Annual review ROME 2012

nSHIELD

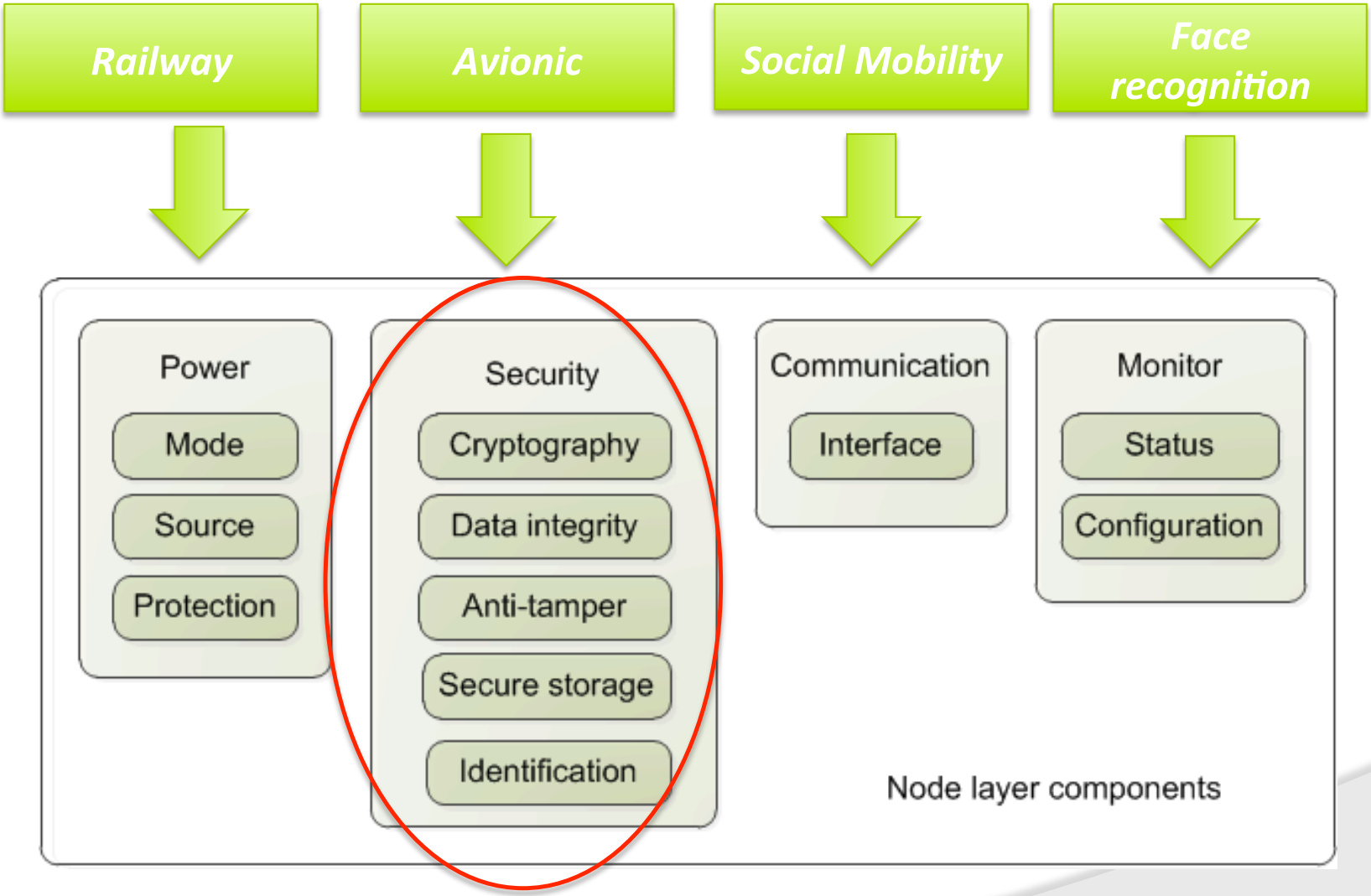
Lessons learned from first year:

Trusted Execution Environments (TEEs)

Christian Gehrmann (SICS)

