Survey on Security Systems for Mobile Network

Lokesh Giripunje [1], Sonali Nimbhorkar [2]

[1]Student (ME), Department of Computer Science and Engineering
G.H.Raisoni College of Engineering
Nagpur, India
lokeshgiripunje@gmail.com

[2]Assistant Professor, Department of Computer Science and Engineering
G.H.Raisoni College of Engineering
Nagpur, India
sonali.nimbhorkar@raisoni.net

Abstract: ***21st century have witnessed an explosive growth in the use of mobile devices as the enabling technology for accessing Internet based services, as well as for personal communication needs in networking environments. Security issues mobile device directly questions credibility of applications and services. Currently available network security mechanisms are inadequate, since there is a greater demand to provide a more flexible, reconfigurable, and scalable security mechanism. Hence, mobile security is no longer inherent, but of vital importance. Security model that adapt to the various capabilities and security requirements of a mobile system is necessary. This analysis paper provides a brief overview of mobile network security.***

Keywords: mobile network security, comprehensive, scalable, security requirements.

1. Introduction

Nowadays, handheld devices (i.e., cellular phones and PDAs) with many mobile applications, such as wireless internet services, mobile access services and mobile e-commerce are popularly and widely used by people in many fields of our society. Smartphone epoch can be seen as beginning with the new millenary. Since then, numerous new "smart" devices like Blackberries, iPhones and, recently, Android-based phones have been introduced that revolutionized the market. Overview of global sales figures and market share for mobile operating systems for third quarter of 2009 and 2010 shows that Android is clearly market leader [1].

Today world is changing from the Internet world to a mobile world where more and more access to information is done by previously dumb phones. In an interconnected mobile world, the interactions among mobile devices, systems, and people are growing rapidly [2].

Now internet can be access through the mobile phone, this leads in interest of service providers to provide various internet services. Mobile phones can be connected to networks conveniently at anytime or anywhere and the data transfer speed becomes higher and higher as the wireless communication technology is developing rapidly.

At the same time people are more and more concerned about the security issues and fast transmission of sensitive digital information over wireless channels. The security issues include issues such as the quick spread of viruses and malicious of software. According to F-Secure [3], there are more than 200 mobile viruses or malware programs are causing problems to the system. Also low computational power is a major issue in mobile system. Many organizations are increasingly interested in deploying mobile application to enhance productivity and enable new capabilities [7].

The rest of the paper is structured as follows. Section 2 describes background notions on wireless and networking technologies In Section 3 we present an attacker-centric threat model for mobile platforms, followed by description of basic cryptographic concepts in Section 4.Various Security models available for mobile system are presented in Section 5. Section 6 concludes the paper.

2. Mobile Technologies

Polla et. al. in [6] provides some background notions on wireless and networking technologies that, even if not originally created for a mobile environment, but favored Smartphone environment as well.

2.1 Wireless Telecommunication Technologies

The most important wireless technologies targeted at mobile communications are GSM, GPRS, EDGE and UMTS.

2.1.1 GSM: Global System for Mobile communications (GSM) is the first and most popular standard in Europe for mobile telecommunication system and is part of the second-generation (2G) wireless telephone technology. Developed in 1990 by Group Special Mobile, a group created in 1982. GSM provides data transmission, digital fax, e-mail, call forwarding, teleconferencing service and Short Message Service (SMS).

2.1.2 GPRS and EDGE: General Packet Radio Service (GPRS), also referred as 2.5G network, provides higher transmission rates and lower access time compared with previous GSM standard. GPRS uses packet switching mechanism for data exchange replacing circuit switching in 2G systems. Wireless Application Protocol (WAP) and Multimedia Messaging Service (MMS) is also supported by GPRS. Enhanced Data rates for GSM Evolution (EDGE) improve the features offered by GPRS by supporting higher data rate and higher reliability. EDGE also referred as 2.75G [6].

2.1.3 UMTS: The Universal Mobile Telecommunications System (UMTS) was introduced in Europe in 2002. This standard represents the third-generation (3G) on cellular system. The transmission rate is higher than 2G and 2.5G by providing a transmission speed up to 2Mbps. Circuit switching connections are supported simultaneously with packet switching connections [17].

