DECOIT

IDACCS Wireless 2014

Integrity protection in a smart grid environment for wireless access of smart meters

Prof- Dr.-Ing. Kai-Oliver Detken
DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
URL: http://www.decoit.de
E-Mail: detken@decoit.de

Consultancy & Internet Technologies

DECOIT

Table of Contents

- Motivation
  - National project SPIDER
  - Smart meter scenario
- Threat analysis and Trusted Computing approaches
  - STRIDE
  - TPM and TNC
  - TCN
- Device integrity in smart grids
- Wireless security in smart grids
- Conclusions

DECOIT

Motivation and smart meter scenario

Consultancy & Internet Technologies

Motivation

Changes of the energy market

- Fluctuating decentralized energy generation versus stability
- Consideration of different interests
- Intelligent regulated energy grids
- German law EnWG §21 postulates intelligent systems

Intelligent ≠ Secure

- Critical infrastructure has to be secure
- Personal allowance data has to be protected
- Creation of trust by security mechanisms is important
- The German Federal Office for Information Security (BSI) defines security requirements and specification for critical infrastructure

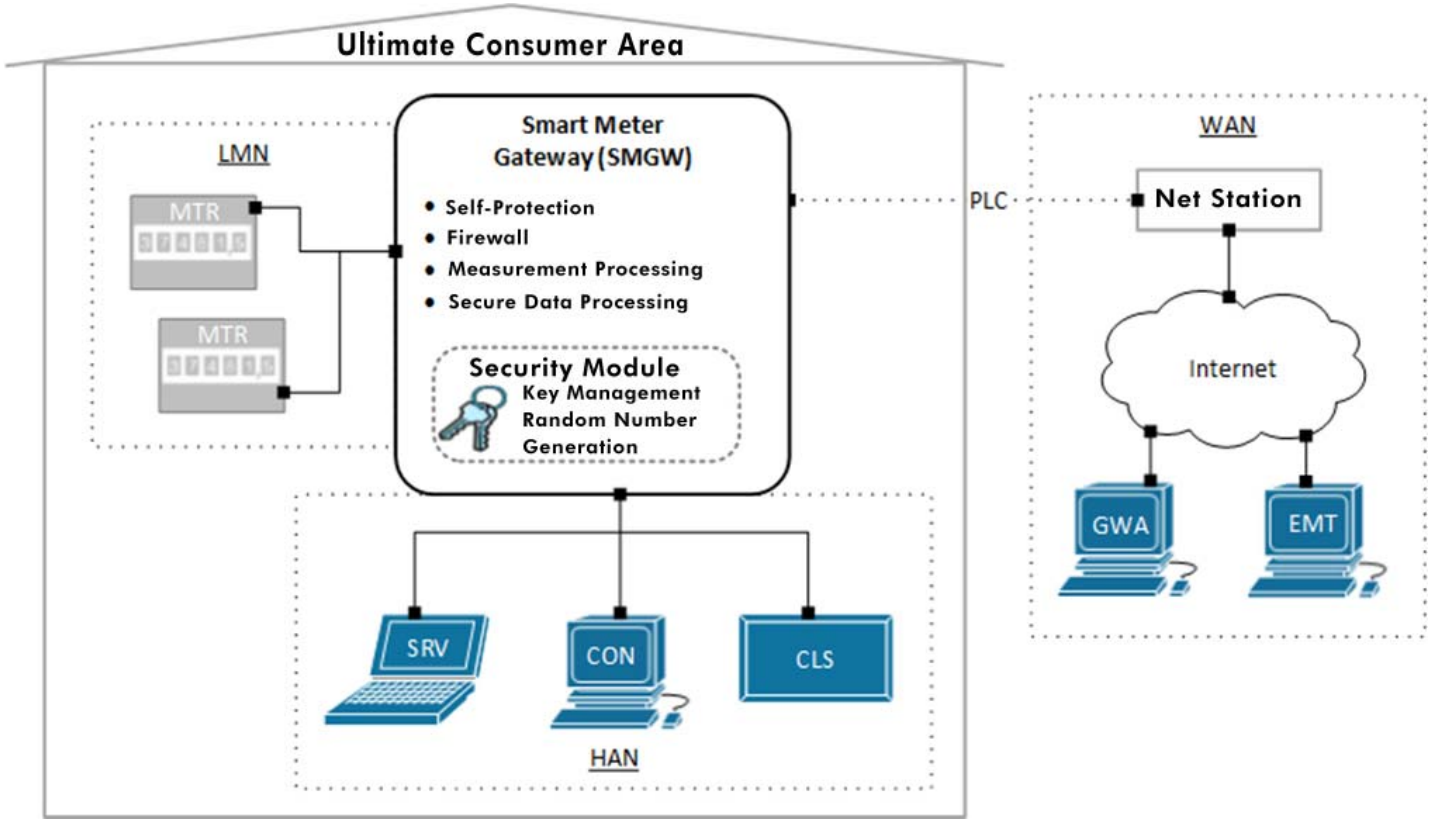
National research project SPIDER

- Secure Power-line Data communication within intelligent energy grids (SPIDER)
  - 2 years project of ZIM (BMWi)
  - Lifetime: 1st March 2013 till 28th February 2015
  - Budget: 1.2 million Euro
  - Project goal: Development and BSI certification of a Smart Meter Gateway (SMGW)
  - Website: www.spider-smartmetergateway.de
  - Partners:
    - Industrial partners: DECOIT GmbH, devolo AG (project leader)
    - Academicals: University of Applied Sciences of Bremen, Fraunhofer FOKUS, University of Siegen
  - Associated partners: Maxim Integrated, datenschutz cert
  - Energy providers: Vattenfall, RWE

Bundesministerium für Wirtschaft und Technologie

ZIM Zentrales Innovationsprogramm Mittelstand

Smart meter scenario (1)



Smart meter scenario (2)

- Local Metrological Network (LMN): SMs for various commodities (e.g. electricity, gas and water) are connected with the SMGW through the LMN.
- Home Area Network (HAN): Controllable local systems (CLS, e.g. local solar power plants) are connected through the SMGW via the HAN. Utilizing the SMGW as proxy, CLSs can be controlled by external entities (e.g. solar power plant vendors for maintenance). The consumer can interact with the SMGW across the HAN to access the measurement data gathered by its SMs. A service technician is able to readout SMGW system events for troubleshooting purpose through the HAN connection.
