Mobile Computing Security: Issues and Requirements

Enaam Faihan Alotaibi and Adnan Mustafa AlBar
Department of Information Systems, King Abdulaziz University, Jeddah, Saudi Arabia
Email: Enaam_almogati@yahoo.com, ambar@kau.edu.sa

Md. Rakibul Hoque
Department of Management Information Systems, University of Dhaka, Dhaka, Bangladesh
Email: rakibul@du.ac.bd

***Abstract*—In recent years the size of computing machines has decreased with more power of computing, which helped to develop the concept of mobile computing like laptops, PDAs, cell phones, data storage device, and other mobile devices. Most people begin acquisition these devices because of the nature and advantages such as easy of carrying and moving it from place to place. Although the wide spread and popularity of these devices, it has introduced new security threats which were not existing in the traditional computing, and it should be identified to protect the physical devices and the sensitive information of users. In this paper, we will highlight on some of the security issues related to mobile computing systems in order to avoid or reduce them, with addressing the security issues into two aspects: first is related to transmission of information over wireless networks, and the second is related to information residing on mobile devices. Finally, some security techniques and requirements are presented.**

***Index Terms*—mobile computing, security issues, security requirements**

I. Introduction

The rapid development of wireless technology in particular mobile computing technology, that's make its devices more popular and interesting by users these days.

The origination and the emergence of mobile computing have the latest evolution in the areas of computing and information systems. Although these technologies are updated every second, however, it is still as a target of hackers due to the spread of use it, that's led to many users of wireless and mobile technology handled with its applications with little concern of security [1]. Security area of mobile computing has received less attention by mobile users, because the traditional use and purpose of mobile devices is voice communications with little activity of mobile data. The first call of mobile telephone was in 1946 and until the first 60 years, there were available mobile data applications for a limited number of users and that's made security requirements is not important at this time [2]. But now there are thousands of mobile data applications which can access by many mobile users. This led to drive new revenues by mobile carriers, and the same time it's led to new security issues which cause damage to each mobile users and mobile carrier's revenue [3]. This paper consists of three parts: the first part will give an overview of mobile computing with a brief history of mobile computing evolution and comparing it with traditional computing, the second part will be about security and security issues in mobile computing, which divided in two parts: wireless issues and device issues, and the final part will about security requirements of mobile computing.

II. Mobile Computing

Mobile computing is abilities of a computing and communication where its devices are not restricted to a single place, depends on the presence of a suitable distributed systems infrastructure [4]. In simple, mobile computing it's all about portable and small computers with increase in computing power, or defined as computing capabilities which may be used while they are being moved [5]. There are many devices in mobile computing, some of them are laptops, personal digital assistants (PDAs) and mobile phones. This paper is concerned of mobile computing had to know a brief history of the development of this computing through a review of the emergence of some techniques that have a relationship of mobile computing as shown in Fig. 1. The first computing, namely abacus, was used in 500 B.C which may consider as a mobile computing, because abacus have a small size, it can be portable, and the calculating numbers are one part of computing [6]. In the 1800s the advent of electronics and it was the first mobile storage systems can be traced back in that period. The first computer was back in the mid-1900s, and then the concept of networks has appeared during the period 1960-1970, wired and then wireless [7]. In 1970-1980, it was the emergence and use of satellite, and then followed by use of cellular technologies in the period 1980-2000 [8].

Manuscript received June 9, 2015; revised November 15, 2015.

