Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 56 (2015) 376 – 383

Procedia Computer Science

International Workshop on Cyber Security and Digital Investigation (CSDI 2015)

Survey on Mobile User's Data Privacy Threats and Defense Mechanisms

Jalaluddin Khan[a], Haider Abbas[a,b*], Jalal Al-Muhtadi[a]

[a]*Center of Excellence in Information Assurance,*
King Saud University, Riyadh, Saudi Arabia
[b]*National University of Sciences and Technology, Islamabad, Pakistan*

Abstract

Nowadays, mobile devices have become an integral part of our daily life. These have proven to be an advantageous scientific invention that fills personal and business needs in a very efficient manner. In this era, the availability of mobile services has significantly increased because of the rich variety of mobile devices and essential applications provided by mobile device manufacturers. At the same time, numerous mobile security issues and data privacy threats are challenging both manufacturers and users. Therefore, mobile devices are an ideal target for various security issues and data privacy threats in a mobile ecosystem. In this paper, we provide a brief survey of the security challenges, threats, and vulnerabilities of a mobile ecosystem. Furthermore, we discussed some key points required to ensure mobile security and defend against data privacy threats. The emphasis of the discussion is, strong protection and the restriction of malicious activity at the application developer end, application stores end, and operating system and mobile device manufactures end by preventing the user from using non-recommended applications (which may be malicious) and considering biometric features for the authentication of real users in the mobile devices. Also briefly discussing the defense mechanisms that are considered to be a relatively better approach for securing personal and business related data or information in the mobile devices.

Keywords: Mobile Security; Malware; Data Privacy; Threats and Vulnerabilities

1 Introduction

Over the last few years, the use of mobile devices for both business and personal purposes has increased significantly. The appearance of mobile devices and flourishing of mobile applications in recent years have

* Corresponding author*: Tel.: +966568254293; fax: +966(1) 4696452*
E-mail address: hsiddiqui@ksu.edu.sa

doi:10.1016/j.procs.2015.07.223

enhanced personal mobility and business development. There are 6.9 billion mobile users around the world, which is equivalent to 95.5% of the world's population, as estimated by the International Telecommunication Union (May 2014) [19]. Mobile device security is a developing security area of rising significance and cumulative needs, but it is comparatively weak area for protecting a user's data privacy. Although mobile device companies are thinking in terms of a user's security and data privacy, the use of applications from the internet creates complex issues in relation to handling threats and vulnerabilities when securing a user's data privacy. Software applications are mostly designed for an explicit task and are targeted at a specific set of mobile devices. However, because of threats and vulnerabilities, data protection is a very risky task in mobile devices. Applications organize information in a very suitable manner for specific features of a mobile device, and they habitually interact with the operating system and hardware. There are thousands of diverse applications accessible from application stores for each mobile device, and these applications have an extensive range of purposes, including web browsing, entertainment (movies, games, and music), social networking, communication (e-mail, internet messaging,), banking, and location-based services.

This paper describes some important aspects of mobile security, data privacy issues, threats and vulnerabilities. The paper is organized as follows. Section 2 outlines related work. Section 3 provides the security challenges. Section 4 describes threats and vulnerabilities of the mobile ecosystem. Section 5 discusses some related defense mechanisms. Section 6 provides comparative analysis results and a discussion and Section 7 gives the conclusion and outlines future work.

2 Related Work

In this section, we discuss a few of the mobile security and data privacy mechanisms. The researches presented in[1,2,3,4,5] described high-level attacks as those against user specific applications and use mechanisms, collected data, operating systems, architectures, detection principles, and IDS (Intrusion Detection System)-based model tools. Similarly[7,8,9,10,11,12] described how permission- and behavioural-based techniques are useful in android mobile devices and protecting against cybercrime by using a mobile ecosystem. Other researchers[13,14,15] preferred a pure biometric mobile ecosystem and described the challenges, threats, and vulnerabilities of mobile devices. Bose A. and K. G. Shin[16] described the popularity of SMS (Short Messaging Services)/MMS (Multimedia Messaging Services)/IM (Instant Messaging) messaging, and investigated Bluetooth virus transfer attacks and the spread of propagation worms, malware, and viruses from all types of messages in mobile devices. Yang L. et al.[20] implemented mobile SMS security module and mobile privacy threat module in Android security Labware. Deng R. et al.[21] showed that the functionality limitation of mobile devices results in limited space for malware, with the main focus on the detection and prevention of malware in mobile devices. Hatonen K. et al.[22] described host-based intrusion into mobile devices, as well as improvements to the computing power and storage capabilities of mobile devices. All these schemes had the main aim of providing mobile security and privacy in a mobile device system, and every author described their views and mechanism to overcome threats and vulnerabilities.

