A Survey on Next Generation Challenges and Issues in Mobile Systems

A.Revathy,
PG Student
Sri Manakular Vinayagar Engineering College
Pondicherry,
revy2890@gmail.com

D.Kanimozhi
` PG student
create an attractive target for attackers, as they allow direct
Sri Manakular Vinayagar Engineering College
Sri Manakular Vinayagar Engineering College
kanimozhi516@gmail.com

Abstract –

Mobile phones are becoming increasing intelligent, and are growing ever more like computers in functionality. Many mobile devices are always on and connected, so vulnerability to malicious attacks increases through different communication channels. The major information security threats facing developers of mobile services include the complexity of technological solutions, the illegal copying of content and programs, threats posed by the Internet, the different levels of various players in the service development process, and threats involving the identification of service users and servers and the confidentiality of information. Owe to the vulnerable nature of the mobile network, there are numerous security threats that disturb the development of it. In this paper, we first analyzed the main threats and attacks in mobile network. Then we identified about how it get onto mobile devices. Finally the current security aspects and recommended solutions in the mobile system are discussed.

***Keywords* - Mobile Security, Security Attacks, Threats, Security Issues**

IJERT

1. Introduction

The growing popularity of mobile technology may have finally attracted enough hackers to make the potential for serious security threats a reality. In the world of computers and communications, the more widely a technology is used, the more likely it is to become the target of hackers. Such is the case with mobile technology particularly smart phones; these phones are being used frequently for sensitive transactions like banking, mobile payments, and transmitting confidential business data, making them attractive targets if not protected.

A. Mobile security important

Mobile devices are the fastest growing consumer technology, with worldwide unit sales expected to increase from 300 million in 2010, to 650 million in 2012. Mobile applications are likewise booming. In June 2011, for the first time ever people on average spent more time using mobile applications (81 minutes) than browsing the mobile web (74 minutes).While once limited to simple voice communication, the mobile device now enables us to also send text messages, access email, browse the Web, and even perform financial transactions. Recently over 250,000 Android users were compromised in an unprecedented mobile attack when they downloaded malicious software disguised as legitimate applications from the Android Market. Mobile payments

monetization of attacks. The value of mobile payment transactions is projected to reach almost $630 billion by 2014, up from $170 billion in 2010. Vendors, retailers, merchants, content providers, mobile operators and banks are all actively establishing new payment services. In addition to financial information, mobile devices store tremendous amounts of personal and commercial data that may attract both targeted and mass-scale attacks.

B. Highlights in mobile threats

• Both web- based and app-based threats are increasing in prevalence and sophistication.

•Android users are two and a half times more likely to encounter malware today than 6 months ago and three out of ten Android owners are likely to encounter a web-based threat on their device each year.

•An estimated half million to one million people were affected by Android malware in the first half of 2011; Android apps infected with malware went from 80 apps in January to over 400 apps cumulative in June 2011.

•Attackers are deploying a variety of increasingly sophisticated techniques to take control of the phone, personal data, and money. Additionally, malware writers are using new distribution techniques, such as malvertising and upgrade attacks.

2. Related Work

Many mobile devices do not offer users full control over their device hardware or operating system. To gain complete control, people will “root” or “jailbreak” their device. The process of rooting or jail breaking takes advantage of operating system vulnerabilities to bypass security protections on a device. This conflict of interest between vulnerability disclosure and the ability for people to fully control their own device poses a great security issue. Software vendors want to fix vulnerabilities as quickly as possible, before they can be exploited and used maliciously, so well -intentioned researchers typically disclose vulnerabilities they find to the software vendor. On mobile devices, however, there is a conflict of interest. Because vulnerabilities are often the only way to root or jailbreak devices, many researchers do not want vulnerabilities to get fixed so they can maintain full control over their devices. The desire to gain full control over devices creates a disincentive for researchers to disclosure

disclosure and the ability for people to fully control their own device poses a great security issue. Once a vulnerability being used to root or jailbreak devices becomes public knowledge it may also be used by malicious attackers, like Droid Dream. Until all mobile devices allow users to gain full control without resorting to exploits, this conflict of interest between control and safety is likely to continue.

