International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 09 | Dec-2015 www.irjet.net p-ISSN: 2395-0072

VULNERABILITIES OF SMARTPHONES

Shakuntala P. Kulkarni[1], Prof Sachin Bojewar[2]

[1] PG Scholar, Department of Computer Engineering, ARMIET, Maharashtra, India
[2] Associate Professor, Department of Information Technology, VIT, Maharashtra, India

---

Abstract - ***Nowadays, mobile devices are important part of our lives. Mobile phones allow us to access many services. Current Smartphones offer capabilities of traditional personal computers. Other than the traditional functionality of the phone that is calling, various other functionalities are provided by phones. There are different types of connectivity available in mobile phones such as GSM, GPRS, Bluetooth and Wi-Fi. Due to these facilities, there is a huge increase in use of smartphones. As the advantages of smartphone have increased, there is increase in vulnerabilities of Smartphone as well. Smartphones are easy targets for malware writers. As the vulnerabilities increase, attacks also increase. There are many risks with smartphones. Phone might contain confidential data like bank details. It might also have private data like photos, music, videos etc. If a phone is lost or stolen, all the data stored in phone will be lost as well as leaked. Through various applications, smartphone might unintentionally leak information. Attacker may try to collect confidential information such as credit card details, passwords etc. by using fake applications, SMS, Emails which appears to be genuine. This is known as phishing attack. Attackers may also use spyware attack to attack Smartphones. Smartphones may have spyware application installed, which leaks personal data of user. There are many types of attacks. To save oneself from the attacks, and reduce the vulnerabilities, user must be careful and take few precautions. In this paper, vulnerabilities of smartphones, the various types of attacks on smartphones, and measures to be taken to protect oneself from the attack are discussed in this paper.***

Key Words: *Mobile Security, Intrusion Detection, Mobile Malware, Trusted Mobile.*

1. INTRODUCTION

Smartphone is a mobile phone with much functionalities and features. It has capability as that of personal computers. Smartphones have features of a phone and has additional features like a media player, a digital camera, and/or a GPS navigation unit, web browsing, Wi-Fi, 3rd-party apps, motion sensor and mobile payment. Due to all these features, smartphones have become an important part of the life of the user. As the usage of the smartphones has increased, there is increasing in vulnerabilities exploiting these features. Therefore, smartphones are targets for malware writers. As the vulnerabilities increase, there is Increase in attacks also. There are few solutions given by researchers.

In initial days, smartphones came with standard Operating System (OS). Due to which a single vulnerability led to attack on large number of smartphones causing major security outbreaks. Nowadays many operating systems have come like Symbian OS, Windows Mobile, Android and iPhone OS. Built-up of each OS is different. If the user downloads few applications, it is possible that malicious applications may get installed. Malicious application may leak personal information of the user.

2. LITERATURE SURVEY

2.1 A Survey on Security for Mobile Devices

Mobile phones are very important part of our everyday lives. Since, mobile phones come with much functionality; they are target for many attacks. As the vulnerabilities has increased, number of attacks also have increased. The research field dealing with vulnerabilities and attack on smart phone is still in its starting phase, not explored to depth and is immature. The attacks are grouped into different categories based on detection principles, OS etc. With the categorization it would be easy to find solution to the treats. [1]

2.2 Survey: Data Protection in Smartphones against Physical Threats

In this paper a survey is presented of the data protection of the smartphone against threats like theft or loss of the smartphone. There is increase of the theft of phone, because theft of phone is not only a theft of phone, but theft of bank details, passwords etc. Analysis of the existing system has revealed that existing system doesn't consider user as source of threat. It doesn't provide adequate protection against physical threat. It doesn't take

care of the privacy of the users. Here, the methods to address the security hazards are discussed. [6]

3. THREATS AND ITS SOLUTION

3.1 Resource Draining

Android applications are not having either RAM (memory) or storage (disk). Applications are using devices disk space or memory. Any malicious application can use more memory, disk and CPU hogging is also possible.

Solution

Resource Management**:** This mechanism contains allocation of resource fairly to the applications according to needs of application. It maintains the disk allocation, memory allocation and allocation of other resources to the application. But implementation of such requires kernel level modification. Implementation efforts are high that is configuring kernel to support such system. By doing DOS attack on Smartphone like sending huge amount of SMS/MMS etc. attacker can force device to shut down or drain battery by consuming more CPU usage, deny users to perform regular tasks or deny from using services of the phone.

