Intelligent Quality Performance Assessment for E-Banking Security using Fuzzy Logic

Maher Aburrous
Dept. of Computing, University of Bradford, UK
mrmaburr@bradford.ac.uk

M. A. Hossain
Dept. of Computing, University of Bradford, UK
m.a.hossain1@bradford.ac.uk

Fadi Thabatah.
MIS Department Philadelphia University, Jordan
ffayez@philadelphia.edu.jo

Keshav Dahal
Dept. of Computing, University of Bradford, UK.
k.p.dahal@bradford.ac.uk

Abstract

Security has been widely recognized as one of the main obstacles to the adoption of Internet banking and it is considered an important aspect in the debate over challenges facing internet banking. The performance evaluation of e-banking websites requires a model that enables us to analyze the various imperative factors and criteria related to the quality and performance of e-banking websites. E-banking site evaluation is a complex and dynamic problem involving many factors, and because of the subjective considerations and the ambiguities involved in the assessment, Fuzzy Logic (FL) model can be an effective tool in assessing and evaluating of e-banking security performance and quality. In this paper, we propose an intelligent performance assessment model for evaluating e-banking security websites. The proposed model is based on FL operators and produces four measures of security risk attack dimensions: direct internal attack, communication tampering attack, code programming attack and denial of service attack with a hierarchical ring layer structure. Our experimental results show that direct internal attack risk has a large impact on e-banking security performance. The results also confirm that the risk of direct internal attack for e-banking dynamic websites is doubled that of all other attacks.

1. Introduction

Electronic banking systems provide users with easy access to banking services, including, retrieving the balance of an account, money transfers between accounts, retrieving an account history, etc [8].

The number of personal computers and internet users are increasing. Customers often like to use new information technologies for the various online transactions related internet banking and online shopping. In online shopping, the internet provides customers with the selection flexibility and saves them a great deal of time in making shopping decisions. The increasing volume of electronic commerce generates a corresponding demand for electronic payment processes offered by financial institutions and banks. Furthermore, other follow-up activities such as paying bills, transferring funds between accounts, and credit card-related transactions need to be processed online [7]. Therefore, the customer-oriented demand on internet banking increases.

Security has been widely recognized as one of the main obstacles to the adoption of internet banking [4]. The performance evaluation of e-banking websites requires a model that enables us to analyse the various important factors related to the quality and performance of e-banking websites. Since e-banking site evaluation is a complex and dynamic problem, Fuzzy Logic (FL) can be an effective tool in assessing and evaluating e-banking security performance since FL offers a natural way of dealing with quality factors rather than exact values.

In this paper, we investigate the different quality dimensions related to internet banking security by trying to answer questions such as: What are the most important criteria with reference to security that satisfies e-banking customers and bankers. Moreover, we design and formulate a simple method to assess the quality of e-banking websites for customers and decision-makers. The different criteria selected for evaluating the e-banking websites are derived through a comprehensive investigation, exploratory fieldwork, interviews, observations, survey questionnaire, automated assessing scanning tools and consultation with several experts.

The paper is organized as follows: Section 2 presents the methodology used to collect data and Section 3 discusses the security architecture of internet banking and FL Expert System. Section 5 presents the proposed FL model for e-banking security performance and quality assessment. Section 6 shows the different rule base structure and entries for all the proposed model phases. Section 7 reveals the implementation results after defuzzification process and then conclusions are given in Section 8.

2. Research Methodology

2.1 Exploratory Fieldworks: Case Study

We conducted an exploratory fieldwork case study on leading private-sector banks in Jordan over three-month period to achieve the research objectives.
The research techniques used in the case study are: open and semi-structured interviews, observations and participation in the project management, and review of documents. We used an open and semi structured interviews with the senior executives of the IT department, e-security and e-banking operations in the banks.

We discovered from the conducted interviews that internet banking in Jordan is facing difficulties that limit the development of e-banking services in the future. These difficulties include: lack of regulations, policies and e-banking laws and legislation to protect customers from internet fraud, lack of internet connections speed and telecommunications infrastructures, lack of internet awareness culture and general computer skills, high internet connection costs and finally security, privacy and trust problems that highly influence the acceptance of internet banking and increases the fear of using it [3].

