USC University of Southern California

Secure Mobile Devices

Melina Eliasyan
Alex Carter

Mobile Device Security

What is mobile device security?

- Mobile security has the same goals as desktop security but the implementation and preventative measures in place are different to match a variety of mobile devices.
- The modern workforce has an increased use of mobile devices such as laptops, phones, tablets, and other mobile devices to meet an organization's objectives.
- Organizations need to utilize specific tools, policies, and procedures to ensure the device and datas security on mobile devices.

Roots of Trust

What are roots of trust?

Roots of trust are hardware/software components that are inherently trusted.

- They must be secure by design.
- Should be small and protected.
- Ideally implemented in hardware, or protected by hardware.

They are trusted to perform one or more security-critical functions, e.g.,

- Measure and/or verify software
- Perform device authentication

Roots of trust in mobile devices face numerous challenges

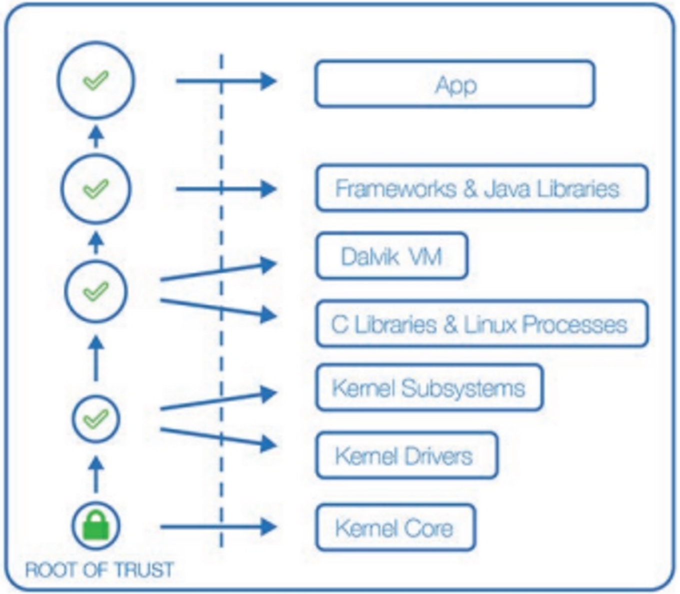
Firmware protection poses a special challenge in mobile devices, IoT firmware and mobile device firmware has shown to be vulnerable.

Mobile devices pose a greater risk of physical attacks, motivating a need for hardware protections

Security Mechanisms

Security mechanisms for mobile devices can be implemented in hardware or protected firmware.

- Mobile software roots-of-trust
- Continuous authentication
- Virtual mobile infrastructure extensions



A measurement chain for the Android

Roots of Trust and the enterprise environment

Roots of Trust can support enterprise mobile device security including bring your own device policies through two approaches.

Application based: We can create a system such as an entrance monitoring device that can automatically determine if a device meets the criteria of an organization for admittance.

Cloud based: We use a root of trust on the device to prove to a server that the device is not running a broken version of a library.

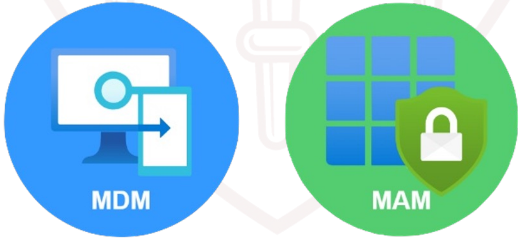
MDM & MAM

Mobile Device Management (MDM)

