Consortium

CASSIDIAN AN EADS COMPANY | ERNW Living Security. | Fraunhofer AISEC | Hochschule Augsburg University of Applied Sciences | Nokia Siemens Networks | RWTH AACHEN UNIVERSITY

ASMONIA

Attack analysis and Security concepts for MObile Network infrastructures supported by collaborative Information exchAnge

SPONSORED BY THE
Federal Ministry of Education and Research

Integrity Protection for Mobile Devices

Sascha Wessel
Fraunhofer AISEC

07.05.2013

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]
  - Improving Mobile Device Security with Operating System-level Virtualization [3]
  - Page-based Runtime Integrity Protection of User and Kernel Code [4]
- Conclusion

Motivation

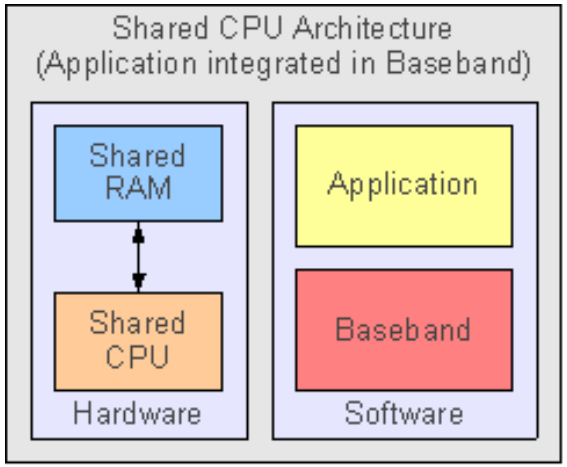
What is to be achieved?

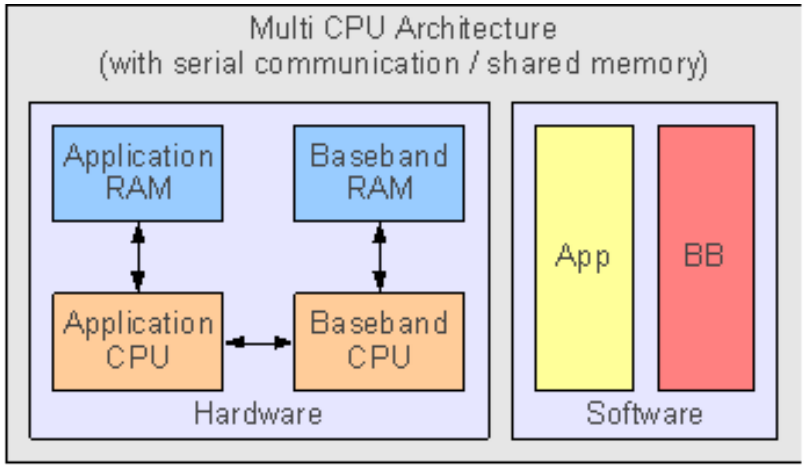
- Guarantee that a piece of software runs *untampered* on the device
  - Detect and prevent malicious modifications *on the device*
  - Detect malicious modifications at connect or during a transaction *in the backend*

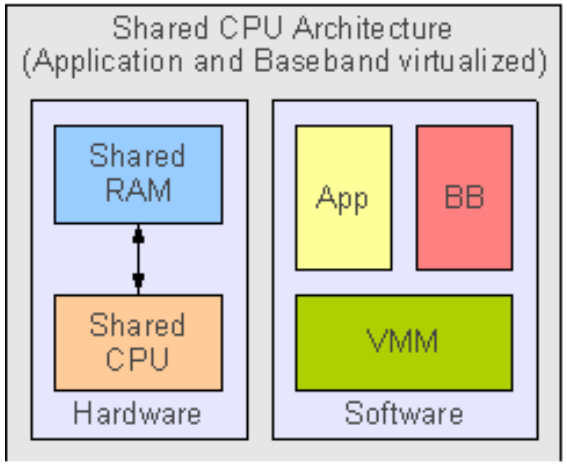
And why?

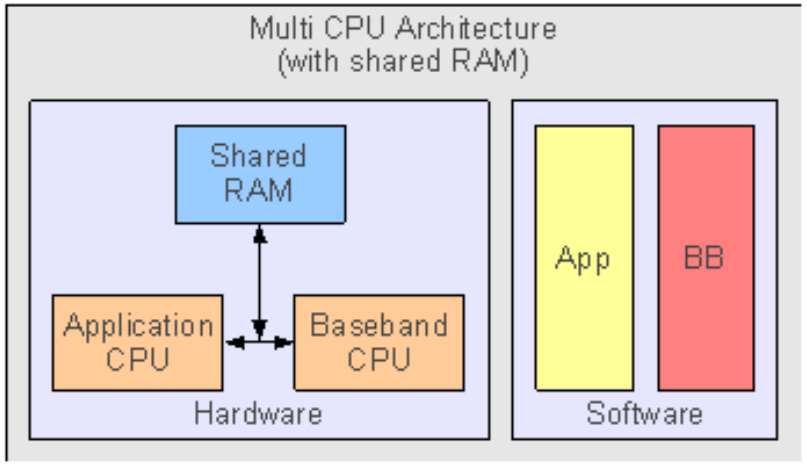
- Securing mobile banking and payment
- Trusted Network Connect
- General attack prevention

