Study on security risks of e-banking system

Gabriela Mogos[1], Nor Shahida Mohd Jamail[2]
[1]Department of Computer Science and Software Engineering, Xi'an Jiaotong-Liverpool University, Suzhou, China
[2]Department of Electrical Engineering, Prince Sultan University, Riyadh, Saudi Arabia

Article Info

Article history:

Received Mar 10, 2020
Revised May 11, 2020
Accepted May 25, 2020

Keywords:

E–banking
Risks
Security
Threats

ABSTRACT

Online banking and other e-banking modes are a very convenient way to banking in terms of speed, convenience and delivery costs, but they have brought many risks alongside them. Online banking has created a new risk orientation and even new forms of risk. Technology plays an important role as both a source and a tool for risk control. The purpose of this research is to identify the security situation of the e-banking application and to analyze the risks and attacks that could occur to the customers that, although it's an e-banking application attacks could happen. Several mitigations were mentioned to overcome attacks like, access control is to mitigate eavesdropping this means that, restricting access to sensitive data is mandatory. Another way to mitigate is, update and patch which is for SQL injection meaning, it's vital to apply patches and updates when it's available. These attacks may attack the whole application or target an individual where private information is stolen or changed. This research also shows how to apply several more different protections measures to protect oneself and organization from being targets of cybercrime.

Corresponding Author:

Gabriela Mogos
Department of Computer Science and Software Engineering
Xi'an Jiaotong-Liverpool University
Suzhou, China
Email: Gabriela.Mogos@xjtlu.edu.cn

1. INTRODUCTION

Payment is an integral part of the business, no difference if it is done traditionally or electronically. The electronic business mode, especially electronic commerce, stipulates some payment techniques that could be examined as an electronic option of the traditional payment system [1]. Because of these traditional instruments, various electronic payment appliances are being developed nowadays. Those might be classified, as follows: Electronic credit card; Electronic cheque; Electronic cash; Electronic payment peer-peer; Electronic wallet; Payment cards; Electronic payment via mobile devices; Electronic asset transfer.

Given the traditional and electronic payment system, the fundamental difference between these can be seen in the design scope, i.e. everything within the second is digital. All the above-mentioned activities point to a sort of specific form of banking that has been developed as internet or electronic banking over the past few years [2]. Risk assessment is a method for determining the likelihood and impact of loss of information integrity, availability, and confidentiality. The risk assessment method includes information asset valuation and identification of threats to, and vulnerabilities of, the target information.

2. RESEARCH METHOD

To determine the likelihood of a future harmful event, it is necessary to analyze threats to an IT system in conjunction with potential vulnerabilities and IT system controls [3]. Impact refers to the extent of the harm that could result from the vulnerability exercise of a threat. The impact level is governed by the potential impacts of the mission and in turn generates a relative value for the affected IT assets and resources.

The hasty advances in banking induce many advantages for financial institutions and consumers, but harmful side effects. However, electronic banking does not set up some new risk profiles but attracts attention to those that are dealt with by any financial institution. These risks, which could be covered in part, will be described briefly below:

a) Operational/Transaction risk – The transaction risk could also emerge from the bank inability to control the third party – provider of the service [4].
b) trategic risk – Sort of risk that affects the investment's long - term earnings due to inappropriate business decisions and inadequate performance. Nevertheless, despite the smaller banks, the huge banks do not make their decisions about implementing the e-banking system because of investment returns and cost-benefit analysis, but because of the challenge of succeeding in the heavy competition. Often, it doesn't mean a certain success.
c) Technology risk – The present and potential risk arose as a result of losses, infringements, abnormalities and breakdown of computer hardware, software, online services, etc.
d) Compliance risk – A type of risk arose from non-compliance with state legislation, policy instruments and ethical principles. The financial institution must subsequently be aware of the law that can be obtained and make sure that it applies to other directions such as branch banking. Compliance risk also includes the need to remain confidential with the data of consumers [5].
e) Reputation risk – The public judgment takes into account a variety of risks that could be quite negative. This could result from the inadequate methods chosen to perform e-banking services [6].
f) Information security risk – The financial institution must identify certain critical factors aimed at protecting itself and consumers in the course of several preventive activities, such as: ensuring the logo of the institution and more to maintain the commercial reputation of the website [7]. Those could be damaged by the individuals and groups ' non-ethical and criminal attitude because it could be seen as a threat to the e- bank system as a whole, but also to consumers.
g) Credit risk – A risk category emerged from the consumer's inability to fulfil his / her financial obligations. E - banking offers customers the opportunity to apply for a loan from anywhere in the world, but this makes it difficult for the bank to recognize the applicants ' credit ability [8].
h) Interest rate risk – Risk related to interest rate movements. Because e–banking gives customers the opportunity to compare different interest rates for banks, banks need to proceed quickly to retain or acquire loans and deposits from customers [9].
i) Liquidity risk – It appears from the bank's inability to meet its financial responsibilities. The costumers are therefore likely to draw from the bank association and go anywhere else where the rate clauses are better.
j) Foreign exchange risk E-banking may encourage residents of a single state to make transactions in their domestic currency, as a result of which many speculative actions may be undertaken by customers [10].