3 Security Challenges for Mobile Device Users

Mobile device applications offer a level of convenience that the world never before considered. At any location (home, office, hotel, playground, road, parking, museum, travelling in different countries, or anyplace in the world), any mobile user can use applications to fulfil their daily needs, including communicating, buying, searching, making payments, selling, entertainment, and finding general information. This extreme level of comfort has brought with it an extreme number of security risks. Some of the mobile device challenges are described below, including ways that vulnerabilities and attackers are reducing mobile application freedom.

3.1 Insecure Data Storage

A user can suffer a data loss after losing a mobile device or experiencing interruption by some malicious application that deletes a user's most valuable information. In this way, all users are at risk by engaging in this type of activity. Some common pieces of data are stored at high risk, including personal information (name, address, date of birth, banking information, family pictures, social networking address, email address),work information (company name, work position, company contact numbers, and official documents if any are available)[30].

3.2 Physical Security

Physically securing a mobile device is difficult, but when a mobile user is constantly using their mobile device (24×7×365) and it is lost, then the task becomes seemingly impossible. Obviously, physical security is the greatest concern for risk-free mobile devices [30]. If a person's mobile device is lost or stolen, the user's sensitive data may be misused by a thief, including personnel information, unsecured documents, business data, and files [30].

3.3 Mobile Browsing

Mobile browsing is the best feature of any mobile device for providing the best use of internet applications. However, normally in mobile devices, a user cannot see the entire URL or web address, making it difficult to determine whether the web address or URL is safe. Thus, browsing can be used as a phishing related attack [32].

3.4 Multiple User Logging

Because of the progressive growth of social media and single sign-on (SSO) in the mobile application ecosystem, it is estimated that 60% of mobile applications are insecure because of using the same login for multiple social networking applications. Hackers who obtain login credentials for a website or app such as twitter or Facebook could possibly gain access to a user's profile page. The use of social media single sign-on is actually to facilitate social interaction. At the same time, developers also gain access to some social information related to users.

3.5 Client Side Injection

The execution of malicious programs on mobile devices over the internet occurs by application or web browsing client side injection. Html injection, SQL injection, or another newer attack (abusing phone dialler, SMS) involves client side injection. Hackers could load a text-based attack and exploit a targeted examiner. In this way, any data source can be injected, including resource targeted files or applications.

3.6 Improper Session Handling

For mobile devices, session handling is an identified security concern for web applications. Improper session handling has vulnerabilities that are pretty common when using internet applications over any platform like mobile devices or PCs. Sessions with long expiry times invite vulnerabilities when performing financial tasks. Poor session management can provide clues to unauthorized access through session hijacking in mobile devices.

3.7 Weak Authentication and Brute Force Attack

Today, many applications rely on password-based authentication, as a single factor. The owners of these applications do not enforce strong passwords and the securing of valuable credentials. Thus, users expose themselves to a host of threats, including stolen credentials and automated brute force attacks.

4 Mobile Threats and Vulnerabilities

A comprehensive overview of threats and vulnerabilities shows that cyber criminals are now focusing increasingly on mobile devices [2,3,4,5]. Mobile devices use many useful applications on the internet, which makes them a prime target for attackers to destroy security mechanisms and cause threats, spread vulnerabilities [6]. The distance between a hacker's capability and an organization's protection is widening day by day. This tendency underlines the need for additional mobile device security cognizance, as well as more flexible, better integrated mobile device security solutions and policies. Some significant mobile threats and vulnerabilities are described:

4.1 Mobile Threats

Threats and attacks that worked well on personal computers are now being tested on unsuspecting mobile devices to see what works (mechanism) and, with protection increasing; there is an adequate number of easy targets. Attackers are definitely penetrating the weakest point in the chain and improving on the most successful scams. Mobile attacks are basically divided into four categories in terms of user perspective, service/content provider perspective, and network perspective, as listed below [33].