Mobile Device Architectures









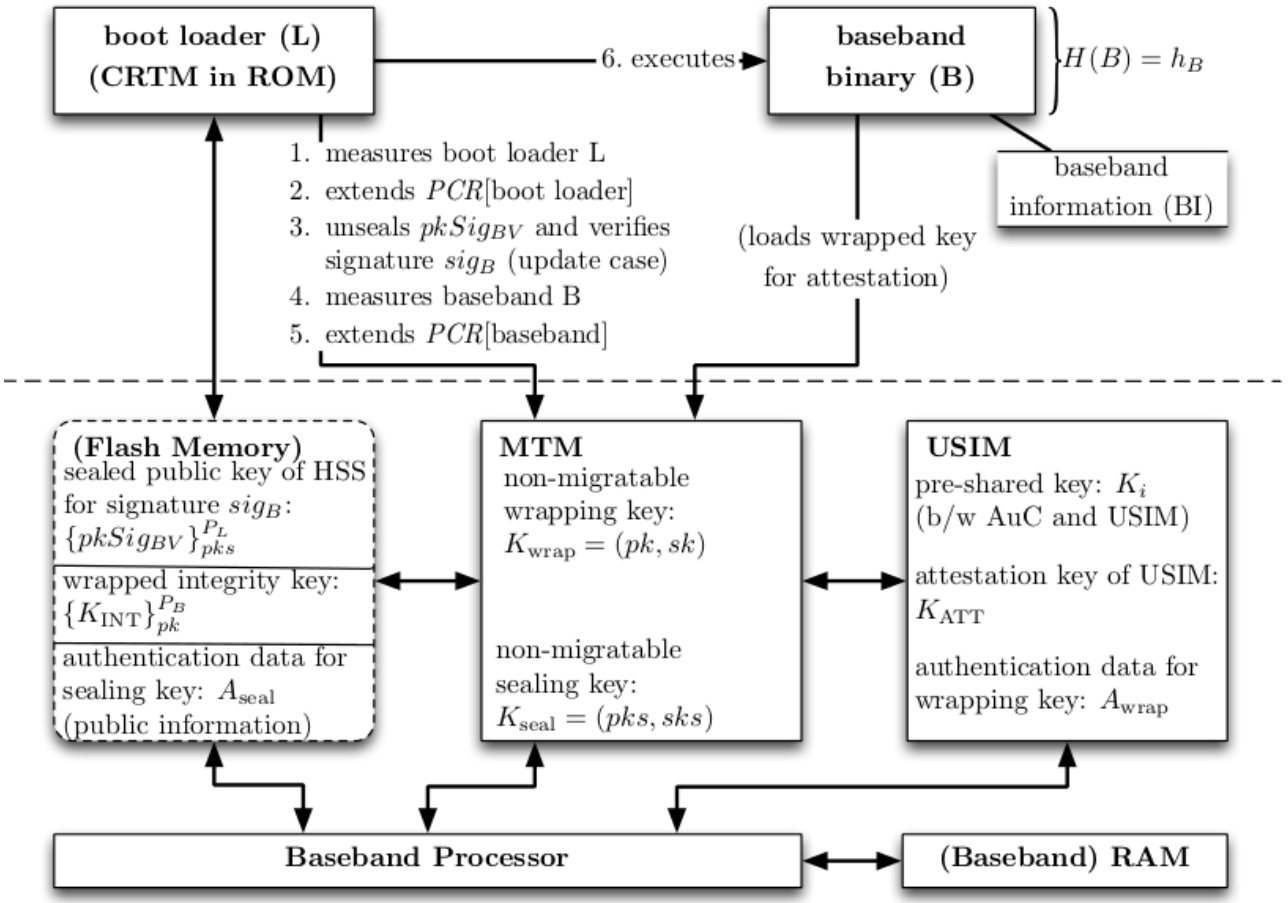
Situation Today

- 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

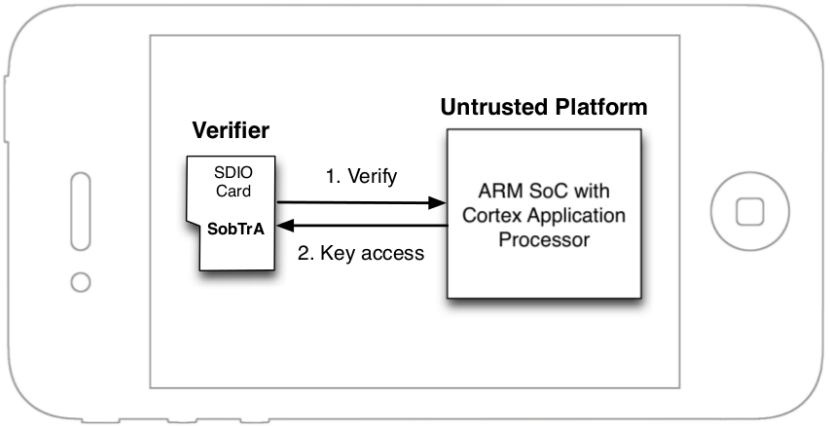
Attestation of Mobile Baseband Stacks [1]

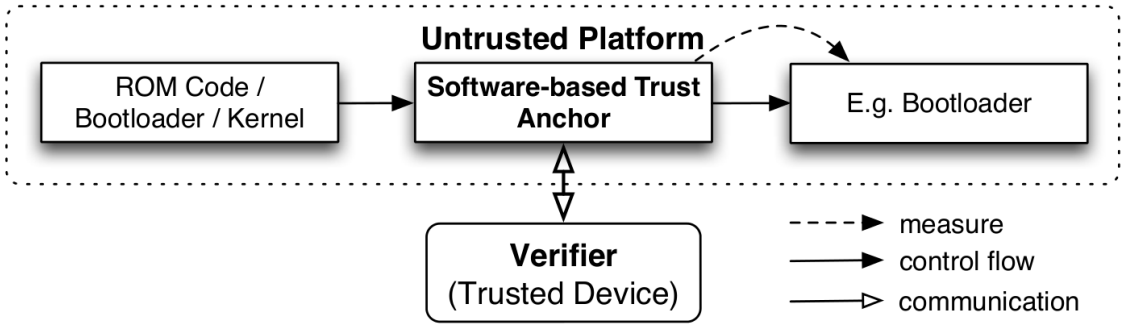
- *MTM*-based attestation
- Attestation of *baseband* at *network connect*
- No network access if attestation fails
- Requires *modifications* of *infrastructure elements* (MME)



SobTrA: A Software-based Trust Anchor for ARM Cortex Application Processors [2]