doi: 10.12720/jait.7.1.8-12

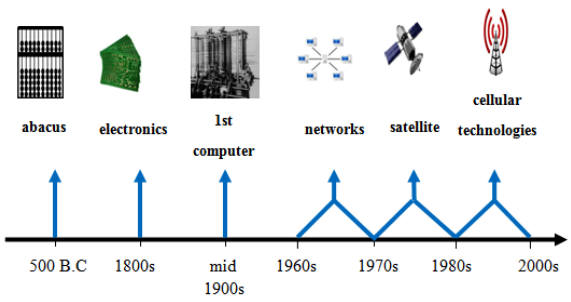

Figure 1. History of development of mobile computing

By comparing mobile computing with other traditional, it shown the most important characteristics of mobile computing which are wireless network connectivity, small size, the mobile nature of using, power sources used, and functions which are particular and needed to mobile users [9]. It also found that the main differences between mobile and traditional computing are the non-fixed positioning or mobility, and providing location transparency to the user. While in traditional computing, there's awareness of the remote physical location of the resources being used by user [10]. Most people are interested in mobile devices because of its features, like the portable that enables easy to carry it, attractive user interface which is characterized it, wireless that enables to easy access Internet, the transmission of voice and typical data, and so on [11]. Although of having many advantages in mobile devices or mobile computing, it has some of the drawbacks and the most serious drawback is a security issues, where it has introduced different new security challenges which were non-existent in the traditional computing.

III. Security

Security is an important consideration and it should be taken in all aspects of computing, especially in mobile computing because the mobile user may face many security threats that may be not exposed to the traditional computing user [12]. These threats include lose or stolen the private and sensitive data of mobile users that stored on their devices or it could be badly used by hackers and other threats. So it can define the threats of computing system as a situation that has the possibility to cause loss or damage to the system. A mobile computing defined as the capabilities of computing that rely on the existence of distributed systems infrastructure. So it can be considered the mobile computing as an extension of distributed systems, and it could be argued that there is a relation between security issues of mobile computing with other security issues of information systems [13]. Security principles or aspects of computer systems are related to confidentiality, integrity, availability, vulnerability, non-repudiation, authorization, and anonymity which is shown in Fig. 2.

Where the confidentiality is the detection of stored and transmitted data by authorized people, Integrity refers to modification, addition, and deletion of data only by those users who have authorized to access it, and the transmission of data is done by using cryptographic mechanisms [14]. Availability is an access of data or resource by only authorized users when needed or it is an ensuring that the system remains operate even with malicious code, a denial of service attacks may occur in this aspect [15]. Vulnerability is a general weakness in the security system and Non repudiation means the users cannot disavow about sending and receiving the message [16]. Authorization is giving different access to different types of users. Anonymity that all the identities information should be private for all users, and also the users can act with a pseudonym and without detection of their true identity [17]. According to the concepts of general security aspects, it can limit the major security threats of any computing system such as Interruption: if there is a lost or unavailable data in system, Modification: if an unauthorized people have tampers with data, Interception: if an unauthorized people have access to data and Fabrication: with an unauthorized people create things that were not found in system [18].

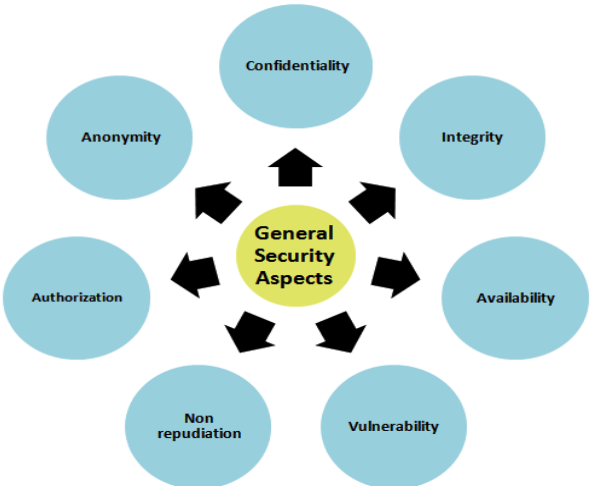

Figure 2. General security aspects

IV. Security Issues of Mobile Computing

The mobile computing is the communication between computing devices without a physical connection between them through wireless networks, which mean there are some of new mobile security issues that are originated from wireless security issues. The security issues and threats of mobile computing can be divided into two categories: security issues that related to transmission of information over wireless networks, and the issues that related to information and data residing on mobile devices [19].

A. Wireless Security Issues

The security issues that related of wireless networks are happened by intercepted of their radio signals by hacker, and by non-management of its network entirely by user because most of wireless networks are dependent on other private networks which managed by others, so the user has less control of security procedures. There are some of the main security issues of mobile computing, which introduced by using of wireless networks are:

Denial of Service (DOS) attacks: It's one of common attacks of all kinds of networks and specially in wireless network, which mean the prevent of users from using network services by sending large amounts of unneeded data or connection requests to the communication server by an attacker which cause slow network and therefore the users cannot benefit from the use of its service [20].