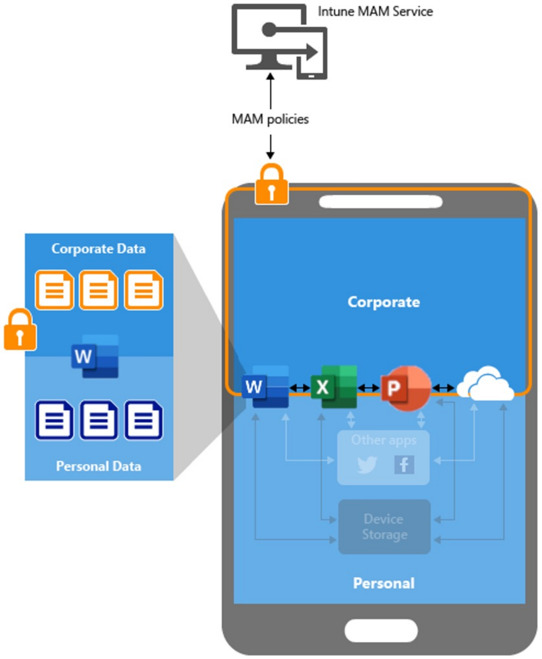
- For enforcing policies on corporate-owned mobile devices & BYOD
    - Ensure device encryption
    - Enforce strong PIN code
    - Ensure device screen-lock when idle
    - $4.3 billion in 2020, expected to be $15.7 billion in 2025

Mobile Application Management (MAM)

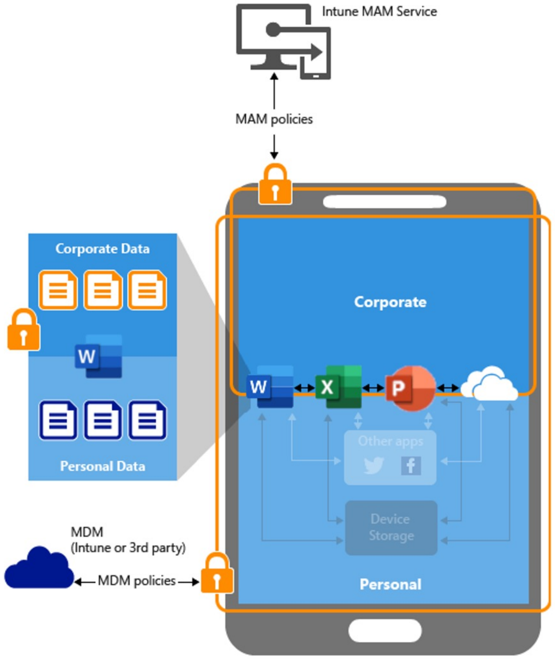
- For securing web browsers, email clients, and other applications
    - Emphasis on BYOD
    - App configuration and updating
    - App performance monitoring
    - Default and custom policies



MAM only



MDM & MAM

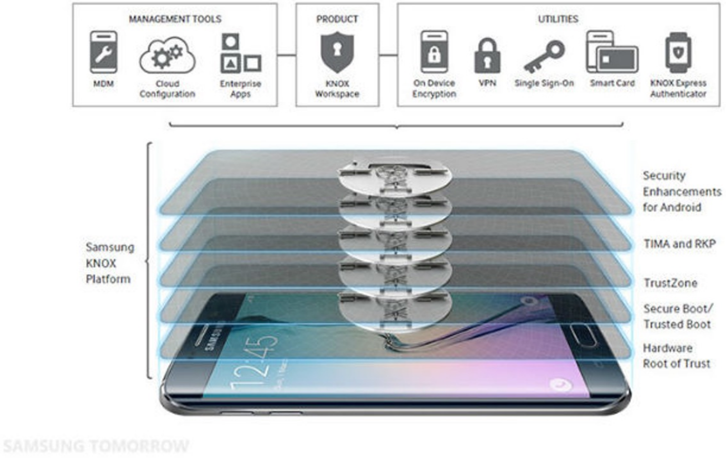


Secure Containers for Mobile Devices

- Sandboxing
- Third-party mobile application used to separate and secure a portion of a device’s storage from the rest of the device.
- Samsung - Knox & AT&T - Toggle
- Isolate applications, disable certain functions of apps, remotely wipe devices.
- Unified security approach
- Employers can push documents, media and other resources to employee devices.

