RESEARCH ARTICLE OPEN ACCESS

Comparative Analysis of Mobile Security Threats And Solution

Hezal Lopes*, Rahul Lopes**
*(Department of Computer Engineering, Mumbai University, Universal College of Engineering)
** (Technical Manager, Ambuja Cement

ABSTRACT
Presently, 96% of smartphones do not have pre-installed security software. This lack in security is an opportunity for malicious cyber attackers to hack into the various devices that are popular i.e. Android, iPhone and Blackberry. Traditional security software found in personal computers (PCs), such as firewalls, antivirus, and encryption, is not currently available in smartphones. Smartphones are small and are easy to carry anywhere. Unfortunately, the convenience of using smartphones to do personal task is the loophole cyber attackers need to gain access to personal data. In this paper, we have tried to identify threats and deal with the subject of security in four fields. These four areas include: Security of mobile device, security of operating system on mobile device, security of mobile database and security of mobile network. This paper also discusses the solutions for above problem.
Keywords – Android, Ios, Mobile Security, Threats.

I. INTRODUCTION

Need for security for Mobile devices is flourishing and diversity is growing. Mobile devices are often used precisely where they're most vulnerable – in public places like trains, lobbies, taxis, etc. But only a few are secured against the potential hazards of security attacks. This leads to data loss; probing or downloading of data by unauthorized persons. Hence, mobile security is the need of today.

In mobile communication, since wireless medium is available to all, the attackers can easily access the network and the database becomes more vulnerable for the user. In this paper we have discussed how one can save their mobile data, database from hacker and threat.

II. MOBILE THREATS

A threat is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm. Mobile threats are on the rise, with more mobile malware coming from lookalike banking apps, adult-only entertainment apps, targeted Trojan viruses and spyware, according to a new report from security solutions provider McAfee Inc.

III. SECURITY THREATS

Here we will deal with the subject of security in four fields [2]. These four areas include: security of mobile device, security of operating system on mobile device, security of mobile database and security of mobile network. We identify a set of security vulnerabilities on mobile database and try to apply appropriate technique to decrease side affect for mobile database security. Important security issues for mobile device, mobile operating system and mobile network that maybe affect on mobile database security are discussed along with possible solution.

III.I Threats that may occur for mobile Device [3]

A very first threat to mobile device is physical risk. Attacker can theft the mobile and can access account details. Next is Bloover/II a proof-of-concept application that runs on Java and is used as a phone auditing tool (snarfs phonebooks). It is also called the "Bluetooth Wireless Technology Hoover" because of how it can "vacuum" phone details. This application runs on J2ME-enabled cell phones. Another threat is Bluebug that exploits vulnerability in Bluetooth security to generate outbound phone calls, such as premium lines with expensive connection fees. Attackers are able to abuse the AT command set (industry-standard commands for modems) of a device to make use of SMS and the Internet connectivity of mobile devices. An attacker may also impersonate the victim, using their device for all such communications. Next is BlueBump which is Similar to key bumping—exploiting link keys on mobile devices. The attacker uses social engineering to gain trusted status with a targeted device, and so asks the victim to keep the connection open but to delete the link key. The connection to the device remains active, letting the attacker connect to the device as long as the key is not deleted again. Bluesnarf is nothing but AT commands are sent to a mobile device that sends data back to the attacker without authentication to steal (snarf) information without user consent. This attack makes it possible to retrieve information such as phone books, business cards, images, messages, and voice recordings. Bluesnarf++ forces re-keying, telling the partner device to delete pairing, and connects to unauthorized channels to gain full

read/write access to the compromised device file system.

III.I.I Solution

Install anti phone theft software. There are suppliers that provide modern anti theft software for your phone. The software enables us to remotely contact our mobile and stay in control. Register phone with network operator. If phone is stolen, report the loss to them immediately. Using mobile IMEI number, they may be able to block your hand set and account details. Use the security lock code, or PIN feature, to lock your phone. This will make it less valuable to a thief and deny them access to personal numbers stored on your Authentication verifies that users or systems are who they claim to be, based on identity (e.g., username) and credentials (e.g., password). Most highly publicized breaches are attributed to weak authentication - from unlocked laptops to wireless networks with cracked passwords. Many embarrassing incidents could be avoided by providing vigorous authentication to mobile devices and their networks. Data Encryption refers to Mathematical calculations and algorithmic schemes that transform plaintext into cyphertext. Cyphertext - non-readable to unauthorized parties. The recipient of an encrypted message uses a key which triggers the algorithm mechanism to decrypt (decode) the data. This transforms it to the original plaintext version.

