

A Large-Scale Study on [...] TEE-based Features on Android

Dr. Davide Bove

August 1, 2024

IT Security Infrastructures Labs
Department of Computer Science
Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)

Is anyone even using the
cool security features
we¹ developed over the years?

¹the Trusted Computing and Mobile Security community

These are the contributions of our paper:

- Large-scale analysis of **TEE usage** in Android applications.
 - 4 different APIs built into the Android framework
 - **333,475** popular Android apps
- Mobsec Analytika, a framework for **large-scale static analysis**, created for security researchers and professionals.

Background

Trusted Execution Environments (TEE)

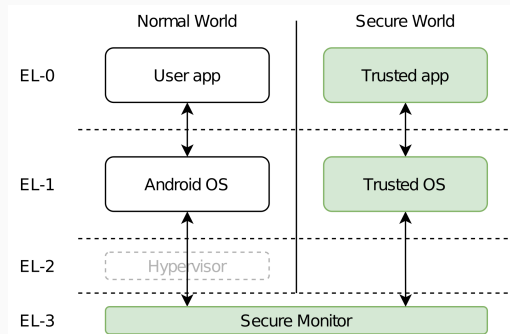
Goal: give security guarantees for specific applications

Even if

- OS compromised
- Hardware compromised

How it works:

- Hardware-based isolation of software
- Encryption



System architecture of an Android device with ARM TrustZone

Result: Reduced attack surface of critical software

Trusted Execution Environments (TEE)

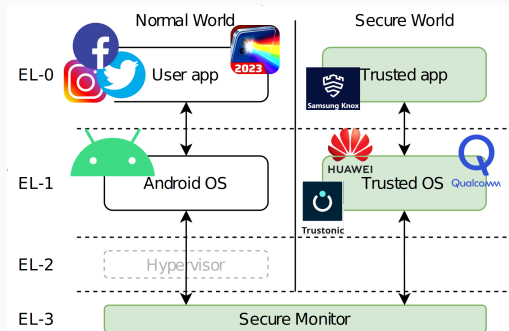
Goal: give security guarantees for specific applications

Even if

- OS compromised
- Hardware compromised

How it works:

- Hardware-based isolation of software
- Encryption

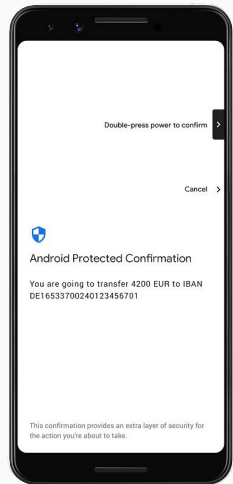


System architecture of an Android device with ARM TrustZone

Result: Reduced attack surface of critical software

Protected Confirmation

- Hardware-protected user interface
- Two parts residing in TEE
 - **Keystore**: for generating keys
 - **ConfirmationUI**: generates cryptographic statement



Source: [AOSP](#) (CC BY 4.0)

How apps use TEEs





How apps use TEEs

- Analyzed 333,475 apps from Play Store
 - Recent apps (last update: 01/2020)
 - Relevant (10k+ installs)
 - No games

How apps use TEEs

- Analyzed 333,475 apps from Play Store
 - Recent apps (last update: 01/2020)
 - Relevant (10k+ installs)
 - No games

We looked at 4 APIs:

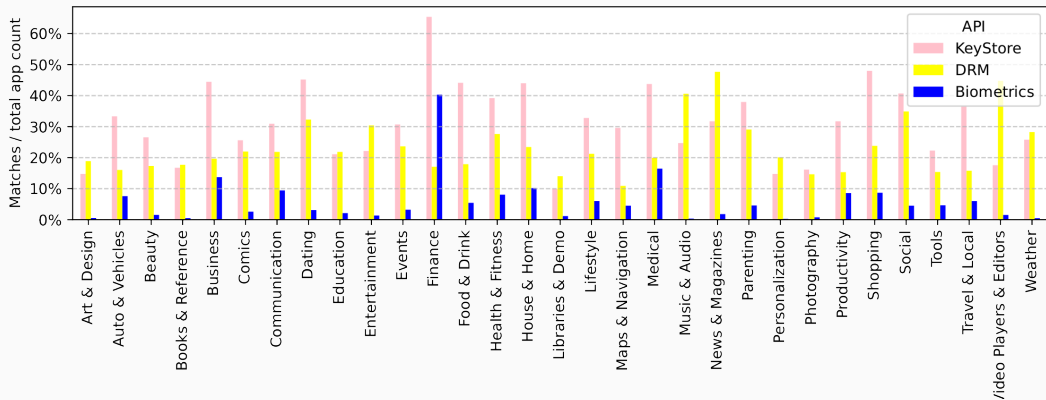
-  Biometrics
-  DRM
-  KeyStore
-  Protected Confirmation

