ISU KESELAMATAN PERANTI MUDAH ALIH DALAM DUNIA DIGITAL UNTUK INSTITUSI PENGAJIAN TINGGI

SHEKH ABDULLAH AL-MUSA AHMED*

NIK ZULKARNAEN KHIDZIR **

TSE GUAN TAN***

almusa.c17e002f@siswa.umk.edu.my*, zulkarnaen.k@umk.edu.my**, tan.tg@umk.edu.my ***

Abstrak

Keselamatan mudah alih, atau lebih khusus keselamatan peranti mudah alih, menjadi semakin penting dalam pengkomputeran mudah alih untuk literasi digital. Literasi digital adalah kumpulan kecekapan yang diperlukan untuk penyertaan penuh dalam pengetahuan masyarakat. Ini merangkumi pengetahuan, kemahiran, dan tingkah laku yang melibatkan penggunaan alat digital yang berkesan seperti telefon pintar, tablet, komputer riba untuk tujuan komunikasi, ekspresi, kolaborasi dan sokongan. Yang menjadi perhatian utama ialah keselamatan institusi pengajian tinggi kini disimpan di telefon pintar. Seiring dengan perkembangan ini muncul sejumlah masalah keselamatan yang mempengaruhi peranti mudah alih. Peluang untuk memiliki peranti kecil dan kuat yang dihubungkan dengan internet membolehkan komunikasi berlaku dari mana sahaja di institusi pengajian tinggi. Di institusi pengajian tinggi, yang telah melekatkan telefon pintar peribadi mereka ke rangkaian institusi telah mengetahui cara mudah untuk melakukannya. Secara khusus, ada beberapa kes di mana pelajar telah membenarkan capaian peranti mudah alih peribadinya ke rangkaian institusi pengajian tinggi. Walau bagaimanapun, pentadbir sistem menghantar arahan jarak jauh ke peranti dan memerintahkannya untuk menyimpan semua data agar tidak jatuh ke tangan yang salah. Oleh itu kini wujud istilah *rooting* pada peranti Android. Hal merujuk kepada proses mendapatkan akses root ke peranti. Biasanya, ini melibatkan aplikasi atau skrip yang memberikan akses root kepada pengguna. Setelah akses diberikan, pengguna di institusi pengajian tinggi, dapat melakukan apa sahaja yang diinginkan tanpa sekatan. Namun, salah satu kelemahan proses ini adalah peranti ini terdedah kepada bahaya yang lebih besar dari ancaman luaran. Justeru artikel ini memberi tumpuan kepada masalah keselamatan peranti mudah alih dalam dunia digital di institusi pengajian tinggi. Hal ini bertujuan supaya pelajar institusi memiliki kebolehan kritis dan kreatif ketika melayari media massa, budaya popular dan media digital. Oleh kerana media digital menggunakan telefon pintar untuk maklumat dan artikel ini juga merujuk cara menjaga keselamatan data telefon pintar ini memandangkan kadar capaian maklumat yang semakin kerap dan cepat.

Kata kunci: Enkripsi, Remoteness, Digital affixing signature, Serangan Trojan Horse, Malware, Serangan Kejuruteraan Sosial, Literasi Digital, Media Digital.

Dihantar : 5 Oktober 2019 Disemak : 5 November 2019 Diterbit : 31 Mac 2020

* Pascasiswazah PhD di Fakulti Teknologi Kreatif dan Warisan, Universiti Malaysia Kelantan

** Profesor Madya di Fakulti Teknologi Kreatif dan Warisan, Universiti Malaysia Kelantan

*** Pensyarah Kanan di Fakulti Teknologi Kreatif dan Warisan, Universiti Malaysia Kelantan

MOBILE DEVICE SECURITY ISSUES IN DIGITAL LITERACY FOR HIGHER LEARNING INSTITUTION

SHEKH ABDULLAH AL-MUSA AHMED*

NIK ZULKARNAEN KHIDZIR **

TSE GUAN TAN***

almusa.c17e002f@siswa.umk.edu.my*, zulkarnaen.k@umk.edu.my**, tan.tg@umk.edu.my ***