In our study, for modelling and analysis, we used Microsoft Threat Modeling Tool 2016

3. RESULTS AND DISCUSSION

Security is the combination of systems, applications, and internal controls used to protect data and operating process integrity, authenticity, and confidentiality. Proper security is based on developing and implementing appropriate security policies and measures for bank processes and communication between the bank and external parties. Security measures are combinations of hardware and software tools and staff management that help build secure systems and operations.

3.1. Distinction of risks at service

a) Level Information Service (Low Risk). This is the most basic form of online Internet service that provides one - way communication covering advertising, promotional material, and so on. Websites are often hacking targets that vandalize and mutilate the original information being processed resulting in reputational harm.
b) Interactive Information Exchange (Medium risk). Customers can communicate with the bank, conduct account inquiries and complete application forms, etc. The risk of these websites depends on whether they have direct links to the internal network of the bank [11].

c) Transactional Service (High risk). This service is the most vulnerable because the customers are executing online money transfers, bill payments, online shopping and other financial transactions and this is the highest risk category that requires the strongest control.

3.2. Authentication techniques

Confirming that a particular request for communication, transaction or access is legitimate is essential in banking. Banks should therefore use reliable methods to verify new customer identity and authorization as well as authenticate the identity and authorization of established customers seeking to initiate electronic transactions. It can be a difficult task to establish and authenticate the identity and authorization of an individual to access banking systems in an open network environment that is purely electronic. Legitimate user authorization can be misrepresented through a variety of "spoofing" techniques [12, 13].

As authentication methods continue to evolve, banks are encouraged to monitor and implement sound industry practices in this area, such as [14]:

a) Authentication databases - providing access to e - bank customer accounts or sensitive systems is protected against corruption and tampering. Any such manipulation should be detectable, and to document such attempts, audit trails should be in place.
b) Any addition, deletion or change of an individual, an authenticated source is duly authorized by the agent or system in the authentication database.
c) Appropriate measures are in place to control the connection of the e-banking system so that known customers can’t be displaced by unknown third parties.
d) Authenticated e-banking sessions remain secure throughout the session or should the session require re-authentication in the event of a security lapse.

3.3. Vulnerability statement

Threats can target vulnerabilities when data is at rest (in storage on media of many types), during processing (while they are being input, filtered, parsed, manipulated, and so on) or while in transit (wired, wireless, or even internal to a system). The risks at these three data stages can be very different and therefore need to be analyzed individually [15, 16]. This threat modelling diagram as shown in Figure 1 is used to find out the login vulnerabilities in online banking.