A. Classification of Mobile Security

• Network access control involves the use of a protocol or defined set of rules for user access to a network. Users access a network based on a defined set of security policies that are enforced by an organization. The policies use a protocol to define the device access as well as what the end user can do with the mobile device on the network.

• Virtual private networks are networks that provide encryption and security applications that ensure only authorized users can access the network. A virtual private network is accessed through a browser and Internet connection and does not require additional software installation on the devices of the end users.

3. Mobile Security: Issues And Threats

The mobile threats can be broadly categorized into the following five categories

1. Physical Threats
2. Application-Based Threats
3. Web-based Threats
4. Network Threats

A. Physical threats

Mobile devices are portable and designed for use throughout our daily lives; their physical security is an important consideration.

Lost or Stolen Devices

Lost or stolen devices are one of the most prevalent mobile threats. The mobile device is valuable not only because the hardware itself can be re-sold on the black market, but more importantly because of the sensitive personal and organization information it may contain.

Users' access and share data securely through the encryption and security applications that are stored on the virtual private network.Organization Devices use their own handheld devices to connect to the organization network is of growing concern when it comes to security risks. As a result, most organizations are issuing their own devices for the workers to use remotely to access the company network. Although this security method is more costly to implement, the cost of security breaches to sensitive and confidential data outweigh the cost of device implementation. While it is often software, it can also appear in the form of devices for added security.

B. Web-based threats

Because mobile devices are often constantly connected to

vulnerabilities. This conflict of interest between vulnerability

the Internet and used to access web-based services, web-based threats that have historically been a problem for PCs also pose issues for mobile devices:

Phishing scams use web pages or other user interfaces designed to trick a user into providing information such as account login information to a malicious party posing as legitimate service. Attackers often use email, text messages, Facebook and Twitter to send links to phishing sites. Phishing attacks are designed to trick users into divulging account or personal information to web pages that appear to be reputable sites such as financial institutions, but are actually fake.

Phishing" is an email or an SMS text message (dubbed, "SMiShing") sent to trick a user into accessing a fake website, sending a text message or making a phone call to reveal personal information (such as a Social Security number in the United States) or credentials that would allow the hacker access to financial or business accounts[2].

C. Application-based threats

Downloadable applications present many security issues on mobile devices, including both software specifically designed to be malicious as well as software that can be exploited for malicious purposes.

IJERT

Malware short for malicious software used or created by hackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. As a result, most organizations are issuing their own devices for the workers to use remotely to access the company network.

Boot kits, a malware that replaces or bypasses system startup, also threatens mobile devices. Although rooting one's own phone or e-book reader opens the device to extra features or to replacing the OS, it can also allow attackers to load their own modified OS. Whereas a mobile root kit will simply modify the existing OS to evade detection, a boot kit can give an attacker much greater control over a device. "Weapon of Mass Destruction" WMD mobile penetration-testing tool installs itself to load Linux on Windows Mobile phones and allows the user to reboot to the original OS.

Spyware designed to collect or use data without a user's knowledge or approval. Data commonly targeted by spyware includes phone call history, text messages, location, browser history, contact list, email, and camera pictures. Spyware generally fits into two categories: it can be targeted, designed for surveillance over a particular person or organization, or untargeted, designed to gather data about a large group of people. Commercial spyware applications—such as FlexiSpy (www.flexispy.com), Mobile Spy (www.mobile-spy.com), and MobiStealth (www.mobistealth.com) are readily available and effective at concealing their presence from the user of an infected device.

These spyware applications enable an attacker to monitor SMS and Multimedia Messaging Service (MMS) messages, emails, inbound and outbound call logs, and user locations.

Privacy threats may be caused by applications that are not necessarily malicious (though they may be), but gather or use more sensitive information (e.g., location, contact lists, personally identifiable information) than is necessary to perform their function or than a user is comfortable.

Vulnerable Applications contain vulnerabilities that can be exploited for malicious purposes. Such vulnerabilities can often allow an attacker to access sensitive information, perform undesirable actions, stop a service from functioning correctly, automatically download additional apps, or otherwise engage in undesirable behavior. Vulnerable applications are typically fixed by an update from the developer.

