Android Security

Ing. Pavol Lupták, Nethemba s.r.o.

Android Security - Index

- Android architecture overview
- Localization services
- Mobile malware
- Security-aware applications
- Security testing and auditing
- How to protect yourself

Android Security Architecture

- Lower layer based on Linux kernel
- Higher layer based on JaCa and C code
- Many application's permissions are translated directly to Linux capabilities, but not all – some of them are checks in higher layer
- Regardless of security flaws, Android system collects a lot of sensitive information and wrong files/folders permissions
- Log interface with unified logs available for all applications and the system

Localization Services

- GSM localization (no need for built-in GPS or Wifi) – every BTS is identified by MCC, MNC, LAC, CID
- GPS localization
- Wifi localization
- Google maintains the database of all wifi APs and GSM BTSes

Geolocation using logging facility I

- Android uses a specific logging facility with built-in logcat tool to manipulate the logs
- Radio log contains history of user's visited BTS (MCCs+MNCs,LACs, CID)!
- Attacker can reveal the victim's location just by forcing him to run malware with READ_LOGS permission only!
- No access to Android geolocation API is necessary!

Geolocation using logging facility II

- This information can be sent to the attacker without INTERNET permission:
- The attacker write his results into the system log (no permission needed!)
- Voluntarily crashes the application when needed (no permission needed!)
- If the user reports the crash, system log is sent to the developer using the Google Feedback client in plaintext

Geolocation using logging facility III

- Android NDK (Native Development Kit) can be used to completely bypass permission model by calling native functions
- Arbitrary file access, code execution, network access..

Geolocation using social engineering/XSS

- The attacker forces the victim to open a special URL that connects to your home wifi router and obtains its MAC address
- Google Location Service is used to resolve MAC address to GPS coordinates
- Firstly published by Samy Kamkar – How I Met Your Girlfriend
- All Androids are special “Google” agents

Mobile malware

- Android/iOS becomes a really popular market for malware
- Bigger “trust” in the mobile applications than classical desktop applications
- People do not care about application's permissions
- “Carrier IQ” keylogger (officially used for “statistical purposes”)

Building 'malware' online

- MITM attack during application download over wifi:
- The new Android Market & Android Downloader Managers sends an application name, description, permissions in plaintext HTTP
- It should be easy to change application descriptions, permissions and content using active MITM and install malware application

Security-aware applications

- Do not trust to GSM/3G, use encrypted calls based on SIP/TLS and SRTP (Bria, Media5-Fone, Acrobits) and your trusted call center
- Use encrypted PGP/SMIME emails (APG, K9Mail)
- Use encrypted Jabber with OTR (Gibberbot), do not use proprietary services like Skype, ICQ, ..
- Use encrypted storage (B-Folders, Encryption Manager, AES Crypto, ..)

Security testing and auditing

- OWASP Mobile Security Project

1. Insecure Data Storage
2. Weak Server Side Controls
3. Insufficient Transport Layer Protection
4. Client Side Injection
5. Poor Authorization and Authentication
6. Improper Session Handling
7. Security Decisions Via Untrusted Inputs
8. Side Channel Data Leakage
9. Broken Cryptography
10. Sensitive Information Disclosure

How to protect yourself?

- Install applications from the trusted official repository
- Make your applications and OS up-to-date
- Disable “sophisticated” localization services
- Check for applications using NDK, don't install application requiring READ_LOGS, don't submit bug reports
- Disable radio logs and reduce logcat buffer size
- NSA Hardened Kernel for Android
- Google Android Hardening Checklist

References

- Renaud Lifchitz – Android geolocation using GSM network
- Samy Kamkar – How I met your girlfriend

Thank you for your attention!