Phishing Detection Taxonomy for Mobile Device

Cik Feresa Mohd Foozy[1], Rabiah Ahmad[2] and Mohd Faizal Abdollah[3]

[1,2,3] Center for Advanced Computing Technology, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Karung Berkunci No. 1752 Pejabat Pos Durian Tunggal, 76109 Melaka Malaysia

Abstract

Phishing is one of the social engineering attacks and currently hit on mobile devices. Based on security report by Lookout [1], 30% of Lookout users clicking on an unsafe link per year by using mobile device. Few phishing detection techniques have been applied on mobile device. However, review on phishing detection technique on the detection technique redundant is still need. This paper addresses the current trend phishing detection for mobile device and identifies significant criterion to improve phishing detection techniques on mobile device. Thus, existing research on phishing detection technique for computer and mobile device will be compared and analysed. Hence, outcome of the analysis becomes a guideline in proposing generic phishing detection taxonomy for mobile device.

Keywords: Mobile, Phishing, Security, Social Engineering, Taxonomy

1. Introduction

A mobile device is defined as a very small, lightweight device that provides functionality like a laptop computer [2]. Examples of mobile devices are Palm and other PDAs, tablet PC and smart mobile[3]. Mobile devices have become so popular for business and personal use because of their features such as portability and long battery life.

However, the rapid growth of mobile devices has contributed to security problem due to its functionality connect to Internet. According to a website *mysecurecyberspace.com*[4], one example of security problem in mobile device is the security threat such as mobile banking password, contact number, photo and others. Moreover, Symantex [5] also has reported the increasing intrusion and identity theft on mobile phones.

The purpose of phishing attack is to steal valuable information such as credit card and social security numbers, user IDs and passwords [6]. According to Boodae [7], mobile device users are three times more likely to enter a web-based phishing attack than desktop users. Since the reported shows the increasing phishing attack on mobile device, many studies has been done to detect the phishing attack. Thus, to get clear view what is criterion for modern mobile device phishing detection, taxonomy for mobile device will be proposed.

This paper proposes phishing detection taxonomy on mobile device and structured into four sections as follows: In Section 2, describes the related work in phishing. In Section 3 also discusses, the methodology used to identify the categories of phishing attacks and detection techniques in mobile devices. Moreover, section 4 conducts the analysis on detection technique. Finally, in Section 5, the proposed taxonomy and future work for the next research are presented.

2. Related Work

Current studies in phishing are much focused on specific phishing detection technique for mobile devices and most of the studies are more on verifying the validity of the computer website. Therefore, this section will review the phishing attack and detection for desktop and mobile device.

2.1 Taxonomy

Taxonomy can be defined as a simple classification to categories into the specific groups [8]. There are few techniques to mitigate phishing attack such as filtering on browser and toolbar, anti-virus, anti-phishing and through education and training.

2.2 Phishing

Phishing term has been introduced in early 1990's by America Online (AOL) because of the stolen data happened on that time. Since, financial lost and stolen data can be happened in mobile device, few phishing detection techniques on mobile device that have been proposed are filtering on browser and toolbar, anti-virus, anti-phishing and via education and training. There are some advantages and disadvantages of each techniques mention above. For example, one of the limitations of anti-phishing is the signatures phishing need to be

updated frequently. However, the advantages, it is widely used in industries and easy to be updated.

Maggi et al. [9] has done a research on phishing of voice channel and found the phishing attack can be categories into traditional and modern type. Email method is identified as traditional way to attack and for modern phishing attack, instant message, social network and phone system phishing.

Crain et al.[10] classified the phishing defense method into technical and educational method. Example of technical defense method are browser toolbar, email verification, anti-phishing. There are several limitations of defense method on toolbar and anti-phishing such as frequent update the phishing signature, unsecure connection between server client and user can switch off the anti-phishing on client [11]. Moreover, for training and educational methods it requires times for human to adapt with new process.

In addition, Kumaruguru et. al [12] listed several defense method through education and training but it becomes a problem when the worker leaves the organization. Moreover, the company must frequently train their for phishing awareness. However, a study by Alnajim and Munro [13] categories the defense mechanism into technical and training techniques. The defense mechanism consists of anti-phishing for email, web, IQ test, class assessment and tool bar.

There are few detection techniques that have been proposed to overcome the phishing issues in education and technical part. However, this paper review detection technique and focus on technical based solution for phishing attack on mobile device.

