://channy.creation.net/blog/data/channy/2010/sns-social-interaction.pdf>> Retrieved 17th September 2010.

Zinoviev, D. and Duong, V. (2009). Towards Understanding Friendship in Online Social Networks. *Journal of Technology, Knowledge and Society*, 5(2).pp.1-8

Zikmund, W. G., Babin, B. J., Carr, J. C., and Griffin, M. (2010). Business Research Methods (8th edition). South-Western Cengage Learning. Stamford. Connecticut.

Appendices

Appendix I

The Importance of Attributes on Online Social Networks

[Exit this survey](#)

1. Introduction

Online social networking (e.g. Facebook, MySpace etc) has become very popular in the last couple of years. Using online social networks involves displaying your personal details which are commonly known as attributes on a profile. The profile acts like an online identity card.

The aim of this questionnaire is to establish which of these typical attributes, when displayed on a public social networking profile, would be the most important in identifying someone.

Please take 5 minutes to answer the questionnaire.

If you have any questions about the questionnaire or the research then email Sophia Alim at salim@bradford.ac.uk

Thank you in advance

[Next](#)

Powered by **SurveyMonkey**
Create your own [free online survey](#) now!

The Importance of Attributes on Online Social Networks

[Exit this survey](#)

2. About You

Please specify your gender and age. This information will be used for statistical purposes only.

1. What is your gender?

- Male
 Female

2. How old are you?

- Under 18
 18-24
 25-34
 35-44
 45 or over

[Prev](#)[Next](#)

Powered by **SurveyMonkey**
Create your own [free online survey](#) now!

The Importance of Attributes on Online Social Networks

Exit this survey

3. Attributes

The table below contains a list of attributes. You are required to specify how important or not you think they are when it comes to disclosing someones identity.

1. Please select either more important, not important or less important for each of the attributes.

	Not Important	Important	Very Important
Full Name	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Gender	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Profile Picture	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Age	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Date of Birth	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Email Address	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Current Address	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hometown	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Marital Status	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Religion	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sexual Orientation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ethnicity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Contact Number	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Zodiac	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Smoker	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Drinker	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Levels of Education	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Places of Education	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Occupation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Prev

Done

Powered by **SurveyMonkey**
Create your own free online survey now!