Consortium

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

ASMONIA

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

SPONSORED BY THE Federal Ministry of Education and Research

Integrity Protection for 4G Devices and NW Elements

Manfred Schäfer, NSN Munich
Sascha Wessel, FhG-SIT Garching/Munich

WP 2 Contribution

ASMONIA Workshop

29.3.2011

Content

- **WP2 Overview**
  Crypt. SW integrity protection, hardening, malware detection
- **Motivation and Requirements** (partially ..)
  - Fundamental SW-IP expectations and needs
  - 3GPP (eNB, HeNB), UE view (smart phones)
  - …
- **Cryptographic SW integrity protection**
  - Use cases & examined methods
- **Hardening**
  - Examined methods, example
- **Conclusions & Outlook**

WP2 Overview

WP 2

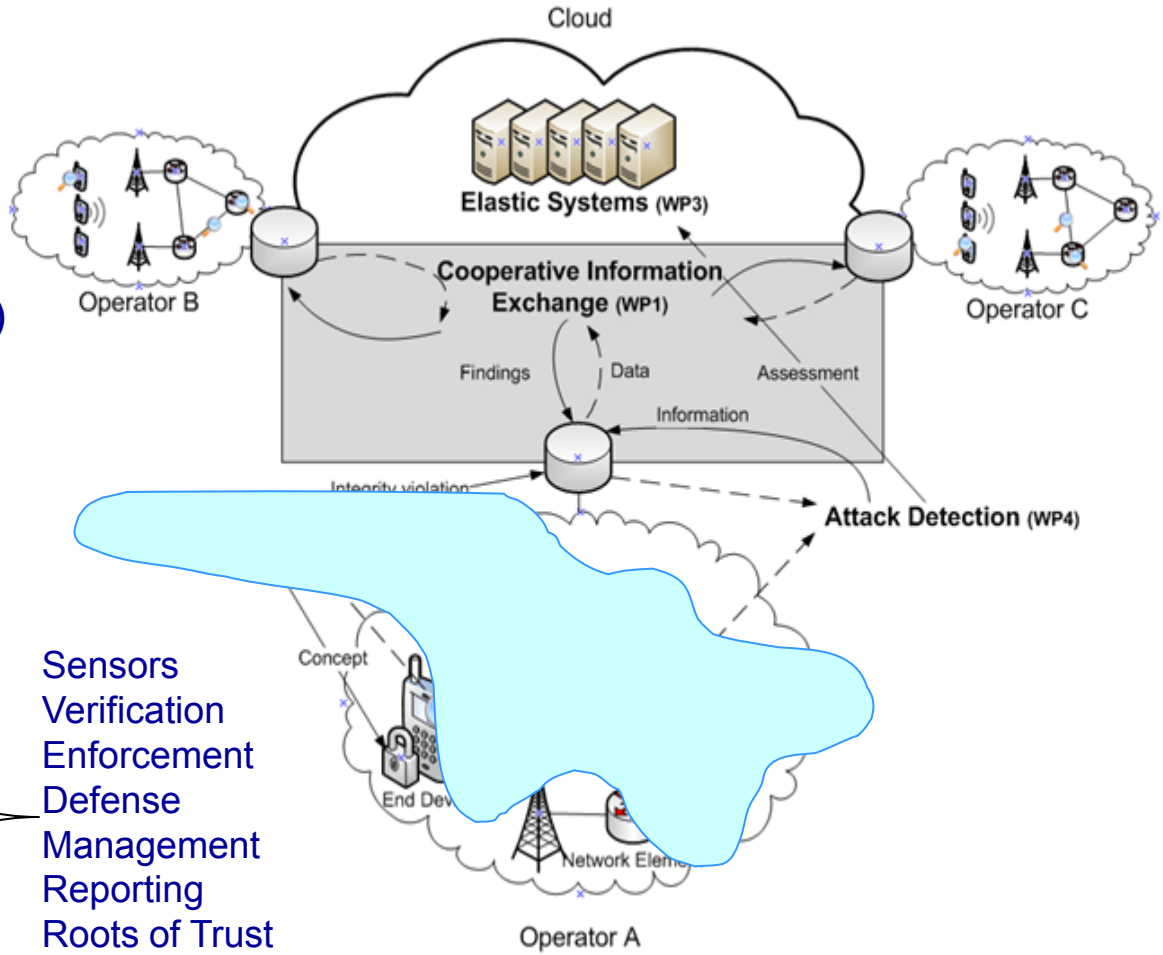
Methods for

- **Protection concepts**
  (Hardening, cryptographic integrity assurance, remediation, disinfection,...)
- **Anomaly detection**
  - Integrity breaches
  - Malware incidents

Dedicated mechanisms in

- **User equipment**
- **Network elements**
- **Infrastructure**
  (Vendors, Operators)

Sensors
Verification
Enforcement
Defense
Management
Reporting
Roots of Trust
....



WP2 Fundamental Expectations …

SW-IP enables to

- Ensure that SW or data has not been altered after creation process