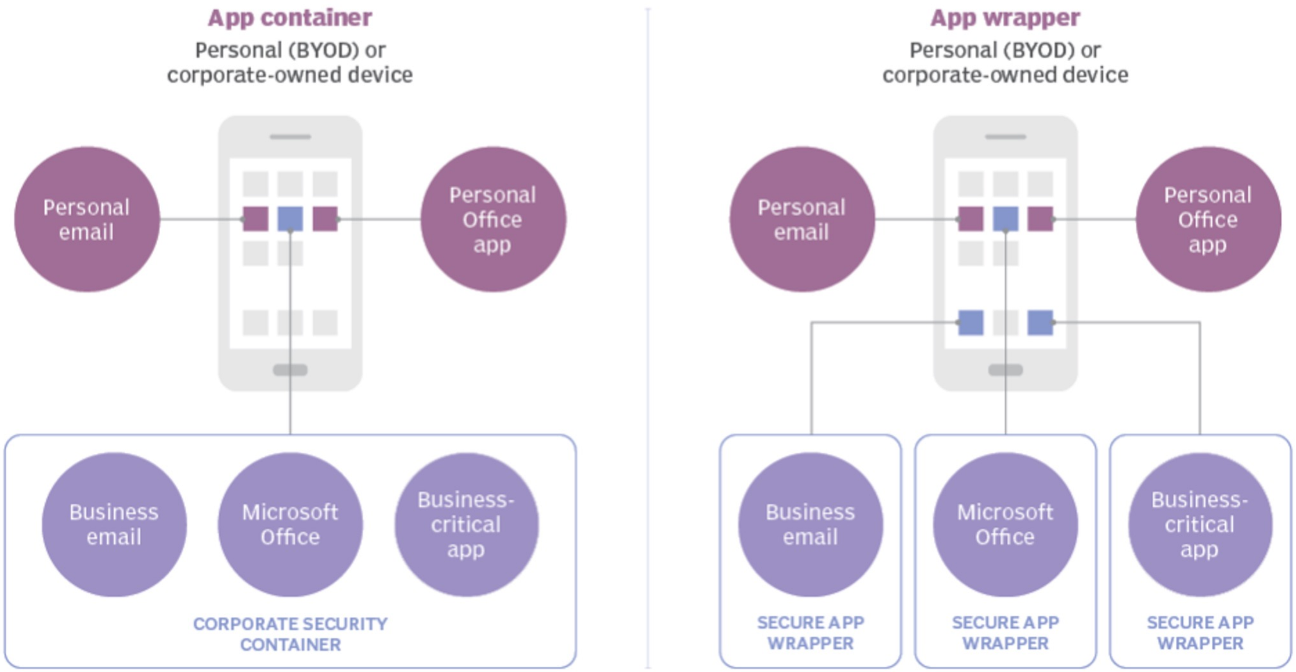
Secure Containers for Mobile Devices

- Limitations on placing certain applications in containers
  - Media pushed by IT vs. User created files
  - Email & Attachments vs. Files
- Requires MAM or MDM infrastructure to implement
- Compatibility problems, new interface



App container vs. app wrapper

Containers and wrappers protect business and personal information on multiuse devices.