Physical Threats

Mobile devices are designed to be used in daily life, and physical security is an important issue [13,14,15]. Some of the physical threats are described below.

- *Bluetooth*

This is a short-range radio technology that provides wireless connectivity in very short ranges, and many potential threats, vulnerabilities, and exploits have been recognized with Bluetooth [16]. Malware can spread from device to device through Bluetooth services. When two devices come within range and are paired using default

Bluetooth passwords (code), malicious data are transferred to the other device by the Bluetooth services [13,14,15,17].

- *Lost or Stolen Mobile Devices*

The loss or theft of valuable mobile devices is also a serious threat because these valuable applications and hardware devices can be resold on the market, which threatens a user's personal sensitive data [17].

Application-Based Threats

Many downloadable applications are available over the internet, and most of these have multiple security problems. Malicious applications are available on websites, with the greatest concern being fraud or scams. Application-based threats can be classified as one or more of the following mobile applications [13,14,15,17].

- *Spyware*

This is designed to collect personal, private data without a user's knowledge or endorsement. Spyware-targeted data commonly include the user's location, contact list; private or financial photos, email address, browser history, and call history. The stolen information might be used for identity theft or financial fraud [13,14,15,17,29].

- *Malware*

Malware (malicious software) accomplishes malicious action after being installed in a user's mobile device without the user's knowledge or approval. It can add charges (call charges) to a user's phone bill, send unwanted messages to a user's contact list, and give an attacker full control over the mobile device [13,14,15,17,29].

- *Vulnerable Application*

Vulnerable applications are those applications that contain faults that can be exploited with malicious intent. They give an attacker permission to perform unwanted actions, access sensitive personal or business information, stop correctly performing activities, and download applications without approval[13,14,15,17].

- *Privacy Threats*

Privacy threats can be caused by mobile applications in addition to malicious applications. For example, the global positioning system (GPS) can provide information about any place a user visits [24,25].An attacker or hacker can steal a user's information and identity, which can cause serious problems [31].

Network-Based Threats

Mobile devices provide the best support to cellular networks, as well as wireless LAN IEEE 802.11, both of which have different types of threats for the user [13,14,15,17]. Some network-based threats are described below.

- *Denial of Service Attack (DoS)*

Denial of service means an attacker or hacker denies access to application services or other services. In relation to mobile devices (Smartphone's), this type of attack typically involves robust connectivity and compact capabilities. With limited hardware issues, a skilled attack on a mobile device can be accomplished with very little effort, and even one attacker may be sufficient to make a device insecure [13,14,15,16,25,29].

- *Network Exploits*

This type exploits the faults in the mobile device operating system or other application software that operates on a wireless or cellular network. When mobile devices are connected through a network, they (network) install some malicious application software on users' mobile devices without the approval of the users [13,14,15, 17, 25].

- *Mobile Network Services*

Mobile network services like MMS, SMS, and voice calls can also be used for attacking mobile devices. In this case, a new attack like a phishing attack occurs in the mobile devices. A phishing attack is nothing but a means to gain sensitive or business information from the user by representing oneself as a reliable unit[13,14,15,29].

- *Wi-Fi Sniffing*

Wi-Fi sniffing means intercepting data between the mobile devices and Wi-Fi access point from the air. It also considers that every application and web page has some vulnerabilities. Thus, passing data in the Wi-Fi medium is a big risk. Unencrypted data can easily be grabbed by attackers or hackers [17,25,].

Web-Based Threats

In mobile devices, there are always mobile users that use web-based applications over the internet. Thus, threats related to such activity is a major concern, and some researches have proved that web-based threats are a much more serious problem for mobile devices [13,14,15,17,]. Some web-based threats are described below.

- *Drive by Downloads*

This is a concept involving the automatic download of an application when visiting a web page (malicious web address). When a user always wants to see every downloaded item when clicking it, this causes the mobile device to become unstable. Thus, a user can take precautions against this type of activity in any website [17].

- *Browser Exploits*

This type of attack benefits from the vulnerabilities of a user's mobile web browser or an application (software) launched by the browser, such as PDF reader, flash player, and image viewer. Generally, when visiting an unsafe website, clicking in a browser can install a malicious software or application on a mobile device [17,26,]. A browser can contain two types of attacks, from web apps and native apps, when a mobile user downloads a hacker's browser-based malware by clicking a link in an insecure area where the hacker has full control, which can expose the user's information and facilitate data privacy theft [32].

