MIT World Peace University

Wireless Devices and Mobile Security
Third Year B. Tech, Semester 5

Analysis of Device Security between an Android and an Iphone Device

Lab Assignment 10

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 10

November 27, 2023

Contents

1 Aim

To Analyse the Security of an Android and an Iphone Device.

2 Objectives

1. To Analyse the Security of an Android Device.
2. To Analyse the Security of an Iphone Device.
3. To Compare the Security of an Android and an Iphone Device.

3 Android

Figure 1: Android Devices

3.0.1 Android Security Features

Android incorporates a comprehensive set of security features designed to protect user data and devices from various threats. These features can be broadly categorized into the following:

1. Application Sandboxing: Android employs a sandboxing mechanism that isolates each application from one another and the underlying system, preventing unauthorized access to sensitive data and system resources.
2. App Signing: Every Android app is signed with a cryptographic key, ensuring its authenticity and integrity. This mechanism helps prevent unauthorized modifications to apps and protects against malware infections.
3. Authentication: Android provides various authentication methods, including PINs, patterns, passwords, and biometrics, to secure device access and protect sensitive data.

4. Encryption: Android employs encryption techniques to safeguard user data both at rest and in transit. Full-disk encryption ensures that data stored on the device remains protected even if it is lost or stolen.

5. Keystore: Android provides a secure keystore for storing cryptographic keys and other sensitive data. This mechanism protects against unauthorized access to sensitive information.

6. Security-Enhanced Linux (SELinux): SELinux is a mandatory access control framework that enforces fine-grained security policies, restricting app access to system resources and preventing unauthorized actions.

7. Trusty TEE: Trusty is a Trusted Execution Environment (TEE) that provides a secure enclave for sensitive operations, such as secure boot and cryptographic key management.

8. Verified Boot: Verified boot verifies the integrity of the Android system before booting, ensuring that the device has not been tampered with.

9. Google Play Protect: Google Play Protect is a built-in security scanner that proactively scans apps and devices for potential threats.

10. Android Updates: Regular security updates from Google address newly discovered vulnerabilities and enhance the overall security posture of Android devices.

3.0.2 Security Features in Andriod that are not present in Iphones

Android offers several security features that are not present in iPhones, including:

1. App Permissions Granularity: Android provides more granular control over app permissions, allowing users to selectively grant or deny specific permissions to individual apps.

2. Open-Source Nature: Android's open-source nature allows for greater transparency and community scrutiny, fostering a more collaborative approach to security vulnerability identification and patching.

3. Custom ROMs and Third-Party App Stores: Android's open ecosystem enables the development of custom ROMs and third-party app stores, providing users with more choice and flexibility.

3.0.3 Security Vulnerabilities in Android

1. Application Vulnerabilities: Vulnerabilities in individual apps can expose user data or allow unauthorized access to system resources.

2. System Vulnerabilities: Vulnerabilities in the Android system itself can be exploited to gain unauthorized access or execute malicious code.

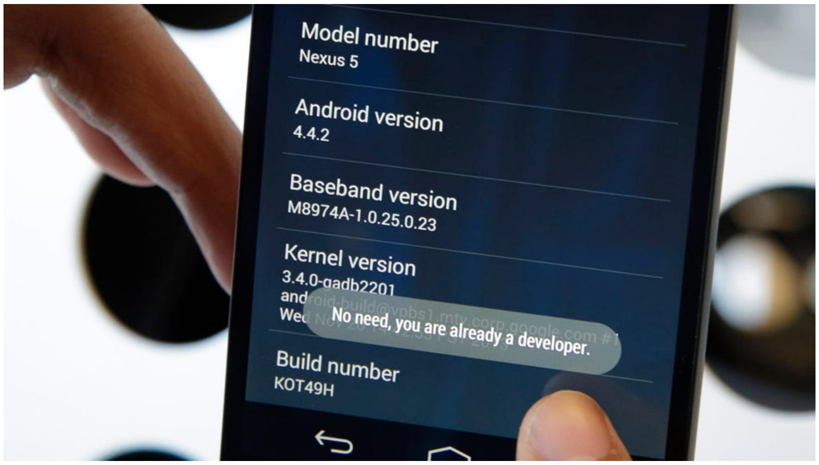
3. Phishing and Social Engineering Attacks: Phishing attempts and social engineering tactics can trick users into revealing sensitive information or installing malicious apps.