Examples: The battery exhaustion attack, water torture attack (drain battery or consume compacting resources by sending bogus frames)

Intrusion Detection System: Undetected malware can drain the resource by remaining hidden. By using host based IDS we can detect the malwares that are using more disk space or memory.

3.2 Reading Contents

Applications in android can read the data or contents of Smartphone by implicitly or explicitly gaining the permission and on wireless communication eavesdropping can be done by attackers remotely.

Solution

Encryption of data: By encrypting data on Smartphone user can protect the important or sensitive data. The data is secure if anyone stele the device then also he or she cannot read the information because only owner knows the key to decrypt the data.

Login: By setting login password user can protect the private information from exposing. If attacker stele device he can't do anything without password.

Firewall: By implementing firewall we can inspect the network traffic to and from android Smartphone. Configure firewall such that it can examine all packets that are whether android application is sending private contents outside and accordingly it can block such traffic. If firewall operates at kernel level malicious applications can't bypass it. Only drawback of firewall is that it can't block the sending data from phone through SMS/MMS. Malicious apps can send data through SMS/MMS.

Access control: By implementing strong access control mechanisms such as context aware access control (CAAC) we can limit the access to device. Implementation of this solution requires high efforts. We can limit access to the contents while device is connected to cellular network or Wi-Fi.

Remotely managing data: If the device is stolen one can retrieve the data remotely from the device by implementing such solution. For that device must be connected to the network.

3.3 Attack Through Installed Application

Android application asks for permission to data, phone, message, contacts, network etc. to use it at the time of installation. These types of attack have high impact on device.

Solution

Selected permission to android application: By providing user to give certain permissions or to choose such permission by which application can't perform malicious activities. Current scenario is that android apps are asking for the whole permissions it is requesting or none that is user cannot install application on device before he grant all the permission requested by the application.

3.4 Compromised private network

Hacker use the android device to compromise another network device by running port scanner, email, warms, SMS, worms, mms worms etc.

Solution

Managing network remotely: A centralized remote management system can be used to solve the problem of managing network remotely. We can apply certain security policies when operating within the private network. Remote administrator of private network can control all the activities or forcing security policies.

Virtual private network: By implementing L2TP (layer 2 tunneling protocol), PPTP (point to point tunneling protocol) and IPsec in VPN will gives us the solution to above problem. We can also apply encryption, authentication, and authorization policies for protection of communication.

Access control mechanism: In VPN dynamic remote management mechanism as context aware access control

(CAAC) can be used. This mechanism can activate security mechanism permission mechanism we have to do certain modification in application installer of android.

Firewall: By implementing firewall application on android we can analyze the application or malware behavior. We can analyze the outgoing traffic that is weather application already installed on device is sending content or data over network.

Certification: Certification of application is one of the solutions to application with malicious behavior. For certification every application is verified and checked before installation. But the cost requires verifying all applications is more.

Intrusion Detection system: By implementing IDS we can detect the malicious activities of application. Various intrusion detecting systems proposed earlier for ex: enhancing security with a self-built intrusion detection system. Such as connection encryption, message authentication etc.

3.5 Exploring vulnerabilities of kernel

Application on android can exploit the vulnerabilities in Linux kernel

Solution:

Security enhanced Linux is the only solution to the above problem.

4. METHODS USED FOR ATTACKING

4.1 Wireless

Various types of wireless attacks are there compromising the sensitive data of Smartphone. The most popular attack is eavesdropping on transmission media to get the password like sensitive information. Wireless attack can misuse the MAC address of device.

4.2 User based

User should know the fundamental of basic security mechanisms. Attacker can use different tricks to trap user's device. User should keep the confidential data in encrypted form. User should identify malicious links and trusted links to click and should know to keep their password secret.

4.3 Worm based

Smartphones have facilities with various connectivity tools. Worm based attack can be done through Bluetooth , downloading infected files , inserting infected memory card , email , SMS/MMS etc. Well known way to spread the worms is Bluetooth connection. Worms can also attack on networks and compromise the phone to use the network services.

4.4 Break in

In this attack the attacker find out the vulnerabilities in kernels core libraries, applications and break in. attacker can gain full control of device. For ex: Doom boot-this Trojan installs corrupted system libraries into C: drive of device.

4.5 Infrastructure based attack

In this type of attack the attacker attacks on services like making/receiving calls or SMS. This type of attack can happen in GSM, GPRS, UMTS, EDGE networks.

4.6Botnet

Android Smartphone can be part of botnets. Attacker can use Smartphone device as client/bots to attack other device or networks.