2.2 Networking Technologies

Popularity of Wireless Local Area Network (WLAN) increased drastically in recent years using these technology devices can be connected to network or other device the most popular WLAN standards are Bluetooth and IEEE 802.11[6].

2.2.1 Bluetooth: Bluetooth is a standard that enables devices to exchange data over a small area (1-100 meters) through short wavelength radio transmissions. Bluetooth is a personal networking technology that enables the creation of Personal Area Networks with high levels of security.

2.2.2 Wireless LAN IEEE 802.11: Wireless LAN IEEE 802.11 family includes several protocols for communicating at different frequencies (2.4, 3.6 and 5 GHz). These standards can be used in two operation mode:

1) In the infrastructure mode,
2) In the infrastructure-less mode (adhoc mode)

The most popular protocols included in this standard are defined by the 802.11b and 802.11g protocols.

3. Threat Model for Mobile Platforms

Delac et. al. in [4] present an attacker-centric threat model for mobile platforms. The threat model provides a broad overview of challenges in mobile devices security and is divided into three sections: attack goals, attack vectors and mobile malware.

3.1 Attack Goals:

Three basic motives for breaching mobile device's security are

3.1.1 Collect Private Data: Mobile devices are used to store private and personal data, and hence they are becoming attractive target for attackers.

3.1.2 Utilize Computing Resources: The increase in computing resources is setting mobile devices into focus for malicious exploits.

3.1.3 Harmful Malicious Actions*:* Harmful malicious actions create discomfort for device user. These attacks can be easily identified, but cause damage. The attack example includes data loss, draining devices battery and generating huge network traffic.

3.2 Attack vectors: Attack vectors are classified into four categories: mobile network services, Internet access, Bluetooth, and access to USB and other peripheral devices [9].

3.2.1Mobile network services: The attacker can gain sensitive information from the user behaving as true entity, like a bank or insurance company using Cellular services like SMS, MMS and voice calls.

3.2.2 Internet access: Long lasting connection to the Internet using Wi-Fi networks or 3G/4G services provided by mobile network operators increases the chances of a successful malicious attack. The attack will be intense on public network over a Wi-Fi hotspot.

3.2.3 Bluetooth: Bluetooth is the easiest way to spread malicious contents from one device to other over a range.

3.2.4 USB and Other Peripherals: Synchronization of the mobile device with a personal computer via USB can lead to malware attack if the software used to synchronize the mobile device was compromised. Also attacker can access private information.

3.2.5 Message virus: SMS (Short Message Service) and MMS (Multimedia Message Service) are popular message service system and easiest virus spread based on phone number.

3.3 Mobile Malware: Security threats characteristic for PCs are migrating to mobile devices as operating system resembles. This subsection provides a brief overview of the most common mobile malware [6].

3.3.1Trojan horse: A malicious mobile application by which the attacker could gain control over the device.

3.3.2 Botnet: Botnet is a set of compromised devices which can be controlled and coordinated remotely.

3.3.3Worm: Worm is a self-replicating malicious application designed to spread autonomously to uninfected systems.

3.3.4Rootkit: Rootkit is a malicious application which masks its presence from the user by modifying standard operating system functions to run in a privileged mode.

4. Cryptographic Terminology

William Stallings [9] provide a detailed description of commonly employed security concepts and terminology. The concern for security in practice is addressed by choosing a security protocol, which achieves all the required security objectives. Security protocols realize the security objectives through the use of appropriate cryptographic algorithms.

Basic Security Terminologies used in cryptography are:

A message present in a clear form, which can be understood by any casual observer, is known as the plaintext. The encryption process converts the plaintext to a form that hides the meaning of the message from everyone except the valid communicating parties, and the result is known as the cipher text. Decryption is the inverse of encryption. The processes of encryption and decryption are controlled on a quantity known as the key, which is ideally known only to the valid users. Strength of a security scheme depends on the secrecy of the keys used [9].