2.3 Phishing Detection

Phishing launch the attack through browser and email[14]. Additionally, for mobile device, phishing can attack via bluetooth, SMS, Voice Over IP, mobile application and mobile browser.

One of phishing detection technique on mobile device are using content-based filtering[15]. Moreover, there are more detection techniques that will be discuss in this section later.

Phishing detection technique is a research area that can help to reduce the effect of phishing attack on mobile device. Commonly, phishing attack will attack website, client application, visual and images. G. Xiang, et al. [16] listed two phishing detection techniques such as blacklist and feature-based. Moreover, J. a. Huh and H. Kim [17] listed three types of detection techniques such as blacklist, whitelist and heuristic. In addition, Zhang et al.[18], listed blacklist and heuristic as common phishing detection. Moreover, Chhabra [19] listed three email detection techniques such as blacklist, whitelist and graylist. Table 1 shows the summary desktop and wired phishing detection techniques that has been discusses in the literature.

However, phishing solutions for desktop and wired computers are not suitable for wireless and mobile devices due to processing, power and storage limitations[20],[21]. Thus, phishing detection must be lightweight and high accuracy in detecting phishing attack on mobile device.

2.4 Common Phishing Detection Technique on Mobile Device

The possibilities of lost and risks for mobile device are increasing when the device is connected to the network[22]. This shows the phishing detection for mobile device is still a significant research area to be improved since phishing attack has revolutionized the strategies into mobile device.

In addition, mobile operating systems and browsers not have secure application[23]. Losing money and stealing data such as password, contact number, account number and etc. can be occurred if mobile application and website are interacting with each other.

Approximately 1 in 20 users will click on a phishing link every year on Android devices[1], since phishing detection for mobile device is different from wired computers, developing taxonomy for phishing attack and detection techniques is needed in order to propose an overview for suitable phishing detection technique for mobile device.

Dunham [21], identify the phishing attack on mobile devices into Bluetooth phishing, Short Message Service (SMS) phishing and Voice over IP Phishing or known as vishing.

Example Bluetooth phishing attack has been discuss by [21], the Bluetooth phishing attack works when user connect to the Wi-Fi hotspot. Attacker can steal the data when the user connects to the Wi-Fi.

Figure 1 shows the example of SMiShing attack in Malay language and this attack can be used as a strategy to trick mobile phone user to transfer money to their bank account.

Fig. 1 Example SMiShing attack

Based on the findings, common phishing detections for mobile device are SMS phishing detection, voice call phishing detection and mobile web browser phishing detection. Thus, below are common detection techniques for mobile device that has been review:

i. Content Based Filtering:

This technique has shown a successfully detection phishing attack on email. J. W. Yoon, et al.[15] implement this technique with challenge-response scheme. The combinations of these techniques are needed to improve the traditional spam filtering detection technique on mobile device since the content-based filtering alone is less efficient. Moreover, content-Based filtering can be divided into rule based and statistic based [24].

ii. Blacklist:

Blacklist is a method that need human to verification. Since this technique have very low False Positive(FP), it is widely applied in the industries as anti-phishing in toolbar. If user enter the blacklist website, a warning will be appeared. However, this method is not suitable to detect new phishing attack[16]. This technique is also not efficient in update and verify the phishing attack database globally [17],[25]. In addition this technique have less capablities to protect users [26]. Moreover, this technique also has been implemented in fraud telephony(vishing)[27] and SMS filtering by [28].

iii. Whitelist:

Whitelisting method is different from blacklist-based, this technique need to maintain all website in the cyber world. The limitation of this technique is impossible to cover all website [25]. This technique has been implemented by [28] to detect SMS phishing.

3. Methodology

The aim of this paper is to classify phishing attack and identify the defense technique on mobile device. The data in this study were retrieved from various databases such as ACM Digital Library, SpringerLink, IEEE Xplore, ScienceDirect, Google, Google Scholar, and Yahoo.

Using these databases, a statistical analysis on every selected article about phishing detection and filtering was done to propose taxonomy of phishing detection on mobile device.

Step 1: Analysis phishing attack on mobile device category

Step 2: Analysis of phishing attack classification and detection techniques.

The purpose of the first step is to identify the phishing attack on mobile device. This paper discusses the preliminary analysis on phishing attack by identifying the common attack on mobile device and finally to propose taxonomy of phishing detection attack on mobile device. Figure 2 shows the overview of the analysis process.