2.2 Mail Questionnaire Survey

We designed a mail questionnaire, which has been sent to a number of random Jordan Ahli Bank employees and clients. The primary objectives of the questionnaire were (1) to assess the satisfaction of customers regarding the performance quality and security procedures of Jordan Ahli Bank internet banking website (2) to reveal the perception of clients in terms of using the internet both as communication tool and as a delivery channel.

The questionnaire survey showed that the security factor is considered one of the most important factors related to e-banking since services such as money transfers and electronic payments cannot be vulnerable to any kind of attacks [19]. Furthermore, the lack of assurance, trust, privacy and security hinder the e-banking development. In other words, when customers don't trust security and privacy in e-banking, they don't make transactions related to money via the internet [20].

2.3 Automatic Security Scanning Tools

With the help of automated hacking and cracking tools as well as web scanner applications, we managed to test and assess the level of security and vulnerability of the e-banking websites case study. This process helped us in determining and analyzing the critical factors related to scanning, testing and assessing e-banking websites performance factors. For example, we used Acunetix Web Vulnerability Scanner (WVS) [1] for automatically testing web sites for vulnerabilities such as SQL attacks, Cross Site Scripting, CRLF injection, Directory Traversal, Authentication Hacking and Google Hacking.

So we can see from the case study, the survey conducted, and the automatic security scanning tools that the greatest challenge to e-banking websites is winning the trust of customers over privacy and security. Different quality and performance dimensions related to internet banking security assessment were also produced from these experiments as well as specifying all the security risks categories and criteria that can damage and hinder e-banking websites and threat their existence.

3. Internet Banking and Fuzzy Logic

3.1 Internet Banking Security Architecture

There are many threats that any internet banking dynamic website can fall into, including, spoofing, denial-of-service attack, SQL injection, phishing attacks, sniffing, page hijacking, brute force, buffer overflows, and social engineering. Financial institutions engaging in any form of internet banking should have effective and reliable methods to authenticate their customers. These methods include, the use of customer passwords, personal identification numbers(PIN), digital certificates using public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug0-ins, transaction profile scripts, and biometric identification [11]. Moreover, most internet banks offer other protective measures to ensure information is safe and secure such as secure logins, limited logins (lock out if exceed) and limited sessions (require to re-login if inactive for a period of time [18].

Internet attackers have become more sophisticated since they moved from network level attacks such as abusing firewall and filtering rules to application level, that of attacking and exploiting code within web applications such as SQL injections or input validation attacks and direct internal level such as social engineering and phishing attacks.
Direct internal attacks are the primary threat to computer systems since they are likely to have specific goals and objectives, and have legitimate access to the system. This type of attack can be extremely difficult to detect or protect against [13]. The direct internal attack can affect all components

of computer security and the confidentiality of information on the system.

3.2 FL Expert System

A fuzzy expert system is an expert system that uses FL instead of Boolean logic. In other words, it is a collection of membership functions and rules that are utilised to reason about data [6].

Fuzzy approach requires sufficient expert knowledge in the formulation of the rule base, the combination of the sets and the defuzzification. In General, the employment of FL might be helpful for complex processes such as when there is no simple mathematical model. Fourali [12] highlights the relevance of FL to the task of measuring educational achievement in which he introduced the principles behind FL and illustrated how these principles could be applied by educators in the area of assessment using portfolio evidence. Murphy [17] discussed the primary risk factors in developing projects and the keys to a successful risk management programme. Cox [9] examined the organisation of a business rule systems and looked at how these rules should be organised and written in order to address the uncertainty and imprecision of business decisions using FL.

Abdul Rahim [2] showed the utilisation of fuzzy technology in modeling subjective, vague and uncertain web usability and design guidelines. Yuksel [20] determined the key quality dimensions in internet banking using survey questionnaire. Davoli [10] presented a Fuzzy Quality Tree for web inspection (FQT4web), a qualitative, robust and efficient inspector-based methodology for website evaluation that has a hierarchical structure. In his paper, he produced six measures of quality dimensions and an overall quality score for web sites. Finally, Alasgarova [5] examined the beneficial aspects of using fuzzy database for credit risk prediction decision.