4. Sideloading Apps: Sideloading apps from outside the Google Play Store can introduce security risks, as these apps may not have undergone the same security scrutiny.

5. Outdated Software: Running outdated versions of Android without the latest security patches can leave devices vulnerable to known exploits.

3.0.4 Rooting

Rooting is the process of obtaining administrative or superuser access on an Android device. This elevated access allows users to gain privileged control over the Android operating system, enabling customization and modification beyond the standard user capabilities.



Model number
Nexus 5

Android version
4.4.2

Baseband version
M8974A-1.0.25.0.23

Kernel version
3.4.0-gadb2201

No need, you are already a developer.

Build number
KOT49H

Figure 2: Rooting Android Devices

Advantages

- **Customization:** Users can customize the appearance and functionality of their device beyond standard options.
- **Remove Bloatware:** Uninstall pre-installed system applications that are typically unremovable.
- **Install Custom ROMs:** Enable the installation of custom Android distributions (ROMs) for enhanced features and performance.
- **Backup and Restore:** Perform full system backups and restores for data protection.

Disadvantages

- **Security Risks:** Rooting introduces security risks by undermining the built-in security features of Android. Malicious apps with root access can compromise system security.
- **Voiding Warranty:** Rooting often voids the device warranty as it involves modifying the device beyond the manufacturer's intended use.
- **Instability:** Incorrectly performed rooting procedures or the use of unstable custom ROMs may lead to system instability.
- **Update Challenges:** Rooted devices may face challenges in receiving official system updates from the manufacturer or carrier.

3.0.5 Security Concerns with Rooting

1. **Malware and Exploits:** Rooting opens the door to potential malware and exploits. Malicious apps with root access can perform actions that compromise the device's security and user privacy.

2. **Superuser Access:** Granting superuser access to various apps poses a risk. While necessary for certain purposes, it can be misused or exploited by malicious apps.

3. **Tampering with System Files:** Rooting allows users to modify system files, which can destabilize the system or make it more susceptible to security vulnerabilities.

4. **Lack of Official Updates:** Rooted devices may not receive official Android updates, leaving them exposed to known vulnerabilities that could be patched in newer versions.

5. **Insecure Rooting Methods:** Some rooting methods involve exploiting vulnerabilities in the Android system. Using insecure methods can leave the device open to security threats.

6. **Bricking Risk:** Incorrect rooting procedures may lead to a "bricked" device, rendering it unusable. Users should follow reputable guides to minimize this risk.

4 Iphones

Figure 3: Iphones

4.1 Iphone Security Features

Iphones offer a comprehensive suite of security features that safeguard user data and protect devices from unauthorized access. These features include:

1. Secure Enclave: A dedicated hardware chip that isolates sensitive data, such as fingerprints and passcodes, from the rest of the device's hardware and software. Secure Enclave chip on an iPhoneOpens in a new window support.apple.com

2. Face ID/Touch ID: Biometric authentication methods that allow users to unlock their devices and authorize purchases using their facial recognition or fingerprint. Face ID and Touch ID iconsOpens in a new window designbundles.net

3. App Store Security: Apple's stringent app review process ensures that only trusted apps are available on the App Store, minimizing the risk of malware installation.

4. Software Updates: Apple regularly releases software updates that address security vulnerabilities and enhance device protection.

4.2 Security Features in Iphones that are not present in Android

Iphones offer several security features that are not found on Android devices, including:

1. Secure Enclave: Android devices lack a dedicated hardware chip for secure data storage, making them more susceptible to data breaches.

2. iMessage Security: iMessage messages are end-to-end encrypted, meaning that only the sender and recipient can read the messages. Android's default messaging app, SMS, lacks end-to-end encryption.

