The Social Engineering Attack Spiral (SEAS)

Andrea Cullen and Lorna Armitage

Abstract - Cybercrime is on the increase and attacks are becoming ever more sophisticated. Organisations are investing huge sums of money and vast resources in trying to establish effective and timely countermeasures. This is still a game of catch up, where hackers have the upper hand and potential victims are trying to produce secure systems hardened against what feels like are inevitable future attacks.

The focus so far has been on technology and not people and the amount of resource allocated to countermeasures and research into cyber security attacks follows the same trend. This paper adds to the growing body of work looking at social engineering attacks and therefore seeks to redress this imbalance to some extent. The objective is to produce a model for social engineering that provides a better understanding of the attack process such that improved and timely countermeasures can be applied and early interventions implemented.

Keywords— security; social engineering; iterative spiral model; targeted attack

I. INTRODUCTION

Social engineering is an issue for organisations and individuals alike. This type of attack is associated with exploiting people who are often considered to be the weakest link in any information system [1]. It is not a new phenomenon; however, technology exacerbates the effect and the effectiveness of this type of attack by the type and amount of data available and the opportunity for users of systems to make mistakes or deliberately divulge sensitive data. To clarify, social engineering is the ability to trick users into doing something that goes against the interest of security [2][3] which "u*ses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not"* [4]. It is a term first used in the 1930s with entire populations in times of war and unrest and was adopted by hackers where it has been used since the 1980s to describe a non-technical attack. It can include computer-based deception (e.g. phishing emails) and human interaction based deception. In any event, it is the various techniques used to obtain information in order to bypass security systems [5].

Given time and persistence, it is suggested that a social engineer can obtain any and all information, causing huge security issues. As attacker, attack and victim are all human, the ability to adapt, change and react unexpectedly is an additional concern. *"The human factor is truly the weakest link"* [4]. This paper firstly discusses different social engineering attack types and current models. It then goes on to consider existing countermeasures for social engineering attacks and the issues these fail to address. The Social engineering attack spiral (SEAS) is then developed using a series of scenarios taken from real world attacks. Conclusions are then presented and future work identified.

II. TYPES OF ATTACK

The two main types of social engineering attacks can be termed as targeted and target of opportunity. Each type has a very different process and structure and as such ultimately requires a very different solution or set of solutions. A target of opportunity attack is distributed as far as possible in the hope that a number of responses are sent, whilst a targeted attack is very specific and a particular victim is selected as a target. These types of attack also have very different chances of success. Targeted attacks can be time consuming but this time spent by hackers' returns very positive results. This paper considers the process steps in a targeted social engineering attack with a view to developing realistic and effective countermeasures.

III. SOCIAL ENGINEERING MODELS

A number of models have been developed to explain social engineering attacks, however these have focused on the actors within the attacks as a way of developing countermeasures, as in Chitrey et al [1]. The model suggests that vulnerabilities are present in four entities: humans; organsiation security policies; technologies; and government laws [1]. They also suggest that social engineering attacks take place over a number of phases where each phase requires an amount of information gathering; in particular they highlight the exploit phase in this respect. This is in contrast to other work [6] suggesting that information gathering takes place at the start of a phased attack. Chitrey et al [1] suggest that the methodology to adopt for preventing a successful social engineering attack is defense in depth. A methodology adopted by others [7].

Others adopt a pragmatic view for model development suggesting that trying to successfully detect a social engineering attack whilst working in a stressful environment is problematic [5]. They go on to discuss the psychological vulnerabilities of individual and triggers in order to develop a model for detection from the perspective of the victim. Bezuidenhout et al [5] suggest that in

contrast to training that is soon forgotten, their model of awareness raising on a daily basis is an effective countermeasure to social engineering threats.

Janczewski and Fu [8] present a model of social engineering attacks initially based on literature and refined through interviews with organsiations. They highlight a series of twelve social engineering based attacks and the impact these have had. One aim of their work is to consider how organsiations can defend against a social engineering attack. They suggest a multifaceted defense approach to include physical security, policy, awareness training, technical controls, security enhanced product and education. Other work looks to highlight awareness raising as a countermeasure to social engineering in an attempt to explore how the effect of a social engineering attack can be reduced [9]. What becomes clear is the need for a systematic and holistic approach towards the defense from social engineering attacks as different and distinct from technical attacks.

Mitnick and Simon [4] proposed a social engineering cycle to include information gathering, development of a relationship, exploitation of the relationship and finally execution to achieve objectives. Nohlberg and Kowalski [10] further develop this staged attack cycle to produce a complex and holistic model suggesting three different cycles: the attack cycle with control; the defense cycle and the victim cycle. Although risk forms part of the model, this is used as way of indicating the reduction of risk to an acceptable level for the attacker.