Drive-by-downloads may use spam or advertising to bring users to a site that, in turn, delivers malware by automatically starting a download. Such attacks are a significant concern on devices where applications can be downloaded outside of official markets because malware distributed through websites can evade the greater scrutiny that markets provide. ***Direct exploitation*** is a significant threat to mobile browsers, as there are a number of large code bases on mobile devices that malicious web pages can target, including the browser itself, image viewers, Flash, PDF readers, and more. Weskit, the popular rendering engine, is a systematic risk because the default browsers on Android, Blackberry, and iOS all use it, creating a homogenous ecosystem where a single vulnerability can potentially affect the majority of mobile devices. Browser exploits are also very difficult to fix because mobile browsers and their associated libraries are often revision with firmware, which can be extremely slow to update.

D. Network threats

Mobile devices typically support cellular networks as well as local wireless networks. There are a number of threats that can affect these networks:

Network exploits take advantage of software flaws in the mobile operating system or other software that operates on local (e.g., Bluetooth, WI-Fi) or cellular (e.g., SMS, MMS) networks. Bluetooth and Wi-Fi effectively increase the connectivity of mobile devices within a certain range, but they can be easily exploited to infect a mobile device with malware or compromise transmitted data [2].

To completely block incoming connection requests from unknown devices, a local firewall should be installed and run on the mobile device-another traditional security practice that can be extended to the mobile environment.

Setting the device's Bluetooth to an undiscoverable mode and turning off the device's automatic Wi-Fi connection capability, especially in public areas, can help reduce risks.

Wi-fi sniffing can compromise data being sent to or from a device by taking advantage of the fact that many applications and web pages do not use proper security measures, sending their data in the clear (not encrypted) so that it may be easily intercepted by anyone listening across an unsecured local wireless network. Wi-Fi Sniffing is a technique where nearby attackers can get access to data transmitted to or received from a mobile device.Firesheep20 is a desktop browser plug-in that monitors unencrypted

Wi-Fi networks for nearby computers and mobile devices accessing popular websites (e.g. Twitter, Facebook, GMail) in an insecure way and allows an attacker to trivially hijack user accounts accessing those sites. Man in the middle attacks any mobile device that connects to a wi-fi network is open to this type of attack the attacker becomes a middle man in a communication stream and logs all information between the communicating parties

4.Attacks On Mobile Networks

Because mobile networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile network than in the wired network.

A. Lack of secure boundaries

The meaning of this vulnerability is self-evident: there is not such a clear secure boundary in the mobile network, which can be compared with the clear line of defense in the traditional wired network. This vulnerability originates from the nature of the mobile network: freedom to join, leave and move inside the network. The attacks mainly include passive eaves dropping, active interfering, leakage of secret information, data tampering, message replay, message contamination, and denial of service[5].

IJERT

B. Sms vulnerabilities

An incident of the early times of mobile phones (not even smart phones at that time) was an implementation bug in the SMS parser of the Siemens S55: receiving a short message with Chinese characters lead to a Denial of Service. This bug required a local firmware update, forcing the users to bring or send their device to customer service. This class is expected to be of less importance in the future, because modern smart phone architectures are increasingly allowing local or remote firmware updates.

C. Lack of centralized management facility

Mobile networks do not have a centralized piece of management machinery such as a name server, which lead to some vulnerable problems. The absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network.

In one word, the absence of centralized management machinery will cause vulnerability that can influence several aspects of operations in the mobile ad hoc network.

D. Restricted power supply

Due to the mobility of nodes in the ad hoc network, it is common that the nodes in the ad hoc network will reply on battery as their power supply method. The first problem that may be caused by the restricted power supply is denial-of-service attacks. Furthermore, a node in the mobile ad hoc network may behave in a selfish manner when it finds that there is only limited power supply, and the selfishness can cause some problems when there is a need for this node to cooperate with other nodes to support some functions in the network.

E. Mms vulnerabilities

In 2006, a remote code execution exploit for mobile phones using MMS as the attack vector was published by Mulliner. It exploited a buffer overflow in the MMS handling program of Windows Mobile CE 4.2. Being the first of its kind, it supported the public fear of that time that mobile devices would start to become commonly attacked. The exploit received some attention by a technical audience and the MNOs, who published patches for affected devices. Anti-virus companies added the exploit to their signature databases, but the exploit never appeared as part of mobile malware and thus not much harm was caused by it.