5. EFFECTS OF A VULNERABILITY ATTACK

- By using permission approved by user at the time of installation application can do malicious activities from the device such as infecting other device, scanning, sending spam or sniffing etc., Application can do these activities by exploiting vulnerabilities of core component of android.
- Hardware malfunctioning can occur.
- Entering into device by receiving email, spam, MMS/SMS.
- By remotely exploiting vulnerabilities of core component of android attacker can eavesdrops on communication, delete/alter/modify/corrupt the contents on device.
- Attacker can disable the functionalities of device by using permissions granted by user or do the same by exploiting vulnerabilities of core components.
- Attacker can misuse the services that costs the user such as making phone calls , sending SMS/MMS or diverting calls to high rate numbers by using permission granted or by exploiting vulnerabilities of core components exposed on network.
- Pushing adds while using the internet will interrupt while doing important work.
- Attacker can acquire full control of device
-

6. SECURITY TOOLS FOR SMART PHONES

- **Spam filter:**
  Spam Filter blocks MMS/SMS, calls and emails from unwanted users.

- **Selective android permission:**
  It provides greater security by granting selected permission to application. The tool called secure application interaction is available for this. But by using this applications will not work properly.

- **Login:**
  It provides screen locking by maintaining secret password by user. It prevents unauthorized use of device. It is inbuilt in android device.

- **Data encryption:**
  Encryption of content of device is done. It is available on android device now days. It prevents access to sensitive information.

- **Intrusion detection system:**
  Detect the malware, virus by abnormal behavior of phone. It prevents malware attacks to Smartphone. Andromaly, droidhunter tools are available for android. Also various intrusion detection/prevention systems were proposed by various researchers over the years like host based IDS, Behavior based IDS etc.

- **Antivirus :**
  This tool scans memory, files, emails, scripts, SMS/MMS for virus, worms, root kits, malware etc. to prevent attacks or malicious activities. Droidhunter, mocana, Smobile antivirus etc. tools are available for android.

- **Resource management:**
  This system allows managing the resources such as memory, CPU, disk space, networks, I/O etc. by allocating them to various applications on the phone fairly. It can prevent DNS attack. No such tool is available as such.

- **Firewall:**
  It can check the traffic going or coming to phone. It can check each and every packet. It prevents various types of network attack. Smobile, netfilter/Iptable is available tools for android but they work with certain dependencies.

- **Application certification:**
- It provides signatures that signs applications by certificate authority. It can prevent damage from untrusted applications. The open mobile terminal platform's application security framework tool is available for android.

7. CONCLUSION

Smartphones have become a very essential part of everybody's life. Smartphone has lot of personal information about the user. Smartphones have made individual's life easy. But at the same time there is much vulnerability also. There are many ways in which data present in the Smartphone can be lost or damaged. There are tools available by which loss of data can be prevented.

REFERENCES

[1]. La Polla. M., Martinelli. F., Sgandurra, D., "A Survey on Security for Mobile Devices," Communications Surveys Tutorials, IEEE, vol.15, no.1, pp.446, 471, First Quarter 2013'

[2]. Lei Zhang, Jiangchuan Liu, Hongbo Jiang, Yong Guan, "SensTrack: Energy-Efficient Location Tracking With Smartphone Sensors," Sensors Journal, IEEE, vol.13, no.10, pp.3775,3784, Oct. 2013'

[3]. Jilong Liao, Zhibo Wang , Lipeng Wan , Cao, Q.C. , Hairong Qi "Smart Diary: A Smartphone-based Framework for Sensing, Inferring and Logging Users Daily Life", IEEE Sensors Journal'

[4]. Yanni Li, Zhijuan Li, Zheng Lv, Haopeng Sun "An analysis of internet accounts security threats by mobile phone password protection", Journal of Chemical and Pharmaceutical Research, 2014, 6(7):2477-2483'

[5]. SOPHOS Security Threat Report 2013' Impact of Smartphones on Society, European Journal of Scientific Research ISSN 1450-216X / 1450-202X Vol. 98 No 2 March, 2013, pp.216-226'

[6]. Ildar Muslukhov, "Survey: Data Protection in Smartphones Against Physical Threats"

BIOGRAPHIES

Shakuntala P. Kulkarni received her Bachelor of Engineering degree in 2012 from University of Mumbai. Since 2013 she has been working towards Master of Engineering degree from University of Mumbai.

Mr. Sachin Bojewar has 25 years of rich teaching experience and is currently working as an Associate Professor in Vidyalankar Institute of Technology