The model produced here draws on this earlier work and using a number of attack scenarios, looks at the process steps of a social engineering attack with a view to considering interventions at both an early stage and at all later stages of the attack process. The suggestion is that interventions differ depending on the stage of the attack. With this in mind, work conducted into modeling social engineering is combined with technical attack models and is refined with application to industry scenarios. Two scenarios are therefore developed to demonstrate the structure of the attack and how the chances of a successful attack can increase with time and effort. The model here therefore differs from earlier work in that it looks at the stages of a social engineering attack and then suggests where countermeasures and interventions could be the most affective.

IV. Existing Technical Attack Model

Social Engineering differs from technological attack types in that both the hacker and vulnerability are human and therefore both are unpredictable. Models of attack structures for technological attacks can assume that the technology they are attacking is relatively predictable and known. Social engineering has similarities with this perspective but also significant differences. These differences will now be explored with a view to developing a model that is able to predict the process steps of a social engineering attack and later the relevant countermeasures to be applied.

The intrusion kill chain which was first introduced by Hutchins et al [6] to look at addressing targeted, manually operated intrusions. Assumptions prior to this model were that response should happen after the compromise (corrective actions) and that the vulnerability that initially allowed the attack to take place was fixable [6]. However, since this time, this perception caused issues within a technical attack scenario. For example, it can be assumed that the longer the response takes, the more damage is possible. The kill chain looked at interventions at each stage of the attack timeline and indicated courses of action as early as the reconnaissance phase. It is suggested here that for a social engineering attack, early interventions are also possible and the issues highlighted within a technical attack can be compounded when highly vulnerable and unpredictable individuals are involved. As Rader and Walsh [11] point out, cyber security is a people problem where users of computer systems often make bad choices. Countermeasures so far for social engineering have focused on awareness raising and training, defense in depth, or a multifaceted defense approach. Others suggest building a framework of trust and carrying out periodic tests. This paper in contrast presents a comprehensive process structure such that interventions can be applied throughout the attack timeline. It is difficult to ever suggest that a human vulnerability can be completely fixed, however an understanding of the attack process can help with relevant countermeasures at the most appropriate time.

The Kill chain suggests an attack structure starting with reconnaissance, weaponization, delivery, exploitation, installation, command and control and finally action on objectives. Although Huber et al [12] states that social engineering starts with gathering background information, Chitrey et al [1] in contrast suggest that reconnaissance or information gathering for a social engineering attack takes place throughout the attack process; particular within the exploitation phase. Huber et al [12] also suggest that building and maintaining rapport with an individual in order to exploit them is also a time consuming task. It is suggested here that this type of social engineering attack is also very risky for the victim and for the attacker. The longer this activity goes on, the more likely the attacker is to be identified either during or after the attack but also the more likely the victim is to personally suffer from the effects of the attack. In addition, the risk to the organsiation as victim increases as the potential for more information to be divulged over a prolonged period of time also increases.

Although the kill chain is therefore useful for highlighting the process steps in any penetration attack, it does not fully consider the risks to the organsiation or individual or the need for constant information gathering on the part of the perpetrator.

Moore et al [13] look to model and document information security attacks in a structured way. In order to do this, they show how to model possible attacks in the form of attack trees. The trees indicate how an attacker can compromise information and ultimately the organisations' ability to be successful. The suggestion is that security analysts will be able to use the attack structures to identify commonly occurring attack patterns. The developed trees show how attackers conduct a series of steps with alternative methods used to achieve the same or similar objective. For example, in order to exploit a Web server vulnerability, an attacker may either: access sensitive shared intranet resources directly; or access sensitive data from privileges accounts on a Web server. The concept of attack trees in interesting in terms of a social engineering attack as an attacker is likely to make and changes decisions on the fly depending on interactions with victims. The suggestion here is that a social engineer follows a defined set of attack stages but can be iterative in nature, returning to gather information, attempting various techniques, returning to previous stages of the attack process until the attack is successful. As such, a linear attack line is unlikely to represent the attack process for a social engineer.

Michalopolos and Mavridis [14] consider a risk-based approach to the prevention of grooming attacks. They look at modeling the hazards that potential victims are faced with online. They then consider existing risk modeling methods with a view to establishing how they can be adopted within an attack detection system. Although this work looks at vulnerable young children as potential victims of grooming attacks, this work has obvious parallels with social engineering attacks [10], in particular the acknowledgement and introduction of risk.