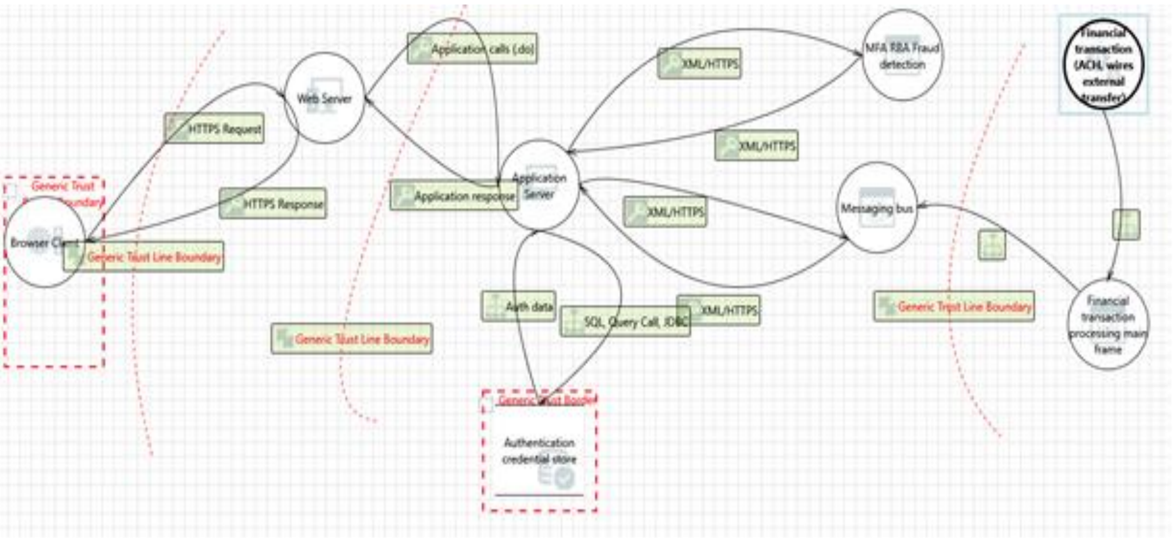

Figure 1. The login vulnerabilities in online banking

3.3.1. Interaction: REQUEST

Trust Line Boundary as shown in Figure 2.

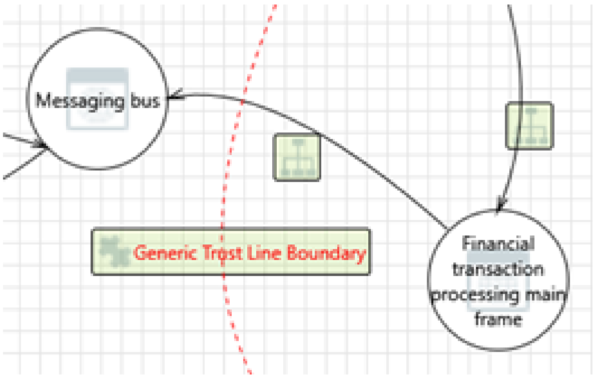
Messaging bus
Generic Trust Line Boundary
Financial transaction processing main frame

Figure 2. Trust line boundary

a) Elevation using impersonation [State: Not started] [Priority: High]
Category: Elevation of Privilege
Description: Messaging bus may be able to fill the context of Financial transaction processing main frame in order to obtain additional privilege.

b) Financial transaction processing main frame process memory tampered [State: Not started] [Priority: High]
Category: Tampering
Description: If Financial transaction processing main frame is given the ability to control what Messaging bus executes, then Financial transaction processing main frame can tamper with Messaging bus.

c) Spoofing the messaging bus process [State: Not started] [Priority: High]
Category: Spoofing
Description: Messaging bus may be spoofed by an attacker and this may lead to information disclosure by Financial transaction processing main frame [17]. Consider using a standard authentication mechanism to identify the destination process.

3.3.2. Interaction: LOG IN RESPONSE

Interactions as shown in Figure 3.

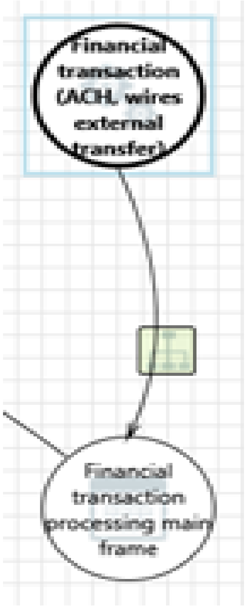
Financial transaction (ACH, wires external transfer)
Financial transaction processing main frame

Figure 3. Interactions

a) Financial transaction (ACH, wires external transfer) Process Memory Tampered [State: Not Started] [Priority: High]
Category: Tampering
Description: If Financial transaction (ACH, wires external transfer) is given the ability to control what Financial transaction processing main frame executes, then Financial transaction (ACH, wires external transfer) can tamper with Financial transaction processing main frame [18].

b) Elevation using impersonation [State: Not started] [Priority: High]
Category: Elevation of Privilege
Description: Financial transaction processing main frame may be able to impersonate the context of Financial transaction (ACH, wires external transfer) in order to gain additional privilege.

3.3.3. Interaction: APPLICATION CALLS (.do) (Figure 4)
a) Cross site scripting [State: Not started] [Priority: High]
Category: Tampering
Description: The web server 'Application Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.