- Identify that SW is coming from a specific, authorized source (Proof of Origin)
- Determine that SW is trustworthy and authorized for a specific purpose, time or target system
- Bundle SW with unmodifiable directives for usage, according to claims of an authoritative source
- Support enforcement of actions to be taken in the target system
- Get reliable knowledge of a system's state
- Achieve protection of many 'static (i.e. before SW is executed)' and 'dynamic (while SW is executed)' SW protection uses cases
- Apply efficient control mechanisms and to take advantage of security best practices and future-proofness ..

WP2 … and needs

But, when applying SW-IP

- No guarantee can be given that
  - (any mix of..) code is free of vulnerabilities
  - Multiple OS and applications on same system do not attack each other
  - Unsecure (web-) applications do not compromise sensitive functionality
    Example: JIT-compiled ‘data’ running as native code ...
- SW-IP methods themselves must be protected
  - Roots of trust
  - Measurement components
  - Verification and enforcement components

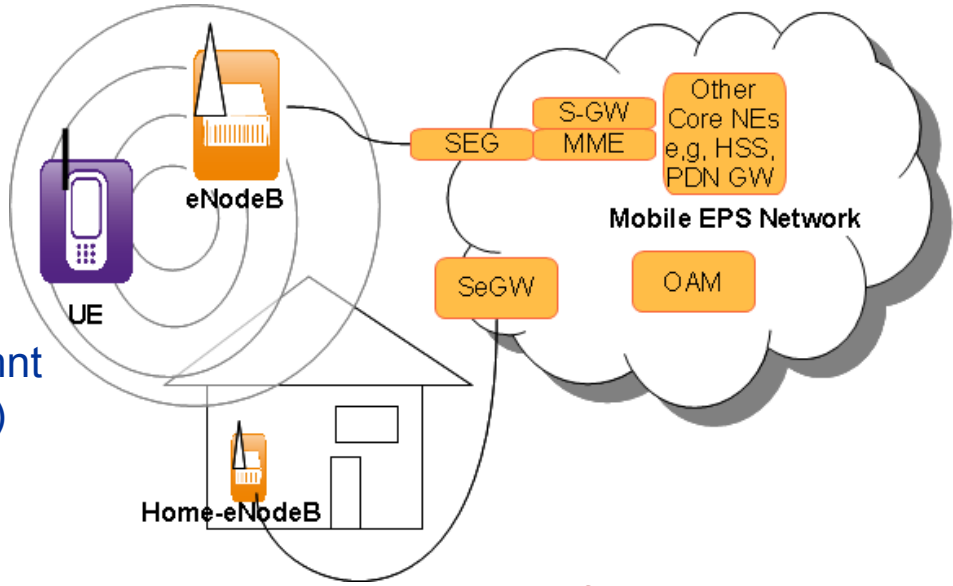
➔ **‘Hardening’ is another essential building block for system protection**

- Benefit / overhead trade-offs have to be balanced

WP2 3GPP Requirements

3GPP SA3: 4G Requirements including "SW Integrity protection"...