ARTEMIS

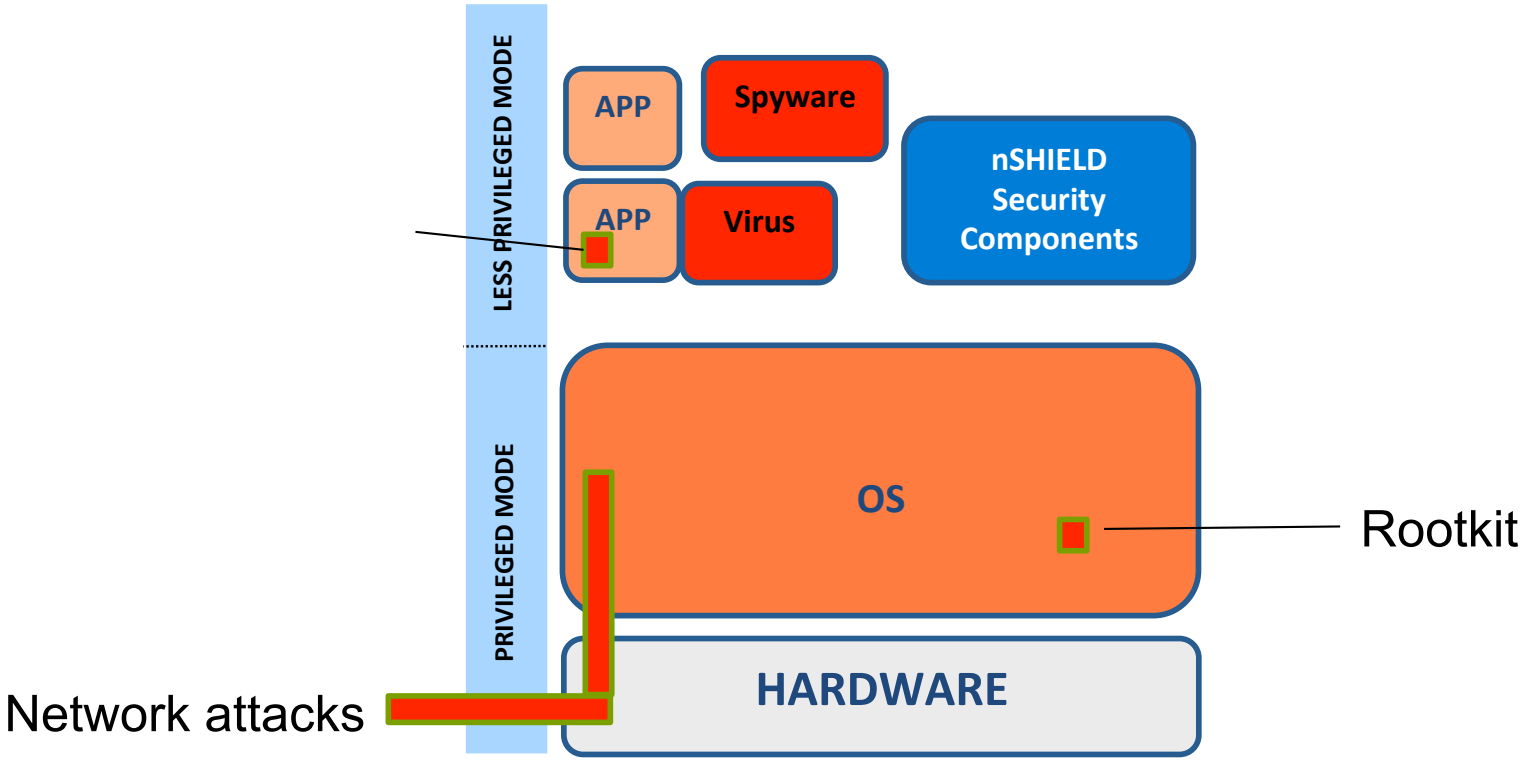
nSHIELD architecture and TEEs



Security critical functions!

nSHIELD

Threats!