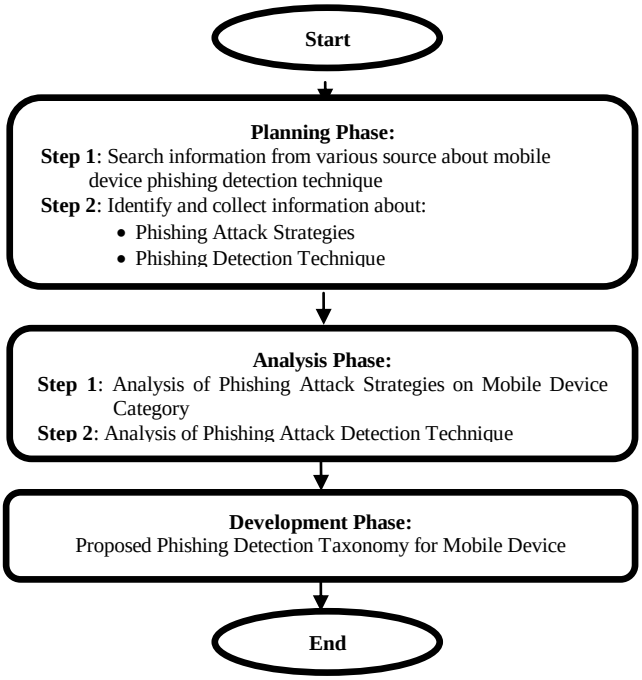

Fig. 2 Overview the analysis process

4. Analysis and Findings

According to the [29], phishing is a type of technical-based social engineering. This attack is dividing into traditional and modern attack where email is traditional attack and phone system phishing such as mobile device is a type of modern phishing attack. There are three types of modern phishing strategies on mobile device such as SMS, Voice Call and Bluetooth.

4.1 Taxonomy Elements for Mobile Device Phishing

The development phishing taxonomy is to provide basic understanding on phishing attack and detection concept on mobile device. Main elements of proposed taxonomy are consisting of the Attack Strategies and Phishing Detection Techniques.

In the proposed taxonomy, all these elements will be applied to build phishing detection taxonomy for mobile device. This can be as alternative to understand the components to build a framework of phishing detection for mobile device. Figure 3, shows the main elements in intrusion detection taxonomy.

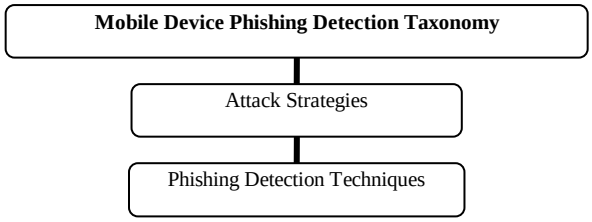

Fig. 3 Main elements of intrusion detection taxonomy

4.2 Mobile Device Phishing Attack Strategies

Table I listed few study by [21], [30] and [23] on mobile device phishing attack strategies. All listed phishing type is relevant to be included in the taxonomy since it has been discussed by the researchers.

Table 1. Analysis of phishing attack on mobile device (item found=√)

References / Phishing Attack Strategies	[21]	[30]	[23]
Bluetooth Phishing	√		
SMS Phishing	√	√	
Vishing	√		
Mobile Web Application Phishing			√

4.3 Mobile Device Phishing Detection Techniques

In addition, Table II listed the phishing detection technique that has been studies by the researchers below. This shows, the content based filtering and blacklist is widely used to detect phishing on desktop and it has been applied to detect phishing attack on mobile device.

Table 2. Analysis of phishing attack on mobile device (item found=√)

References / Phishing Detection Techniques	[15]	[24]	[27]	[28]	[31]	[32]
Content Based	√	√				
Blacklist			√	√		
Whitelist				√		
Hotspot					√	
Gaussian Mixture Model						√

4.4 Mobile Device Phishing Detection Techniques Based on Attack Strategies

In addition, Table III listed the relation between Attack Strategies and Phishing detection Techniques. These explain that each attack strategies have different phishing detection techniques. Blacklist detection techniques have more than two occurrences which applied at SMS, Vishing and Mobile Application. For whitelist, it also have more than one occurrence and been applied at SMS and web application.