Abstract

Mobile security, or more specifically mobile device security, has become increasingly important in mobile computing for digital literacy. Digital literacy is the set of competencies required for full participation in knowledge of society. It includes knowledge, skills, and behaviors involving the effective use of digital devices such as smartphones, tablets, and laptops for purposes of communication, expression, collaboration and advocacy. Of particular concern is the security of higher learning institution is now stored on smartphones. Along with this expansion came a number of security issues to affect mobile devices. A chance to have a tiny and powerful device that is Internet linked allows communication from anywhere in the higher learning institution. In higher learning institution, those who have attached their personal smartphones to institutional network would have found out the easy way of doing so. Specifically, there have been a handful of cases where learners who attached their own personal devices to a higher learning institutional network. However, a system administrator sent out a remote command to the device and instructed it to store itself of all data to keep it from falling in the wrong hands. Hence in Android device having heard the term of rooting the device. Concisely, this refers to undertaking a process of gaining root access to a device. Typically, this involves running an application or script that grants root access to the user. Once access is granted, the user in the higher learning institution can do pretty much whatever the institution want on the system without restriction. However, one of the downsides of this process is that the device is now exposed to greater danger from external threats as well. Moreover, this article focuses on mobile device security issues in digital literacy in higher learning institution. It is about developing institutional learners to critical and creative abilities when it comes to mass media, popular culture and digital media. Since digital media is using smartphone for store information and article also referring how to maintain security of these smartphone data.

KEYWORDS: *Encryption, Remoteness, Digital Affixing Signature, Trojan Horse Attacks, Malware, Social Engineering Attacks, Digital Literacy.*

Submitted: 5 Oktober 2019 Revised: 5 November 2019 Published: 31 Mac 2020

* PhD Candidate at Faculty of Creative Technology and Heritage, University Malaysia Kelantan

** Associate Professor at Faculty of Creative Technology and Heritage, University Malaysia Kelantan

*** Senior Lecturer at Faculty of Creative Technology and Heritage, University Malaysia Kelantan

1.0 Introduction

The rapid adoption of the mobile device in the higher learning institute has already established two apparent consequences: a rise in productivity and capability in addition to a corresponding rise in the number of security hazards. The designers of devices have frequently made a trade off between security and features by angling toward features, with security being an afterthought (Abawajy, 2014). Whilst new security features have helped to somewhat reduce the issues present, many of the devices have problems to be resolved. Nevertheless, digital literacy is the set of competencies required for full participation in a knowledge society. It includes knowledge, skills, and behaviors involving the effective use of digital devices such as smartphones, tablets, and laptops for purposes of communication, expression, collaboration and advocacy. While digital literacy initially focused on digital skills and stand-alone computers, the focus has shifted from stand-alone to network devices including the Internet and social media.

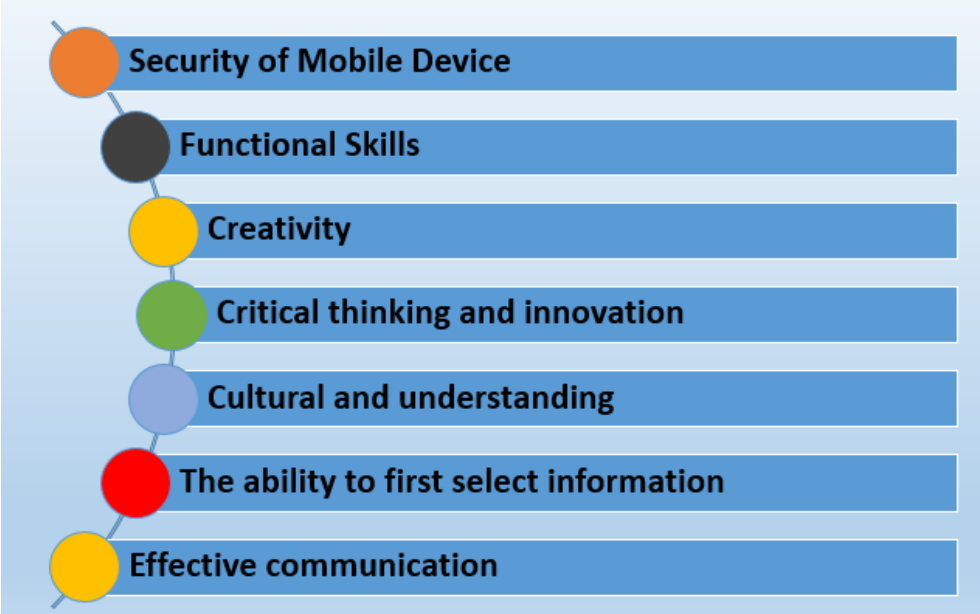

Figure 1: Various aspects of digital literacy awareness

However digital literacy as the usage and comprehension of information in the digital age, and also emphasized the importance of digital technologies as an essential life skill in the higher learning institution (Adrian, 2017 & Cojazzi, 1996).