- ... essentially exist for Access Network
  - eNB: TS 33.401, clause 5.3 ...
  - HeNB: TS 33.320 (more stringent security requirements) ...
- Threads may arise from
  - Termination of security relations, requiring to locally store long term key material (backhaul, OAM)
  - Re-ciphering in node (data, session keys, user + signaling plane)
  - Need to protect radio part operation / mgmnt (licensed spectrum, regulatory constraints)
  - Exposition to public / home areas, outside an operators security domain
  - Usage of well known IP technology
  - Potential usage of Open Source Software and OS (hacker skills, tools/attacks become applicable and available)



Many of these issues may be mapped to SW-IP !

WP2 3GPP Requirements (related to SW-IP)

eNB, TS 33.401	
5.3.1 General	.. valid for all types of eNBs
5.3.2 Setup and Configuration	The eNB shall be able to ensure that software/data change attempts are authorized' 'The eNB shall use authorized data / software' 'Integrity / confidentiality protection of software transfer towards the eNB shall be ensured'
5.3.5 Secure Environment	'The secure environment shall support the execution of sensitive parts of the boot process' 'The secure environment's integrity shall be assured' 'Only authorized access shall be granted to the secure environment, i.e. to data stored and used within, and to functions executed within'.

related to 5.3.3 (key protection) and 5.3.4 (data protection)

also see 7.1; 8.3.2.2; 8.4

HeNB, TS 33.320	
4.4.4 Requirements on H(e)NB	The integrity of the H(e)NB shall be validated before any connection into the core network is established The configuration and the software of the H(e)NB shall only be updated in a secure way, i.e. the integrity of the configuration data including the licensed radio parameters and the integrity of the software updates must be verified.
5.2.1 Trusted Environment	The secure boot process shall include checks of the integrity of the TrE performed by the root of trust. Only successfully verified components shall be loaded or started... . The TrE , after having been successfully started, shall proceed to verify other components of the H(e)NB
6.1.2 Protection of trusted reference values	The TrE shall securely store all trusted reference values at all times. The TrE shall detect un-authorized modifications of the trusted reference values necessary for trusted operation of the device.

implies 'autonomous validation'

TR-069:signed DF

WP2 UE Requirements / scenarios

- Isolation of untrusted applications
  - E.g. 3rd party apps, untrusted web applications, controlled resource usage
- Trustworthy execution environment / attack resilience
  - supporting e.g., intrusion and anomaly detection (malware / SW-IP) and prevention
- Application whitelisting (with cryptographic signatures)
  - only trusted system components (e.g. kernel), trusted storage
- Separation of multiple environments
  - E.g. private and corporate part, radio part
- Policy enforcement
  - E.g. password policies, software update policies, device encryption
- Restricted functionality and locked devices (operator polices..)
  - E.g. SIM Lock, Net Lock
- Secure domains
  - E.g. for secure PIN entry for user authentication in mobile payments and banking
- Theft of devices
  - Remote wipe, device location, remote execution of commands

Use Cases for SW Integrity Protection

- **SW Delivery / Distribution:** Protect for one-time verification ...
- **Stored on repository:** Long-time storage / versioned and revoked SW
- **SW installation:** Update and installation, including download for install
- **Trusted Boot:** Remote Attestation, Trusted Reporting (TPM / DRTM)
- **Secure boot:** Autonomous validation, as for HeNB / eNB
- **Runtime aspects**
  - **SW download:** executed during system is running (as for Java / UE)
  - **Load-time:** each time before SW is used
  - **Store-time:** while SW remains installed
  - **Execution-time (in memory):** while SW is executed

State of the art: Zoos of different mechanisms, SW technologies, methods, ... --> need for harmonization and generalization

