Security in Smartphone & Tablets

Sunil Kumar Sahu
Department of Computer Science & Engineering
Parthivi College of Engineering & Management
Bhilai, CG, India

Hemant Sahu
Department of Computer Science & Engineering
Parthivi College of Engineering & Management
Bhilai CG, India
Hemusahu19

Ravi Verma
Department of Computer Science & Engineering
Parthivi College of Engineering & Management
Bhilai CG, India

***Abstract*—Smartphone's are now become best friend for everybody due to its existence in life. No one can imagine a single day without his or her Smartphone's. A Smartphone is basically a mobile phone with large additional features like digital camera, wi-fi, third party apps, web browser, touch screen interface, GPS, media player, banking facility and many things. Smartphone has changed the user's life due to its extremely good features. Due to popularity of Smartphone's there is some attacks and security aspects for smart phones and tablets. In this paper we provide the different attacks and security points to secure Smartphone's and Tablets.**

Keywords-Android; Smartphonesg; Encryption;

I. INTRODUCTION

1.1 Security

Security in computing world is defined as developing a mechanism to secure Laptops/computers, smart devices, networks (LAN/MAN) and internet. It describes the measures against unauthorized accesses, defense of critical data, information and unintentional events. Security measures are achieved by three processes on the basis of various policies and system components. These are following-

i Threat Prevention
ii Detection
iii Response

The policies include the following:

i System files, vital data and information will be protected by User access control and cryptography, respectively.
ii Firewalls (a software or hardware) are most common efficient security measures for a network. It prevent from some virus attacks and unauthorized access by using packet filtering.
iii Intrusion Detection Systems.
iv And response is up gradation of security measures.

1.2 Encryption

Encryption is defined as the method of converting a plain text into a cipher text. Encryption doesn't present any protection besides hacking but make positive that the work of hacker will be in vain by converting the message. Encryption is carried out by subsequent an encryption method which generally include a plaintext, to be encrypted and a key. The Key length depends on the algorithm used for encryption. The output is a cipher text which is in the form of unreadable text. And then obtain the original information after applying the decryption method.

There are two types of encryption process:

i) Symmetric Key (private) Encryption: In symmetric key encryption the key is same i.e. private key for encryption and decryption of data.

ii) Public Key Encryption: In public key encryption there are two keys viz. public key and private key. Public key is used for and Private Key is used for decryption to get reverse the original text message.

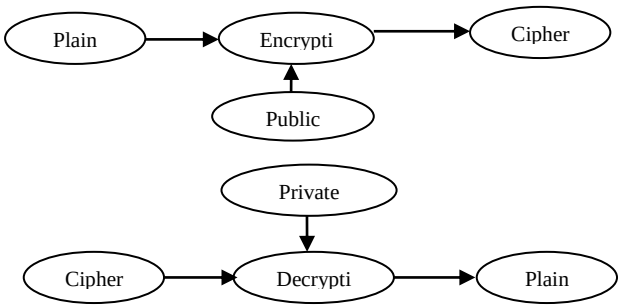

Fig.1 Asymmetric key Encryption

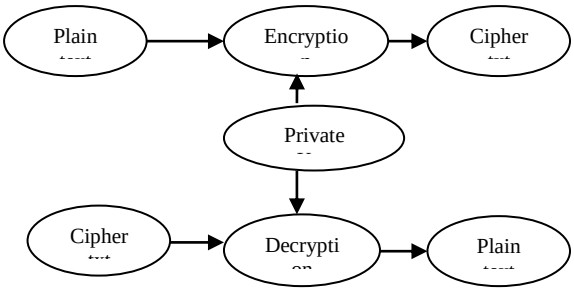

Fig. 2 Symmetric key Encryption

1.3 Decryption

Decryption is defined as reverse process of encryption. It exactly reverses the process of encryption. The encrypted text message along with the key used for encryption is used to decrypt the message.