V. VULNERABILITIES

In order to compromise any information an attacker must exploit vulnerability. In social engineering, the vulnerability is a person and/or a process. The specific person based vulnerability is by its nature, difficult to detect. Bulee et al [9] state that humans are a weak link in cyber security, where apparent harmless actions can be made to look legitimate. They consider how persuasion can influence the effectiveness of an attack and to what extent an intervention in the form of an awareness campaign is successful in reducing the effects of social engineering.

Bezuidenhout et al [5] suggest the ability of people to make conscious, rational judgments and therefore good decisions is not always possible. They attribute this to limited information processing capacity, the use of shortcuts which can lead to judgmental errors, personal preferences, the ability to be influenced by emotions and how relatively easily individuals may be manipulated by others [5]. They go on to state that an individual follows a series of steps to come to a decision where risk will always be an integral part of the process and the outcome uncertain. Previous research therefore indicates that there can be an iterative nature to a social engineering attack; it should consider the role of risk and the ability of an attacker to change the attack structure and methods on the fly and at any time dependent upon the decision made by the victim. In addition, although countermeasures for social engineering attacks have previously been proposed, these do not appear to be aligned to the attack process and do not take into account the chancing vulnerabilities in people.

VI. PREVENTATIVE AND DETECTIVE CONTERMEASURES

Current countermeasures for information security attacks can be termed as preventative, detective or corrective. So far, the countermeasures identified for social engineering attacks have included training, education, technical controls, process development, hiring and employment strategies, defense in depth and the development of policies. These can be seen to be mainly preventative measures and therefore take place prior to a potential attack. Some work has been done to identify the countermeasures and strategies that may be appropriate whilst an attack is in progress. The Social Engineering Attack Detection Model: SEADM developed by Bezuidenhout et al [5], is one such model, which can be used by workers to detect social engineering attacks in a call center environment. It looks at how workers can detect if a caller is trying to manipulate them into giving out information. They suggest that awareness raising is not a one off activity but should be conducted on a daily basis to be effective. Considering previous work, and the differing nature of a social engineering attack, detective and corrective actions can happen simultaneously as the victim and attacker are part of the attack process at the same time. Countermeasures therefore have to take into account this simultaneous delivery and consumption of an attack. The victim becomes part of the process and can often simply hand the information over to the social engineer without realizing the potential repercussions of their actions. Although preventative measures (e.g. training and policy) or detective measures (continuous awareness raising) can suggest what

should be done in an ideal world, as suggested earlier, individuals still use shortcuts, are susceptible to persuasion, are very vulnerable to emotions or may simply make bad decisions.

Corrective countermeasures are useful for changing the circumstances that allowed the attack to take place in the first place (fixing the vulnerability) and for returning the situation back what it was before the attack happened. Corrective actions are often aligned with incidence response and consider the post attack scenario to limit damage and achieve business continuity. Corrective countermeasures for social engineering attacks do not appear to be fully explored in the literature to date.

VII. Motivation

Chitrey et al [1] suggest that the level of damage caused by an attack can depend on the purpose of the attack itself. It is also suggested here that motivation can have a huge impact on the outcome of any social engineering attack. With this in mind, Janczewski and Fu [8] suggest a number of motivational factors to include: fame; revenge; destruction of a system; theft of data; monetary gain; illegal information disclosure; and competitive advantage. Although perpetrator motivation is outside the scope of this paper, it is worth considering how this could ultimately impact upon the outcome of any attack. Motivation will be considered in future work where the model will be developed further. The model will now be proposed and then developed using two attack scenarios.

VIII. Outline of the Proposed Model

The model developed here differs from previous work in that it considers the process steps in a social engineering attack; it takes into account the potential iterative nature of an attack; the need for reconnaissance and information gathering throughout; the inherent consideration of risk; and the changing nature of an ongoing attack and therefore the ability of the attacker to adapt. It also looks to establish how and where the attacker could leave a trace of activity and therefore how ultimately any defense might consider the complete set of countermeasures to include preventative, detective and corrective actions.

Within customer service design, the customer has often been established as part of the process. For example, in self-service restaurants, people can queue and collect food and clear tables to speed up the service, reduce bottlenecks and to make service more effective and efficient. Social engineering defense can take from this work by looking at the vulnerability in the system and using this vulnerability as part of the solution. This could be seen as key to the development of realistic and effective detective and corrective countermeasures. Two scenarios will now be presented to show how these attack structures align with the suggested model.

