



Understanding of Mobile Hacking with existing vulnerabilities



Department of Computer science, Kean University, Union, NJ

By Komal Sharma with Dr. Jing-Chiou Liou (Advisor)

Introduction

In this project we study current Mobile security problems. Mobile devices are used for our most sensitive transactions, including email, banking, and social media. But they have a unique set of vulnerabilities, which hackers are all too willing to exploit.

We need to know how to close the gaps and protect devices, data, and users from attacks.

Ensure the Security

- To ensure the highest mobile shopping security, you should follow these steps:
- Download authorized apps from Apple and Google stores only.
- Ignore the apps that want to access your contact, message and also requires a password.
- If the developer is untrusted and unusual, do not use their apps.
- Always see the warning message while you download any app.
- Keep your device updated with the latest OS.
- Do not use public Wi-Fi without any serious reason and use VPN.
- Only browse “HTTPS” e-commerce sites. Because they have security encryption.

Mobile Threats

- Bluetooth
- Wifi
- App cracked
- Root Access(super Admin)
- Data Storage
- Internet
- Mobile Adware Pop-Ups
- Mobile Spyware Programs
- Wireless Sniffers & Signal Jammers

Mobile Platform

- Android – It is the biggest and by far most popular. So it is also the biggest target.
- iOS – The next biggest platform is Apple’s iOS. It seems to be more secure than Android.
- Windows – Windows Mobile which is now known as Windows 10. Its market share is reducing day by day.
- BlackBerry – It is not used much nowadays.

Mobile Vulnerabilities

- Operating System – The first vulnerability is actually found in the Operating System. There are specific vulnerabilities in each OS that bad actors exploit to gain access or implant malware, etc.
- Apps / App Stores – There are a few rogue app stores that hackers have put out into the market from people download malicious apps.
- Malware – There are malwares that are specifically written for mobile platforms and perform activities like blocking device, data stealing, send SMS or spoof email, etc.
- “Jail Breaking” – It is also known as rooting. In the attacker try to get access to the actual OS.
- Privacy – Mobile device is a personal property and if it gets compromised in any form it is a big privacy mobile vulnerability.
- Physical Theft – Because of the size and portability property of a mobile device, it can be easily stolen and the whole device is automatically compromised.