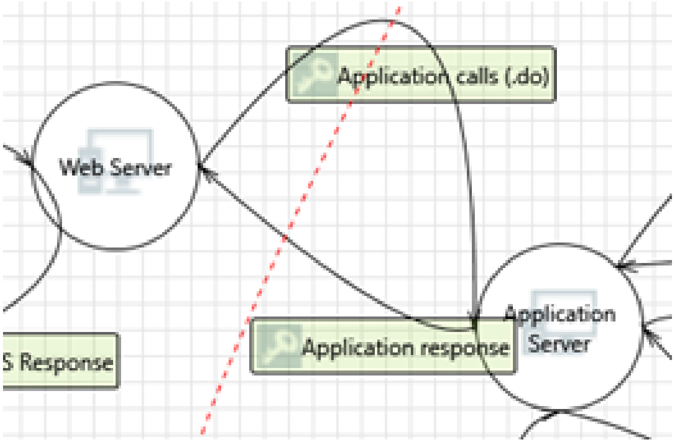

Figure 4. Interaction: Application call

b) Elevation using impersonation [State: Not started] [Priority: High]
Category: Elevation Of Privilege
Description: Application Server may be able to play a role as the context of Web Server in order to obtain additional privilege.

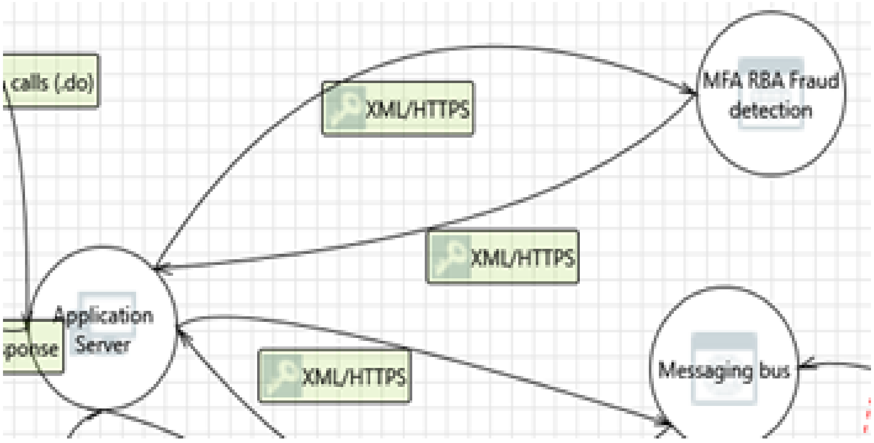

Figure 5. Interaction XML/HTTPS

3.3.4. Interaction: XML/HTTPS (Figure 5)

a) Elevation using impersonation [State: Not started] [Priority: High]
Category: Elevation of Privilege
Description: Application Server may be able to do an impression of the context of MFA RBA Fraud detection in order to gain additional privilege.

b) Cross site scripting [State: Not started] [Priority: High]
Category: Tampering
Description: The web server 'Application Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.

3.3.5. Interaction: Authentication SQL QUERY RESPONSE

a) Potential data repudiation [State: Not started] [Priority: High]
Category: Repudiation
Description: Server claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

b) Potential process crash or stop for server [State: Not started] [Priority: High]
Category: Denial of Service
Description: Server crashes, halts, stops or runs slowly [19]; in all cases violating an availability metric.

3.3.6. Interaction: DATA

Spoofing of source data store database [State: Not started] [Priority: High]
Category: Spoofing
Description: Database may be spoofed by an attacker and this can determine incorrect data delivered to server. It can be considered a standard authentication mechanism to identify the source data store [20, 21].

3.4. Risk mitigation

Security control selection means a tailored set of security controls, documented in the system security plan and approved by the system's authorizing official. The e-banking system typically needs to address a large number of security controls and information system considerations related to access control, including identification and authentication, user authorization, and system and communications protection [22].

There are many options for mitigating a risk, and again, the focus is not always on trying to eliminate the risk, but rather to reduce the risk exposure to an acceptable level.

The first two are the most common, but in some cases, it may be possible to change the sensitivity of the resource. The sensitivity could be reduced, however, if the data from production was scrambled in some random manner before being copied to development [23]. This way the data would still be good for testing, but a few of the sensitive fields like customer name or account number could be obfuscated.