- Wide Area Network (WAN): The GWA is able to interact with a SMGW through the WAN for management purpose. The SMGW may also communicate measurement data to authorized external entities via the WAN.

DECOIT

Threat analysis and Trusted Computing approaches

Consultancy & Internet Technologies

Threat categories

- The BSI defined three categories of security threats based on the described SMGW scenario
  - Disclosing data of the infrastructure by data collection
  - Manipulation of data of the SMGW by fraud or disruption
  - Alteration and control of involved systems (e.g. CLS, SMGW)
- Motivation for attackers
  - Attacker from the WAN interface → high motivation (external person)
  - Attacker from the HAN interface → small motivation (energy customer)

STRIDE approach

STRIDE approach - further analysis after security requirements

- STRIDE = Spoofing, Tampering, Repudiation, Information disclosure, Denial of service und Elevation of privilege
- Using STRIDE additional threats were discovered (e.g. in the class of tampering and Denial of service)
- From BSI's point of view, integrity can be established by a hardware seal only
- However, solutions exist in Trusted Computing to recognize and control these threads more effectively

Threat	Security aspect
Spoofing	Authentication
Tampering	Integrity
Repudiation	Data acceptance
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of privilege	Authorization

Trusted Computing (TC) of TCG

- Trusted Platform Module (TPM)
  - Hardware-based identity (hardware trust anchor, Root of Trust)
  - Integrity measurement of hard- and software
  - Trusted boot process (Trusted Boot)
- Trusted Network Connect (TNC)
  - System integrity validation (remote attestation)
  - Can be used for authentication and monitoring

TRUSTED COMPUTING GROUP™

DECOIT

Trusted Core Network (TCN)

- TCN is a hardware-based approach from Fraunhofer SIT to enable device identity and integrity checks in a distributed environment
- Each endpoint device checks its next neighbors
- Splitting of security and functional communication
- TPM should be used to build a TCN with help of
  - Secure storage for cryptographically keys and device status information
  - Random number generator
  - Signature calculation with the chip directly
  - Authentic attestation of the device status
- TPM has a EAL-4+ certification and Common Criteria EAL-5 certification for the chip design

Fraunhofer SIT

Goals of the Trusted Core Network

Distributed, redundancy control (peer-to-peer)