III.II Threats that may occur for operating system on mobile device [3]

Payload is the primary action of a malicious code attack. For example, a downloader Trojan maybe used to install rogue software, where rogue software is the payload of the attack for financial gain. Next is rogue software illegitimate software designed to goad the user into purchasing a defunct software product and/or one that was illegally installed? These programs frequently include limited functionality, erroneous scan results, and aggressive warnings in an attempt to persuade the user into purchasing software. Next is Trojan. A Trojan is malicious software that masquerades as something it is not. It does not replicate. Next is Virus. Malicious software that infects a host files in order to spread. Worm is Malicious software that creates a copy of itself (a.k.a., clones itself) as it spreads. Rootkits are used to subvert both the operating system and security software, while boot kits attack encryption and can replace legitimate boot loaders.

III.II.I Solution

Operating system vendors bake security into the core of the OS. OS include included data-execution protection as well as address-space layout randomization. These security methods make it harder for attackers to compromise a victim's machine. Encryption technologies have also boosted OS protection in recent year. Install antivirus software for mobile devices. Secure password storage. Secure boot functions. Antimalware defences, Enhanced reputation capabilities.

Advances in the OS boot loader security feature have already caused researchers to show how they can be subverted through legacy BIOS. With further development around extensible firmware interface specifications—designed as a software interface between the operating system and platform firmware to enforce a secure boot and to replace legacy BIOS.

III.III Threats that may occur for mobile database [3]

In the case of a mobile database application that it is a distributed database, there are security challenges due to the distributed nature of the application and the hardware Constraints of mobile devices. The major issues in multilevel security on Distributed Security Manager are authentication, data confidentiality, identification and accessibility.

- Confidentiality
  - Loss of business data.
  - Loss of customer's personal data.
  - Loss of financial data.
  - Loss of employee's data.
  - Loss of intellectual properties etc.
  - Monetary losses.
  - Loss in existing Business.
  - Loss of new business opportunity.
  - Loss of credibility.
  - Losing competitive edge over the competitor.
- Accessibility
  - Resource uptime.
  - High Availability / Recoverability.
  - Archive.
  - Snarf:-Unauthorized theft of data. A slang term for stealing information from another device.

III.III.I Solution

- Virus scanning has to be performed on a regular basis.
- Implement Firewall effectively.
- It is advisable that the database should require authentication before returning any type of data. It is advisable to use industry standard cryptography algorithm over home grown algorithm.
- Apply firmware and software patches or upgrades on regular basis.
- Use IPSec or SSL to protect access to databases.
- Router Configuration Changes.
- Firewall Configuration Changes.
- Auditing and logging is implemented, working and also access to log file is secured. Also make sure that sensitive information like passwords are not logged.
- Do not save sensitive data like Passwords, credit cards numbers in clear text format. All sensitive data should be encrypted.

- If possible, use the latest generation of database server.
- Install the latest vendor-provided patches for the database. Be sure to include patches for database support software that is not directly bundled with the database.
- Every server should be configured to only allow trusted IP addresses and only those ports which are required should be opened.
- Remove sample databases and database users.
- Create alternative administrative users for each DBA, rather than allowing multiple individual users to regularly use the default administrative account.

III.IV Threats that may occur for mobile Network [3]

Attackers can access our mobile network without any authentication that is nothing but unauthorized access. Eavesdropping a transmission is nothing but access to the medium, looking for passwords, credit card numbers, or business secrets hijacking or taking over a communication inspect and modify any data being transmitted. IP spoofing or faking network addresses Impersonate to fool access control mechanisms redirect connections to a fake server. Denial-of-Service is an attack designed to disrupt and/or deny use of a device, service, or network.

III.IV.I Solution

Password protects your device and changes this password every 60 days. Delete your browsing history, system cache, picture cache, network cache, installation log, viewed SMS, and viewed email from your phone. Verify the applications your download before your install them. Scan the operating system for Trojans, malware, etc. Turn-off Bluetooth when not in use. Use anti-virus software and keep the definition file up-to-date. Use a firewall.

IV. MOBILE THREAD REPORT [5]

Mobile malware continues to grow at an exponential pace and remains the most popular hacking technique for devices.[4] Mobile malware professional are maximizing their return on investment by targeting android because of its global market dominance and open platform. Like legitimate business people, malware professionals look to exploit the largest market opportunity. Here is the summary how attacker can attack on the android phone.