Another option for this example might be to reduce the threat universe by implementing firewall rules to limit source networks that are allowed to connect to the database server. Again, this option would not limit the severity of the exposure or change the sensitivity of the database server, but it would reduce the likelihood of abuse by reducing the number of entities who can access the server. To limit the severity of an exploit, it needs to somehow contain the compromise. This approach to risk mitigation recognizes that it can't necessarily prevent the compromise, but it can limit the scope of the breach or react quickly to prevent further escalation. Most controls in this category will be detective and response focused. A typical example is limiting the scope of access the attacker would have when exploiting the account.

Using the SSL alone does not trust the bank that its Internet service is secure. The VPN option requires additional remote workstation software and hardware. The VPN software is closely integrated with the remote workstation and server, requiring software drivers to be installed and may require hardware readers. This can be done for closed user groups, but it is not feasible to allow potential customers to access the general population. Methods are likely to evolve towards treating the internet banking customer group of the bank as a closed user group on a VPN, but in the short term this is not feasible.

It is recognized that this point has not yet been reached by global best practice and that implementing tokens may not be feasible in the short term. All banks have adopted the EMV smart card that offers security of transactions and most of them have attached a token to increase the security degree [23]. [24]. New token applications compatible with mobile phones raise new security issues. Meanwhile, although SSL does not overcome the risks discussed in this section, it provides advantages as discussed above for payment transactions and should therefore be deployed by all banks introducing Internet services [25].

4. CONCLUSION

The concept of electronic banking (e-banking) refers to the atomized delivery through electronic or some additional communication channels of some new or conventional banking products and/or services in a straight line to consumers. The bank's strategy should be readjusted to meet new challenges with risk balance and to be focused on potential negative impact on key business objectives. When we think from the security perspective, we see that there are many security issues and risk on the application specially, for an online application and it's important to guarantee a secured environment that must therefore, be authentic, available and confidential and possess high level of integrity and efficiency etc. Banks should regularly look at their evolving risk exposures and solutions to help weather a storm if an incident occurs. Risk and/or insurance managers should collaborate with business units when coordinating and agreeing to prevention, mitigation, and response plans.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the Xi'an Jiaotong-Liverpool University (XJTLU), Suzhou, China. especially to Department of Computer Science and Software Engineering (CSSE). This work was partially supported by the Artificial Intelligence Data Analytics Lab (AIDA), Prince Sultan University, Riyadh, Saudi Arabia.

REFERENCES

[1] Kumar, Pradeep, and Mohammad Khan. "Systems, methods, and computer readable media for payment and non-payment virtual card transfer between mobile devices," U.S. Patent 10,026,076, issued July 17, 2018.

[2] Akhisar, İlyas, K. Batu Tunay, and Necla Tunay, "The effects of innovations on bank performance: The case of electronic banking services," *Procedia-Social and Behavioral Sciences*, no. 195, pp. 369-375, 2015.

[3] Theohary, C. A., *Terrorist use of the internet: Information operations in cyberspace*, Diane Publishing, 2011.

[4] Grody, Allan D., Fotios Harmantzis, and Gregory J. Kaple, "Operational risk and reference data: Exploring costs, capital requirements and risk mitigation," *Capital Requirements and Risk Mitigation*, vol. 1, no. 3, pp. 130-187, 2006.

[5] Bamberger, Kenneth A., "Technologies of compliance: Risk and regulation in a digital age," *Tex. L. Rev*, no 88, pp. 669, 2009.

[6] Nami, Mohammad Reza, "E-banking: Issues and challenges," In *2009 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing*, pp. 263-266. 2009.

[7] Jerman-Blažič, Borka, "An economic modelling approach to information security risk management," *International Journal of Information Management*, vol. 28, no. 5. pp. 413-422, 2008.

[8] Angelakopoulos, Georgios, and Athanassios Mihiotis, "E-banking: challenges and opportunities in the Greek banking sector," *Electronic Commerce Research*, vol. 11, no. 3, pp. 297-319, 2011.

[9] Nitsure, Rupa Rege, "E-banking: Challenges and opportunities," *Economic and Political Weekly*, vol. 38, no. 51, pp. 5377-5381, 2003.

[10] Ahmad, Ala'eddin Mohd Khalaf, and Hasan Ali Al-Zu'bi, "E-banking functionality and outcomes of customer satisfaction: an empirical investigation," *International journal of marketing studies*, vol 3, no 1, pp. 50-65, 2011.