Table 3. Analysis on mobile device phishing detection techniques based on attack strategies (item found=√)

Attack Strategies / Phishing Detection Techniques	Bluetooth	SMS	Vishing	Mobile Web/ Application
Content Based		√		
Blacklist		√	√	√
Whitelist		√		√
Hotspot Wireless Defense Tool	√			
Gaussian Mixture Model			√	

5. Result

As a result from the analysis section, the elements that will be includes in our taxonomy are the Attack Strategies and the Phishing Detection Techniques. Since, phishing attacks are widely discussed in many areas, it is less consideration for mobile device phishing detection technique.

This section discussed the outcome of the analysis which is about Mobile Device Phishing Attack Strategies Taxonomy, Mobile Device Phishing Detection Techniques and Mobile Device Phishing Detection Techniques Taxonomy.

5.1 Mobile Device Phishing Attack Strategies Taxonomy

From the Table I, [21], [30] and [23] has listed several attack strategies on mobile device and taxonomy are illustrate as Figure 4.

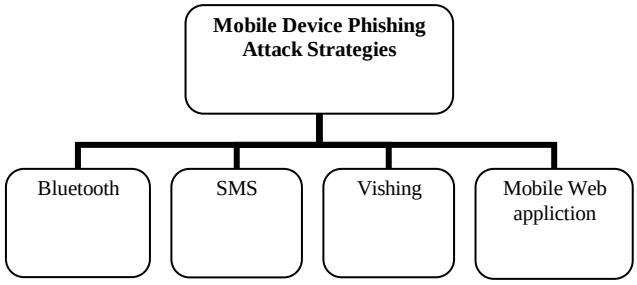

Fig. 4 Mobile Device Phishing Attack Strategies Taxonomy

5.2 Mobile Device Phishing Detection Techniques

Phishing detection techniques on mobile device also have been compared in order to develop phishing taxonomy and the advantages and disadvantages of each method are summarizes in the Table IV.

There are six detection techniques that has been review such as Content Based, Blacklist, Whitelist, Hotspot, Gaussian Mixture Model and Graylist. According to the table, Content based detection technique has been review by [15] and [24].

For blacklist detection attack, this techniques has been applied by [27] and [28]. Whitelist is also a detection techniques that has been aplied by few researchers to detect phishing attack on SMS and Mobile Web. This method has been discussed by [28]. This techniques need to collct the data of trusted senders and only can detect phishing from the known sanders.

Moreover, bluetooth phishing attack can be defense by using wireless hotspot defense tools[32]. The advantages of this tools it can detect wireless attack and it can check any changes on ESSID, MAC address of the access point, MAC address of the default gateway and radical signal strength fluctuations on the network. However, this tools need and expert to monitor and understanding the changes happened on the network.

This technique has been applied by [31], the result shows this method is effective to detect vishing attack on mobile device and can identifies lies and true statements.

Table 4. Summary of phishing attack detection techniques for mobile device

Phishing Attack Strategies	Technique	Advantage	Disadvantage
• **SMiShing**	Content Based Filtering	• Flexible	• Less efficient
• **SMiShing** • **Vishing** • **Mobile Web**	Blacklist	• Low False Positive • Effective detection known phishing URL	• Not suitable to detect new attack • Less efficiency in updating and verify the attack in database • Inefficient to protect user from phishing attack
• **SMiShing** • **Mobile Web**	Whitelist	• Have list of trusted senders	• Detect phishing from known sender
• **Blueetooth**	Wireless Hotspot Defense Tools	• Check any changes on MAC address and etc.	• Need expert to review and monitor the network.
• **Vishing**	Gaussian Mixture Model	• Identifies lies and true statements	• To assign pattern into lies and true voice pattern

5.3 Mobile Device Phishing Detection Techniques Taxonomy

The mobile device phishing detection taxonomy has been developed as Figure 5. The taxonomy shows the general view on phishing attack strategies and phishing attack detection techniques for mobile device.

As a social engineering based attack, phishing need to be countermeasure and various defense solutions has been introduced to detect phishing but not many alternatives solutions to detect phishing attack on mobile devices. Since, mobile device is one of modern technology that essential today, this attack has evolving their strategies into mobile device.