A security protocol formally specifies a set of steps to be followed by communicating parties, so that the mutually desired security objectives are satisfied. The four main security objectives include:

1. Confidentiality: This means that the secrecy of the data being exchanged by the communicating parties is maintained, i.e., no one other than the legitimate parties should know the content of the data being exchanged.
2. Authentication: It should be possible for the receiver to ensure that the sender of the message is who he claims to be, and the message was sent by him.
3. Integrity: It provides a means for the receiver of a message to verify that the message was not altered in transit. It checks originality of message.
4. Non-repudiation: The sender of a message should not be able to falsely deny later that he sent the message, and this fact should be verifiable independently by an independent third-party without knowing too much about the content of the disputed message(s).

Security objectives thus provide trust on the Web. They are realized through the use of cryptographic algorithms which are divided into two categories depending on their characteristics. These categories are:

1. Symmetric algorithms: These algorithms use the same key for encryption and decryption. They rely on the concepts of "confusion and diffusion" to realize their cryptographic properties and are used mainly for confidentiality purposes.
2. Asymmetric algorithms: These algorithms use different keys, known as the public key and the private key, for encryption and decryption, respectively. They are constructed from the mathematical abstractions which are based on computationally intractable number-theoretic problems like integer factorization, discrete logarithm, etc.. They are primarily used for authentication and non-repudiation [9].

5. Secured Mobile Systems

This section describes various security models available for mobile systems.

5.1 J2ME CLDC Security Architecture

Debbabi et. al. in[15] presents high-level J2ME CLDC architecture and have difference between CLDC and MIDP as security concerns are distributed in between two.J2ME CLDC platform security model provides low-level security, application security, and end-to-end security.

5.2 Android Security Model

Android is an application execution platform for mobile devices comprised of an open source operating system, core libraries, development framework and basic applications.

The model is based on application isolation in a sandbox environment [16]. Each application assigned a unique Linux user ID executes in its own environment and is unable to influence or modify execution of any other application. Also applications cannot access files that belong to other applications without being granted appropriate permissions. Each file can be assigned read, write and execute access permission.

Additional security is achieved by utilizing memory management unit (MMU). The Android security model depends on reliability of applications from sources and application requests permissions for its intended operation.

5.3 iOS Security Model

iOS security model described in [4] differs with the Android security architecture. Every new application submitted is checked for its integrity and safety by professional developers. If found safe, then it is added to application store. iOS application might access local camera, 3G/4G, Wi-Fi or GPS module without asking user's unlike Android. Developers create secure applications using iOS secure APIs and prevents entry of malicious applications.

Secure networking functions can be carried out with the help CF Network API. The Security Server uses the Keychain Services API and the Certificate, Key, and Trust services API.

5.4 Public key cryptography based security systems:

The public key cryptography is majorly used as computation complexity is negligible but the key management is an issue. Wireless networks has the problem of eavesdropping, shared data over wireless networks.

In public-key systems cost of underlying mathematical operations is one of difficulties. However, with high computing power public-key systems can be implemented on mobile devices.

Dr. R. Shanmugalakshmi in [10] observed that ECC's provides high security; high speed in a low bandwidth with by smaller key size than RSA .This paper explains the use of ECC in the security development in the field of information security and for mobile devices with low computational power. Study in [11], suggest that ECC is a promising cryptosystem for the next generation and expected widespread use in devices with low computational power constrained environment. Hardware implemented ECC has less overhead than RSA.

A study in [12], is conducted and observed that the existing authentication protocols, based on RSA asymmetric cryptography are not suitable for such devices due to their confines in computing power, memory capacity, key sizes and cryptographic support. For that reason, ECC is replacing RSA in most applications. In [14] an efficient

authentication scheme using an elliptic-curve-cryptosystem is suggested for mobile terminal authentication. The scheme requires one scalar point multiplication operation and two short messages for key verification.

A study in [13] compared the performance four different popular secret key algorithms such as DES, 3DES, AES, and Blowfish. Encryption of input files of varying contents and sizes shows Blowfish is found to be best among other.
Selvi et. al. [5] proposes a secure authentication scheme which incurs high level of security and less time consumption by using Rabin Public-key Cryptosystem which is similar to RSA.

5.5 Comprehensive Security Service Systems for Mobile Network

Tao et. al in [8] provides comprehensive mobile network security system. This system solves the new security requirements. Reliable security services can protect the mobile terminals. SSP (Security Service Provider), SWP (Software Provider) and MTM (Mobile Trusted Module) are added to the existing WCDMA mobile system. This system provides overall security solution for the whole secure mobile activities, including the trusted start up, access authentication, integrity checking, software downloading and software running which is not provided by earlier discussed systems. Hence, comprehensive security system for mobile network is widely implemented in distributed network.