[11] Oh, Yunsang, and Takashi Obi, "Identifying phishing threats in government web services," *International Journal of Information and Network Security*, vol. 2, no. 1, pp. 32, 2013.

[12] Hassan, Moatamad, A. Younes, M. R. Hassan, and H. Abdo, "Solving the File Allocation Problem in the Distributed Networks by using Genetic Algorithms," *International Journal of Information and Network Security*, vol. 2, no. 1, pp. 109, 2013.

[13] Pashazadeh, Saeid, "Modeling and verification of access rights in take-grant protection model using colored Petri nets," *International Journal of Information and Network Security*, vol. 2, no. 1, pp. 78, 2013.

[14] Pradhan, Sushma, and Birendra Kumar Sharma, "An Efficient RSA Cryptosystem with BM-PRIME Method," *International Journal of Information and Network Security*, vol 2, no 1, pp. 103, 2013.

[15] Moul, Katelin A, "Avoid Phishing Traps," *In Proceedings of the 2019 ACM SIGUCCS Annual Conference*, pp. 199-208, 2019.

[16] P. Sharma, R. Johari, S. S. Sarma, "Integrated approach to prevent SQL injection attack and reflected cross site scripting attack," *International Journal of System Assurance Engineering and Management*, vol. 3, no. 4, pp. 343-351, 2012.

[17] Claycomb, William R., and Alex Nicoll, "Insider threats to cloud computing: Directions for new research challenges," *In 2012 IEEE 36th Annual Computer Software and Applications Conference*, pp. 387-394, 2012.

[18] Elibol, Fürkan, Uğur Sarac, and Işin Erer, "Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system," In *2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO)*, pp. 1767-1771, 2012.

[19] Mishra, Anupama, B. B. Gupta, and Ramesh Chandra Joshi, "A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques," In *2011 European Intelligence and Security Informatics Conference*, pp. 286-289, 2011.

[20] Angeleski, Marjan and Kostoska, Olivera and Janeska, Margarita, "Risk-based analysis of electronic banking," *International Journal of Strategic Management and Decision Support Systems in Strategic Management*, vol. 12, no. 3-4, pp. 74-76, 2007.

[21] Al-Alawi, Adel Ismail, "Online banking: security concerns and the acceptance of mature customers," In *3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications*, Tunisia, pp. 27-31. 2005.

[22] Mohammed G. G., "Data security in big data using parallel data generalization algorithm," *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, vol. 8 no. 1.2 (2019) S I, pp. 75-79, 2019.

[23] Lim K. S., Norafida I. and Syed Z. M. S., “"The preparation of cross-site scripting in automated web application vulnerability assessment: The quantitative analysis," *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, vol. 8, no. 1.6, pp. 57-63, 2019.

[24] Sami H., Qing T. and Rebeca S. C., "A hybrid model for information security risk assessment," *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE),* vol. 8, no. 1.1, pp. 100-106, 2019.

[25] Hydara, I., Sultan, A. B. M., Zulzalil, H., and Admodisastro, N, "Current state of research on cross-site scripting (XSS)–A systematic literature review," *Information and Software Technology*, no. 58, pp. 170-186, 2015.

BIOGRAPHIES OF AUTHORS

Gabriela Mogos (M’05) is an Associate Professor in the Department of Computer Science and Software Engineering (CSSE) at the Xi'an Jiaotong-Liverpool University (XJTLU), Suzhou, China. She received her PhD in Computer Science from the *Alexandru Ioan Cuza* University of Iasi, Romania, in March 2010. She followed this with postdoctoral research positions at the University of Oradea, Romania, from 2010-2013. Her research interests are in the areas of Information Security / Quantum cryptography and are driven by a strong desire to bridge computer science and quantum physics and to design new quantum cryptographic protocols, and, to embed quantum-safe equipment in large networks.

Nor Shahida Mohd Jamail is currently in Prince Sultan University, Riyadh, Saudi Arabia as an Assistant Professor. She obtained her PHD in Software Engineering from Universiti Putra Malaysia. Her specialized are purely in Software Engineering, Software Process Modelling, Software Testing and Cloud Computing Services. She had involved in Machine Learning Research Group in Prince Sultan University and also involved in research project which collaborated with National and International University. Email: njamail@psu.edu.sa