- *Phishing Scams*

Phishing scams are a means of obtaining sensitive or business information from a user by representing oneself as a reliable unit using a link on a social networking website, text message or email (spam) on a malicious website, or gaining information about login credentials[17,29].

4.2 Mobile Vulnerabilities

Mobile vulnerability is a security exposer that results from a mobile device weakness that the application developer for a mobile device did not expect to introduce and will fix once when it is discovered [18]. Vulnerability includes three steps, a device has susceptibility, attackers access the flaw, and a capable attacker exploits it [13,14,15].

- *Rootkit*

Rootkits attain their malicious target by infecting the operating system. Generally, rootkits hide malicious user spaces and data files in the operating system or install some malicious application in the mobile device [4,5].

- *Worm*

A worm is program code that makes multiple copies of itself from one mobile device to another, using diverse carriage techniques by the network. A worm damages or compromises the security of the mobile device [2,5].

- *Trojan Horse*

A trojan horse installs other malicious (worm or botnet) applications and gathers sensitive information from the mobile devices. It is also used in a phishing attack. Trojan horses widely affect businesses with the purpose of stealing information from devices [15].

- *Botnet*

A botnet is a collection of compromised devices that are infected by virus programs that give an attacker the capability of remotely supervising them. It represents a serious money-related security threat around the world [10,16,15]. It is also responsible for sending spam mail to commit DoS attacks [14,15].

5 Defensive Mechanisms

Security and data privacy need multiple means of protection and restrictions on mobile devices. In general, the world now faces threats without correlation among all aspects of security breaches. In this regard, it is essential to ensure appropriate (restrictions and precautions) security mechanisms at all stages (development to final stage) when manufacturing mobile devices. The section also takes into account, the precautions and actions from European advisory body opinions [34] regarding smart devices. These involve correlations among the application stores, operating system device manufacturers, application developers, non-recommended applications, and biometric approaches (authentication/ verifications) in mobile devices to reduce security issues and data privacy threats, and provide a secure mobile ecosystem. Figure 1 shows the defensive mechanisms that need to be considered and implemented to solve mobile users' security issues and data privacy threats in the appropriate way.

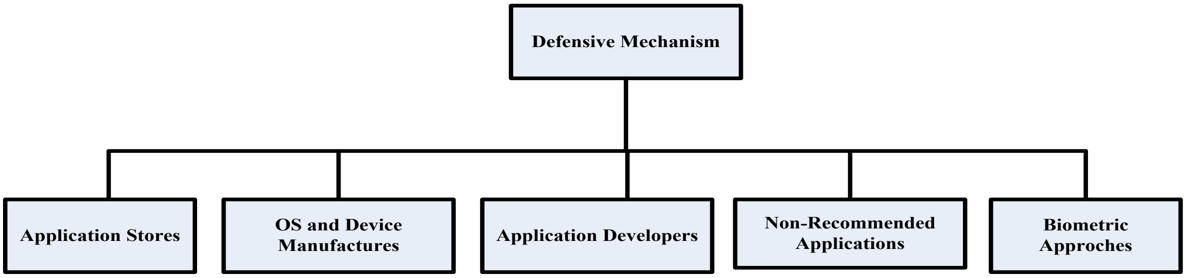

Figure. 1. Defensive Mechanism Architecture

5.1 Application Stores

Mobile device application stores like blackberry world, App store, Google play store, Nokia Ovi store, and Samsung Galaxy apps should contain genuine applications. If any application shows alteration (in the meaning of threats attacks) or malicious behavior in the application store, the authorized application store should delete that application until the application vender provides a valid security specification without any data privacy threats and vulnerabilities in the near future [28]. This type of action is necessary for each manufacturer application store. In that way, every application should be functionally fit and tested with high priority in terms of data security and privacy.

5.2 OS and Device Manufacturers

Operating system and device manufacturers give attention to mobile security and data privacy threats at every step of updating their software versions and releasing new mobile devices. They should ensure processing security and employ data privacy based on the design moralities to protect user data. Implementing a security friendly atmosphere and tools preclude malicious behavioral applications from scattering and allow functionality to be uninstalled/installed effortlessly. Systematic suggestions are made that facilitate consistent security related updates. Active assistance improves and facilitates icons that show users the diverse data usage by the applications.