Total analyzed apps: 333,475

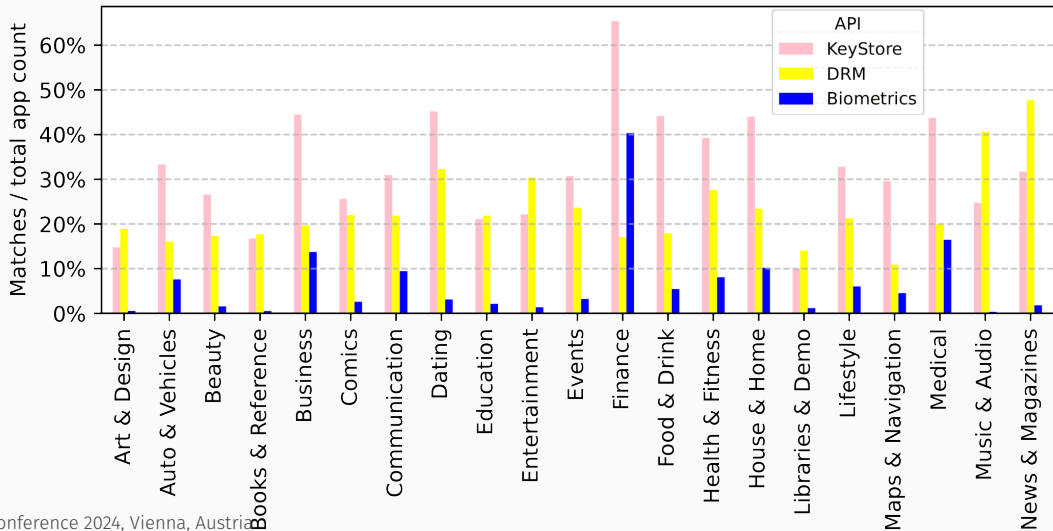
- Biometrics: 22,313 6.6%
- DRM: 77,007 22.8%
- KeyStore: 101,983 30.3%
- Protected Confirmation: 7 0.0%

No matches: 193,664 57.5%

Matches per category



Matches per category



Of all apps with an API match:

- ~ 91.7 % show **inlib** usage
- ~ 14.5 % show **inmain** usage

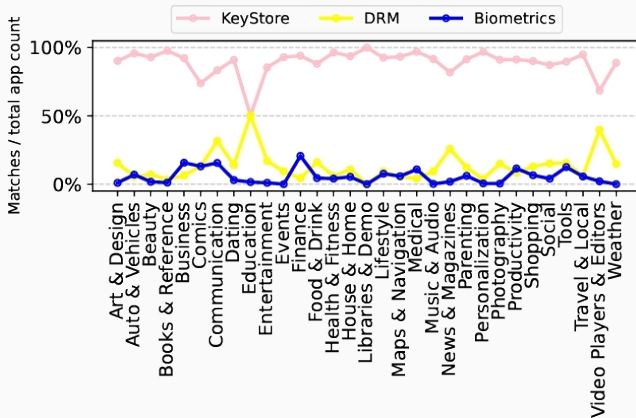
From 134,693 apps with at least one **inlib** match:

- 66.3 % include Keystore
- 55.7 % include DRM
- 15.6 % include Biometrics
- 5 apps use Protected Confirmation

inmain usage

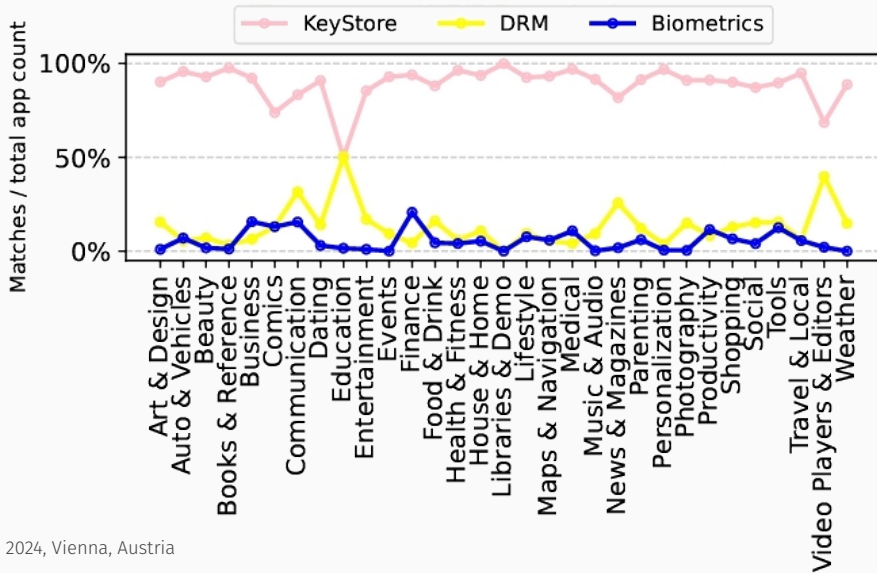
From 20,508 apps with at least one **inmain** match:

- **86.9 %** include Keystore
- **14.7 %** include DRM
- **8.1 %** include Biometrics
- **2 apps** use Protected Confirmation



Relative API matches per app category for inmain usage.

inmain usage



Conclusion

Summary of the study

The **first** study on the usage of TEE features on Android:

Summary of the study

The **first** study on the usage of TEE features on Android:

- Most used: KeyStore (1/3 of all apps)
- Protected Confirmation **not used**
- Only 6.2% of apps directly invoke APIs

⇒ Developers do not use TEE features as much as they could!

⇒ Most don't know they might be using them.

I want more!

Contact me: davide.bove@fau.de

Download this presentation: <https://d4vi.de/android-tee-study>



This presentation is licensed under a
[Creative Commons Attribution International 4.0 License](https://creativecommons.org/licenses/by/4.0/).