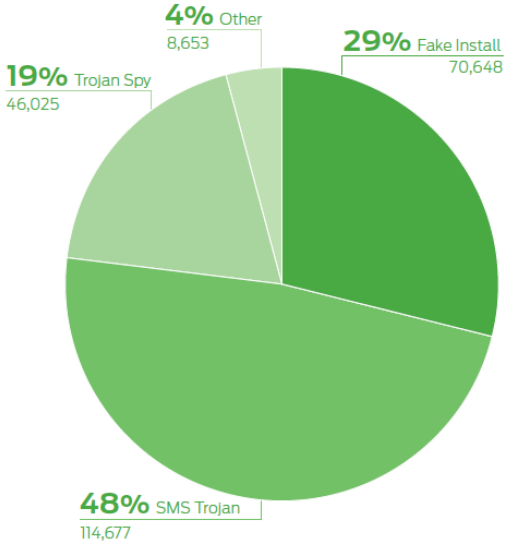

Fig 1: Attack Makeup of March 2013- Android[4]

V. MOBILE PLATFORM COMPARISON [6]

Although history has repeatedly demonstrated that it is virtually impossible to create a perfectly secure system, mobile operating system developers have learned from security mistakes of the PC world. Android and iOS have each taken an innovative approach to securing both the operating system and application distribution process.

V.I iOS

On the device itself, Apple's iOS security model runs each third-party application in an isolated environment so that the application may only access its own data and permitted system resources. All third-party applications are granted access to the same data and capabilities on the device with the exception of a few, such as location data and push notifications, which require a user to opt in for each application.

In terms of app distribution, Apple's App Store for iOS utilizes a curated app review model in which all apps submitted by developers go through a manual review process with restrictions based on policies regarding issues such as data collection, API usage, content appropriateness, and user interface guideline compliance. This model is designed with the assumption that apps will only be downloaded from Apple's App Store, as some security restrictions are enforced during the review process but not necessarily enforced on the device itself. The assumption generally holds, as iOS devices prevent users from loading applications from sources other than Apple's App Store unless the device has been "jailbroken." Jailbreaking is a process whereby the user can alter the phone's operating system to gain full access (or root access) to the operating system and allow applications not officially vetted by Apple, many of which take advantage of operating system capabilities otherwise restricted by Apple's review policies.

V.II Android

Android has an operating system security model that supports its open application distribution model. In the Android OS security model, an application's capabilities are gated by "permissions" that the application declares when it is installed and cannot be changed at a later time. When installing an application, users are presented with the list of permissions requested by the application and can determine whether the permissions are appropriate for the functionality of the app. Permissions allow applications to access specific data and capabilities on a device, including location, contacts, SMS messaging, identity information, and the ability to access the Internet. If an application's permissions seem overreaching, a user may choose not to install the app or may identify it as suspicious. While the Android permissions model enables developers to provide a broad range of functionality in their apps, it does rely on end users' ability to evaluate permissions requested by an app at the time of installation.

In terms of app distribution, the Android operating system utilizes an open application distribution model that allows users to download applications from a variety of sources, including Google's Android Market, Amazon's Appstore for Android, carrier markets such as Verizon's V CAST network, and other alternative app markets. Android also has a setting, often referred to as sideloading, which enables or disables the capability to download applications from other sources outside of the Android Market. Android enables multiple application distribution methods. For example, Amazon's Appstore for Android and Verizon's V CAST apps utilize a curated model with a manual review process similar to Apple's, while Google's Android Market is based on a community-enforced model where some security checks are performed when applications are submitted to the market, but it is expected that the community as a whole will participate in identifying malicious or otherwise undesirable applications. This allows Android developers to update their applications much more quickly than with the curated model.

VI. CONCLUSION

The value of data is steadily increasing, possibly even more so than actual money and threats to mobile devices are pervasive and escalating. Everyday mobile users and enterprises are facing some or other kind of mobile attacks like malware, loss and theft, exploitation and misconduct, communication interception, and many more.

With effective use of security mechanism as mentioned above, organizations and individuals can cost-effectively guard against current and emerging threats, while retaining optimal productivity and flexibility in their use of mobile devices.

REFERENCES

[1] http://www.itbusiness.ca/news/mobile-threats-are-growing-mcafee-report-finds /42231

[2] Ghorbanzadeh, Parviz; Shaddeli, Aytak; Malekzadeh, Roghieh; Jahanbakhsh, Zoleikha "A Survey of Mobile Database Security Threats and Solutions for It." Information Sciences and Interaction Sciences (ICIS),3rd International Conference Chengdu, China Aug 2010

[3] Ken Dunham, "Mobile Malware Attacks and defence", 2009

[4] http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf

[5] Cyber_Security_and_Mobile_Threats__The_Need_for_Antivirus_Applications_for_Smart_Phones.pdf

[6] https://www.lookout.com/resources/reports/mobile-threat-report