6. Conclusion

In this paper, the various mechanisms for secure computing environment for mobile network are described. The traditional virus detecting mechanism cannot meet the new security demands. Security requirements for mobile devices are entirely different from stationary machines. Most of the techniques available do not provide a complete security solution.

For complete security integration of more than one security systems, however the installation/maintenance cost of multiple systems, significantly adds to the high operational expense of these devices during their life-cycles. Trusted computing with public key cryptography provides comprehensive security service system for mobile network The trusted mechanism can ensure the system security of mobile terminal and provides security features such as the confidentiality, authenticity, integrity and non-repudiation.

References

[1] Gartner Research, “Gartner Says Worldwide Mobile Phone Sales Grew 35 Percent in Third Quarter 2010; Smartphone Sales Increased 96 Percent,” 2010, http://www.gartner.com/it/page.jsp?id=1466313

[2] Michael Becher, Felix C. Freiling,Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, and Christopher Wolf, “Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices,” 2011 IEEE Symposium on Security and Privacy, pp. 97–111, 2011.

[3] F-secure, “New Century in Mobile Malware,” F-secure, 2006. [Online]

[4] G. Delac, M. Silic and J. Krolo, “Emerging Security Threats for Mobile Platforms,” MIPRO 2011, May 2011.

[5] K.Saravana selvi, T.Vaishnavi, E.G.S.Pillay, “Rabin PublicKey Cryptosystem for Mobile Authentication,” IEEE-International Conference on Advances in Engineering, Science and Management (ICAESM - 2012) pp. 854-860, March 2012.

[6] Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra, “A Survey on Security for Mobile Devices”, IEEE Communications Surveys & Tutorials,1553-877X/12/ ,pp:1-26, 2011.

[7] Jim Luo, Myong Kang, “Risk Based Mobile Access Control (RiBMAC) Policy Framework,” The 2011 Military Communications Conference - Track 3 - Cyber Security and Network Operations, pp. 1448-1453, 2011.

[8] Li Tao, Hu Aiqun, “Mobile Trusted Scheme Based on Holistic Security Service System,” 2011 International Conference on Network Computing and Information Security, 978-0-7695-4355-0/11, pp. 150-155, 2011.

[9] William Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition”, Prentice Hall, 2006

[10] Dr. R.Shanmugalakshmi, "Research Issues on Elliptic Curve Cryptography and Its applications -IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.6, Pp.19 -22, June 2009.

[11] Marisa W. Paryasto (2009), “Issues in Elliptic Curve Cryptography Implementation “- Internetworking Indonesia Journal, Volume No. 1, Pg.No 29-3, 2009.

[12] S. Prasanna Ganesan, Dr. GRD College of Science, "An Asymmetric Authentication Protocol for Mobile Devices Using Elliptic Curve Cryptography” 978-1-4244-5848-6/10, Pp. 107-109, 2010.

[13] "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005. First International Conference, 2006-02-27, PP. 84-89.

[14] Caimu Tang, Member, IEEE, and Dapeng Oliver Wu, Senior Member, IEEE"- An Efficient Mobile Authentication Scheme for wireless networks” IEEE transactions on wireless communications, vol. 7, NO.4, APRIL 2008.

[15] Mourad debbabi, Mohamed Saleh, Chamseddine Talhi and Sami Zhioua., Google Android: “Java for Mobile Devices: A Security Study”, Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC), pp. 1-10, 2005.

[16] A. Shabtai, et al., Google Android: “A Comprehensive Security Assessment”, IEEE Security & Privacy, vol. 8, no. 2, March-April 2010, pp. 35-44.

[17] UMTS 23.01: Universal Mobile Telecommunications System (UMTS): General UMTS Architecture. ETSI, 1999.

Author Profile

Lokesh Giripunje is a ME Student in G.H. Raisoni College of Engineering, Nagpur (India).

Sonali Nimbhorkar has completed M-Tech (CSE) and is presently working in G.H. Raisoni College of Engineering; Nagpur (India).She has published papers in many international journals.