Device Integrity White Paper

Authors:

Sonali Rajpure
Ghanshyam Ahire

Table of Contents

1. Overview

A few years ago, mobile devices were primarily used for calls and SMS communication. Today, they serve a much broader purpose, encompassing social, business, financial, and personal applications that contain sensitive user data, including financial information.

Mobile devices have become the primary medium for information consumption, and the mobile app market is expanding at an unprecedented rate. With this evolution, user expectations have increased in terms of simplicity, clarity, security, and intuitiveness.

Ensuring device security is critical, as mobile devices are increasingly targeted by cyber threats. A security application must verify that a device is protected against malicious apps, unsafe environments, and unauthorized modifications. Additionally, wireless networks such as Wi-Fi, though essential for connectivity, can be highly vulnerable to attacks if not properly secured. Implementing strong security measures is necessary to protect sensitive user information from cyber threats.

Device Integrity is a crucial feature that ensures a mobile device's environment is free from vulnerabilities, providing protection against malware, fraudulent activities, and network attacks. Organizations and government agencies, especially with the rise of remote work, face new security challenges that necessitate robust device integrity mechanisms.

2. Introduction

Device Integrity is an essential security feature that protects mobile devices from vulnerabilities, unauthorized modifications, and insecure networks. This feature actively scans the device environment, identifying security threats that could compromise sensitive data.

A device is considered secure when its environment remains unchanged from its manufacturer settings, ensuring that applications, including payment apps, operate in a safe ecosystem. Furthermore, wireless security measures protect users from unauthorized network access and data interception, maintaining overall device integrity.

3. What is Device Integrity?

Device Integrity is an essential security feature that protects mobile devices from vulnerabilities, unauthorized modifications, and insecure networks. This feature actively scans the device environment, identifying security threats that could compromise sensitive data.

A device is considered secure when its environment remains unchanged from its manufacturer settings, ensuring that applications, including payment apps, operate in a safe ecosystem. Any modification to the device’s operating system, such as rooting, jailbreaking, or bootloader unlocking, can expose the device to security risks, making it more vulnerable to cyber threats.

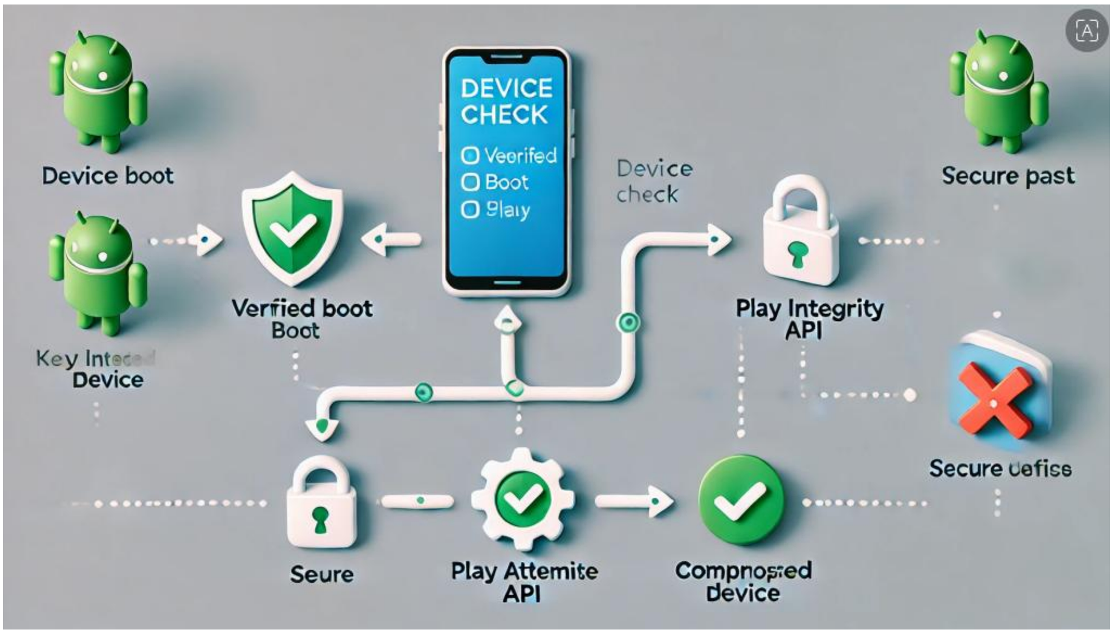
Device Integrity solutions employ advanced security mechanisms to detect and prevent such unauthorized modifications. By implementing real-time monitoring and security checks, these solutions help users maintain a trusted device environment. Additionally, device integrity assessments can detect signs of tampering, malware injection, or unauthorized system-level access, ensuring the integrity of applications and sensitive data stored on the device.

Furthermore, wireless security measures play a significant role in maintaining device integrity. Public and unsecured Wi-Fi networks pose a major security risk by allowing cyber criminals to intercept user data, launch man-in-the-middle attacks, or inject malicious payloads. Device Integrity solutions mitigate such threats by assessing Wi-Fi network security, alerting users to unsafe networks, and preventing connections to potentially compromised access points.