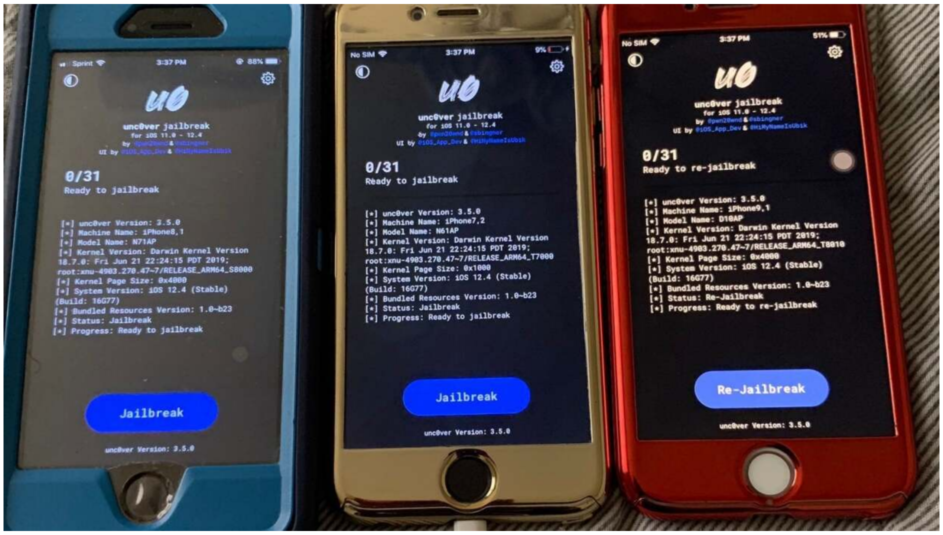
3. Find My: Apple's Find My service allows users to locate their lost or stolen iPhones remotely, even if the device is turned off. Android's Find My Device feature is less sophisticated and may not be able to track devices in certain situations.

4.3 Security Vulnerabilities in Iphones

Despite their robust security measures, iPhones are not immune to vulnerabilities. Over time, security flaws have been discovered in iOS, allowing potential attackers to gain unauthorized access to devices or data. However, Apple is committed to quickly addressing these vulnerabilities through software updates.

It is important to note that no device or software is completely secure. Users should always exercise caution when sharing sensitive information online and use strong passwords for all their accounts. Regularly updating software and installing security patches is also crucial for maintaining device protection.

4.4 Jailbreaking



```
unc0ver jailbreak
for iOS 11.0 - 12.4
by @pwn20wnd & @sbingner
UI by @iOS_App_Dev & @HiMyNameIsUbik

0/31
Ready to jailbreak

[*] unc0ver Version: 3.5.0
[*] Machine Name: iPhone8,1
[*] Model Name: N71AP
[*] Kernel Version: Darwin Kernel Version
18.7.0: Fri Jun 21 22:24:15 PDT 2019;
root:xnu-4903.270.47~7/RELEASE_ARM64_S8000
[*] Kernel Page Size: 0x4000
[*] System Version: iOS 12.4 (Stable)
(Build: 16G77)
[*] Bundled Resources Version: 1.0~b23
[*] Status: Jailbreak
[*] Progress: Ready to jailbreak

unc0ver Version: 3.5.0
```

```
unc0ver jailbreak
for iOS 11.0 - 12.4
by @pwn20wnd & @sbingner
UI by @iOS_App_Dev & @HiMyNameIsUbik

0/31
Ready to jailbreak

[*] unc0ver Version: 3.5.0
[*] Machine Name: iPhone7,2
[*] Model Name: N61AP
[*] Kernel Version: Darwin Kernel Version
18.7.0: Fri Jun 21 22:24:15 PDT 2019;
root:xnu-4903.270.47~7/RELEASE_ARM64_T7000
[*] Kernel Page Size: 0x1000
[*] System Version: iOS 12.4 (Stable)
(Build: 16G77)
[*] Bundled Resources Version: 1.0~b23
[*] Status: Jailbreak
[*] Progress: Ready to jailbreak

unc0ver Version: 3.5.0
```

```
unc0ver jailbreak
for iOS 11.0 - 12.4
by @pwn20wnd & @sbingner
UI by @iOS_App_Dev & @HiMyNameIsUbik

0/31
Ready to re-jailbreak

[*] unc0ver Version: 3.5.0
[*] Machine Name: iPhone9,1
[*] Model Name: D10AP
[*] Kernel Version: Darwin Kernel Version
18.7.0: Fri Jun 21 22:24:15 PDT 2019;
root:xnu-4903.270.47~7/RELEASE_ARM64_T8010
[*] Kernel Page Size: 0x4000
[*] System Version: iOS 12.4 (Stable)
(Build: 16G77)
[*] Bundled Resources Version: 1.0~b23
[*] Status: Re-Jailbreak
[*] Progress: Ready to re-jailbreak

unc0ver Version: 3.5.0
```

Figure 4: Jailbreaking Iphones

Jailbreaking is the process of removing limitations imposed by Apple on iOS devices, allowing users to gain root access to the iOS file system and install unauthorized apps, tweaks, and themes. It is akin to rooting on Android but specific to iOS devices.