E. Platform vulnerabilities

A number of vulnerabilities have been exploited on both Android and IOS devices. For example, the Droid Dream malware that emerged in the Android Market in the first quarter of 2011 utilized two exploits, exploid and rage against the cag, to break out of the Android security sandbox, gain root control of the operating system, and install applications without user interventions [5].

I. HOW SPYWARE AND MALWARE GET ON TO MOBILE DEVICES

Phishing a fake version of a real site gathers your log-in and other private information.

Spyware silently collects information from user and sends it to eavesdroppers.

App stores copies of legit applications are infected with malicious code and placed in official app stores.

Repackaging is a very common tactic in which a malware writer takes a legitimate application, modifies it to include malicious code, then republishes it to an app market or download site.

Misleading Disclosure have had to contend with spyware and adware that walks the line between being malicious and simply being undesirable, so do mobile devices.

Drive-by-Downloads are a class of technique where a web page automatically starts downloading an application when a user visits it [12].

II. SECURITY STANDARDS AND TECHNOLOGIES

A. Proactive malware protection

Organizations need to protect mobile devices against malware and viruses delivered via email, SMS, MMS, direct download, Bluetooth, or infrared transmission. Security teams also need virus definition updates to be propagated to devices automatically. Further, mobile devices need capabilities for doing real-time scanning of incoming files and scans of internal memory, memory cards, and the entire device, as well as generating automated alerts if malware is detected.

B. Loss and theft protection

To mitigate the risks posed by lost or stolen devices, users and IT administrators need cohesive, integrated mobile device management capabilities. This includes capabilities for using GPS to identify the precise location of a missing device. Organizations and individuals also need the assurance. Safeguards against communication interception

To guard against communication interception, IT teams need to employ VPNs that encrypt communications between mobile devices and corporate networks. Further, they need to establish and enforce corporate mobility policies, combining VPN access control with mobile security.

A. Prevent phishing

a. Always check the URL of the site you are on before you click submit

First of all, are you really on the site you intend to be on? Second, you want to make sure you see the "s" in "https". This is especially important when you are using your phone (or PC) on an unsecured wireless network.

2) If you ever think, "Why are they asking for that?" close your browser.

F- Secure Labs recently analyzed an man-in-the-mobile (mitmo) trojan attack that created a fake bank login page. The page asked for the customer's mobile number so that one-time passwords could be sent through SMS as a security precaution. The page also asked for the phone's international mobile equipment identity (IMEI), which was then used by the trojan to forge a security certificate and infect your phone.

3) Use only one credit card for all of your online purchases

In some countries, using a credit card limits your fraud liability, making credit cards a safer choice than ATM cards. Regardless if this is true for you, a smart strategy is to use the same credit card for all your online purchases and check that account weekly. The sooner you spot a fraud, the less damage you are likely to incur.

4) If you are going to make transactions on your phone, make sure it's protected.

Handheld mobile devices are as powerful as PCs, and they need to be protected like PCs. F-Secure Mobile Security's Browsing Protection protects users against phishing scam. Your phone has access to your email and other crucial accounts, so it's smart to secure it the way you secure your PC.

5) When in doubt, go in the bank

The clock is always ticking. You're late; you want to save some time. That's when your mobile phone makes life easier. However, for your most crucial interactions, such as large transfers, you best choice is to go into the branch itself. That way you don't have to worry about phishing or mobile Trojans[11].

B. Preventing Spyware

a. Install good anti-spyware software

When there's a large number of traces of Spyware such as Backdoors that have infected a computer, the only remedy may be to automatically run a Trojan scan for Backdoors from

IJERT

a good spyware cleaner designed to remove and block spyware.

2) Obtain Windows Security updates

Install Windows Security Update to get the latest security updates. Regularly use Windows Security Update to help you improve your computer's security settings and to help make sure that your computer has important security updates installed.

