Google

Security on Android

The Good, The Bad and The Ugly

Cristian Neagu

About Me

- Android Eng for approximately 10 years
- Android passionate for even longer
- Fitbit Eng since 2019
- Joined Google in 2021

What does Security mean

Security - Definition

- **Security** is protection from, or resilience against, potential harm caused by others, by restraining the freedom of others to act.

- **IT security (a.k.a. cybersecurity)** is the protection of computer systems from information disclosure, theft of, or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

Data Protection

- User data protection
  - Locally stored data
  - Network data
- Application code protection

Why do hackers want your data?

- Sell it to other criminals
- Identity Theft
- Phishing attacks and extortion
- Ransomware

How can I keep my hw & sw secure?

- Never share them with anyone
- Never use the internet
- Never leave your home

How can I keep my hw & sw secure? (for real)

- Use multiple layers of security
- Only use trusted sources

Android + Security

= ❤️?

Data Security

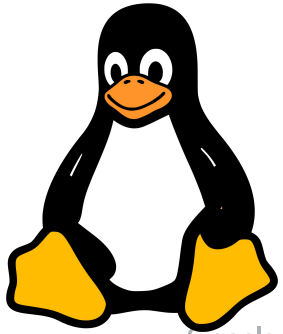
- OS Level Security
- Application Level Security
- User Behaviour

OS Level Security

- Android is developed on a Linux kernel
- Application Sandbox
- Cryptography
- Biometrics
- User-based permissions

Linux Kernel

- Security-Enhanced Linux (SELinux)
- Java applications run on ART
- All low-level operations (e.g. hardware interactions) are handled by the system.
- Security patches



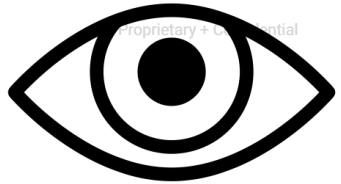
Application Sandbox

- Unique ID for each app
- Separate process and memory region
- Isolated path in internal and external storage
- User-based permission system
- Inter-Process Communication

Cryptography

- Native support for cryptographic operations (symmetric and asymmetric encryption)
- File-based encryption (symmetric, added in Android 7)
- Full-disk encryption (added in Android 9)
- Hardware-backed Keystore

Biometrics



- Supported natively for screen lock and app authentication
- Fingerprint, Face/Iris authentication
- Biometric Classes (3-1) for different levels of security

User-based Permissions

- Gives user control over:
  - Restricted data
  - Restricted actions

- You should show rationale for permission request

Application Level Security

Or what can us as developers do to ensure data protection

Application Level Security

- Protection of locally-stored data
- Protection of network data
- Password/Biometric protection
- Protection of application code

Protection of locally-stored data

- Never store user credentials on device storage
- Try not to store sensitive user data locally
- Encode sensitive user data
- Never-ever store sensitive data in SharedPreferences (or a plain text file)

Protection of network data

- Always use secure communication protocols (e.g. HTTPS)
- Optional payload encryption for sensitive data
- Use third-party authentication
- Store session tokens in the Hardware-backed Keystore or AccountManager

Using web views

- Think twice before enabling JS
- Enforce HTTPS
- Make sure webviews cannot be accessed via deeplinks

Sharing Data

- IPC should be done moderately and with care
- Use Content Providers for sharing application data
- Give temporary access to the files owned by your application

App defined permissions

- Your app can define its own permissions
- Restrict interactions with your app’s activities, services, content providers (etc.)

Application Code Protection

- What can we do to protect our precious code?
- Aviod storing keys or any kind of sensitive data in application code
- Obfuscate, obfuscate, obfuscate
- Example

User Behaviour

- Never rely on the user to protect their data
- Try to educate the user
- Password-protect sensitive areas of the application

Conclusions

- Android provides a level of security for the device
- We, as developers, need to prevent security leaks
- Don’t rely on the user

Thank you