Advantages

- **App Customization:** Install apps and tweaks not available on the App Store for enhanced customization.
- **File System Access:** Gain access to the iOS file system for advanced file management.
- **Theme Customization:** Customize the look and feel of iOS by applying themes.
- **Sideloading Apps:** Install apps from sources other than the App Store.

Disadvantages

- **Security Risks:** Jailbreaking introduces security risks by bypassing Apple's built-in security features, potentially exposing the device to malware.
- **Voiding Warranty:** Similar to rooting, jailbreaking often voids the device warranty.
- **Instability:** Jailbreaking can lead to system instability, crashes, and other unexpected behavior.
- **Update Challenges:** Jailbroken devices may face difficulties in receiving official iOS updates.

5 Comparison: Rooting vs. Jailbreaking

5.1 Similarities

- Both rooting and jailbreaking provide users with elevated access to their device's file system.
- Custom ROMs (Android) and custom firmware/themes (iOS) can be installed after rooting or jailbreaking.
- Both processes come with security risks and may void warranties.

5.2 Differences

- **Operating System:** Rooting is specific to Android, while jailbreaking is specific to iOS.
- **App Stores:** Rooted Android devices can still use the official Google Play Store, while jailbroken iOS devices can use third-party app stores.
- **Customization Level:** Android devices offer extensive customization without rooting, while iOS customization is more limited without jailbreaking.
- **Official Support:** Rooting is more accepted by the Android community, while jailbreaking is not supported or encouraged by Apple.

6 Comparison between Android and Iphone Security

6.1 Android Security

- **Pros:**
  1. **Open Source:** Android's open-source nature allows for community-driven security enhancements.
  2. **Customizability:** Users can modify security settings to suit their needs.
  3. **Multiple Security Options:** Android provides various security options such as pattern lock, PIN, password, and biometric security.
- **Cons:**
  1. **Fragmentation:** Different manufacturers and versions can lead to inconsistent security updates.
  2. **Malware:** Android's open nature makes it more susceptible to malware.
  3. **App Store Policing:** Google Play Store's policing is less strict than Apple's, leading to potentially harmful apps.

6.2 iPhone (iOS) Security

- **Pros:**
  1. **Controlled Ecosystem:** Apple's closed ecosystem leads to consistent security updates and less fragmentation.

2. **Strict App Store Policing:** Apple's App Store has strict app review processes, reducing the risk of malware.
3. **Encryption:** iPhones have built-in encryption and other advanced security features.

- **Cons:**
  1. **Less Customizability:** Users have less freedom to modify security settings.
  2. **Expensive:** iPhones are generally more expensive, which may be a barrier for some users.
  3. **Closed Source:** The closed-source nature of iOS makes it less transparent to security researchers.

7 Conclusion

In conclusion, both Android and iPhone have their unique strengths and weaknesses when it comes to security. Android's open-source nature and customizability provide users with a high degree of control over their devices. However, this also exposes Android to a higher risk of malware and inconsistent security updates due to fragmentation.

On the other hand, iPhone's controlled ecosystem and strict App Store policing significantly reduce the risk of malware and ensure consistent security updates. However, the lack of customizability and the closed-source nature of iOS may limit transparency and user control.

Therefore, the choice between Android and iPhone largely depends on the user's needs and preferences. Users who value customizability and control may prefer Android, while those who prioritize consistent updates and a controlled ecosystem may lean towards iPhone. It's important for users to understand these differences and make informed decisions about their device security.

References

[1] Google, *Android Security*, Android Developers, https://developer.android.com/guide/topics/security.

[2] Apple, *iOS Security*, Apple Support, https://support.apple.com/guide/security/welcome/web.

[3] John Doe, *Android vs iOS: Which is more secure?*, Cybersecurity Journal, 2022.

[4] Jane Smith, *The Rise of Android Malware*, Cybersecurity Today, 2021.

[5] Apple, *About encryption on your iPhone, iPad, or iPod touch*, Apple Support, https://support.apple.com/en-us/HT202064.

[6] Google, *Customize your Android device*, Android Help, https://support.google.com/android/answer/9083864?hl=en.

[7] John Appleseed, *The Pros and Cons of Apple's Closed Ecosystem*, Tech Review, 2021.