By leveraging robust security technologies, Device Integrity features provide users with a secure digital ecosystem where personal and financial data remain protected from emerging cyber threats.

4. Importance of Device Integrity

- **Prevents Fraud**: Blocks access from modified environments.
- **Enhances Security**: Protects sensitive user data and app logic.
- **Ensures Compliance**: Meets industry standards for secure environments.



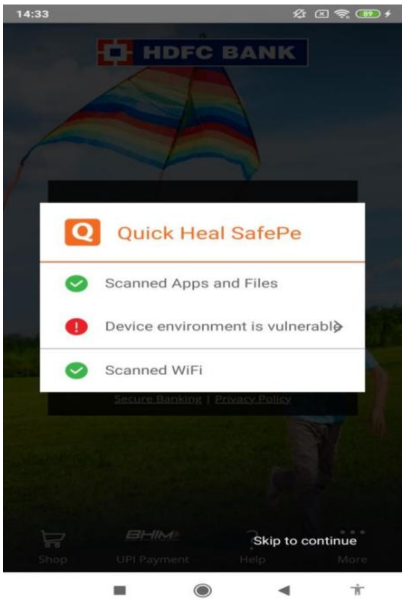
5. How Device Integrity Works

Device Integrity functions by:

- **Device Environment Scan:**
  - Detects unauthorized OS modifications (e.g., rooting, API hooking, bootloader unlocking, custom firmware flashing)
  - Ensures that the device environment remains unchanged from its manufacturer settings
- **Play Integrity API**

  Provides real-time checks to verify:

  - App integrity (genuine app installation from Play Store).
  - Device integrity (unmodified hardware and software).
  - User account integrity (legitimate user activity).
  - Replaces the deprecated SafetyNet Attestation.
- **Wi-Fi Security Scan:**
  - Evaluates the security of the currently connected network
  - Flags unsafe networks such as open Wi-Fi, weakly encrypted connections, and captive portals
  - Detects DNS poisoning attacks

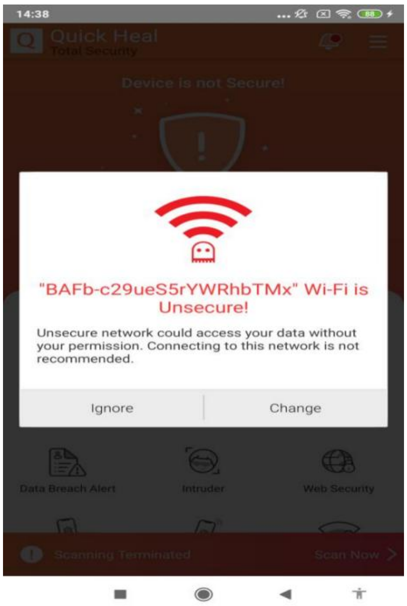


Quick Heal SafePe

Scanned Apps and Files

Device environment is vulnerable

Scanned WiFi



"BAFb-c29ueS5rYWRhbTMx" Wi-Fi is Unsecure!

Unsecure network could access your data without your permission. Connecting to this network is not recommended.

Network Scan Criteria:

Connection Type	Security Status
Mobile Network	Safe
Open Wi-Fi (no password)	Unsafe
Weak Encryption (e.g., WEP)	Unsafe
Captive Portal (public login)	Unsafe
DNS Poisoned Network	Unsafe
Secure WPA/WPA2 Wi-Fi	Safe

6. Key Security Features

6.1 SafePe

SafePe is a security feature that allows users to store and manage their banking and e-commerce payment apps in a secure vault. Before launching any payment application, SafePe scans the device environment for security threats and alerts the user if vulnerabilities are found.

SafePe Features:

- Device Scan: Checks for device root status, system integrity, and security vulnerabilities.
- System Scan: Scans system apps and files for potential threats (mandatory security check).
- Network Scan: Evaluates the security of the currently connected network.
- User Controls:
  - Users can toggle Device and Network scan settings under SafePe settings.
  - System Scan remains compulsory to ensure maximum security.

6.2 Wi-Fi Security

Wi-Fi security ensures that users are protected while connecting to wireless networks. The security status of a connected network is evaluated based on:

- Open Networks (no password protection) → Insecure
- Captive Portals (login-based access) → Insecure
- Weak Encryption (WEP) → Insecure
- Strong Encryption (WPA/WPA2) → Secure
- DNS Poisoned Networks → Insecure

Wi-Fi security safeguards users from unauthorized network access, data interception, and cyber threats associated with unsafe wireless connections.

7. Conclusion

Device Integrity plays a crucial role in ensuring the security of mobile devices. By scanning for unauthorized modifications, securing network connections, and preventing fraudulent activities, device integrity solutions provide users with a safer digital experience.

The methods outlined in this white paper offer best practices for implementing device integrity, helping organizations and individual users mitigate security risks. By integrating modern security tools such as SafePe and Wi-Fi Security, mobile users can enhance their device protection and maintain a secure digital environment.

As mobile threats continue to evolve, continuous security monitoring and proactive defense mechanisms will remain essential for protecting sensitive user data and maintaining trust in mobile applications.