Traffic Analysis: It's identifying and monitoring the communicating between users through listening to traffic flowing in the wireless channel, in order to access to private information of users that can be badly used by attacker [21].

Eavesdropping: The attacker can be log on to the wireless network and get access to sensitive data, this happens if the wireless networks was not enough secure and also the information was not encrypted [22].

Session Interception and Messages Modification: Its interception the session and modify transmitted data in this session by the attacker through scenario which called: man-in-the-middle which inserts the attacker's host between sender and receiver host [23].

Spoofing: The attacker is impersonating an authorized account of another user to access sensitive data and unauthorized services [24].

Captured and Retransmitted Messages: Its can get some of network services to attacker by get unauthorized access through capture a total message and replay it with some modifications to the same destination or another [25].

B. Device Security Issues

Mobile devices are vulnerable to new types of security attacks and vulnerable to theft not because of the get these devices itself, but because of get to sensitive data that exist within its devices. This is also demonstrated by Data Breaches documents that published in 2008 by Privacy Rights International's that the 20% of security breaches related to data was due to mobile device losses [26]. Mobile computing, like any computer software may damage by malware such as Virus, Spyware and Trojan. A virus is a real part of malicious software and Spyware is gathering information about the user without his knowledge. Trojan is performing a desirable action but with malicious purpose [27]. Some of main new mobile computing security issues introduced by using mobile devices include:

Pull Attacks: Its control of the device as a source of data by an attacker which obtained data by device itself [10].

Push Attacks: It's creation a malicious code at mobile device by attacker and he may spread it to affect on other elements of the network [28].

Forced De-authentication: The attacker convinces the mobile end-point to drop its connection and reconnection to get new signal, then he inserts his device between a mobile device and the network [29].

Multi-protocol Communication: It is the ability of many mobile devices to operate using multiple protocols, e.g. a cellular provider's network protocol, most of the protocols have a security holes, which help the attacker to exploit this weakness and access to the device [30].

Mobility: The mobility of users and their data that would introduce security threats determined in the location of a user, so it must be replicate of user profiles at different locations to allow roaming via different places without any concern regarding access to personal and sensitive data in any place and at any time. But the repetition of sensitive data on different sites that increase of security threats [31].

Disconnections: When the mobile devices cross different places it occurs a frequent disconnections caused by external party [32].

V. Security Techniques and Requirement

There are a number of security requirements which valid with security issues relating to distributed systems, such as identification and authentication of trusted people by using authentication mechanisms like passwords, cryptographic techniques, access control by using information and rules of access control, information confidentiality by using mechanisms of confidentiality like encryption, information integrity by using integrity mechanisms those provide a verification of integrity checks and availability and prevention of denial of service [4]. That's security requirements which related to traditional computing, but with mobile computing the security requirements have become highly important, especially with regard to data security. One of the most important security measures is maintaining of the latest update of network or mobile elements and their software. There are different security requirements and techniques which valid for both mobile devices and networks, some of them include:

Encryptions: If there is an important information that stored in a mobile device, it should be encrypt this information to save it from unauthorized access by external party or in case if a mobile is stolen. It also contributes to the security aspects of confidentiality and integrity [33].

Standards: It should ensure that the mobile devices are protected and have a set of requirements like: locking, backups, antivirus software, and a strong password protection [34].

Network Access Control (NAC) solutions: This is a system used to check which mobile devices trying to connect to the network, that's provide protection of the network from any infections or malicious code that may damage of mobile devices [35].

Control Access: Control access to functions of mobile computing systems depending on the current location of the user, and there are already some security models which identifies some functions to certain user to use these functions [35].

Application Sandboxing: When creating mobile applications, it determined declarative permissions which will not be changed at runtime of application, these permissions can be improve to the security aspect of mobile devices by isolation and control of application from accessing to the system or interact with other applications that may be infected by malware code and virus, it also contributes to determine of resources that may be shared [36].

