

1) What is Android SafetyNet attestation, and how does it enhance security?

- a. Android SafetyNet attestation is a method used to bypass security measures on Android devices, allowing unauthorized access to protected data and services
- b. Android SafetyNet attestation is a feature that enables users to clone and replicate their Android devices, allowing them to use multiple instances of the same device simultaneously
- c. Android SafetyNet attestation is a feature that verifies the integrity and compatibility of an Android device's operating system and software, ensuring a secure environment for sensitive applications

2) Select the wrong statement

- a. Verify Apps (Google Play Protect) is a system-level security feature that scans and protects against potentially harmful or malicious apps on the Google Play Store
- b. SafetyNet Attestation helps protect sensitive applications by ensuring they run on trusted devices and protecting against potential attacks
- c. SafetyNet Attestation and Verify Apps are both security features provided by Google for Android devices, but they serve different purposes

Safetynet runs at the physical layer while the other runs at the application layer. Safetynet checks also for hardware components if they were compromised. The other one is wrong because it runs on the device locally, so it's scanned there.

3) What is Project Treble, and how does it impact Android device updates?

- a. Project Treble is a program that allows Android users to customize the appearance and layout of their device's user interface, providing a more personalized experience.
- b. Project Treble is an architectural change in the Android operating system that separates the vendor implementation from the core Android framework. It simplifies the process of delivering Android updates to devices by enabling faster and more frequent updates from manufacturers.
- c. Project Treble is a feature that improves battery life on Android devices by optimizing power consumption and managing background processes efficiently.

4) Which one is an example of MAC on Android?

- a. App Permissions
- b. File System Permissions
- c. SELinux policies

5) What is the role of SELinux in Android, and how does it enhance the operating system's security?

- a. SELinux in Android is a security mechanism that enforces discretionary access control policies, limiting the actions and permissions of processes and applications based on their security contexts.
- b. SELinux in Android is a security mechanism that enforces mandatory access control policies, limiting the actions and permissions of processes and applications based on their security contexts.

- c. SELinux in Android is a feature that scans and detects malicious apps on the device, providing real-time protection against potential security threats.

6) Which one is NOT a direct consequence of unlocking the Android bootloader?

- a. compromise the device hardware components
- b. exploiting a vulnerability to install malware that can compromise the device's security
- c. running untrusted software that may contain security vulnerabilities

7) What is Android TrustZone, and how does it contribute to the security of the operating system?

- a. Android TrustZone is a hardware-based security extension that provides a secure execution environment for handling sensitive operations and storing sensitive data.
- b. Android TrustZone is a security mechanism that prevents unauthorized access to the device by encrypting all data stored on the device's internal storage.
- c. Android TrustZone is a feature that enables users to securely transfer files between Android devices using encrypted communication channels.

As seen by slides, this is basically an ARM feature, depending on the architecture.

8) What is defense in depth?

- a. cybersecurity strategy that involves implementing multiple layers of security controls to protect against the different threats
- b. cybersecurity strategy that involves implementing multiple layers of security controls to protect against the same threat
- c. a vulnerability scanning tool