The inference process in FL goes through four steps [9] Fuzzification, . Inference, Composition and Defuzzification**.**

4. System Design

Since FL offers a more natural way of assessing security factors instead of exact values, we used it to evaluate and assess the security of the dynamic internet banking websites by classifying all the online security risks, threats and vulnerability according to an important weight. This classification will enable us to produce an overall security score for an e-banking website. The proposed system shown in Figure 1 has been implemented in MATLAB and is designed using four main e-banking risk criteria, including: Direct internal attack risk, communication tampering attack risk, code programming attack risk and denial of service attack risk. Two IT auditors from each bank (5 banks) and a questionnaire have been used for judging the importance of the above four criterions.

From each case-study, we choose two IT auditors to answer the questionnaire, which consisted of 80 scaled questions (20 questions for each risk). Instructions have been given to the IT auditors to tick the corresponding box on the satisfaction scale, then to decide the minimum position and the maximum position he/s accepts. For instance, an assessor might think that question 2 for the selected risk criteria is fair but not strong, hence he may tick box 5 on the scale, and then he may realize also that a lower rating, i.e. 4 is acceptable [12]. Calculation of the assessment criteria can be computed as follows: Average outcome**: (1*1+2*2+2*3+3*4+2*5)/10 = 3.3**

Analysis of the data collected from the IT auditors revealed that the internal direct attack is the highest security risk factor, and other risks have lower impact. In other words, the internal direct risk attack factor is double that of others. The internal direct attack deals with human factor, which is not easy to be controlled and managed. On the other hand, the other security risk factors can be controlled and eliminated by the various kinds of hardwares and softwares such as: firewalls, automated scanning tools and antivirus applications to protect the network. The complete framework is demonstrated in Figure 1 with all criteria.

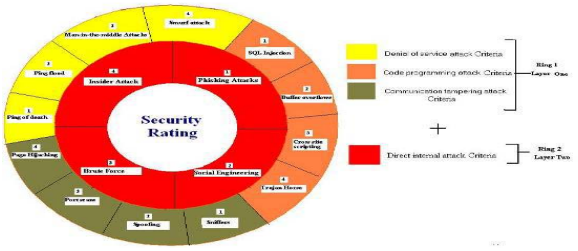

Figure 1: Structure of the system in MATLAB

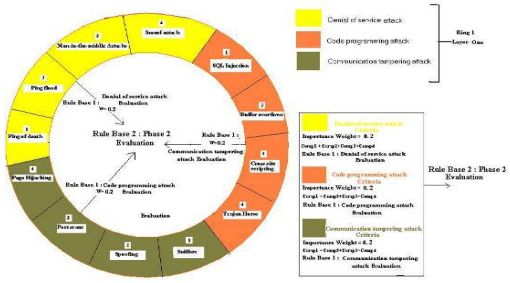

Figure 2 : Ring layer 1 - Phase 2 evaluation

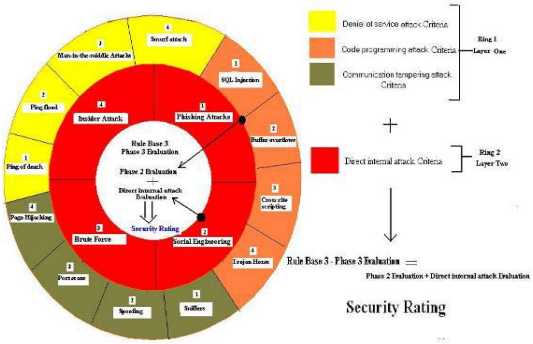

Figure 3 : Pahse 3 evaluation - Final Security Rating

5. System Criteria

5.1 Criteria Considered in Evaluating the Security of E-banking Sites

Security assessment is performed based on four risk attack criteria: direct internal attack, communication tampering attack, code programming attack and denial of service attack. There are four components for each criterion as shown in Table 1, which explains the relationship between criteria and components. Table 1 also shows that there are two ring layers, where the first ring layer contains: communication tampering attack, code programming attack and denial of service attack and the second ring layer contains only the direct internal attack.