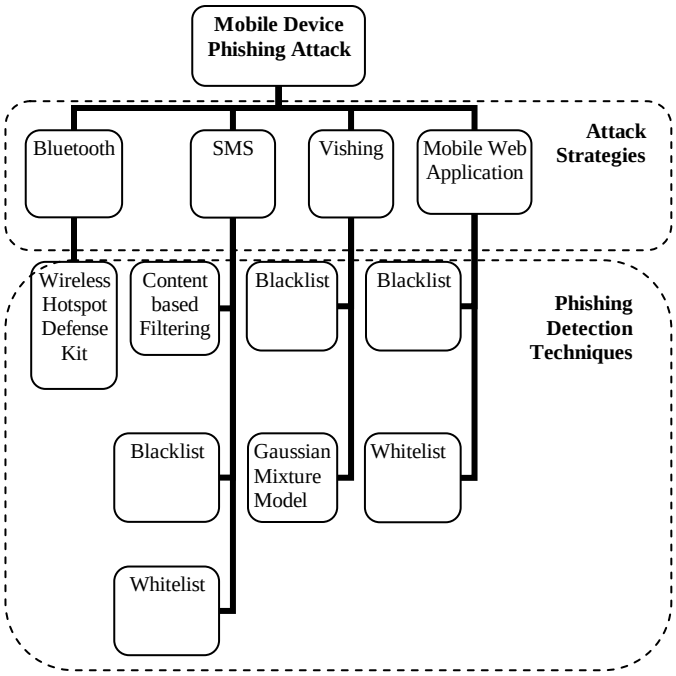

Fig. 5 Mobile device phishing detection attack taxonomy

6. Conclusion

According to[32], there is no anti-phishing solution dedicated to mobile device. Thus, a review on mobile device phishing detection technique will help to develop phishing detection taxonomy because taxonomy can help user to have understanding about the specific topic.

This paper discusses mobile device phishing attack and the develop taxonomy has classifies the mobile device phishing attack strategies into several phishing attack. This paper is a preliminary study for future work and it contributes ideas on how to identify mobile device phishing attack.

Acknowledgments

The authors would like to thank University Tun Hussein Onn Malaysia(UTHM) and Ministry of Higher Education Malaysia for supporting this research.

References

[1] I. Lookout, "Lookout Mobile Threat Report August 2011," 2011.

[2] H. Wen-Chen, *et al.*, "Mobile Data Protection Using Handheld Usage Context Matching," in *Mobile Data Management: Systems, Services and Middleware, 2009. MDM '09. Tenth International Conference on*, 2009, pp. 594-599.

[3] J. Stonemetz, *et al.*, "Handheld Devices Anesthesia Informatics," ed: Springer New York, 2009, pp. 409-424.

[4] MySecureCyberspace.com. (2011, The Trend of Tablet PCs. Available: http://www.mysecurecyberspace.com/articles/features/the-trend-of-tablet-pcs.html

[5] S. Corporation, "Symantec Intelligence Report: July 2011," 2011.

[6] Microsoft. (2011, 8th June). *Email and web scams: How to help protect yourself*. Available: http://www.microsoft.com/security/online-privacy/phishing-scams.aspx

[7] M. Boodae, "Mobile Users Three Times More Vulnerable to Phishing Attacks," in *Trusteer* vol. 2012, ed, 2011.

[8] P. Rich, "The Organizational Taxonomy: Definition and Design," *The Academy of Management Review*, vol. 17, pp. 758-781, 1992.

[9] F. Maggi, *et al.*, "A social-engineering-centric data collection initiative to study phishing," presented at the Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, Salzburg, Austria, 2011.

[10] J. Crain, *et al.*, "Fighting Phishing with Trusted Email," in *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, 2010, pp. 462-467.

[11] S. Abu-Nimeh and S. Nair, "Bypassing Security Toolbars and Phishing Filters via DNS Poisoning," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, 2008, pp. 1-6.

[12] P. Kumaraguru, *et al.*, "Protecting people from phishing: the design and evaluation of an embedded training email system," presented at the Proceedings of the SIGCHI conference on Human factors in computing systems, San Jose, California, USA, 2007.

[13] A. Alnajim and M. Munro, "An evaluation of users' tips effectiveness for Phishing websites detection," in *Digital Information Management, 2008. ICDIM 2008. Third International Conference on*, 2008, pp. 63-68.

[14] P. Soni, *et al.*, "A phishing analysis of web based systems," presented at the Proceedings of the 2011 International Conference on Communication, Computing; Security, Rourkela, Odisha, India, 2011.

[15] J. W. Yoon, *et al.*, "Hybrid spam filtering for mobile communication," *Computers & Security*, vol. 29, pp. 446-459, 2010.

[16] G. Xiang, *et al.*, "CANTINA+: A Feature-Rich Machine Learning Framework for Detecting Phishing Web Sites," *ACM Trans. Inf. Syst. Secur.*, vol. 14, pp. 1-28, 2011.