2.0 The Challenge Of Digital Media Literacy On Mobile Security

Several steps have recently been taken, but overall there is an attempt to strategy the challenge of digital media literacy on mobile security through five key areas (Hinson, 2007). Each address a specific problem or needs.

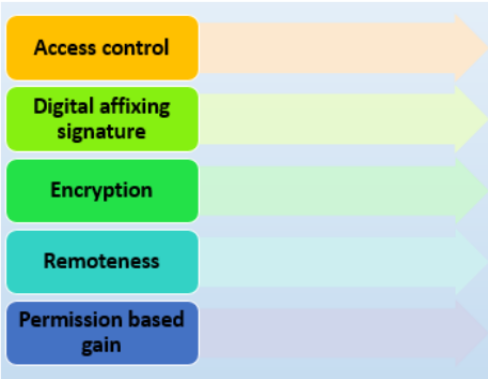

Figure 2: The Challenges of Digital Media Literacy in Higher Learning Institution

2.1 ACCESS CONTROL

This is utilized to protect mobile devices, which includes passwords, biometrics, and least-privilege technologies in the higher learning institution.

2.2 DIGITAL AFFIXING SIGNATURE

The digital affixing signature to be now parts of the application model of most if not all mobile OSs. This feature allows applications to be authorized to enable them to be verified that they originated from a specific author, and in addition they simply cannot be tampered with without such activities being recognized. While digital signing is not necessary, Android will not allow the setting up of applications from unidentified sources by default. In iOS, applications from unidentified sources may not be installed at all unless the particular owner specifically modifies the phone to allow this.

2.3 ENCRYPTION

Encryption is another essential component for digital media literacy of the security model of a mobile OS. Encryption is applied on devices to ensure that data is stored safe in the event a tool is lost, stolen, or compromised. Although not constantly implemented on many mobile devices during the past, this has changed, with Android 6. 0 (codename Marshmallow) even requiring storage space encryption by default (Nik. Z. & Shekh. A. 2019; 2018).

2.4 REMOTENESS

Remoteness , which seeks to limit the access an software has, is an important issue addressed in mobile devices. Essentially, this is a form of least privilege for applications, where if in the higher learning institution don't need access to sensitive data or processes, only a specific get it.

2.5 PERMISSIONS-BASED GAIN

In the higher learning institution, permissions-based gain access to control

works much as it will on server and desktop operating systems. This kind of feature limits the opportunity of access of an application by blocking those actions and the user may attempt but has not been granted access to it.

2.6 DIGITAL MEDIA LITERACY IN THE HIGHER LEARNING INSTITUTION

Whether a new to smartphone or have some experience, digital media literacy will help to develop a fundamental understanding of smartphone or tablet or laptop in the higher learning institution. It help learn the essential skills to begin digital media with confidence, be more productive at home and at work, stay safe online, use technology to complement of life style. Digital media literacy is the marrying of the two terms digital media and literacy. However, there is a large significance as a result of the combination of these two terms. Digital media information is a symbolic representation of data, and literacy refers to the ability to read for knowledge, write coherently, and think critically about the written word in the higher learning institution. A digitally media literate individual will possess a range of digital media skills, knowledge of the basic principles of mobile devices, and skills in using internet. The individual has the ability to engage in online communities and social networks while adhering to behavioral protocols. The individual is able to find, capture, and evaluate information (Nik. Z., Shekh. A. & Tan. T., 2018). Digital media literacy requires the individual to understand the social institution issues raised by digital technologies and possess critical thinking skills. These skills can be possessed through digital experiences that push individual to think in a variety of ways through a multitude of media platforms. The evolution of digital media has quickly integrated into literacy. Digital education for media literacy often uses an inquiry-based pedagogic model that encourages learern to ask questions about what they watch, hear, and read (Nina Godbole, 2017). Media literacy education provides tools to help people critically analyze messages, offers opportunities for learners to broaden their experience of media, and helps them develop creative skills in making their own media message .