The proposed model is based on fuzzy operators for e-banking website security evaluation, which produces four measures of security risk attack dimensions with **a hierarchical ring layer structure**. The four criteria have been prioritized according to their importance using weights as concluded from the survey where each criterion is divided further into four components as shown in Table 1. Developed in the model are two ring layers where the criteria of the least important ones are placed in the first layer with a weight equal to **0.2**, and their union produces Rule base 2 (Phase 2 evaluation). The criteria with the greater importance are placed in the second ring layer and assigned a weight of **0.4,** and it produces rule base 1 (Direct internal attack evaluation) as shown in Figure 3. The combination of rule base 2 and rule base 1 derives rule base 3 (Phase 3 evaluation) which represents the final security rating as shown in Figure 4.

Final Rating = 0.4* Direct internal attack crisp [second ring layer] + ((0.2*Communication tampering attack crisp)+(0.2*Code programming attack crisp) + (0.2 *Denial of service attack crisp)) [First ring layer] **Or**

Final Rating = 0.4* Direct internal attack Crisp [second ring layer] +0.6*Phase 3 crisp [First ring layer]

Table 1: Layers of e-banking risk attacks criteria.

Criteria	No.	Component	Layer nol
Direct internal attack	1	Phishing Attack	**Layer Two (2) Second Ring** **Subtotal Weight =**
	2	Social Engineering	
	3	Brute Force	
	4	Insider Attack	
Communication tampering attack	1	Sniffing	**Layer One (1) First Ring** **Subtotal Weight = 0.6**
	2	Spoofing	
	3	Port Scans	
	4	Page Hijacking	
Code programming attack	1	SQL Injection	
	2	Buffer Overflow	
	3	Cross Site Scripting	
	4	Trojan Horse	
Denial of service attack **(Weight =0.2)**	1	Ping of Death	
	2	Ping Flood	
	3	Man in the Middle	
	4	Smurf Attack	
Total Weight			1

5.2 Primary Inputs and Output of the System

There are four criteria and for each criterion there are four components. Therefore, there are sixteen components in total, where for each component, five questions are defined and a component is judged on the scale 1-5 inclusive based on the outcome of these five questions. Each component takes one integer value as primary input [14]. Membership values of the three fuzzy sets ("**low risk**", "**moderate risk**", "**high risk**") were produced using fuzzification to the integer crisp values of the four components of each criterion. Defining five output fuzzy sets: "annoying", "harmful", "destructive", (triangular membership function) and "safe","catastrophic" (Trapezoidal membership function).

6. The Rule Base

6.1 The Rule Base for Phase 1

The rule base has four input parameters and one output and contains all the "IF-THEN" rules of the system. For each entry of the rule base, each component is assumed to be one of three values and each criterion has four components. Therefore, the rule base contains (3^4) = 81entries. A sample of the structure and the entries of the rule base for phase 1 are shown in Table 2. The system structure for direct internal attack is the joining of its four components

(phishing attack, social engineering attack, insider attack, and brute force attack), which produces the direct internal attack rule base 1.

Table 2 : Sample of the rule base1 structure and entries for direct internal attack valuation

Rule	Phishing Attack	Social Engineering Attack	Insider Attack	Brute Force Attack	Direct Internal Attack
1	Low Risk	Low Risk	Low Risk	Low Risk	Safe
3	Low Risk	Low Risk	Low Risk	High Risk	Harmful
27	Low Risk	High Risk	High Risk	High Risk	Catastrophic
28	Mod. Risk	Low Risk	Low Risk	Low Risk	Annoying
30	Mod. Risk	Low Risk	Low Risk	High Risk	Harmful
54	Mod. Risk	High Risk	High Risk	High Risk	Destructive
55	High Risk	Low Risk	Low Risk	Low Risk	Harmful
57	High Risk	Low Risk	Low Risk	High Risk	Destructive
79	High Risk	High Risk	High Risk	Low Risk	Catastrophic

6.2 The Rule Base for Phase 2

In phase 2, there are three inputs, which are (denial of service attack, communication tampering attack and code programming attack) and one output. A sample of the structure and the entries of the rule base for phase 2 are illustrated in Table 3.
The system structure for phase 2 is the combination of three attacks (denial of service attack, communication tampering attack and code programming attack), which produces rule base 2.