WP2 SW-IP Methods examined

- **'Hash based' TCG Methods**
  - TPM / CRTM / DRTM, known attacks
  - Trusted Network Connect

- **Standard Methods applying Code Signing**
  - TCG: Mobile Trusted Module (MTM)
  - Microsoft Authenticode (for MS executables)
  - JAVA signing
  - Nokia / Java signing (PKI, testing house) / Symbian Signed
  - Lotus Notes (IBM)
  - Open Source communities / Web of Trust mechanisms (e.g. RPM, PGP)

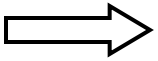
- **Methods providing runtime protection**
  - IBM IMA (TPM based load time extension)
  - Afick; Samhain; Tripwire
  - Arbaugh; Catuogno & Visconti; DigSig / BSign
    (Load-time protection f. ELF binaries, integrated signatures, OS dependent, CPU independent)
  - Intel's SIS architecture (using SMM, run-time memory checks, CPU dependent, platform indep.)

Conclusions on SW-IP Methods

- **Major discriminating aspects of examined methods**
  - (Restrictions in) scope and use cases / platform, HW dependencies
  - Infrastructure implications: Trust/key management / SW provisioning / preconditions ...
  - Mechanisms for secure reporting
  - Upgradability / long-term cryptography / evolution concepts
  - Expressiveness / security governance & control
  - Implementation efforts and security
- **Some reasoning**
  - Heterogeneity of existing methods is a challenge ...
  - Certificates / signatures show significant advantages vs. *pure hashes*
  - For vendor controlled products hierarchical key management (PKI) preferred over WoT
  - SW-IP Integration into Mobile NW only partly considered e.g. for HeNB / Tr.069
  - TCG/TPM methods not considered in 3GPP (proprietary infra @ MNO?)
  - Preventive protection methods such as *sufficient hardening* is a must …

WP2 Hardening methods examined

- **Compile-time software hardening**
  - Software isolated processes
  - Memory corruption mitigation methods
- **Linux Operating System Extensions**
  - Container-based operating system virtualization
  - LSM (Linux Security Modules)
- **Process Virtualization and Sandboxing**
  - Byte code translation (JIT)
  - SB for untrusted native code
- **System Virtualization**
  - VMMs (XEN, KVM, VMware, L4 microkernel,..)
  - Smart phone example



WP2 Outlook

Implications for future work

- **Most relevant SW-IP research topics**
  - Adaptation to identified requirements ... e.g., regarding 3GPP compliance
  - Harmonization (common components, paradigms, infrastructure, integration)
  - Secure implementation (hardening) of suited 'Roots of Trust'
  - Keeping impacts on operator infrastructure minimal
  - Integration of (3GPP standards for) upcoming NEs, such as eNB relay nodes
  - Lightweight attestation

- **Most relevant research topics in hardening focus**
  - Isolation mechanisms
  - Trustworthy virtualized components, e.g., for security applications
  - Runtime protection
  - Remediation
  - SW/HW balance wrt. attack resilience

WP2 Discussion

WP2 Backup

WP2 Evaluation Criteria

- Complexity
- Implementation feasibility
- Attack resistance
- Efficiency
- Performance
- Scalability
- Required modifications on existing components
- Reusability of existing source code (also license aspects)

Common

- Low performance impact
- Modest additional memory (as far as possible)
- No additional hardware (as far as possible)
- A small TCB size (as far as possible)
- Power management awareness (the battery is an exclusive resource and frequent wakeup events prevent energy saving)
- Immune against memory corruption attacks (as far as possible) or make them more difficult
- Designed for long time operation without reboot

Mainly relevant in UE context

WP2 Evaluation Criteria

- 3GPP compliance
- Use case coverage / adaptability
- Restrictions / applicability
- Appropriateness for long-term usage
- Implications for the mobile network infrastructure
- Fulfillment of manufacturer obligations and responsibilities
- Implementation aspects such as platform and HW dependencies
- Common components

Mainly relevant in NE context