5.3 Application Developers

In the mobile ecosystem, the developer has a key role in providing safeguards and improved accessibility for using software applications. Mobile companies or device manufacturers take care of applications or new features in the application by the application developers. The application developer is responsible for all kinds of data handling for that particular application, and sometimes software improperly handles data in the mobile device as a result of a mistake (bug) of the application developer [24]. Sometimes, an application developer can directly access a user's mobile data by using some specific software and steal valuable business or personal data from the user's mobile device. Therefore, there should be control and restriction mechanisms for developers.

5.4 Non-Recommended Applications

Device manufacturers or mobile companies are providing many usable mobile applications for the ease of the mobile user. There is so much business competition between mobile devices companies to provide better applications to achieve user satisfaction and business profits. In this regard, third party applications have entered the markets, which are not recommended by application stores and manufacturers. Sometimes installing these type of non-recommended application causes data privacy theft because it is a valuable weapon for hackers or attackers for making threats (malware) and exploiting the vulnerabilities of mobile devices[24,28]. Avoiding this type of software application is better for the security and data privacy of the mobile devices.

5.5 Biometric Approaches

Biometric approach for authentication of the users is considered to be more beneficial as biometric mechanism involves the automated use of behavioral or physiological features to determine or verify identity. In this process, there are two main functions: enrollment and authentication (verification). The enrollment process is the first step for providing a user's specific information such as physiological (face, fingerprint, hand, iris, and DNA) and behavioral (keystroke, signature, and voice) data to generate a reference outline for succeeding authentication [27]. In this process, a physiological or behavioral biometric sample (user related information) is scanned by a suitable sensor, and a reference outline is generated by extracting the user profile and its training set, and then storing the data in the database that the system needs to use for comparison and authentication in the future [18].

6 Comparative Analysis and Discussion

In this comparative analysis and discussion, we are going to analyze and discuss mobile devices' security issues, data privacy in terms of types of attacks, security mechanisms, and the key emphasis of the research schemes.

Table 1. Comparative Analysis

Scheme	Type of Attacks	Security Mechanism	Emphasis
Malware: Detection and Prevention on Mobile Phones [3,4,5]	All types of attacks, especially malware threats and vulnerabilities [3,4,5].	Based upon detection principles, operating systems, and architectures, especially focusing on IDS (Intrusion detection system)-based models and tools [1,3,5] .	Focusing on high-level attacks such as those against user-specific applications [3,5].
Cybercrime and Portable Devices [7,8,9,12]	Cybercrime affecting mobile devices [7,8,9,10,12].	Permission-based security model and behaviour-based	Results show behaviour-based detection method still

		detection method in android mobile devices [7,8,9,12].	most valuable for data privacy in android operating system [7,8,9,12].
Mobile Device Threats, Vulnerabilities and their Defensive Mechanism [13,14,15]	All types of threats and vulnerabilities [13,14,15].	Preferring biometric security in mobile devices [13,14,15].	Suggesting iris biometric traits for their reliability and accuracy [13,14,15].
Bluetooth Services Exploitation [16]	SMS/MMS/IM messaging and Bluetooth viruses transfer attack [16].	An investigation of viruses, worms, and malware by agent-based malware modelling framework or simulators [16].	Focusing on SMS/MMS/IM and Bluetooth transfer of malicious behavioural worms, malware, and viruses [16].
Android Security Labware [20]	All types of threats and vulnerabilities attack.	Using android security Labware (Lab), implementing Mobile SMS security module and mobile privacy threat module [20].	Learning approach to mobile security on Android-based operating system [20].
Mobile Phones Malware [21]	Malware attacks on mobile devices [21].	State of the Art mobile malware, academic research and industrial effort against mobile malware [21].	Focusing on effective malware detection and prevention on mobile devices [21] .
Mobile Devices Intrusion Detection [22]	Based on intrusion over mobile devices [22].	Host based intrusion detection approach because sometimes network based intrusion not sufficient [22.]	Computing power and storage capabilities evolve into mobile devices [22.]