4.0 METHODOLOGY

Mobile operating systems come in four flavors, such as , Blackberry, Windows Mobile, Google Android, and Apple OS. Of these, the Apple OS and Google Android operating systems are by far the ones most commonly found in the higher learning institution. Both of these operating systems have been designed to address some of the most basic threats and risks right out of the box, such as the following:

- Trojan Horse Attacks
- Network-based attacks
- Various types of Viruses
- Social engineering attacks
- Resource and service availability abuse
- Malicious and unintentional data loss
- Attacks on the integrity of data

Before analyzing the security models of these two operating systems, a brief recap of each of these attacks as they relate to mobile devices might be helpful.

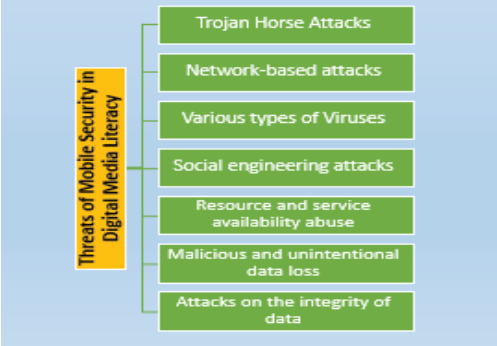

Figure 4: The threats of mobile security in digital media literacy

4.1 TROJAN HORSE ATTACKS

These are typically launched by malicious websites or compromised legitimate web- sites. The attacking website sends malformed network content to the victim's browser, causing the browser to run malicious logic of the attacker's choosing web site.

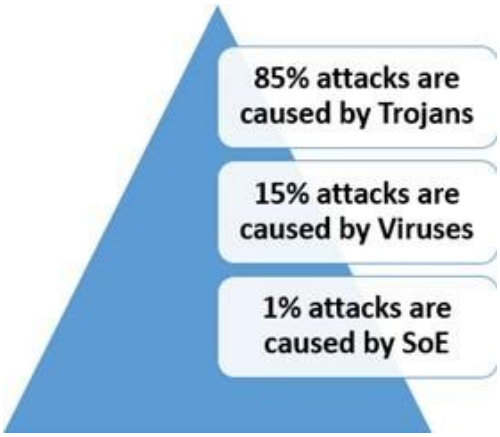

Figure 3: Different Types of Malware detected in The Higher Learning Institution

4.2 DIFFERENT TYPES OF VIRUS

In the higher learning institution viruses can be broken into three high-level categories such as, traditional computer viruses, computer worms, and Trojan horse programs. Much like traditional systems, malware does plague mobile systems, and in fact there are pieces of malware designed exclusively for mobile devices.

4.3 SOCIAL ENGINEERING ATTACKS

In the higher learning institution social engineering attacks such as phishing attempt to trick the user into disclosing sensitive information. Social engineering attacks can also be used to entice a user to install malware on a mobile device. In many cases social engineering attacks are easier to accomplish on mobile devices largely because of their personal nature and the fact that they are already used to share information on social media and other similar services.

4.4 DATA LOSS

Data loss occurs when a device used to store sensitive data is either carried away by a malicious person or is lost. While many of these situations can be mitigated through encryption and remote wipes, the problem is still very serious in the higher learning institution.

4.5 DATA THEFT

This is one of the bigger problems in the higher learning institution such as that have emerged with mobile devices because criminals target them for the information that learner contain. Malware has been observed on mobile devices that steals sensitive information.