App container

Personal (BYOD) or
corporate-owned device

Personal email

Personal Office app

Business email

Microsoft Office

Business-critical app

CORPORATE SECURITY CONTAINER

App wrapper

Personal (BYOD) or
corporate-owned device

Personal email

Personal Office app

Business email

SECURE APP WRAPPER

Microsoft Office

SECURE APP WRAPPER

Business-critical app

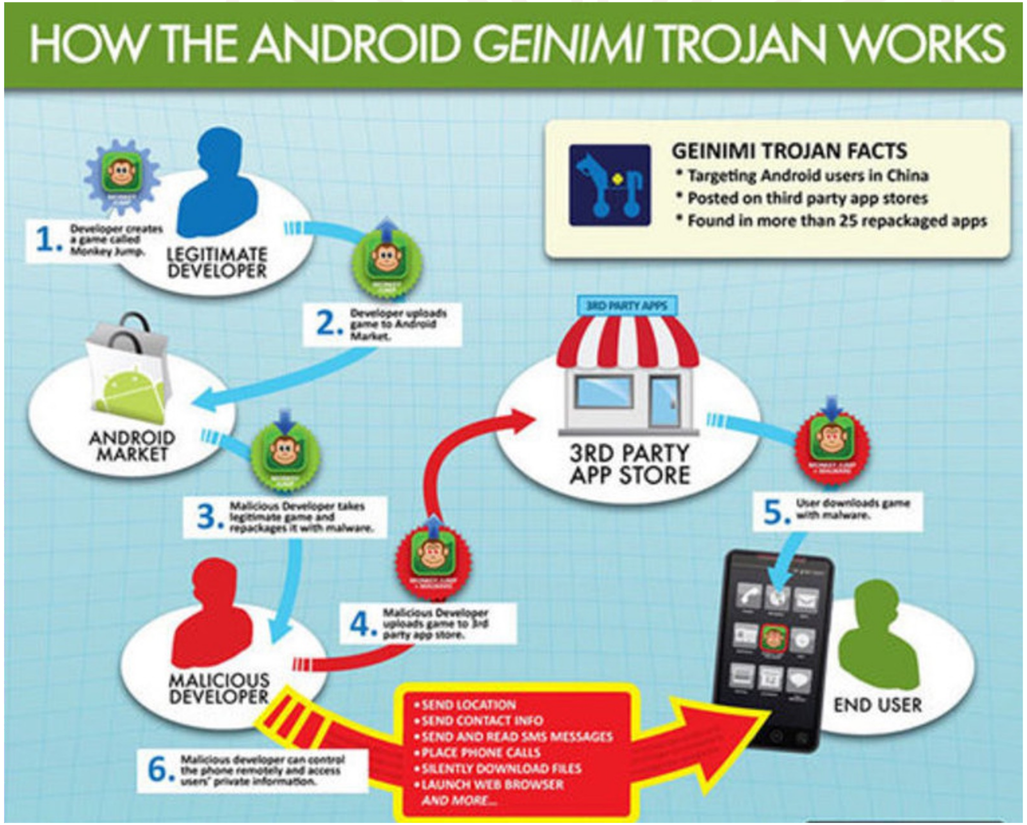
SECURE APP WRAPPER

Secure Mobile Device Advantages

- Regulatory Compliance
- Security Policy Enforcement
- Supports “BYOD”
- Application Control
- Data Backup

Secure Mobile Device Vulnerabilities

- Malicious Applications
- Applications with Weak Security
- Out-of-Date Devices
- Data Leakage
- Usecure Wifi
- Phishing Attacks


HOW THE ANDROID *GEINIMI* TROJAN WORKS

GEINIMI TROJAN FACTS

- Targeting Android users in China
- Posted on third party app stores
- Found in more than 25 repackaged apps

