International Journal of Research in Advent Technology, Vol.2, No.5, May 2014
E-ISSN: 2321-9637

A Study on the Security of Mobile Devices, Network and Communication

Umair Rasheed[1], Aized Amin Soofi[2], M.Umer Sarwar[3], M. Irfan Khan[4]
[1,2,3,4] *College of Computer Science and Information Studies, Government College University Faisalabad, Pakistan*
Email: umair514@gmail.com[1], aizedamin@yahoo.com[2]

Abstract- The mobile revolution is bringing a remarkable and fundamental change in the world. More and more users and businesses use smart phones not only as a communication media but also as a means of planning and managing their work and private life. Mobile devices are expected to access different networks; hence many sensitivity data are stored in them. The security of information and applications about mobile devices becomes a difficult problem. Despite of many benefits of using this technology it suffers with some security threats. These threats exploit security flaws related to smart phones that can come by means of communication like SMS, MMS and WiFi networks. There is a need to gain the trust of users by eliminating the possible vulnerabilities in this technology. In this paper an attempt is made to provide detailed view of security issues in mobile devices, network and communication. Some of the existing security measures or solutions are also discussed in this work.

Index Terms- Mobile devices, Mobile communication, Mobile network, Communication security

1. INTRODUCTION

With the passage of time a number of mobile communication systems have been deployed and several service providers and equipment vendors are bringing to market a secure stream of new innovations. The next age group of open operating systems would not be on desktops or mainframes but on the small mobile devices we carry every day. New technologies provide information about design specifications and the physical properties that define the abilities and limitations of mobile communication networks [1]. Advanced computing and electronic technologies in mobile device, communication and networks are the need of time. The advancement of these technologies arises various security aspects.

In [2] a survey on note-book, laptop, tablet, and cell phone use is conducted. According to obtained results nearly 63% of employees make use of their mobile phones for business as well as personal use. This survey also reveals the fact that most mobile devices including Blackberries were accepted and organized by IT company employees. So, the security issues with mobile devices should be taken seriously to avoid any kind of problems in near future. In [3] major mobile security concerns are highlighted which include; storage of sensitive information, authorization techniques, usability, network availability and application environment. Computing and electronics have gone mobile without us changing our security approach [3].

The issues like management of assets which are stored in mobile devices, communicate in trusted and non-trusted environments and secure interaction must be strongly protected [4]. The application scope of mobile devices is increasing day by day which creates new challenges for information and security. Therefore, how to protect the security of information and applications about mobile devices becomes an exigent problem [5]. The growth of mobile computing network is leading to new security challenges [6]. In figure 1 some of the important security risks associated with mobile devices are presented.

One of the major concerns in computing environment is security especially in the context of wireless communication [7].Implementation of communication security on mobile networks can be both harder and easier. Communication between mobile and fixed network create particular problem regarding security protocol design [1]. The rapid growth and development of the mobile systems over the past years has showing the potential and effective availability of mobile communication [8]. There is a strong call for advanced and efficient security mechanism for mobile data network technologies [8]. The new technologies to access mobile networks are developing rapidly and will be much mingled. These technologies raised new security issues to all network layers [9].

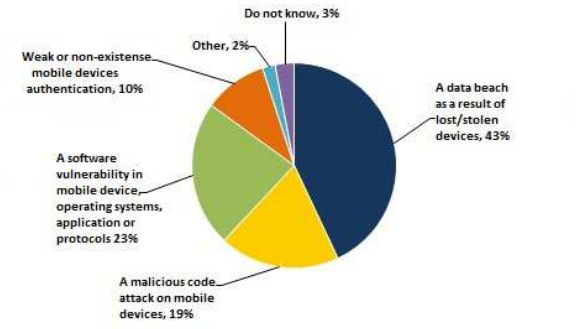

Fig. 1. Biggest Security Risk Associated with Mobile Devices [15]

2. METHODOLOGY

The selection criteria through which we evaluated study sources is based on the research experience of the authors and in order to select these sources we have considered certain limitation: studies included in the selected sources must be related to our problem and these sources must be web-available.

The review protocol is developed by using keywords; mobile devices, mobile communication, mobile networks, communication security and the following list of sources has been considered to conduct the systematic review: IEEE, Elsevier Ltd, Springer and IT Professional Magazine.

Another step in the search process is performed by searching the related work area of the selected papers to improve the review potency by confirming that no helpful reference is fails to notice during the explore process. Once the sources had been defined, it was necessary to describe the process and the criteria for study selection and evaluation.