II. LITERATURE REVIEW

Basically android became the world's leading Smartphone platform at the end of 2010. Android is a Linux-based operating system for mobile devices such as Smartphone and tablet computers. It is developed by the Open Handset Alliance, led by Google, and other companies. Android has a large community of developers writing applications ("apps") that extend the functionality of the devices. Developers write primarily in a customized version of Java. Apps can be downloaded from third-party sites or through online stores such as Google Play (formerly *Android Market*). For the first quarter of 2012, Android had a 59% Smartphone market share worldwide, with a 331 million devices installed base and 85 million activations or 934,000 per day.

There is following important features of Android phone-

1. **Handset layouts** - The platform is adaptable to larger, VGA, 2D graphics library, 3D graphics library based on OpenGL ES 2.0 specifications, and traditional smartphone layouts.
2. **Storage** - SQLite, a lightweight relational database, is used for data storage purposes.
3. **Connectivity**-Android supports connectivity technologies including GSM/EDGE, IDEN, CDMA, EV-DO, UMTS, Bluetooth, Wi-Fi, LTE, NFC and Wi-MAX.
4. **Messaging** - SMS and MMS are available forms of messaging, including threaded text messaging and now Android Cloud To Device Messaging (C2DM) is also a part of Android Push Messaging service.
5. **Multiple language support** - Android supports multiple languages.
6. **Web browser-** The web browser available in Android is based on the open-source WebKit layout engine, coupled with Chrome's V8 JavaScript engine. The browser scores 100/100 on the Acid3 test on Android 4.0
7. **Java support-** While most Android applications are written in Java, there is no Java Virtual Machine in the platform and Java byte code is not executed. Java classes are compiled into Dalvik executables and run on Dalvik, a specialized virtual machine designed specifically for Android and optimized for battery-powered mobile devices with limited memory and CPU. J2ME support can be provided via third-party applications.
8. **Media support-** Android supports the following audio/video/still media formats: WebM, H.263, H.264 (in 3GP or MP4 container), MPEG-4 SP, AMR, AMR-WB (in 3GP container), AAC, HE-AAC (in MP4 or 3GP container), MP3, MIDI, Ogg Vorbis, FLAC, WAV, JPEG, PNG, GIF, BMP, WebP.
9. **Streaming media support** - RTP/RTSP streaming (3GPP PSS, ISMA), HTML progressive download (HTML5 <video> tag). Adobe Flash Streaming (RTMP) and HTTP Dynamic Streaming are supported by the Flash plug in. Apple HTTP Live Streaming is supported by RealPlayer for Android, and by the operating system in Android 3.0 (Honeycomb).
10. **Additional hardware support-** Android can use video/still cameras, touchscreens, GPS, accelerometers, gyroscopes, barometers, magnetometers, dedicated gaming controls, proximity and pressure sensors, thermometers, accelerated 2D bit blits (with hardware orientation, scaling, pixel format conversion) and accelerated 3D graphics.
11. **Multi-touch-** Android has native support for multi-touch which was initially made available in handsets. The feature was originally disabled at the kernel level (possibly to avoid infringing Apple's patents on touch-screen technology at the time).
12. **Bluetooth-** Supports A2DP, AVRCP, sending files (OPP), accessing the phone book (PBAP), voice dialing and sending contacts between phones. Keyboard, mouse and joystick (HID) support is available in Android 3.1+, and in earlier versions through manufacturer customizations and third-party applications.
13. **Video calling-** Android does not support native video calling, but some handsets have a customized version of the operating system that supports it, either via the UMTS network or over IP. Video calling through Google Talk is available in Android 2.3.4 and later. Gingerbread allows Nexus S to place Internet calls with a SIP account. This allows for enhanced VoIP dialing to other SIP accounts and even phone numbers. Skype 2.1 offers video calling in Android 2.3, including front camera support.
14. **Multitasking-** Multitasking of applications, with unique handling of memory allocation, is available.
15. **Voice based features-** Google search through voice has been available since initial release. Voice actions for calling, texting, navigation, etc. are supported on Android 2.2 onwards.
16. **Tethering-** Android supports tethering, which allows a phone to be used as a wireless/wired Wi-Fi hotspot. Before Android 2.2 this was supported by third-party applications or manufacturer customizations.
17. **Screen capture-** Android supports capturing a screenshot by pressing the power and volume-down buttons at the same time. Prior to Android 4.0, the only methods of capturing a screenshot were through manufacturer and third-party customizations or otherwise by using a PC connection (DDMS developer's tool). These alternative methods are still available with the latest Android.
18. **External storage-** Most Android devices include MicroSD slot and can read MicroSD cards formatted with FAT32, Ext3 or Ext4 file system. To allow use of high-capacity storage media such as USB flash drives and USB HDDs, many Android tablets also include USB 'A' receptacle. Storage formatted with FAT32 is handled by Linux Kernel VFAT driver, while 3rd party solutions are required to handle other popular file systems such as NTFS, HFS Plus and exFAT.
19. **Google Play-** Google Play is an online software store developed by Google for Android devices. An application program ("app") called "Play Store" is