[17] J. a. Huh and H. Kim, "Phishing Detection with Popular Search Engines: Simple and Effective Foundations and Practice of Security." vol. 6888, J. Garcia-Alfaro and P. Lafourcade, Eds., ed: Springer Berlin / Heidelberg, 2012, pp. 194-207.

[18] Y. Zhang, *et al.*, "Cantina: a content-based approach to detecting phishing web sites," presented at the Proceedings of the 16th international conference on World Wide Web, Banff, Alberta, Canada, 2007.

[19] S. Chhabra, "Fighting Spam, Phishing and Email Fraud," Master of Science in Computer Science, UNIVERSITY OF CALIFORNIA RIVERSIDE, 2005.

[20] S. Abu-Nimeh, *et al.*, "Distributed Phishing Detection by Applying Variable Selection Using Bayesian Additive Regression Trees," in *Communications, 2009. ICC '09. IEEE International Conference on*, 2009, pp. 1-5.

[21] K. Dunham, "Chapter 6 - Phishing, SMishing, and Vishing," in *Mobile Malware Attacks and Defense*, D. Ken, Ed., ed Boston: Syngress, 2009, pp. 125-196.

[22] J. Networks, "Malicious Mobile Threats Report 2010/2011," 2011.

[23] A.P. Felt and D. Wagner, "Phishing on Mobile Devices," 2011.

[24] H. Peizhou, *et al.*, "A Novel Method for Filtering Group Sending Short Message Spam," in *Convergence and Hybrid Information Technology, 2008. ICHIT '08. International Conference on*, 2008, pp. 60-65.

[25] Y. Cao, *et al.*, "Anti-phishing based on automated individual white-list," presented at the Proceedings of the 4th ACM workshop on Digital identity management, Alexandria, Virginia, USA, 2008.

[26] S. Sheng, Wardman, B., Warner, G., Cranor, L., Hong, J., & Zhang, C, "An empirical analysis of phishing blacklists," *6th Annual Conference on Email and Anti-Spam (CEAS), Mountain View, CA.*, 2009.

[27] Devinder Singh, *et al.*, "Telephony Fraud Prevention," US Patent, 2011.

[28] T. M. Mahmoud and A. M. Mahfouz, "SMS Spam Filtering Technique Based on Artificial Immune System," *IJCSI International Journal of Computer Science Issues*, vol. 9, 2012.

[29] R. A. Cik Feresa Mohd Foozy, Mohd Faizal Abdollah, Robiah Yusof and Mohd Zaki Mas'ud, "Generic Taxonomy of Social Engineering Attack," *Malaysian Technical Universities International Conference on Engineering & Technology*, 2011.

[30] O. Salem, *et al.*, "Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks," in

Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on, 2010, pp. 1418-1423.

[31] J. H. Chang and K. H. Lee, "Voice phishing detection technique based on minimum classification error method incorporating codec parameters," *Signal Processing, IET*, vol. 4, pp. 502-509, 2010.

[32] Saeed Abu-Nimeh and S. Nair, "Phishing Attacks in a Mobile Environment."

Cik Feresa Mohd Foozy is currently working with Universiti Tun Hussein Onn Malaysia (UTHM), Malaysia. Feresa holds a Master's degree in Computer Science(Information Security) from Universiti Teknologi Malaysia, Malaysia and a Bachelor's degree in Information Technology and Multimedia from Universiti Tun Hussein Onn Malaysia (UTHM), Malaysia. She is currently pursuing her PhD at the Universiti Teknikal Malaysia Melaka, Malaysia.

Rabiah Ahmad is an Associate Professor at the Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka,Malaysia. She received her PhD in Information Studies (health informatics) from the University of Sheffield, UK, and M.Sc. (information security) from the Royal Holloway University of London, UK. Her research interests include healthcare system security and information security architecture. She has delivered papers at various health informatics and information security conferences at national as well as international levels. She has also published papers in accredited national/international journals. Besides that, she also serves as a reviewer for various conferences and journals.

Mohd Faizal Abdollah is a Senior Lecturer at the Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka,Malaysia. He received his PhD in Computer and Network Security from Universiti Teknikal Malaysia Melaka,Malaysia, and M.Sc. (Computer Science) from the University Kebangsaan Malaysia. His research interests include network and mobile security and network monitoring. He has delivered papers at various network security conferences at national as well as international levels. He has also published papers in accredited national/international journals. Besides that, he also serves as a reviewer for various conferences and journals