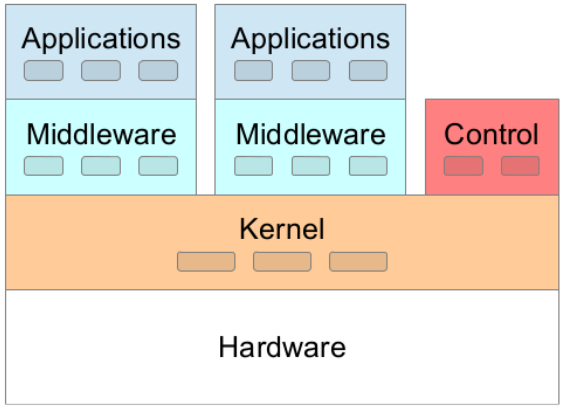
- Secure boot without hardware-based trust anchor in ROM
- Locally connected *verifier device*, .e.g., microSD card using SPI or SDIO
- Implementation based on *self-checksumming code*

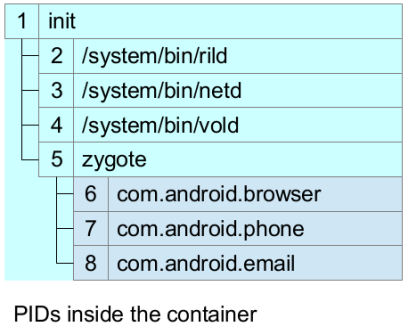




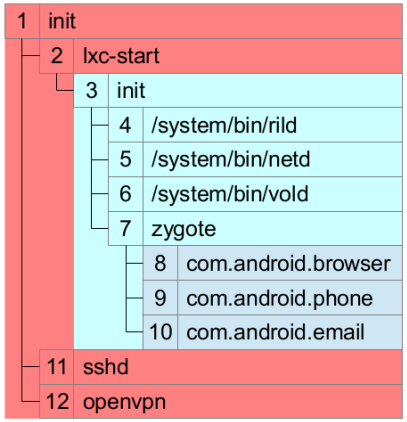
Improving Mobile Device Security with Operating System-level Virtualization [3]

- Multiple Android userland instances on one device
- Isolation based on Linux *namespaces* and *cgroups*
- Integrity protection based on *Linux Security Modules (LSM)*