Memory Randomization: Memory Randomization or Address Space Layout Randomization (ASLR) which is also prevent malicious code or virus by locating the memory of application randomly, this has an important role in preventing malicious code or virus from knowing the specific memory location of the application or important memory which want to attack it [37].
Finally, some of the following steps that would increase the security aspects of mobile devices which are:

- Before downloading data or software, it should know the trust vendors who provide original version of software because there is some of unprotected software from external party.
- It should be aware of free applications that are popular but unofficial versions, because it may be an external party used the popularity of the original brand for nefarious purposes.
- It should be aware of public Wi-Fi risky which can be used by hackers to get sensitive information.
- It advised to make a note of the occasions when the user feels something is unusual was happening with regard to their mobile devices like delayed email and text message, and greatly diminished battery life.

VI. Discussion

We explained the security issues of mobile data in two different aspects of mobile environmental, namely: One aspect for the data stored within the mobile devices itself, and the second aspect of the data transmitted through the network between mobile units and mobile support stations. This division was as the result of a relationship of mobile computing with distributed computing, which is a mobile computing rely on the existence of distributed systems infrastructure with one of the most important components are wireless networks. It will be possible in the future work to study a third aspect of mobile security issues for the data transmitted between mobile units and each other. As regards to security requirements in fifth section of the paper, it can be linked with general security aspects that mentioned in the third section as follows: The encryption process contributes in each of the security aspects of confidentiality and integrity. Standards support the concepts of confidentiality and level of vulnerability. Network Access Control (NAC) solutions enhance the concept of availability and authorization. Control access to functions depending on the current location would contribute to each confidentiality, availability, and authorization. Application Sandboxing supports the availability and level of vulnerability. Memory Randomization contributes of level of confidentiality. Each one of these requirements would be to reduce some types of mobile computing threats which are already mentioned in this paper as follows: Encryption is a security technique that can ensure sensitive data is encrypted and unreadable for non-authorized within both mobile and wireless network, so it helps to avoid these threats: Pull Attack, Spoofing, Captured and Retransmitted the Message, Eavesdropping and Traffic Analysis. Standards which contain some of the regular security requirements like antivirus programs and so on, these requirements would reduce both of Push Attack and Multi-protocol Communication threats. Network Access Control (NAC) is a system authentication that contains some of the anti-threat applications such as spyware detection and firewalls, so it helps in reducing the following mobile threats: Denial of Service, Session Interception and Message Modification, Traffic Analysis, Forced De-authentication and Eavesdropping. Control Access is another security technique that uses the current location of the user to organize the accessibility of the mobile functions, thus it can be used to avoid Mobility and Disconnection threats. Application Sandboxing is usually used with unverified applications that may contain a malicious code or virus, which would help in reducing of Push Attack. Memory Randomization, or (ASLR) is a technique used to help prevent attackers from guessing the target address in the memory of a mobile device, so it will be useful to reduce both of Push Attack and Pull Attack. And those requirements can be evaluated in future work.

VII. Conclusion

The emergence of mobile computing has latest evolution in the areas of computing and information systems. Because of the popularity of its devices and of many available mobile data applications have introduced a new security issues which cause damage to mobile users. A brief history of the evolution of mobile computing technologies was reviewed; where it found that the first call phone of mobile was made in 1946. The prevalent different aspects of mobile computing with other computing are: wireless network connectivity, small size, the mobile nature of using, power sources used, and functions which are particular and needed for mobile users. Security aspects of computer systems are: confidentiality, integrity, availability, vulnerability, non-repudiation, authorization, and anonymity. The major security threats of a computing are: interruption, modification, interception and fabrication. While there are two parts of security issues related to mobile computing, which are: issues that related to wireless, networks, and communication system with information transmitted on these medians, and the other issues that related to mobile devices with the data and information residing it. Then have been reviewing some of the security requirements for mobile computing, which included: Encryptions, Standards, Network Access Control, Control access to functions depending on location of user, Application Sandboxing, and Memory Randomization, with some of the steps that are recommended to follow them to increase security aspects of mobile computing in end of the paper.