Table 3 : Rule Base2 structure and entries for phase 2

Rule	Denial of Service Attack	Communication Attack	Code Programming Attack	Rating
1	Low Risk	Low Risk	Low Risk	Safe
2	Low Risk	Low Risk	Mod. Risk	Annoying
9	Low Risk	High Risk	High Risk	Destructive
10	Mod. Risk	Low Risk	Low Risk	Annoying
12	Mod. Risk	Low Risk	High Risk	Harmful
18	Mod. Risk	High Risk	High Risk	Catastrophic
19	High Risk	Low Risk	Low Risk	Harmful
20	High Risk	Low Risk	Mod. Risk	Harmful
27	High Risk	High Risk	High Risk	Catastrophic

6.3 The Rule Base for Phase 3

In phase 3, there are two inputs, which are: the direct internal attack and "Phase2"which is the output from phase 2, and one output. The structure and the entries of the rule base for phase 3 are shown in Table 4.
The system structure for phase 3 is the combination of direct internal attack and "Phase2", which produces rule base 3 and the final security rating.

Table 4: Rule Base 3 structure and entries for phase 3

Rule	Phase 2	Direct Internal Attack	Final Security Rating
1	Low Risk	Low Risk	Safe
2	Low Risk	Moderate Risk	Destructive
3	Low Risk	High Risk	Catastrophic
4	Moderate Risk	Low Risk	Annoying
5	Moderate Risk	Moderate Risk	Destructive
6	Moderate Risk	High Risk	Catastrophic
7	High Risk	Low Risk	Harmful
8	High Risk	Moderate Risk	Destructive
9	High Risk	High Risk	Catastrophic

7. Defuzzification and Interesting experimental Results

Clipping method [15] is used in aggregating the consequences and the aggregated surface of the rule evaluation is defuzzified using Mamdani method [16] to find the Center Of Gravity (COG). Centroid defuzzification technique shown in equation (1) can be expressed as where x^* is the defuzzified output, $\mu i(x)$ is the aggregated membership function and x is the output variable.

$$x^* = \frac{\int \mu_i(x) \times dx}{\int \mu_i(x)\, dx} \qquad \text{Equation (1)}$$

The proposed intelligent e-banking website security evaluation system has been implemented in MATLAB 6.5. The results of some input combinations are listed in Tables 5, 6. The security rating will be low (15.6 %), which means that the e-banking website is secure, highly protected and hard to be hacked or penetrated when all risk attacks have zero inputs. Further, the security rating will be high (84.4 %), which means that the e-banking website is not secured enough and can be easily hacked or penetrated when the direct internal attack has 10 inputs values and all other risks values have zero inputs as shown in Table 5. Whereas, the security risk attack will be equilibrium (50%), which means that the e-banking site is somehow secure and protected but it can be penetrated or hacked when the direct internal attack has zero input and all other risk attacks have the value of 10 inputs as shown in Table 6. This result shows that the direct internal attack is more important than all other risk attacks.

Table 5: Four highest (10) inputs for criteria (Direct internal attack) and all other lowest (0) inputs

№	Denial of Service Attack	Communication Attack	Code Programm Attack	Direct Internal Attack	% Security Rating
1	10	10	10	0	50.0
2	10	10	10	0	
3	10	10	10	0	
4	10	10	10	0	

Table 6: Four lowest (0) inputs for criteria (Direct internal attack) and all other highest (10) inputs

No	Denial of Service Attack	Communication Attack	Code Programm Attack	Direct Internal Attack	% Security Rating
1	0	0	0	10	84.4
2	0	0	0	10	
3	0	0	0	10	
4	0	0	0	10	

8. Conclusions and Future Work

In this paper, we proposed an intelligent performance assessment model for e-banking security evaluation websites. Fuzzy Logic (FL) was used in the design phase and MATLAB was utilised in the implementation phase of our model. The results indicate that the worst security rate equals 87.5% and the best security rate is 15.6% rather than a full range, i.e. 0 to 100, because of the fuzzification process. Moreover, the results show that the direct internal attack risk has a large impact on e-banking security performance since it achieves a security rate of to 84.4 %.