5.0 RESULTS, DISCUSSIONS AND FINDINGS OF GOOGLE ANDROID OS

Initially, android were a market leader in exploration of mobile operating system. Android required condition way back in 2003 at the hands of Android Inc, which was acquired by Yahoo in 2005. Right from the start, the operating system was designed to be considered a mobile platform that has not been only feature rich, powerful, and mobile but also open source. As designed, Android can be installed on an array of hardware, and it supports and has a build-in with a lot of advanced software technologies. It absolutely was also designed to integrate with exterior data sources, cloud services, and other technologies as well as to run applications locally. In order to provide these features is to do so safely and securely. This lead in to safeguard users, data, applications, these devices, and the network around it. Android was envisioned and created with a multilayered security model that allows for the versatility essential within an open system, while providing protection for users and applications. An additional goal of the operating system is to compliment developers and make the platform easy to work with and easy to interact security controls. In practice, programmers should be able to easily call on the safety controls of the system, of course, if they are experienced programmers, they can weak the controls as needed. Less experienced developers or those not familiar with proper security configurations are protected because the system puts default configurations in destination to ensure that safety and security are maintained. Just as Android originated to make it easy on developers to develop and deploy applications, the system was created with the user in brain. For this end the system was developed with the expectation that attacks would happen, including the common adware and spyware issue, data theft, while others. It also was designed with the concept the users themselves might try things that may negatively impact the system in the higher learning institution. Google android was designed to enable the learner to work with the system is to do everyday duties but not provide them with a high level of gain access to specifically, Android does not let the learner have root access to the device without the user intentionally overriding this

protection. Google android, under the hood, is a series of components working together to make the system work. Every single component in the system is self-contained and concentrates on performing whatever activity it was designed to do. Each component concentrates on security measures for itself and assumes that every other component is also doing the same. In addition, in a normal installation, only a very small area of the Android OS ever operates with root access, this being the kernel, and everything else runs with less access and in a software sandbox to further isolate and protect each application.

6.0 FINDING RESULTS OF APPLE IOS

The second most popular mobile operating system in the higher learning institution is Apple's iOS, which is present on multiple devices including the iPod, iPad, and iPhone. Much as Android is based on the Linux kernel, iOS is a slimmed down version of OS X for the Mac. However, while it is based on OS X, which is based on FreeBSD, it is not fully Unix compatible. Unlike Android, which covers all five core components of system design, iOS only cover four.

6.1 TRADITIONAL ACCESS CONTROL

In the higher learning institution the traditional Access Control iOS provides traditional access control security options, including password configuration options as well as account lockout options.

6.2 APPLICATION PROVENANCE

Application Provenance just as Android items that are in the Google Play store have been verified and therefore trusted, in iOS it's the same type of deal with apps being created by Apple-approved developers, who have the ability to sign their app before placing it in the store.

6.3 ENCRYPTION

In the higher learning institution Encryption iOS uses hardware-accelerated AES-256 encryption to encrypt all data stored on the device as well as additional encryption for email and other services.

6.4 ISOLATION

Isolation The iOS operating system isolates each app from every other app on the system, and apps aren't allowed to view or modify each other's data, logic, and the like.

7.0 PENETRATION TESTING FOR MOBILE SECURITY ISSUES

In many ways the process is similar to what we are already using in a traditional set-ting but with some minor differences along the way .Here is a showing of how to evaluate the Penetration Testing for Mobile Security Issues .

7.1 FOOTPRINTING

Many of the scanning tools we examined in our footprinting phase can be used to locate and identify a mobile device plugged into a network. A tool like Nmap, for example, can be used to fingerprint an OS under many conditions and return information as to its version and type. Once you find mobile devices in the environment, make sure to note their information such as MAC address, IP address, version, type, and anything else of value (Shekh. A., Nik. Z., & Tan. T. 2019) .

7.2 SCANNING

Scanning For mobile de vices attached to the network you are evaluating, use a piece of software such as Kismet to find out which wireless networks the devices are looking for.

7.3 EXPLOITATION

Exploitation Use man-in-the-middle attacks, spoofing, ARP poisoning, and other such mechanisms to attack a device. Use traffic insertion attacks to deliver client-side exploits to vulnerable systems and devices or manipulate captured traffic to exploit back-end servers.

7.4 POST EXPLOITATION

Post Exploitation Inspect sensitive data areas on mobile devices for information such as the Short Message Service (SMS), and browser history databases. Note that forensic tools are available for cell phones that can extract this information as well (Shekh. A., & Nik. Z., 2018).

8.0 COUNTERMEASURES

In higher learning institution just like securing desktops, servers, systems, and other equipment, some basic steps to make mobile devices more resistant to attacks. Exactly what is included here is some basic guidance however, not a comprehensive set of all that can be carried out is possible.