Acknowledgment

The authors would thank the reviewers for their suggestions and insightful comments.

References

[1] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf, "Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices," in *Proc. 2011 IEEE Symposium on Security and Privacy*, May, 2011, pp. 96-111.

[2] A. Gangula, S. Ansari, and M. Gondhalekar, "Survey on mobile computing security," in *Proc. 2013 European IEEE. Conference on Modelling Symposium*, November 2013, pp. 536-542.
[3] J. Korhonen, T. Savolainen, and J. Soininen, *Deploying IPv6 in 3GPP Networks: Evolving Mobile Broadband from 2G to LTE and Beyond*, John Wiley & Sons. E, 2013.
[4] I. Mavridis and G. Pangalos, "Security issues in a mobile computing paradigm," *Communications and Multimedia Security*, Springer. E, vol. 3, p. 61, August, 1997.
[5] J. York and P. C. Pendharkar, "Human–computer interaction issues for mobile computing in a variable work context," *International Journal of Human-Computer Studies*, vol. 60, no. 5, pp. 771-797, 2004.
[6] R. B'far, *Mobile Computing Principles: Designing and Developing Mobile Applications with UML and XML*, Cambridge University Press. L, 2004.
[7] M. Castells, *The Rise of the Network Society: The Information Age: Economy, Society, and Culture*, vol. 1, John Wiley & Sons, 2001.
[8] R. Malladi and D. P. Agrawal, "Current and future applications of mobile and wireless networks," *Communications of the ACM*, vol. 45, no. 10, pp. 144-146, 2002.
[9] M. Satyanarayanan, "Fundamental challenges in mobile computing," in *Proc. the Fifteenth Annual ACM Symposium on Principles of Distributed Computing*, May 1996, pp. 1-7.
[10] M. I. Ladan. (2013). Mobile Computing: Security Issues. [Online]. Available: http://weblidi.info.unlp.edu.ar/ WorldComp2013-Mirror/p2013/ICW7143.pdf
[11] E. Newcomb, T. Pashley, and J. Stasko, "Mobile computing in the retail arena," in *Proc. the SIGCHI Conference on Human Factors in Computing Systems*, April 2003, pp. 337-344.
[12] R. A. Botha, S. M. Furnell, and N. L. Clarke, "From desktop to mobile: Examining the security experience," *Computers & Security*, vol. 28, no. 3, pp. 130-137, 2009.
[13] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," *Wireless Communications*, vol. 11, no. 1, pp. 38-47, 2004.
[14] B. Bakmaz, M. Bakmaz, and Z. Bojkovic, "Security aspects in future mobile networks," in *Proc. 15th International Conference on Systems, Signals and Image Processing*, June 2008, pp. 479-482.
[15] M. Cremonini, E. Damiani, S. C. di Vimercati, P. Samarati, A. Corallo, and G. Elia, "Security, privacy, and trust in mobile systems," *Encyclopedia of E-Commerce, E-Government, and Mobile Commerce, Hershey: Idea Group Reference*, pp. 973-978, June 2006.
[16] R. Sheikh, M. S. Chande, and D. K. Mishra, "Security issues in MANET: A review," in *Proc. 2010 Seventh International IEEE Conference on Wireless and Optical Communications Networks*, September 2010, pp. 1-4.
[17] I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong, "Freenet: A distributed anonymous information storage and retrieval system," *Designing Privacy Enhancing Technologies*, Springer Berlin Heidelberg, January 2001, pp. 46-66.
[18] J. Li, M. N. Krohn, D. Mazieres, and D. Shasha, "Secure untrusted data repository (SUNDR)," *OSDI*, vol. 4, p. 9, December, 2004.
[19] I. Stojmenovic, I. (Ed.). *Handbook of Wireless Networks and Mobile Computing*, vol. 27, John Wiley & Sons, 2003.
[20] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," *USENIX Security*, pp. 15-28, August 2003.
[21] T. S. Sobh, "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art," *Computer Standards & Interfaces*, vol. 28, no. 6, pp. 670-694, 2006.
[22] A. Beach, M. Gartrell, and R. Han, "Solutions to security and privacy issues in mobile social networking," in *Proc. IEEE International Conference on Computational Science and Engineering*, vol. 4, August 2009, pp. 1036-1042.
[23] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, S. Ehlert, and D. Sisalem, "Survey of security vulnerabilities in session initiation protocol," *IEEE Communications Surveys and Tutorials*, vol. 8, no. 1-4, pp. 68-81, 2006.
[24] S. A. Schuckers, "Spoofing and anti-spoofing measures," *Information Security Technical Report*, vol. 7, no. 4, pp. 56-62, 2002.
[25] W. Stallings, *Network Security Essentials: Applications and Standards*, Pearson Education India, 2007.
[26] S. J. Cereola and R. J. Cereola, "Breach of data at TJX: An instructional case used to study COSO and COBIT, with a focus on computer controls, data security, and privacy legislation," *Issues in Accounting Education*, vol. 26, no. 3, pp. 521-545.
[27] S. Ramu, "Mobile malware evolution, detection and defense," *EECE 571B, Term Survey Paper*, 2006.
[28] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2, pp. 293-315, 2003.
[29] J. J. V. Rensburg and B. Irwin, "Wireless security tools," *Computer Science*, vol. 83, no. 944, p. 3924, 2006.
[30] T. Hardjono and J. Seberry, I*nformation Security Issues in Mobile Computing*, University of Wollongong, Australia, 1995.
[31] M. Decker, "A security model for mobile processes," in *Proc. 7th International IEEE Conference on Mobile Business*, July 2008, pp. 211-220.
[32] G. H. Forman and J. Zahorjan, "The challenges of mobile computing," *Computer*, vol. 27, no. 4, pp. 38-47, 1994.
[33] F. M. Heikkila, "Encryption: Security considerations for portable media devices," *IEEE Security & Privacy*, vol. 5, no. 4, pp. 0022-27, 2007.
[34] S. Schwiderski-Grosche and H. Knospe, "Secure mobile commerce," *Electronics & Communication Engineering Journal*, *vol. 14, no. 5*, pp. 228-238, 2002.
[35] J. Friedman and D. V. Hoffman, "Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses," *Information, Knowledge, Systems Management*, vol. 7, no. 1, pp. 159-180, 2008.
[36] H. Dwivedi, *Mobile Application Security*, Tata McGraw-Hill Education, 2010.
[37] G. Chang, C. Tan, G. Li, and C. Zhu, "Developing mobile applications on the android platform," *Mobile Multimedia Processing*, Springer Berlin Heidelberg, 2010, pp. 264-286.