Interesting results can also be noticed when the direct internal attack has four input values from ten, and all other attacks have (0) input value since the security rating produced was 55.7%. This means that the e-banking website is somehow secure, but it can be penetrated. Proper training of e-banking customers on recognising and avoiding the direct internal security attacks may help improving the security and enhancing the customers overall confidence over long terms. The utilisation of FL in assessing e-banking security evaluation is still wide open research area, which can reveal quite interesting results. We are going to examine in near future how the results and security rate are changed when more risk criteria, ring layers and different relative importance weight for these risks are added and taken into accounts.

References:

[1] http://www.ebankingsecurity.com.

[2] A. R. Ahmad and O. Basir. Fuzzy Inferencing in the Webpage Layout Design. Working Paper. System Design Engineering University of Waterloo, Waterloo, Canada, 2003.

[3] A. Al Sukkar and H. Hasan. Toward a Model for the Acceptance of Internet Banking in Developing Countries. Information Technology for Development, Vol. 11(4) 381-398 Wiley Periodicals, 2005.

[4] A. M. Aladwani. Online banking: a field study of drivers, development challenges, and expectations. International Journal of Information Management 21 (4), 213-225, 2001.

[5] A. N. Alasgarova. Financial Credit Risk Prediction with Fuzzy System. Engineering and Applied Sciences department, Khazar University, 2005.

[6] J. Buckley and D. Tucker. Second generation fuzzy expert system. *Fuzzy Sets and Systems*, 31:271{284, 1989.

[7] F. O. Celikcapa and G. G. Emel. E-Banking Options: Which one best fits for customer?. Uludag University, Bursa, 16059, Turkey, 2002.

[8] J. Claessens, B. Preneel and J. Vandewalle. A Tangled World Wide Web of Security Issues. First Moday, Vol. 7, No. 3, 2002.

[9] E. Cox. FL and Measures of Certainty in E-Commerce Expert System. Article. Scianta Intelligence, Chapel Hill, 2001.

[10] P. Davoli, E. Corradini, E. Garzillo, M. Nuccio, and A. Russo. Inspection of Museum Web Application Quality- Analysis of Selected European Sites. Proceeding CDROM. Toronto: Archives & Museum Informatics, March 2004.

[11] Federal Financial Institutions Examination Council. Authentication in an Internet Banking Environment, FFIEC gencies (August 2001 Guidance).

[12] C. Fourali. Using FL in Educational Measurement: The Case of Portfolio Assessment. Research Department, City & Guilds, London. Vol.11, No. 3, 1997.

[13] P. Gaonjur and C. Bokhoree. Risk of Insider Threats in Information Technology Outsourcing: Can deceptive techniques be applied?. School of Business Informatics, University of Technology, Mauritius, 2006.

[14] M. S. Hasan, M. A. Hossain and M. L. Rahman. FL Based Decision Support System for E-Commerce Site Assessment. Proceedings International Conference on Computing & Information Technology (ICCIT), pp. ID-72, Dhaka, Bangladesh, 2004.

[15] C. Y. Ho, B. W. Ling, and J. D. Reiss. Fuzzy Impulsive Control of High-Order Interpolative Low-Pass Sigma–Delta Modulators. IEEE Transactions on Circuits and Systems—I: Regular Papers, Vol. 53, No. 10, October 2006.

[16] M. Liu, D. Chen and C. Wu. The continuity of Mamdani method. International Conference on Machine Learning and Cybernetics, Page(s): 1680 - 1682 vol.3, 2002.

[17] Dr. J. Murphy. Assuring Performance in E-Commerce Systems. Proc. of IEE 16th UK Teletraffic Symposium, pp. 29/1-29/7, Harlow, May 2000.

[18] F. Owen. Is Online Banking A Safe Choice. EzineArticles.com, 2006.

[19] C. Ranganathan and S. Ganapathy. Key Dimensions of Business-to-Customer Web Sites. Information and Management, Vol. 39, 2002.

[20] H. Yuksel. Quality Dimensions of Internet Banking: An Empirical Study. 35th International Conference on Computer and Industrial Engineering, 2005.