preinstalled on most Android devices and allows users to browse and download apps published by third-party developers, hosted on Google Play. As of October 2011, there were more than 500,000 apps available for Android, and the estimated number of applications downloaded from the Play Store as of December 2011 exceeded 10 billion. The operating system itself is installed on 130 million total devices.

20. **Privacy**- Android Smartphone have the ability to report the location of Wi-Fi access points, encountered as phone users move around, to build databases containing the physical locations of hundreds of millions of such access points. These databases form electronic maps to locate Smartphone, allowing them to run apps like Foursquare, Latitude, Places, and to deliver location-based ads.

III. VULNERABILITIES

Increase in the fame of smart phones have made them number one device for doing tasks like browsing net, mailing, online transaction etc. Due to their small size, smart phones can be easily accepted in people's pockets, purses or briefcases. Some drawback of Smartphone's is -

1. First object that come into mind is architecture i.e. the operating system used.
2. Operating system of smart devices do not include proper security software to prevent from virus.
3. The lifecycle of OS which is used in smart phone is not long as expected.
4. Android 4.4 Kit Kat (API level 19) was release in September 2013 which is about 3 months after android 4.3 Jelly Bean versions.

There are a variety of threats related with the security measure-

1. Backdoors- It is an algorithm of stealing the plaintext message by passing the usual authentication while left over undetected throughout the process.
2. Denial of Service- Basically it is very dissimilar from other attacks as it doesn't try to grow unauthorized contact of the computer system. It may trap the user to enter incorrect password leading to account to be blocked. Denial of service overworks the capabilities of System.
3. Exploits- It is defined as a series of instructions that takes advantage of any bug available in software to gain maintenance of the computer system.
4. Direct Access Attack- It is defined as additional tempering the devices or system once you have control of it.
5. Eavesdropping- Eavesdropping is spying or listening discussion between host and network. ENISA (European Union Agency for Network and Information Security) has given following 10 risks in smart phones as shown in fig 2.

Data leakage: Due to lost of Smartphone, its internal or external memory is insecure, As a result of this an illegal user access to the confidential information stored on it.

Unintentional disclosure of data: The consumer of Smart devices by mistake reveals important information/data on the smart phone.

Attacks on decommissioned phone: The phone is decommissioned wickedly permitting an unwanted user right of entry to the information on the device.

Phishing attacks: There is chance to collect user secret information i.e. passwords, credit card information, confidential information etc. by using fake app available in app store.

Spyware attacks: Smartphone has spyware installed that allow hacker or third party to alter personal data.

Network spoofing Attacks: An attacker sets up fake access point (wi-fi) and user connect to it that's help attacker to do phishing attack.

Surveillance Attacks: An attacker watches the target user under surveillance through smart phones.

Financial Malware attack: A hacker or unwanted person easily steal financial information from the user like credit card, net banking information etc.

Network Congestion: Due to large uses of network resources by smart phone and tablets there is chance of network congestion.