The inclusion criterion for this study is strictly limited to studies that contain security issues regarding to mobile devices, communication, networks and is relevant for further development of these security issues.

3. SECURITY ISSUES IN MOBILE DEVICES

Mobile devices should be given serious consideration because issue of security act as an obstacle in the development of mobile services. Every security issue needs to be addressed at the very outset of the service development process. The main mobile security threats for the developers of mobile services include the complexity of technical solutions, illegal copying of programs and content and threats provided by the Internet.

In [3] the security issues of mobile devices such as Laptop and PC are focused. Today Laptops are the main personal computing instrument which implies that all information both business and personal is stored in them. The security threats related to secret information in mobile devices can be decreased by encrypting the information stored on the laptop's hard drive and by the usage of removable or storage devices such as USB or Bluetooth disk. Encryption of the USB disk can be mandated in some situations but it often makes the disk unusable since its main purpose is to transfer data from one device to another and encryption prevents that. Technology and security solutions will catch up but for the moment the biggest burden unfortunately remains not just on the security managers but also on the final users.

In [4] point is raised that the scenario of laptop security is changed by the huge number of distribution of laptops and wireless communication. Lost and theft of the laptops are also increasing, if this happens means the lost of your personal data or information. The growth of the mobile internet and the use of new mobile technologies (e.g. mobile devices, mobile and wireless communication) are also pointed in this paper.

In [4] it is explained that technological advances as well as the increased number of mobile applications drive a change in mobile end-user equipment. These advance technologies arise many security issues which include: (1) secure management of assets stored in the mobile devices, (2) secure communication within trusted and non-trusted environments (including privacy issues) and (3) secure interaction with critical IT infrastructures.

The increase in application scope of mobile devices creates new challenges for information security. In [5] secure verification and permission procedure for mobile devices was proposed. The proposed procedure employs biometric recognition and password mechanism that allow different users to access different information with different security levels. In general, information security is based on three basic security requests which include: information privacy, information integrity and information availability. To satisfy these security requests for mobile devices, three major problems should be solved which include: (1) the authorization for accessing resources in mobile devices. (2) Protect data and software stored in mobile devices. (3) Authentication among users, mobile equipments (MEs) and universal subscriber identity modules (USIMs).

In [5] secure authentication and authorization protocol was introduced for mobile devices shown in figure 2. The proposed protocol employs the mobile trusted module (MTM) and biometric identification. To achieve these security protocols the private

cryptography mechanism and public cryptography mechanism was introduced to ensure the security of mobile devices to be more secure and support mobile application.

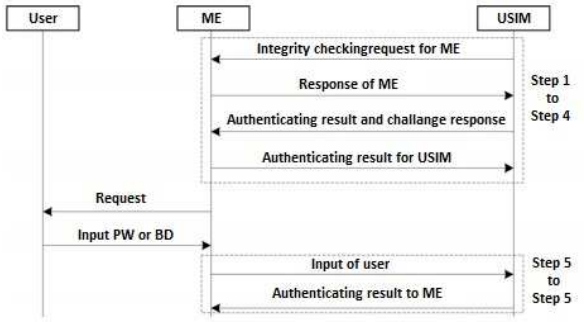

Fig. 2. Secure Authentication and Authorization protocol [5]

From step 1 to step 4 recognition of the integrity checking for ME and realization of mutual authentication between ME and USIM occurs. By the 4 steps, ME and USIM would decide if they have the same owner. This decision is important to access control for mobile device. Then in step 5 the user's passwords (PW) and biometric data (BD) are captured safely by ME and then ME creates the encryption message and delivers h(PW) or BD to USIM. If an application requires stronger security then ME sends BD otherwise ME sends h(PW). In step 6 USIM verifies the signature, and decrypts the received messages and compares the h(PW) or BD with stored PW or BC.

In [10] the present integration challenges facing the organization and workers using mobile devices are examined. Nowadays mobile workforce is using mobile tools for communication and computing. To stay in contact and continue their workflow while on the road many workers have turned to smart phone, personal digital assistances (PDAs), notebook computers and other portable devices that provide network and internet connectivity when these mobile workers want to access the enterprise application and database. While at home they want to upload information from their portable devices onto the company computers. These types of activities raise security as well as the integration concerns. According to industry observers the issue of security is important because the number of mobile workers is about to explode. Another challenge for organizations is synchronizing data between user's mobile devices, PCs and corporate networks.