As shown in Table 1, all the schemes have the main aim of providing mobile security and data privacy in a mobile device system, and the researchers have described their mechanisms concerning threats and vulnerabilities in the mobile ecosystem. A mobile ecosystem is a very vast area when it comes in the internet medium, and every security measure remains handicapped by attackers or hackers and malicious suspicious intrusion applications.

If we carefully analyze the above-mentioned schemes then we observe that the biometric authentication if used as defensive mechanisms has relatively concise features that can encompass all schemes to counter these threats efficiently. Biometric authentication signifies the process that proceeds when a user desires access to the biometric system [27]. At this time, an identification or verification process is performed. The scanned input information is received, extraction is performed using the training set, and the input training set is compared or matched with the already enrolled training set in the database, after which authentication comes in the nature of accepted (yes) or rejected (no) [27]. It is more feasible to authenticate or verify a specific user using a biometric mechanism, in terms of security, usability, and data privacy of the mobile devices. Thus, biometric authentication, as a defensive mechanism can have a relatively good impact on mobile security and data privacy threats in this era and the near future generation of mobile devices.

7 Conclusion and Future Work

A mobile ecosystem is a very vast field, and it is very challenging to handle security threats and data privacy threats when using the internet from a mobile device because there are so many areas of concern, including physical threats, application-based threats, network-based threats, web-based threats, and mobile vulnerabilities. This paper presented a survey about the various security risks involved in mobile ecosystems that might raise serious threats to user's data privacy and security. It also highlights various research thoughts from the research community to address these concerns that are continuously changing due to emerging technology in this filed. The analysis presented in the paper infers that the use of biometric authentication mechanisms for information protection could reduce the risks. The biometric authentication to be used as defensive mechanism focuses on strong protection and the restriction of malicious activity in each of five key areas: the application developer end, application stores end, operating system and mobile device manufactures end and preventing the use of non-recommended applications (may be malicious apps) by the user.

This paper presented and analyzed some preliminary thoughts about the data privacy and security issues in mobile ecosystems and will serve as a baseline to devise a comprehensive protection mechanism for mobile device users in the future.