3) Update your anti-spyware software definitions

Configure your anti-spyware software to check for updates at least on a daily basis. Also, make sure your anti-spyware software is loaded when your computer starts and that it is automatically updating its spyware definitions.

4) Scan for Backdoors

Scan for Backdoors and other parasites by opening the anti-spyware software and clicking the "Start Scan" button. Once the anti-spyware program has completed the scan, checkmark parasites you wish to remove, and then click on the "Start Remove" button to get rid of spyware. Download SpyHunter's scanner to check for Backdoors. SpyHunter's scanner is only a detection tool. After detection of Trojans, the next advised step is to remove Trojans with the purchase of the SpyHunter Spyware removal tool.

5) Anti-virus and anti-malware software

Anti-virus and anti-malware software commonly hooks deep into the operating system's core or kernel functions in a manner similar to how malware itself would attempt to operate, though with the user's informed permission for protecting the system. Any time the operating system does something, the anti-malware software checks that the OS is doing an approved task. The goal is to stop any operations the malware may attempt on the system before they occur, including activities which might exploit bugs or trigger unexpected operating system behavior [7].

III. RECOMMENDATIONS FOR MOBILE SECURITYSCHEMES

As the frequency of mobile threats increase, people can take measures to stay safe while using their mobiles

- Only download apps from trusted sources, such as reputable app stores and download sites. Remember to look at the developer name, reviews, and star ratings.

- After clicking on a web link, pay close attention to the address to make sure it matches the website it claims to be if you are asked to enter account or login information.

- Set a password on your mobile device so that if it is lost or stolen, your data is difficult to access.

- Download a mobile security tool that scans every application you download for malware and spyware and can help you locate a lost or stolen device.

- Be alert for unusual behaviors on your phone, which could be a sign that it is infected. These behaviors may include unusual text messages, strange charges to the phone bill, and suddenly decreased battery life.

- Be careful when accepting files via Bluetooth

- If you do infect your mobile, turn off the Bluetooth functions so that malware does not find new targets

- Delete messages from unknown senders

- Do not install program if you are unsure of their origin

- Download ringtones and games from official websites

- Lock your device with a personal identification number (PIN) or password [3].

- Only install applications (apps) from trusted sources.

- Always log out of banking and shopping sites.

- Turn off Wi-Fi, location services, and Bluetooth when they are not in use.

- Don't click on links or attachments in unsolicited emails or text messages [3].

- Establish a program that continually evaluates new and emerging threats in mobile platforms.

IJERT

5.Conclusion

In this survey paper, we presented common vulnerabilities, threats and security approaches on mobile security. First we briefly introduce the mobile security issues and threats; we then discuss some typical and dangerous vulnerability in the mobile network such as lack of secure boundaries and centralized management facility, sms vulnerabilities and platform vulnerabilities. Finally we also find some points for current mobile security solutions and top ten recommendations that can be further explored in the future.

REFERENCES

[1] I-Lung Kao, Global Strategist, IBM Security Services," Securing mobile devices in the business environment", October 2011.

[2] Quick tips to mobile security

http://www.live.mcafee.webcollage.net/_wc/pdf/Mobilee Guide _Jan2012.pdf.

[3] "Lookout Mobile Threat Report" August 2011 (http://www.lookout.com/resources/reports/mobile-threat-report)

[4] Wenjia Li and Anupam Joshi "Security Issues in Mobile Ad Hoc Networks- A Survey", (http://www.csee.umbc.edu/~wenjia1/699_report.pdf).

[5] Becher, Michael; Freiling, Felix C.; Hoffmann, Johannes; Holz, Thorsten; Uellenbeck, Sebastian; Wolf, Christopher (May 2011). "Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices".2011 ieee symposium on Security and privacy.

[6] Backdoors-from Wiki-security, a source for malware detection and computer security (http://www.wiki-security.com/wiki/Parasite_Category/Backdoors)

[7] Malware-Wikipedia- the free encyclopedia (http://en.wikipedia.org/wiki/Malware)

[8] Mobile security- the free encyclopedia (http://en.wikipedia.org/wiki/Mobile_securt y).

[9]ComputerSecurityFAQ(http://www.kaspersky.com/threats_ faq)

IJERT

IJERT

IJERT