Due to the usage of various kinds of mobile devices by more workers the management of the mobile devices on a large scale is very threatened. A key to successfully integrating remote access devices into the enterprise is developing simple and well defined user requirements. Business and employees must determine what kind of remote access is critical, which devices are best for which users and which business functions need remote-access support to optimize productivity. However, standardization can be easier said than done. Good IT planning and policies can make the effective workplace as productive as possible. The organizations should recommend their employees with that PDA and connectivity software which IT workers are familiar [10].

4. SECURITY ISSUES IN MOBILE NETWORK

Mobile networks are being driven by the need for providing network access to mobile or wandering devices. Although the need for wireless access to a network is evident and new problems are inherent in the wireless medium [11]. Wireless however does not imply mobility. There are wireless network in which both ends of communication are fixed such as in wireless local loops. Thus a study of wireless data networks has its own scope different from networking system in general [12]. In [8] strong need for advanced and efficient security mechanism for mobile data network technologies is discussed. This work also highlights the techniques for mobile data networks that aims to exhibit their potential of integrity, availability and confidentiality are discussed.

As compared to wired networks, wireless networks introduce new opportunities for the users. With the emerging of portable wireless devices, mobile networks are becoming an important part of our everyday networking facilities. The rapid growth of mobile networks leads us to new security challenges. Wireless security networks have various development and implementation stages. Such as 1G system which is not very secure and protective. This follows the 2G systems (GSM) gives user authentication and data confidentiality. Still this system lacked mutual authentication and protection in the core of network of the cellular system. Now 3G systems introduce with the capabilities of speech and data services on high data rates [8]. Some solutions are also provided in [8] to the security issues in GSM, UMTS, CDPD, ATM and VPN.

In mobile cellular networks paging effects contain significant security issues [16]. Paging attacks could be very destructive on the boundary of a mobile operator's network. Cellular networks usually consist of two ends i.e. internet access start and subscribers attach to a 3G network. Mobile operators can take most of the preventive actions on these end points. In [16] some attacks to derive the vulnerabilities in GSM network components due to paging are performed to examine the effects of these attacks.

In [6] issues regarding to the attacks on mobile network are discussed. In which some requirements are proposed for the security of mobile network that include: (1) Confidentiality, the information sent has to be unreadable to unauthorized users. (2) Authentication, able to restrict unauthorized users and identify a node or a user. (3) Integrity, protect the sent message being modified or deleted by attackers. (4) Non-repudiation insured that if an entity sends a message, the entity cannot refute that the message was sent by it. (5) Access control prevent unauthorized user from getting access to the network.

Access control prevents unauthorized users from getting access to the network. Mobile networks are in fact more weak to malicious attacks then fixed networks. Such as the nature of broadcast medium which expose information to passive listeners, the limited battery supply and the mobility. Wireless networks can be easily attacked actively and passively. Passive attack means an attacker does not actively as a spy that identifies loop holes of the network. Active attacks refers that attacker can disperse various topology information, drop or modify transmission packets, fabricate false messages or flood the existing network [6].

According to [6] The advancement of attacking techniques such as nesses scanner, internet security systems (ISS), internet scanner, COPS security checker and N-Stealth results increasing number of various attacks on mobile network. Bluetooth and Ad-Hoc network are very commonly attacked by viruses. There are different types of mobile viruses which attack Bluetooth connectivity and cause a huge damage. These viruses can make your mobile devices unusable generate unwanted messages can disclose your private data and easily steal your sensitive information. In MANET the attack commonly occurs during routing at the network layer or link layers.

5. SECURITY ISSUES IN MOBILE COMMUNICATION

Wireless devices such as mobile phones, PDAs and pagers are less secure than their wired counterparts. This is because of bandwidth, memory and processing capabilities. The other reason is that interruption of the data which is send into the air [14].

In [7] it is stated that establishment of secure wireless communication channels is one of the major requirements in PCs. Some of the important issues, which need attention in designing security scheme for mobile communication such as autonomy of communicating entities, mobility of the users and restriction of hardware. The described scheme provides authentication of the communicating entities, location privacy and secure messaging. They develop mobile computing environment by adopting personal communication scheme (PCS) model. The term workstation used for static computers and term walk station used for mobile computers.

