Attack analysis and Security concepts for Mobile Network infrastructures supported by collaborative Information exchange

Integrity Protection for Mobile Devices

Sascha Wessel
Fraunhofer AISEC
Outline

- Motivation
- Mobile Device Architectures
- Situation Today
- Our Contribution
  - Attestation of Mobile Baseband Stacks [1]
  - SobTrA: A Software-based Trust Anchor for ARM Cortex Application Processors [2]
- Conclusion
Motivation

What is to be achieved?

- Guarantee that a piece of software runs *untampered* on the device
  - Detect and prevent malicious modifications *on the device*
  - Detect malicious modifications at connect or during a transaction *in the backend*

And why?

- Securing mobile banking and payment
- Trusted Network Connect
- General attack prevention
Mobile Device Architectures

- **Shared CPU Architecture (Application integrated in Baseband)**
  - Shared RAM
  - Application
  - Baseband
  - Hardware
  - Software

- **Multi CPU Architecture (with serial communication / shared memory)**
  - Application RAM
  - Baseband RAM
  - Application CPU
  - Baseband CPU
  - Hardware
  - Software

- **Shared CPU Architecture (Application and Baseband virtualized)**
  - Shared RAM
  - App
  - BB
  - VMM
  - Hardware
  - Software

- **Multi CPU Architecture (with shared RAM)**
  - Shared RAM
  - Application CPU
  - Baseband CPU
  - Hardware
  - Software
  - App
  - BB

07.05.2013
Sascha Wessel, Fraunhofer AISEC / Version 1.0 / Copyright © 2013 ASMONIA Project. All rights reserved.
Situation Today

- **Baseband**
  - No integrity protection
  - Bad code quality → highly vulnerable

- **Application**
  - On some devices *secure boot* based on Core Root of Trust for Measurement (CRTM) using manufacturer controlled ROM
  - Application integrity protection at *install time*
  - Typically no *runtime* protection
  - Sometimes isolated parts using a Trusted Execution Environment (TEE), e.g., running in ARM’s TrustZone
Attestation of Mobile Baseband Stacks [1]

- **MTM**-based attestation
- Attestation of **baseband** at network connect
- No network access if attestation fails
- Requires **modifications** of **infrastructure elements** (MME)
SobTrA: A Software-based Trust Anchor for ARM Cortex Application Processors [2]

- Secure boot without hardware-based trust anchor in ROM
- Locally connected **verifier device**, e.g., microSD card using SPI or SDIO
- Implementation based on **self-checksumming code**
- Multiple Android userland instances on one device
- Isolation based on Linux *namespaces* and *cgroups*
- Integrity protection based on *Linux Security Modules (LSM)*

- Implemented in Virtual Machine Monitor (VMM)
- Protection based on memory mappings for guest operating system (executable xor writable)
Conclusion

- Integrity protection for mobile devices has several aspects
  - Our focus was on secure boot and runtime protection
  - Most of the presented mechanisms work independently without network connection on a device (using local whitelists)
  - These mechanisms are the base for remote verification or attestation, e.g., Trusted Network Connect (TNC)
  - Potential sensor for information sharing
- We implemented several prototypes
Thank you for your Attention

Sascha Wessel, Fraunhofer AISEC
sascha.wessel@aisec.fraunhofer.de
References