LESS PRIVILEGED MODE
PRIVILEGED MODE
APP
APP
Spyware
Virus
nSHIELD
Security
Components
OS
HARDWARE
Rootkit
Network attacks

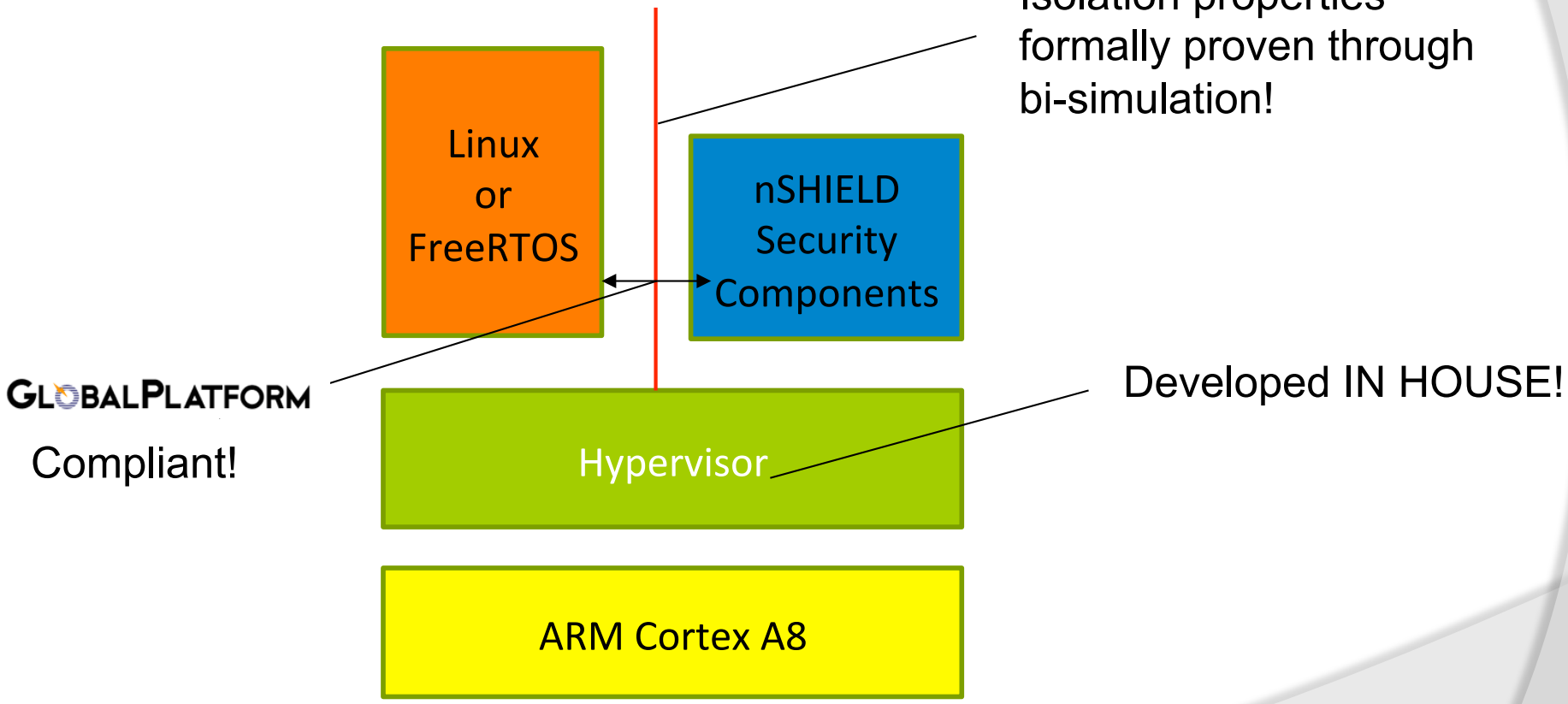
TEE implementation options

- Special purpose hardware modules
  - High security
  - No system monitoring possibilities
  - High cost
- On-chip TEE through virtualization
  - Flexible
  - Low cost!
  - System monitoring

nSHIELD

nSHIELD hypervisor based TEE

Target system!



nSHIELD

Hypervisor based TEE status (I)

