SECURITY AND HACKING

Mobile security is the protection of smartphones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing.

GENERAL SECURITY ISSUES

• Confidentiality

• Integrity

• Availability

• Legitimate

• Accountability

WIRELESS SECURITY ISSUES

Wireless security issues are considered as the primary security issues of mobile computing. These are related to wireless networks. These issues occur when the hackers intercept the radio signals. Most wireless networks are dependent on other private networks, which are managed by others, so after these issues, the users have less control of security procedures. These security issues are:

DENIAL OF SERVICE (DOS) ATTACKS

• The denial of services or DOS attacks is one of the most common attacks of all kinds of networks and especially in a wireless network.

• It prevents users from using network services because the attacker sends a large amount of unnecessary data or connection requests to the communication server.

• It causes a slow network, and therefore the users cannot get benefitted from using its service.

TRAFFIC ANALYSIS

• Traffic analysis is used to identify and monitor communication between users.

• In this process, the service provider listens the traffic flowing in the wireless channel to access the private information of users affected by the attacker.

EAVESDROPPING

• It specifies that the attacker can log on to the wireless network and access sensitive data if

the wireless network was not secure enough. This can also be done if the information is not

encrypted.

SESSION INTERCEPTION AND MESSAGES MODIFICATION

• It specifies that the attacker can intercept the session and modify the transmitted data in this session. This scenario is called “man in the middle “. It inserts the attacker’s host between the sender and receiver host.

SPOOFING

• In this security issue, the attacker impersonates him as an authorized account of another user and tries to access the sensitive data and unauthorized services.

CAPTURED AND RETRANSMITTED MESSAGES

• In this security issue, the attacker can get some of the network services by getting unauthorized access. After capturing the message, he/she can reply to it with some modifications to the same destination or another.

DEVICE SECURITY ISSUES

Following is a list of some mobile computing security issues we face using mobile devices:

PUSH ATTACKS

In the push attack, the attacker creates a malicious code at the user’s mobile device by hacking it and then he/she may spread it to affect other elements of the network.

PULL ATTACKS

The pull attack is a type of attack where the attacker controls the device and handles it in his/her way. He can decide which emails they want to receive. In this attack, the user can decide about the obtained data by the device itself.

FORCED DE-AUTHENTICATION

In this security issue, the attackers convince the mobile end-point or the mobile user to drop its connection and re-connection to get a new signal. Within this process, they insert their device between the mobile device and the network and steal the information or do the fraud.

MULTI-PROTOCOL COMMUNICATION

The multi-protocol communication provides the ability of many mobile devices to operate using multiple protocols. For example, A cellular provider’s network protocol. Most of the protocols have some security loopholes, which help the attacker to exploit this weakness and access to the device.

MOBILITY

This security issue may occur because of the mobility of the users and the mobile devices. You may face these security threats due to a users location, so you must replicate the user profiles at different locations to allow roaming via different places without any concern regarding access to personal and sensitive data in any place and at any time. This repetition of sensitive data on different sites can increase seethe chances of security threats.

DISCONNECTIONS

These types of security issues occur when mobile devices go to different places. It occurs in the form of frequent disconnections caused by external parties resulting in the handoff.

HACKING

Phone hacking involves any method where someone forces access into your phone or its communications.

This can range from advanced security breaches to simply listening in on unsecured internet connections. It can also involve physical theft of your phone and forcibly hacking into it via methods like brute force. Phone hacking can happen to all kinds of phones, including Androids and iPhones

HOW TO KNOW IF SOMEONE IS HACKING YOUR PHONE

One or more of these could be a red flag that some has breached your phone:

Your phone loses charge quickly. Malware and fraudulent apps sometimes use malicious code that tends to drain a lot of power.

Your phone runs abnormally slowly. A breached phone might be giving all its processing power over to the hacker‘s shady applications. This can cause your phone to slow to a crawl.

Unexpected freezing, crashes, and unexpected restarts can sometimes be symptoms.

You notice strange activity on your other online accounts. When a hacker gets into your phone, they will try to steal access to your valuable accounts. Check your social media and email for password reset prompts, unusual login locations or new account signup verifications.

You notice unfamiliar calls or texts in your logs. Hackers may be tapping your phone with an SMS trojan.

Alternatively, they could be impersonating you to steal personal info from your loved ones. Keep an eye out, since either method leaves breadcrumbs like outgoing messages.

ANDROID HACKING TOOLS / ANDROID HACKING APPS

In addition to manual coding, there are many applications built around hacking Android

systems. These range from apps targeted at end users who want to extend their Android devices battery life or customize other parts of its operating system to deep system hacks used by more sophisticated hackers and attackers.

Here are a few of the most popular:

• Apktool – This tool is used for reverse engineering third party, closed, binary

Android applications.

• Dex2jar – This widely available tool works with Android .dex and Java .class files,

enabling the conversion of one binary format to another.

• JD-GUI – This is a graphic utility tool that stands alone and displays Java sources from

.class files.

THE THREE BIGGEST THREATS TO ANDROID DEVICES

Threat One: Data in Transit Mobile devices, including those running Android as an operating system, are susceptible to man- in-the- middle attacks and various exploits that hack into unsecured communications over public Wi-Fi networks and other wireless communication systems.

Threat Two: Untrustworthy App Stores Untrustworthy app stores can cause headaches due to lack of security protocols. Ensure that your app store of choice for Android applications takes adequate security precautions and has a strong security review program in place.

Threat Three: SMS Trojans Malicious apps can sometimes include SMS trojans, which come in the form of compromised applications.

This type of app accesses a mobile devices calling or text message capabilities, allowing them to do things like send text messages with malicious links to everyone in a users address book. These links can then be used by attackers to distribute computer worms and other malicious messages to fee-based services, incurring fees on behalf of the user and profiting scammers.

THREE WAYS TO PROTECT YOUR ANDROID DEVICES

Use TLS Encryption

OWASP shows that insufficient encryption is a big problem for many types of applications. By using Transport Layer Security (TLS), you can encrypt internet traffic of all types for securely generating and exchanging session keys. This protects data against most man-in-the-middle and network spying attacks.

Test Third-Party App Security

The best way to avoid malicious apps is to only use apps from the official Google Play store. Google Play uses significantly better security checks than third-party sites, some of which may contain hundreds of thousands of malicious apps. If you absolutely need to download an app from a third-party store, check its permissions before installing, and be on the lookout for apps which that for your identity or the ability to send messages to your contacts when they don't need to.

Use Caution When Using SMS Payments

Set your Android phone to limit the ability of apps to automatically spend your money. Apps that ask for payment via SMS are a red flag and should be avoided if at all possible.