IX. Scenarios:

The scenarios presented here are taken and modified from real life examples developed as social engineering penetration testing exercises. Targeted social engineering attacks often appear as multi-staged attacks where small amounts of information are used to gain further information, or to test the opportunity for a successful attack and in either case to develop a realistic attack scenario. As with technical attacks, social engineering attacks are becoming ever more sophisticated. These scenarios are simplified for presentation here.

- Scenario 1: The social engineer (SE) uses reconnaissance techniques to find out the PA of a senior manager in an organisation. SE then finds personal information for the PA from social media. After building up a profile of the PA an initial telephone call is made claiming to be an IT engineer. The SE says that there is a fault with the IT systems and if the systems have been running slowly not to worry as they are working hard to fix this. SE makes small talk for a few minutes ensuring that subtle references to the PAs personal life are made (as built up in the profile). This starts to build a familiarity and trust between the SE and the PA. A further telephone call is then made by the SE to the PA, telling the PA that further investigation needs to be done and that her system will need to be looked at. The PA is then asked to provide her login details to the SE. The attack scenario can then be developed depending on the interactions that take place.

- Scenario 2: The SE looked to gain physical access into an office block to obtain confidential sales documents located in the sales director's office. After initial reconnaissance the SE builds up a plan of the building and notices that approximately every hour a number of different staff leave through a side door to go to the smoking shelter. After observing that most staff wear smart clothing and have outdoor clothing on whilst using the shelter, the SE prepares himself with similar clothing and joins staff at the smoking shelter making small talk with a few. When the staff members reenter the building the SE ensures she stays in the middle of the group so that the first person uses their staff card to access the building. She can then enter the

building freely and hold the door for the person after her. After initially ensuring that she can access the building the SE then uses reconnaissance techniques to find out the identity of the sales director's PA and similarly to the first scenario builds up a profile of the PA. This then gives the SE further options to explore the best way to gain access to the sales director's office. Again this attack scenario is developed depending on interactions with the PA.

These scenarios demonstrate that risks are integral to the process and are relevant throughout; that information gathering and reconnaissance is not just conducted at the start but takes place throughout; and that at times, attacks can be complex and multi-staged. The developed model reflects these attributes. The attack model will now be presented building on literature and current models to incorporate a complex multi-staged social engineering attack.

X. The Developed Model

The developed model is discussed in conjunction with some suggested countermeasures to indicate how this model can be useful in designing comprehensive security against social engineering attacks.
Risk is central to the targeted social engineering attack scenario (Figure 1). In addition and as discussed, reconnaissance takes place throughout. Janczewski and Fu [8] presented twelve attack scenarios categorised into: in person; online; and via telephone. All looked at developing trust relationships to some extent, some were iterative and multi-staged in nature and all but one was successful. Indicative of each attack, the developed model therefore represents: multi-staged, iterative, risk driven attacks. Gives opportunity for the attacker to be reactive, develop a unique scenario and is dependent on the attackers' interaction with the victim.

Figure 1 depicts a social engineering attack and can be adapted to incorporate both a very simple and highly complex attack scenario. The social engineering attack starts with a trigger event; indicated at the center of the spiral. The attacker then analyses the risk and carries out initial reconnaissance (recon.). At this stage the attacker is likely to use available online information and published documents as background to learn more about the organisation and the specific victim or victims within the organisation. Organisations could ask who is accessing information and why. The attacker then starts to consider developing a relationship with the victim and to build an initial attack scenario. At this stage, suggested countermeasures could include policy development around published information and information access control. In addition, awareness raising and HR hiring policies are useful.

In the next phase, the attacker looks to build a relationship with the victim. Developing processes and procedures around interaction and disclosure of information could be beneficial at this stage as a reliance on training and awareness raising when the attacker sets out to intentionally mislead the victim is problematic. The attacker will next look to develop a realistic attack to target the vulnerabilities in the system and the individual. Where critical information is involved, organisations could look where possible to continuously review and to make minor changes to procedures such that it is difficult for social engineers to establish consistent vulnerabilities. In addition, separation and rotation of duties could be beneficial. Detection of an attack reduces risk considerably at these early stages of the attack process.

At each iteration, the attacker plans for the next phase. Interaction between the attacker and the victim is however possible throughout the attack development phase. When the attack is fully developed, the attacker executes the attack and acts on the information elicited. At this stage, the organisations security measures move from preventative and early detective to incorporate attack detection and corrective countermeasures. Corrective countermeasures should consider incidence response. Education around what to do in the event of a data breach with clear processes is helpful.

