CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

INSTITUTE : UIE

DEPARTMENT : CSE

Bachelor of Engineering (Computer Science & Engineering)

WEB AND MOBILE SECURITY (Professional Elective-I)

(20CST/IT-333)

TOPIC OF PRESENTATION:

Mobile application: Mobile Malware and App Security.

Lecture Objectives

In this lecture, we will discuss:
•Mobile application: Mobile Malware and App Security

Mobile Malware

- Mobile malware is malicious software specifically designed to target mobile devices, such as smartphones and tablets, with the goal of gaining access to private data.
- Although mobile malware is not currently as pervasive as malware that attacks traditional workstations, it's a growing threat because many companies now allow employees to access corporate networks using their personal devices, potentially bringing unknown threats into the environment.
- The most common method hackers use to spread malware is through apps and downloads. The apps you get at an official app store are usually safe, but apps that are "pirated," or come from less legitimate sources often also contain malware.

Different Types of Mobile Malware

1. Spyware and Madware

- Madware is a combination of the words mobile and adware.
- Adware is typically created for computers but can also be found on mobile devices.
- Adware is unwelcome software that infiltrates a computer and serves up annoying advertising materials. Mobile adware is intrusive advertising on a smartphone or tablet. There are two methods through which mobiles come down with adware: through the browser and through downloaded applications.
- Currently, most madware exists for Android smartphones and tablets due to Android's open platform and its worldwide market share — approximately 72% of mobile operating systems are Android.
- To get madware on your device is by downloading a free app from an app store.
- Once installed, madware creators hope you'll click on an advertisement, whether that's on purpose or on accident.
- When you click on madware, madware creators get paid by how many views the ad gets, how many clicks the ad gets, or how many times the software is added to a device.

https://gs.statcounter.com/os-market-share/mobile/worldwide

- Madware—is not a virus, however, madware can slow down your phone and make it prone to crashing, snarling workplace efficiency and potentially exposing your network to other threats.
- Most madware variants usually include an element of spyware, which collects information about your internet usage and sends it on to a third party.

Together, madware and spyware can:

- Collect user data, including location and search history, and anything else you type on your keyboard like your passwords and your contacts.
- Display unwanted ads in your notification bar.
- Add icons or shortcuts to your screen.
- Replace your ringtone with an audio ad.

2. Drive-by Downloads

- Unintentional download of malicious code to your computer or mobile device that leaves you open to a cyberattack like you open the wrong email or visit a malicious website.
- A drive-by download can take advantage of an app, operating system, or web browser that contains security flaws due to unsuccessful updates or lack of updates.
- These variants are automatically installed on your device and can unleash a range of threats, including spyware, malware, adware or something much more serious such as a bot that can use your mobile device to perform nefarious tasks like sending viruses to other people within your organization or scanning the network for a way in.

Drive by downloads are designed to breach your device for one or more of the following:

- **Hijack your device** — to build a botnet, infect other devices, or breach yours further. Botnets are networks of hijacked computer devices used to carry out various scams and cyberattacks. The term “botnet” is formed from the word's “robot” and “network.”
- **Spy on your activity** — to steal your online credentials, financial info, or identity.
- **Ruin data or disable your device** — to simply cause trouble or personally harm you.

Proper security software or fixes for your vulnerabilities

3. Viruses and Trojans

- Trojans/viruses **act as legitimate applications and infect your phone once the app has been installed**. Unlike worms, Trojans need a user to install them before they can carry out their actions
- A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data. Trojan Horse is a form of malware that capture some important information about a computer system or a computer network
- These viruses may: changing your phone's wallpaper or changing the language. However, most have something much more malicious in mind like mining for passwords and banking information.
- Once activated, Trojans can **infect and deactivate other applications or the device itself and paralyze the device after a certain period of time or a certain number of operations**.
- Banking Trojans target both international and regional banks by using fake versions of legitimate mobile apps.

4. Mobile Phishing

- Traditional phishing techniques involve criminals sending emails to users that appear to originate from a trusted source.
- Mobile phishing takes this tactic one step further and uses applications to deliver mobile malware. The user, often unable to tell the difference between a legitimate application and a fake application is none the wiser as the fake application collects account numbers, passwords and more.
- Smishing involves criminals sending text messages (the content of which is much the same as with email phishing), and vishing involves a telephone conversation.

5. Browser Exploits

- A browser exploit is a form of malicious code that **takes advantage of a flaw or vulnerability in an operating system or piece of software with the intent to breach browser security to alter a user's browser settings without their knowledge**.
- If a user is using a web browser with a particular vulnerability, and visits a malicious or compromised site, a browser exploit could take advantage of the browser vulnerability to send malicious code to the browser, with the aim of accessing personal information, delivering malware

How to Protect Against Mobile Malware

- **Keep applications updated**: By running the newest version of every application on your mobile phone, you can ensure that you are running the version with the latest security patches and updates.
- **Install mobile security software**: Just like antivirus software protects a computer from viruses and malware, a mobile security application will do the same thing.
- **Consider a firewall**: Firewalls not only protect your online privacy when browsing, but can be used to only allow authorized apps to access the internet through a set of firewall rules.
- **Use screen lock protection**: Many mobile devices are compromised when they are lost and stolen. Ensure at the very least that a passcode is used to lock the screen. Even better, use facial recognition or fingerprint recognition technology.
- **Only download apps from official stores**: All vets available on the Apple App Store and Google Play have been vetted to ensure they are safe. That doesn't mean that no app will slip through the net, but you have a much better chance of installing a legitimate app through office sources.

References:

Books:

1. Hacking Exposed Mobile: Security Secrets & Solutions 1st Edition, Kindle Edition, by Neil Bergman, Mike Stanfield, Jason Rouse, and Joel Scambray
2. Hacking Exposed Web Applications, 3rd edition, Joel Scambray, Vincent Liu, Caleb Sima, Released October 2010, Publisher(s): McGraw-Hill

Video Lectures :

1. https://www.crowdstrike.com/cybersecurity-101/malware/mobile-malware/
2. https://www.techtarget.com/searchmobilecomputing/definition/mobile-malware

Reference Links:

1. https://www.crowdstrike.com/cybersecurity-101/malware/mobile-malware/
2. https://www.freecodecamp.org/news/how-to-secure-mobile-apps/
3. https://www.geeksforgeeks.org/difference-between-virus-and-trojan-horse/#:~:text=1.-,A%20Virus%20is%20a%20malicious%20executable%20code%20attached%20to%20another,system%20or%20a%20computer%20network.

THANK YOU