In [7] the term base station is used for some special network devices which have wired and wireless networking functionality. With help of this mobile computing environment the security scheme was designed that scales from indoor wireless LAN's to the PCS infrastructure. In this type of environments, authentication and privacy of communication are two major requirements. The proposed security scheme had four goals. (1) The walk station and the base station must be able to authenticate each other. (2) Once authenticated, the walk station and base station should be able to communicate securely. (3) Walk station should be provided location privacy. (4) The security scheme should be efficient and optional.

In [1] some of the difficulties that system architects faced and some of advantages that mobile networks offer during designing security solutions for mobile communication are discussed. Over the last few years number of mobile communication systems has been developed and numerous service providers and equipment vendors are bringing a steady stream of new innovations. The lack of security and a high level of fraud are seen at conventional e-commerce. Due to significant efforts security of e-commerce is developing. Unfortunately, communication security alone is not enough. Ensuring system security at both the client and the sever end must not be ignored.

In [1] the security threats on the client side were also discussed which include poor platform integrity, the hidden user interface and the huge number of default Certificate Authority (CA) certificate. As well as on the server side almost all reported hacker attacks are targeted against server. Communication security is often described in terms of confidentiality (privacy), integrity (accuracy and consistency), authentication (validation) and non-repudiation of transmitted data.

In [1] a technique was proposed to keep the confidentiality of transmitted data by encrypting the information flow between the communication parties and the encryption can take end-to-end between the communication parties or alternatively on separate legs in the communication path. Authentication of transmitted data is an asymmetric service. The available types of authentication will depend on the security protocol used.

In [1] an issue regarding to non-repudiation was also highlighted. Non-repudiation is similar to authentication; it is an asymmetric security service. Digital signature is the mechanism used for non-

repudiation. Different parties will have different interests regarding authentication and non-repudiation services. Public key cryptography is the basis of several important security services. A PKI refers to an infrastructure for distributing public keys where the authenticity of public keys is certified by Certification Authority (CA).

The network architecture and the security goal together indicate the most appropriate protocol layer where a security service is to be located. They also focus that users receive less security information. If the security is totally hidden from the user he or she would not be able to tell whether it is working the way it was projected and as a result this could allow successful attacks to remain undetected. All this is very fascinating from functionality and flexibility point of view but it causes a formidable threat to the integrity of the client machine [1].

5.1. *Security Issues in Mobile WiMAX (IEEE802.16e)*

The IEEE802.16e is the commonly known as WiMAX. This technology offers broadband wireless access over last mile as an alternative to cable and DSL. Most of the companies are deploying WiMAX to provide mobile broadband. In [13] security issues in mobile WiMAX were highlighted in which IEEE802.16e mobile WiMAX standard with mobility support were discussed. Several potential security threats and vulnerabilities were also pointed and some possible security improvements and solution to abolish these weaknesses were proposed.

In [13] challenges related to the growth of wireless network were discussed. It is important to understand the full range of problems that security systems need to address. These needs are confidentiality, integrity and authentication. The Virtual Private Networks (VPNs), Internet Protocol Security (IPSec), Intrusion Detection System (IDS) and firewall are examples among various security mechanisms that have been proposed to address security issues in wired networks. WiMAX as a new technology seems not to have fully solved the security flaws of wireless LAN. Confidentiality, in wireless networks is a primary concern for a safe transmission. To negotiate authentication mechanisms or protocols many attacks can be launched. We have two main attacks, Message Reply Attach and The Man in The Middle Attack (MITMA).

WiMAX also introduces a service for multicast and broadcast communications to enable the BS (Base Station) to distribute data simultaneously to multiple MSs (Mobile Subscribers) and it uses a common group traffic-encryption key for secure broadcast communication. Most of the management messages defined in IEEE802.16e are integrity protected. However some messages are not covered by any authentication mechanism, this shows some weaknesses. The neighbor advertisement message is also not authenticated. The downlink burst profile change request message to unicast message with no integrity protection, for the ranging request message the standard does not unambiguously defined when an authentication absorb shall be appended [13].

In [13] hash based message authentication code (HMAC) or Cipher based message authentication code (CMAC) technique was proposed in which non authenticated management messages sent on the primary or basic management connection for authentication purpose To protect the management traffic from being read by a competitor all management communication should be encrypted. This can be done when both side established a common key.

5.2. *Security Challenges in the Mobile Internet*

In [9] the security challenges in the mobile internet were discussed. The key objectives were to analyze the security problems to develop appropriate secure solutions related to all layers to implement sample prototype solutions and finally to stimulate the standardization process.