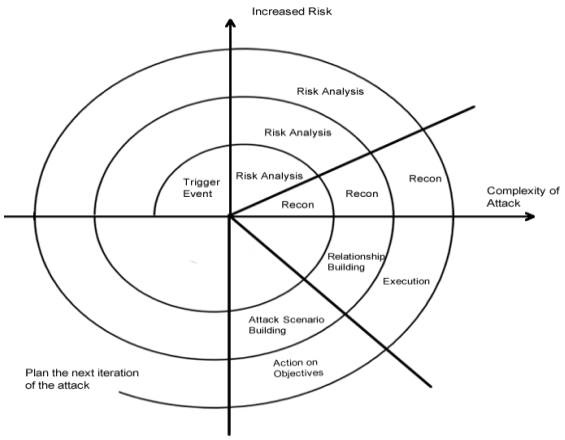

Figure 1. Social Engineering Attack

The model indicates that as the attack is developed, the complexity of the attack scenario increases. In addition, the risks to the organsiation, the victim and to the attacker although present throughout, also increase. Consideration of increased risks at each stage could be better understood through comprehensive and clear risk assessment and management procedures.

XI. Conclusion & Future Work

This model has been developed in order to produce a better understanding of the attack process for social engineering. It has been designed such that it demonstrates all social engineering targeted attacks from the very simple and straightforward to the highly complex. The suggestion is that reconnaissance and risk are integral to the process and are considered throughout and as such, early interventions are possible to stop attacks progressing.

The next stage is to further consider how this model can be useful for implementing a more comprehensive set of timely countermeasures. Early intervention reduces risk and the cost associated with the attack. It is suggested that prevention of an attack, detection should an attack occur and the opportunity for effective corrective action could be beneficial. Disrupting the attack as early as possible is the most desired outcome before costs become too high. This model can be useful in establishing where further interventions are possible and the type of intervention that is the most appropriate at each stage. Further research will be useful in establishing the effectiveness of these. The model can be developed to incorporate motivations, the insider attack and the victim as a greater part of the solution. The model can then be tested using a wider set of scenarios.

References

[1] A. Chitrey, D. Singh, M. Bag and V.Singh, "A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model," International Journal of Information & Network Security (JINS), vol. 1, pp. 45-53, June 2012.

[2] R. J. Boyle and R. R. Panko, "Corporate Computer Security", Prentice Hall, NJ, 2012

[3] I. Mann, "Hacking the Human II: the adventures of a social engineer", Consilience Media, UK, 2013

[4] K. Mitnick and W. L. Simon, "The Art of Deception: controlling the human element of security", John Wiley and Sons, NJ, 2002

[5] M. Bezuidenhout, F Mouton and H. S. Venter, "Social Engineering Attack Detection Model: SEADM", IEEE Information Security for South Africa (ISSA), pp.1-8, 2010

[6] E. M. Hutchins, M. J. Cloppert and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" 6th International Conference on Information Warfare and Security, pp.113-125, 2010

[7] A. J. Cullen and I. Mann, "Hacking the Human: Countering the Socially Engineered Attack", 7th European Conference on Information Warfare and Security (ECIW), Plymouth, 2008

[8] L. J. Janczewski and L. Fu, "Social Engineering-Based Attacks: Model and New Zealand Perspective", IEEE International Multiconference on Computer Science and Information Technology, pp.847-853, 2010

[9] J. W. H. Bulee, L. Montoya, W. Pieters, M. Junger and P. H. Hartel, "The Persuasion and Security Awareness Experiment: reducing the success of social engineering attacks", Journal of Experimental Criminology, Vol. 11 Iss. 1, pp.97-115, March 2015

[10] M. Nohlberg and S. Kowalski, "The Cycle of Deception - A Model of Social Engineering Attacks, Defences and Victims", Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008)

[11] E. Rader and R. Walsh, “Identifying Patterns in Informal Sources of Security Information”, Journal of Cybersecurity Advance Access, Oxford University Press, pp.1-24, December 2015

[12] M. Huber, S. Kowalski, M. Nohlberg and S. Tjoa, “Towards Automating Social Engineering Using Social Networking Sites”, IEEE International Conference on Computational Science and Engineering, 2009

[13] A. P. Moore, R. J. Ellison and R. C. Linger, “Attack Modelling for Information Security and Survivability”, Technical Note, The Software Engineering Institute, Carnegie Melon University, 2001

[14] D. Michalopoulos and I. Mavridis, “Towards Risk Based Prevention of Grooming Attacks”, IEEE Conference Security and Cryptography (SECRYPT), pp.1-4, Athens, 2010