Avoid the distribution of malware

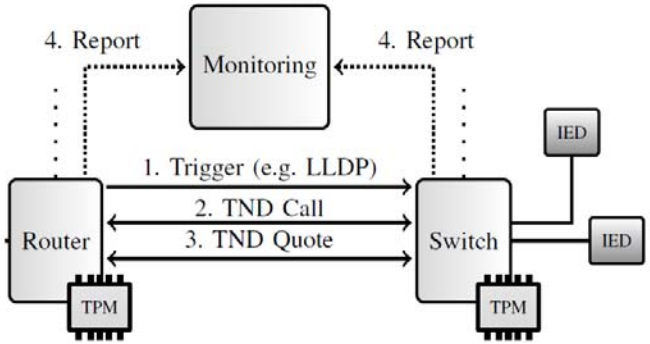
Monitoring with fast alarms

Protection of confidential data

Secure and efficient management processes

TCN architecture

- The core of TCN is the Trusted Neighborhood Discovery (TND) protocol
- It provides an extended link-layer network discovery protocol for anomaly detection
- TND enables the verification of the integrity of software and hardware states of adjacent devices
- When TND is integrated into industrial devices to operate inside industrial back-end networks, it is initiated by the reception of a trigger message from the neighboring device
- Additionally, periodically re-launching the attestation procedure with all devices in the neighborhood provides fresh information
- To avoid Denial of service attacks, the network components are restricted to a valid identity key and a minimum timeout, which is verified before any incoming message is further processed



DECOIT

Device integrity in smart grids

Consultancy & Internet Technologies

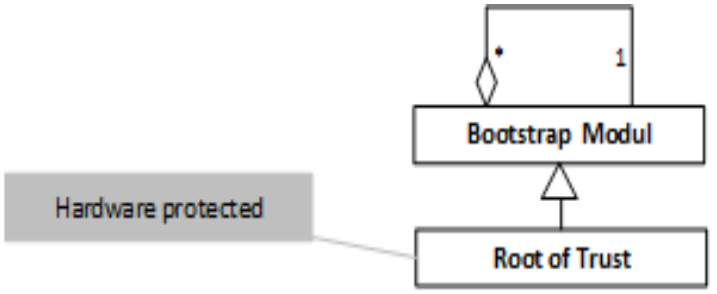
SMGW integrity (1)

Securing of the hardware

- Passive sealing of the SMGW box (defined by BSI)
- Electronical sensor for box opener
- Tamper resistant grid for some components

Securing of the basis integrity

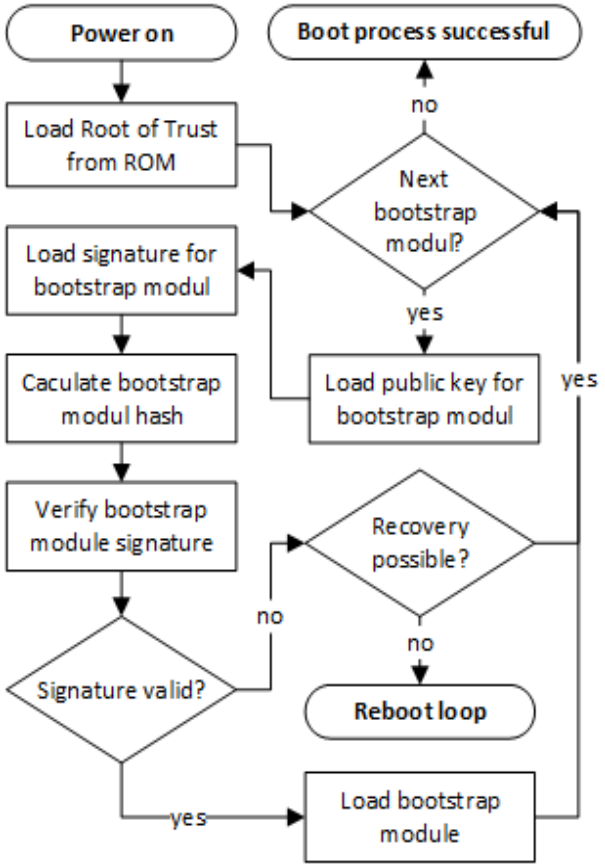
- Use of Secure Boot and Root of Trust in combination
- The boot process is organized as a list of bootstrap modules
- The first module in this list is the Root of Trust, which is protected by hardware



SMGW integrity (2)