We can find a lot of information on the internet, such as information from companies, research institute or governmental organizations. Along with this useful information some of the information must be considered garbage. The problem is that it is hard for the user to know which information he can trust even when he knows an institution as trustworthy, since the information (or the website) might be forged.

Protocol e.g. IPSec or SSL/TLS and some layer 2 protocol like 802.11 and Bluetooth include securities which are known and standardized. But to handle public key information in a very large scale with many communication channels is still very difficult. Rapid changes of the network topology make the job even harder. It is also unclear how security mechanisms for communication like IPSec cooperate with mobile IP and firewalls [9].

Due to the increasing computation capabilities of PCs and workstations efficient cryptographic algorithms in low power environments as they are often found in Ad hoc networks remain unsolved and present. It is too complicated to use security mechanisms; people invent tricks like writing passwords into their address book under “s” like secret. Many people are just frustrated because of the amount of passwords and PINs they have to remember [9].

6. CONCLUSION

In this study different articles and conferences reviewed in order to provide detail view of security challenges in mobile devices, networks and communication. It is found that security of mobile devices is very serious issue. This area needs proper attention of the researchers to overcome the security issues in this domain. None of the work fully solves the whole problem, because of the poor interface of mobile devices, development in mobile networks and the latest technologies in mobile communication. In future these mobile devices access different networks. Therefore, how to achieve new security challenges is a thinkable question. Further research is needed in order to face the security challenges in mobile environment and it should be given serious consideration because their security risk poses an obstacle for users.

REFERENCES

[1] Jøsang, A., & Sanderud, G. (2003). Security in mobile communications: challenges and opportunities. Paper presented at the Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003- Volume 21.

[2] Siddartha (2012). Security Issues with your Mobile Devices. Retrieved March 15 2014 from http://www.gadgetcage.org/security-issues-with-your-mobile-devices/26991/

[3] Pasquinucci, A. (2009). The security challenges of mobile devices. Computer Fraud & Security, 2009(3), 16-18.

[4] Eckert, C. (2005). Security issues of mobile devices Security in Pervasive Computing (pp.163-163): Springer.

[5] Wang, J., & Jiang, N. (2009). Secure authentication and authorization scheme for mobile devices. Paper presented at the Communications Technology and Applications, 2009. ICCTA'09. IEEE International Conference on.

[6] Sudin, S., Tretiakov, A., Ali, R., & Rusli, M. E. (2008). Attacks on mobile networks: An overview of new security challenge. Paper presented at the Proc. Int. Conf. Electron. Design.

[7] Bharghavan, V., & Ramamoorthy, C. (1995). Security issues in mobile communications. Paper presented at the Autonomous Decentralized Systems, 1995. Proceedings. ISADS 95., Second International Symposium on.

[8] Nayak, D., & Rajendran, N., Phatak, D., & Gulati, V. (2004). Security issues in mobile data networks. Paper presented at the Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th.Conference 2004. VTC2004-Fall. IEEE 60th, pp. 3229-3233, 2004.

[9] Bernd, L., Dirk, W., (2002). Security Challenges in the future mobile Internet: Workshop on Requirements for Mobile Privacy & Security", Presented in NEC Network Laboratories.

[10] Goth, G. (1999). Mobile devices present integration challenges. IT professional, 1(3), 11-15.

[11] Ashley, P., Hinton, H., & Vandenwauver, M. (2001). Wired versus wireless security: The Internet, WAP and iMode for e-commerce. Paper presented at the Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual.

[12] Ahmad, A. (2005). Wireless and Mobile Data Networks: Wiley.

[13] Ibikunle, F. A. (2009). Notice of Violation of IEEE Publication Principles Security Issues in Mobile WiMAX (802.16 e). Paper presented at the Mobile WiMAX Symposium, 2009. MWS'09. IEEE.

[14] Nichols, R. K., & Lekkas, P. C. (2002). Wireless security: McGraw-Hill New York.

[15] ESG (2010), Data Breach Incidents Represent the Biggest Security Risk Associated with Mobile Devices, ESG Isights and Publications, http://www.esg-global.com/blogs/data- points-and-truths/data-breach-incidents-represent-the-biggest-security-risk-associated-with-mobile-devices.

[16] Oğul, M., & Baktır, S. (2013). Practical Attacks on Mobile Cellular Networks and Possible Countermeasures. Future Internet, 5(4), 474-489.