References

1. Yan Q., Y. Li, T. Li, and R. Deng, “Insights into Malware: Detection and Prevention on Mobile Phones,” in Security Technology, D. S ́lzak, T.-h. Kim, W.-C. Fang, and K. P. Arnett, Eds. Springer Berlin Heidelberg, 2009, vol. 58, ch. 30, pp. 242–249
2. Becher M., “Security of Smartphones at the Dawn of their Ubiquitousness,”Ph.D. dissertation, Universita ̈t Mannheim,2009
3. Schlegel R., K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang, “Soundminer: A Stealthy and Context-Aware Sound Trojan for Smartphones,” in Proceedings of the 18th Annual Network & Distributed System Security Symposium (NDSS), Feb. 2011
4. Mulliner C. and C. Miller, “Injecting SMS messages into smart phones for security analysis,” in WOOT’09: Proceedings of the 3rd USENIX conference on Offensive technologies. Berkeley, CA, USA: USENIX Association, 2009, pp. 5–5
5. Polla M. La, F. Martinelli, D Sgandurra, "A Survey on Security for Mobile Devices", IEEE Communications Surveys & Tutorials, 2013, Volume: 15, Issue: 1, Page(s): 446- 471.
6. Hypponen M., “Malware Goes Mobile,” *Scientific American*, 2006 vol. 295, no. 5, pp. 46–53.
7. Chiang H. S. and W. J. Tsaur, “Mobile malware behavioral analysis and preventive strategy using ontology, in Proc. the 2010 IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT 2010), pp. 1080-1085, 2010
8. Shin W., S. Kwak, S. Kiyomoto, K. Fukushima, and T. Tanaka, “A small but non-negligible flaw in the android permission scheme,” Policies for Distributed Systems and Networks, IEEE International Workshop, pp. 107-110, 2010.
9. Enck W., M. Ongtang, and P. McDaniel, “Understanding android security,” IEEE Security and Privacy, pp. 7:50-57, January 2009.
10. Shabtai A., Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Glezer. “Google android: A comprehensive security assessment,”. Security Privacy, IEEE, 8(2):35-44, 2010.
11. Shin W., S. Kwak, S. Kiyomoto, K. Fukushima, and T. Tanaka, “A small but non-negligible flaw in the android permission scheme,” Policies for Distributed Systems and Networks, IEEE International Workshop, pp. 107-110, 2010
12. Safavi S., Z. Shukur, R. Razali, "Reviews on Cybercrime Affecting Portable Devices", The 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013), Science Direct.
13. Roberta Cozza, “Forecast: Mobile Communications Devices by Open Operating System, Worldwide, 2008- 2015,” Gartner, April 5, 2011
14. Ruggiero P. and Jon Foote “Cyber Threats to Mobile ”, Produced for US-CERT, a government organization, Carnegie Mellon University-US, 2011
15. Shujithra M., G. Pasdmavati., Mobile Devices Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism, International Journal of Computer Applications (0975-8887) Volume 56-No.14.
16. Bose A. and K. G. Shin, “On Mobile Viruses Exploiting Messaging and Bluetooth Services,” in *Securecomm and Workshops, IEEE,* Sept 2006.
17. Lookout, “What is a Mobile Threat." [Online]. Available:https://www.lookout.com/resources/know-your-mobile/what-is-a-mobile-threat
18. Microsoft, "Definition of a Security Vulnerability" [online]. Available: http://msdn.microsoft.com/en-us /library/cc751383.aspx
19. MobiForge,"Global Mobile Statistics 2014." [Online]. Available: http://mobiforge.com/research-analysis/ global-mobile-statistics-2014-part-a-mobile-subscribers-handset-market-share-mobile-operators
20. Guo M., P. Bhattacharya,M. Yang, K. Qian, L. Yang, Learning Mobile Security with Android Security Labware, SIGCSE'13, March 6–9, 2013, Denver, CO, USA.
21. Yan Q., Y. Li, T. Li and R. Deng, Insights into Malware detection and Prevention on Mobile Phones SecTech,CCIS 58,PP 242-249,2009 Springer Verlag Berlin Heidelberg.
22. Miettinen M., P.Halonen and K. Hatonen, Host-Based Intrusion Detection for Advanced Mobile Devices, 20th International Conference on Advanced Information Networking and Applications, 06 IEEE.
23. Delac K., M.Grgic, A Survey of Biometric Recognition Methods, 46th International SyrnPoSium Electronics in Marine, ELMAR-2004. 16-18 June 2004. Zadar. Croatia, IEEE.
24. Jang-Jaccard J., S. Nepal, A survey of emerging threats in cyber security, Journal of Computer and System Sciences 80 (2014) 973–993, by Elsevier.
25. Dunham K., S. A. Nimeh,M. L. Becher, Mobile Malware Attack and Defense, Syngress Media.
26. Abraham S., I. Shobha,Chengalur-Smith,An overview of social engineering malware: Trends, tactics, and implications, Technology in Society 32 (2010) 183–196,byElsevier and Science Direct.
27. Prabhakar S., S. Pankanti, A. K. Jain, Biometric Recognition: Security and Privacy Concerns, ISBN: 1540-7993/03,IEEE Computer Society.
28. Mylonas A., A. Kastania, D. Gritzalis, Delegate the Smartphone user? Security awareness in Smartphone platforms, computers & security 34(2013) 47e66 Volume 34, May 2013, Elsevier and Science Direct.
29. Dagon D., T. Martin, and T.Starner, Mobile Phones as Computing Devices: The Viruses are Coming!, Published by the IEEE CS and ComSoc..
30. Pasquinucci, The security challenges of mobile devices, Andrea ,Computer Fraud & Security,S1361-3723(09)70035-1, Volume 2009, Issue 3, March 2009, Pages 16–18, Elsevier and Science Direct.
31. Potter B., Mobile security risks: ever evolving, Network Security, S1353-4858(07)70075-2, Issue 8, August 2007, Elsevier and Science Direct.
32. Seo S. H., K. Yim, I. You, Mobile Malware Threats and Defenses for Homeland Security, ISBN 978-3-642-32498-7, Springer Berlin Heidelberg.
33. Leung A., Y. Sheng, H. Cruickshank, The security challenges for mobile ubiquitous services, Information security technical reports 12(2007) 162-171, Elsevier and Science Direct.
34. European Commission, "Opinion on Smart Devices." [Online]. Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation /files/2013/wp202_en.pdf.