Enaam F. Alotaibi received a Bachelor's degree in Computer Sciences from the faculty of Computers and Information Systems of Umm Al-Qura University, Saudi Arabia in 2013. Currently she is a Master student in Computing Information Systems from the faculty of Computers and Information Technology of King Abdul Aziz University in Saudi Arabia. Her research interests are in Information Systems Analysis and Design.

Dr. Adnan Mustafa AlBar is an Assistant Professor at the Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Saudi Arabia. He is an active member of the department where he was a member of the committee who prepared the Executive master degree and also participate in reviewing the IS PhD program. He teaches courses related to enterprise systems, ERP and BPM. He was the first IS department chairman, and the first Vice Dean for Development of Student Affairs. Dr. Albar is a member of the SAP international advisory board for academia. He is the founder and managing director of IT Expert House where he leads a team of consultants to provide consultation for the private sectors. Dr. Adnan is a senior member of IEEE, a member of ACM and ISACA. His main research is in enterprise information systems, enterprise architecture, business process management and technology adoption at the organizational level.

Md. Rakibul Hoque is an Assistant Professor of Management Information Systems at the University of Dhaka, Bangladesh. His research interests include technology adoption, Big Data, e-Health and ICT4D. Mr. Hoque has published a number of research articles in peer-reviewed academic journals, and has presented papers in international conferences. He had the opportunity to work in a number of research projects in Bangladesh, China, Australia and Saudi Arabia. He is a member of the Association for Information Systems (AIS), UNESCO Open Educational Resources Community, IEEE, Internet Society and ISACA. He is currently pursuing his PhD at Huazhong University of Science and Technology, China.