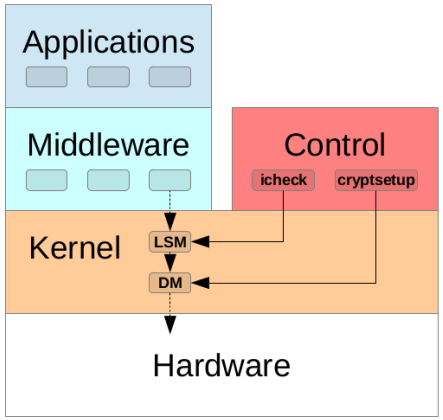




PIDs inside the container



PIDs outside the container

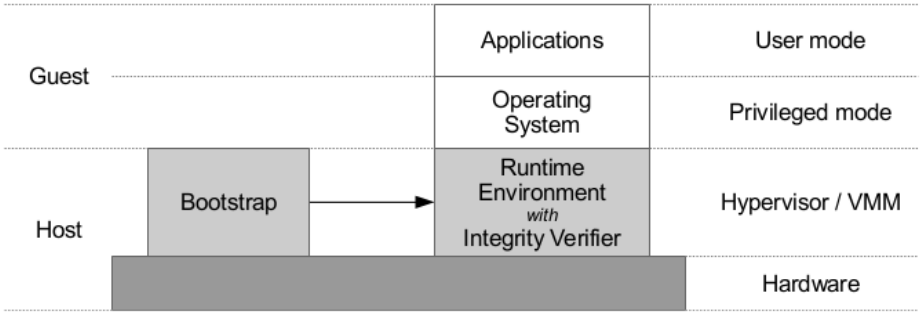


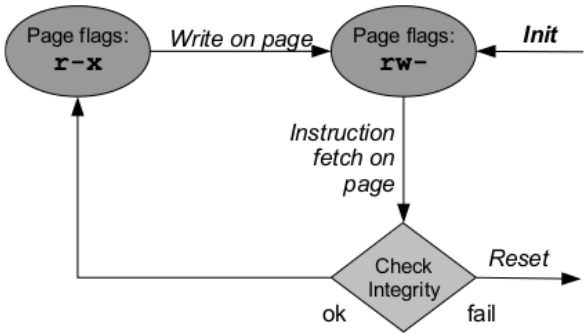
LSM Linux Security Module for system call hooks

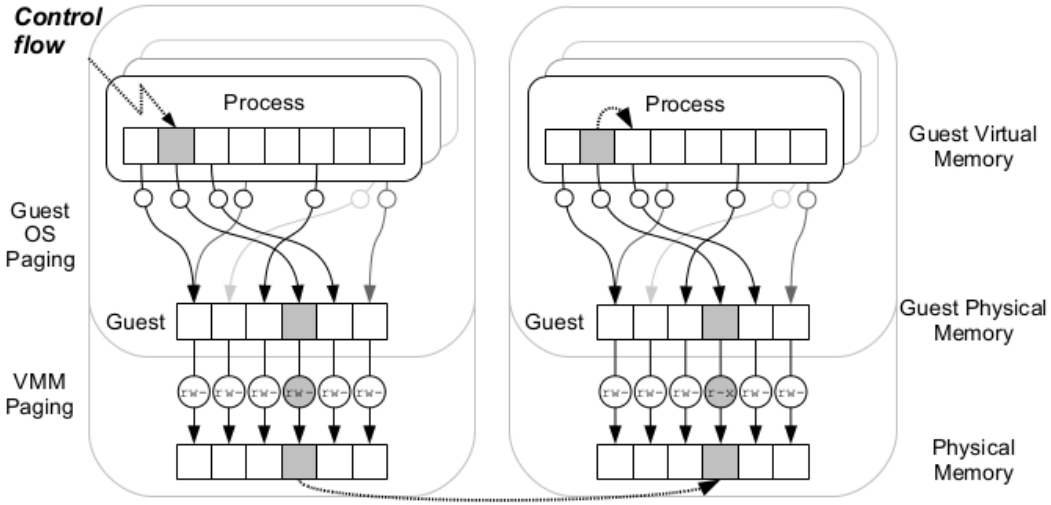
DM Device Mapper for device encryption

Page-based Runtime Integrity Protection of User and Kernel Code [4]

- 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

- [1] Steffen Wagner, Sascha Wessel and Frederic Stumpf, Attestation of Mobile Baseband Stacks, 6th International Conference on Network and System Security, 2012.
- [2] Julian Horsch, Sascha Wessel, Frederic Stumpf and Claudia Eckert, SobTrA: A Software-based Trust Anchor for ARM Cortex Application Processors, currently under review.
- [3] Sascha Wessel, Frederic Stumpf, Ilja Herdt and Claudia Eckert, Improving Mobile Device Security with Operating System-level Virtualization, 28th IFIP TC-11 SEC 2013 International Information Security and Privacy Conference, 2013.
- [4] Sascha Wessel and Frederic Stumpf, Page-based Runtime Integrity Protection of User and Kernel Code, 5th European Workshop on System Security, 2012.