1. Developer creates a game called Monkey Jump.

2. Developer uploads game to Android Market.

3. Malicious Developer takes legitimate game and repackages it with malware.

4. Malicious Developer uploads game to 3rd party app store.

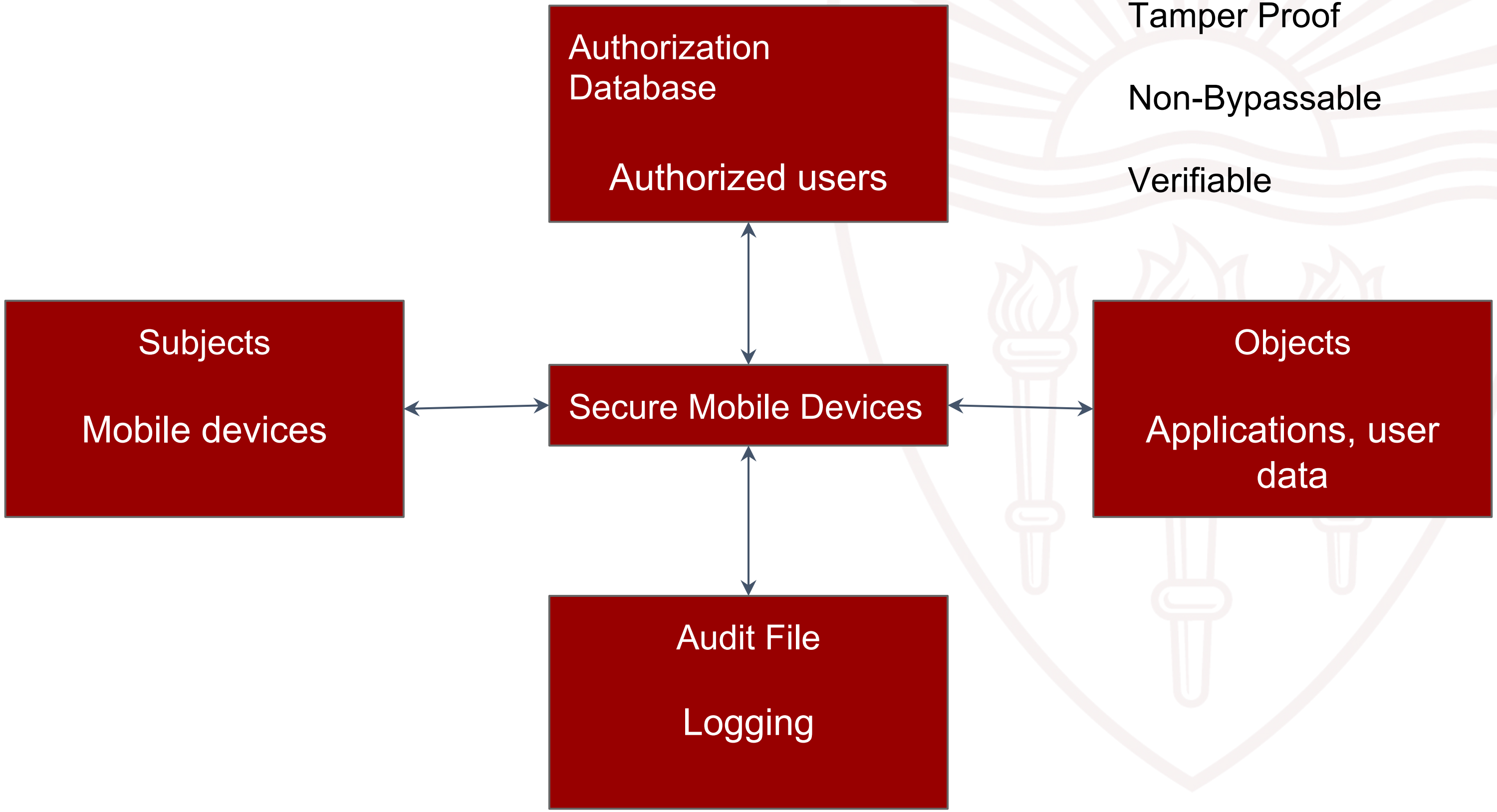
5. User downloads game with malware.

6. Malicious developer can control the phone remotely and access users' private information.

- SEND LOCATION
- SEND CONTACT INFO
- SEND AND READ SMS MESSAGES
- PLACE PHONE CALLS
- SILENTLY DOWNLOAD FILES
- LAUNCH WEB BROWSER

AND MORE...

Reference Monitor Comparison



Authorization Database

Authorized users

Subjects

Mobile devices

Secure Mobile Devices

Objects

Applications, user data

Audit File

Logging

Tamper Proof

Non-Bypassable

Verifiable

References

- https://www.dhs.gov/science-and-technology/mobile-device-security
- https://csrc.nist.gov/CSRC/media/Events/ISPAB-FEBRUARY-2012-MEETING/documents/feb1_mobility-roots-of-trust_regenscheid.pdf
- https://www.dhs.gov/sites/default/files/publications/CSD%202016%20Mobile%20Security%20R%26D%20Program%20Guide%20Vol%201.pdf
- https://www.vmware.com/topics/glossary/content/mobile-device-security.html#:~:text=Mobile%20Device%20Security%20refers%20to,from%20accessing%20the%20enterprise%20network.
- https://www.rd.com/article/mobile-security-threats/
- https://usa.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store
- https://www.techtarget.com/searchsecurity/feature/App-container-app-wrapping-and-other-emerging-mobile-security-tactics
- https://www.techtarget.com/searchmobilecomputing/feature/Pros-and-cons-of-using-secure-containers-for-mobile-device-security
- https://www.techtarget.com/searchsecurity/feature/MDM-vs-MAM-Comparing-enterprise-mobile-security-management-options
- https://www.techtarget.com/searchmobilecomputing/The-ultimate-guide-to-mobile-device-security-in-the-workplace