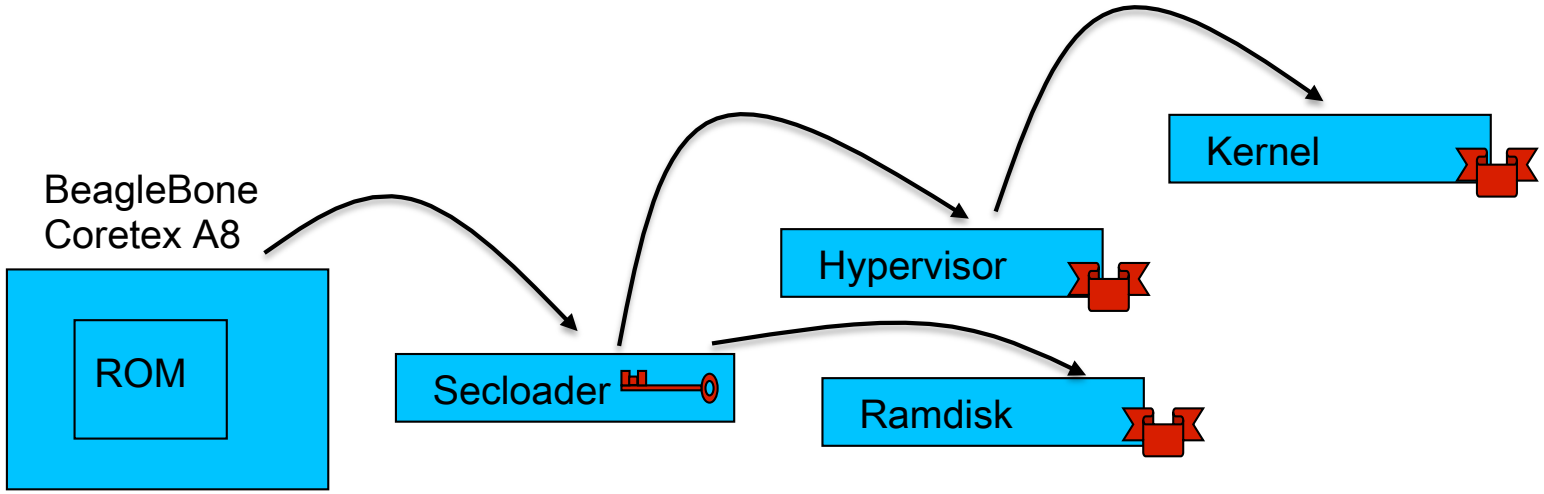
- Supports multiple OS (FreeRTOS) on ARMv5 and ARMv7
- Para-virtualization of OS system calls
- DMA protection through traps (OVP)
- Provides multiple isolated execution environments through arbitrary number of virtual guest modes
  - Kernel mode
  - Task mode
  - Trusted mode
  - Interrupt mode
- Each virtual guest mode has its own memory access configuration
- Efficient and simple hypervisor
  - RTOS performance overhead of 1-10 % (FreeRTOS)
  - ~12KB code
  - < 2KLOC (incl. debug, not HAL)

Hypervisor based TEE status (II)

- Port (ARM Cortex A8 ARMv7 OVP)
  - Ported hypervisor and FreeRTOS to ARMv7 architecture on OVP
  - Preparing hypervisor to run in real hardware
- Porting hypervisor to real hardware
  - Beagleboard and Beaglebone
    - TI OMAP 36XX & AM35X Platform
    - ARM Cortex A8 CPU
- Refactoring the hypervisor code
- Added a Hardware Abstraction Layer (HAL)
- Support for scheduling of multiple guest
- Linux port pre-study
- Started to implement global platform support

TEE and secure boot

- Without a verified boot chain the TEE will have a high risk of being compromised!



nSHIELD

Secure boot chain status

- Verified boot chain implemented on Beaglebone
  - RSA based signatures verified in a special purpose security loader
  - Core root of trust currently not implemented!
- Core root of trust should be in ROM!
  - We expect to have a customized ROM mask for next version of the prototype system!

nSHIELD

Next steps

- Linux port to hypervisor
- Global Platform API support
- Full verified boot chain including core root of trust in ROM
- Port of selected nSHIELD security services to the hypervisor based TEE
- Boot code and hypervisor code security assessment by Search LAB

nSHIELD

The END

That’s all folks!

ARTEMIS