1	Data leakage resulting from device loss or theft	High
2	Unintentional disclosure of data	High
3	Attacks on decommissioned smartphones	High
4	Phishing attacks	Medium
5	Spyware attacks	Medium
6	Network Spoofing Attacks	Medium
7	Surveillance attacks	Medium
8	Diallerware attacks	Medium
9	Financial malware attacks	Medium
10	Network congestion	Low

Fig 3 ENISA 10 risks in Smartphone

IV. SECURING SMARTPHONE

There is following tips to keep Smartphone secure-

1. **Avoid untrusted App-** you may enter into your Applications Settings and set your phone that doesn't install apps from unknown third party sources.

2. **Back up your data**- If your confidential data is stolen, in this case it is necessary to create backup of your data and then recover it to prevent the loss of confidential dat.
3. **Keep up to date your OS-** To access and enjoy the latest features and functionality of operating system, we need to update the OS timely.
4. **Log out of sites -** If you can use your Smartphone's and Tablets for banking transaction, shopping purpose or any E-commerce, you must log out the sites after payment to prevent your confidential information.
5. **Turn off WiFi and Bluetooth -** Always turf off your wifi and Bluetooth whenever it is not in use Because hacker may send any Trojan or virus through wifi or Bluetooth.
6. **Avoid giving your personal information**- Always avoid to give your personal information to the text message that looks to be from your bank. If you found any requests via email or text for giving your account information from any organization, first contact the organization directly to verify the request.
7. **Install an Android security app.-** It is prime important to install trusted android security app from google play store. Security app prevent your data from unwanted security threats.
8. **Protect your investment-** According to a research it is find that 7 out of 10 people lose their device and data.

V. CONCLUSION

With the help of smart devices we can easily find everything like restaurant, street, institute, homes, shopping mall, theater, all banking needs become easier, no need to bore because there is lots of way to entertain yourself and lots of thing present in smart phones and tablets to do in their personal as well as in professional life. So we can say that world is in our Pocket in the form of Smart phones and Tablets. In this paper we present some attacks and security points for securing smart devices. We hope that this paper provides the consumer of Smartphone's and tablets and research scholar to secure their devices and work in this field.

REFERENCES

[1] Ian Angus. An Introduction to Erlang B and ErlangvC. Telemanagement, July-August 2001.
[2] Live Bos and Suresh Leroy. Toward an All-IP-Based UMTS System Architecture. IEEE Network, Januaryvand February 2001.
[3] Jian Cai and David J. Goodman. General Packet Radio Service in GSM. IEEE CommunicationsvMagazine, October 1997.
[4] Microsoft Corporation. New Security Technologies in Windows XP Service Pack 2 (SP2).vhttp://msdn.microsoft.com/security/productinfo/vxpsp2/default.aspx?pull=/library/enus/vdnwxp/html/securityinxpsp2.asp.
[5] Microsoft Corporation. Windows Mobile-based Smartphones. http://www.microsoft.com/vwindowsmobile/smartphone/ default.mspx.
[6] St´ephane Coulombe and Guido Grassel. Multimidia Adaptation for the Multimedia Messaging Service. IEEE Communications Magazine, July 2004.
[7] David Dagon, Xinzhou Qin, Guofei Gu, Wenke Lee, Julian Grizzard, John Levine, and Henry Owen. Honeystat: Local Worm Detection Using Honeypots.
[8] In Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID), 2004.
[9] Trusted Computing Group. TCG TPM Specification Version 1.2: Design Principles . https://www.trustedcomputinggroup.org/home.
[10] Harri Honkasalo, Kari Pehkonen, Markku T. NieMi, and Anne T. Leino. WCDMA and WLAN for 3G and Beyond. IEEE Wireless Communication Magazine, April 2002.
[11] PalmOne Inc. Treo smartphones. http://www.palmone.com/us/products/smartphones/.
[12] Christian Kreibich and Jon Crowcroft. Honeycomb - Creating Intrusion Detection Signatures Using Honeypots. In Proc. HotNets, 2003.
Kaspersky Labs. Viruses move to mobile phones, 2004. http://www.kaspersky.com/news?id=149499226