8.1 SETTING PASSWORDS

Setting passwords on all mobile devices is a requirement of all devices that will be mounted on a corporate network and/or store sensitive data for Digital media literacy. It is worth remembering that enabling certain features such as encryption will require the setting of any password before they will work.

8.2 STRONG PASSWORDS

Strong passwords are recommended on all devices. This task is of particular importance because many mobile devices allow to work with methods to unlock the device aside from passwords. Many devices enabling to set PIN number codes, gestures, and regular alphanumeric passwords (Todd. F., 2016).

8.3 INSTALL ANTI MALWAREAPPLICATIONS

Install antimalware applications to thwart the spread and infection of malware. Ideally, the anti-malware application should scan not only the device but also newly in- stalled applications and email for maximum effect (Veiga. A. & Eloff.J., 2009).

8.4 USE ENCRYPTION

Use encryption on all devices whenever we can to protect both internal storage and secure digital cards. This really is an essential part of protecting data on a device in the event it is lost or stolen. Note that some older devices and elderly systems do not support encryption.

9.0 CONCLUSION AND DISCUSSION

In the higher learning institution a digitally media literate individual will possess a range of digital media skills, knowledge of the basic principles of mobile devices, and skills in using internet. The individual has the ability to engage in online communities and social networks while adhering to behavioral protocols. The individual is able to find, capture, and evaluate information (Wiebke, A., 2009). For digitally media literate portable phones have taken the world by storm and have seen incredibly fast growth and adoption during the last several years for the digital media literacy (Yin, R.K., 1984). Along with this expansion came a number of security issues to affect mobile devices. A chance to have a tiny and powerful device that is Internet linked and allows communication from anywhere at any time is alluring as well as a problem for companies. With the average person today possessing at least three mobile devices and using those devices for both personal and work purposes, the devices pose a problem for the workplace. Functioning systems such as Google's Android and the second-place Apple iOS are in several ways similar to but also totally different from traditional systems, offering securities challenge.

10.0 REFERENCES

Abawajy, J., (2014). User preference of cyber security awareness delivery methods. Behavior & Information Technology, 33(3), 237-248.

Adrian. M., (2017). Running the Risk IT – More Perception and Less Probabilities in Uncertain Systems. Information & Computer Security,25(3),45-59.

Clif A. Ericson, (2016). Hazard analysis techniques for system safety . John Wiley & Sons.

Cojazzi .g, (1996). Preliminary Requirements for a Knowledge Engineering Approach to Expert Judgment Elicitation in Probabilistic Safety Assessment. International Conference on Probabilistic Safety Assessment and Management, 24(2), 491-498.

Hinson, G. (2007). The State of IT Auditing in 2007. The EDP Audit, Control, and Security Newsletter, 36(1), 13-31.

Nik. Z., Shekh. A. (2019). Towards Fact- Based Digital Forensic Evidence Collection Methodology. International Journal for Information Security Research (IJISR),9(1),67-79.

Nik. Z., Shekh. A. (2018). Legal Protection of intellectual property rights(IPR) in Bangladesh. International Journal of Law. Government and Communication, 3 (12) , 71-89.

Nik. Z., Shekh. A. &Tan. T. (2018). Viewpoint of Probabilistic Risk Assessment in Artificial Enabled Social Engineering Attacks. BITARA International Journal of Civilizational Studies and Human Sciences, 1(4), 32-39.

Nina Godbole (2017). Information System Security , Security Management,Metrics, Framework and Best Practices. John Wiley & Sons,Inc.

Shekh. A., Nik. Z., Tan. T. (2019).Towards the Big Data and Digital Evidences Integrity. Journal of Intelek ,14(1),56-63.

Shekh. A., Nik. Z. (2018).An Exploratory Factor Analysis of AI Enabled Social Engineering(SoE) Attacking Risk in Higher Learning Institute , Journal of Mass Communication & Journalism,15(1),32-40.

Todd. F. (2016). Physical Security. Handbook of Information Security Management. Taylor & Francis Group.

Veiga. A. & Eloff.J.(2009). An Information Security Governance Framework. Information Systems Management,24(4), 361-372.

Wiebke, A. (2009). Agents,Trojans and tags: The next generation of investigators. International Review of Law, Computers & Technology, 23(1-2), 99-108.

Yin, R.K. (1984), Case Study Research Design and Method Newbury Park. CA. SAGE Publications.