Boot process with Secure Boot

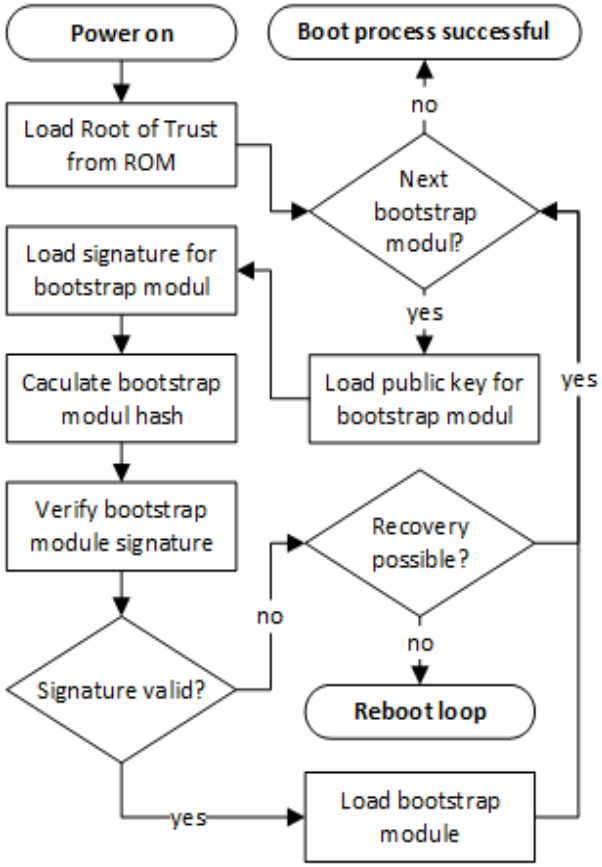
- The Root of Trust holds a reference to the next boot stage, the basic boot loader (bootstrap module *n*)
- Before this module is loaded, the boot loader is verified against a known signature by the Root of Trust, using a configured fixed public key
- Only if the signature of the boot loader is valid, it is loaded
- The boot loader continues the boot process and verifies the system's hardware integrity (e.g. state of the tamper resistant grid and the chassis)
- Additionally, it verifies the operating system software using a known signature and the corresponding public key



SMGW integrity (3)

Boot process with Secure Boot

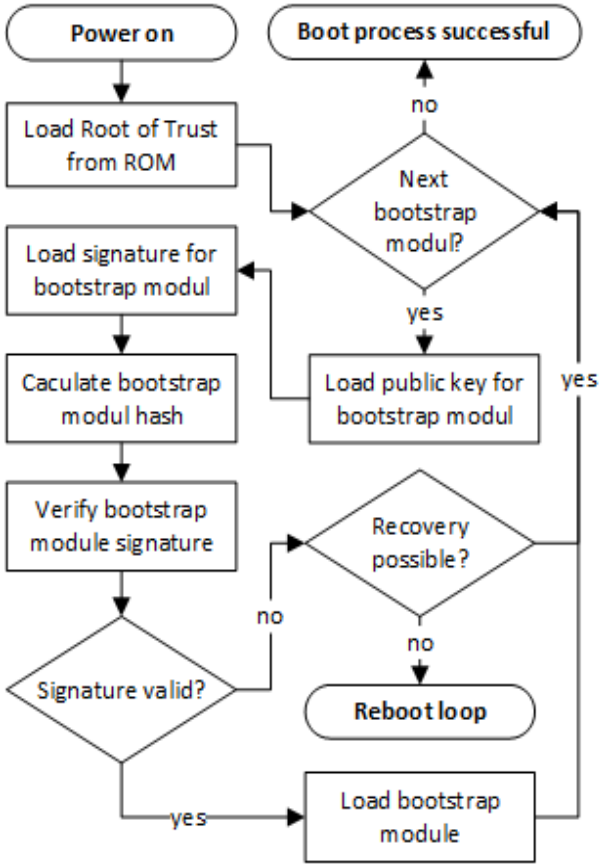
- If the signature is correct, the operating system is loaded and in turn may verify additional software (bootstrap module $n+1$) by using known signatures and public keys
- As soon as the verification fails, the boot process is interrupted and the system returns to a secure state, if system recovery is not possible
- In this case a secure state is a reboot loop
- System recovery is possible due to a second partition, which contains a duplicate firmware



SMGW integrity (4)

Boot process with Secure Boot

- As long as the boot loader is verified correctly, it is possible to load the firmware from the second partition, if the firmware from the first partition is compromised
- Only if both firmware versions are compromised, the reboot loop is entered
- This ensures that a SMGW is only in use, if the initial boot process was trustworthy



DECOIT

Wireless security in smart grids

Consultancy & Internet Technologies

DECOIT

Use of wireless communication

- Within smart grids, the goal of using wireless communication is to connect a large number of low-level endpoints such as sensors (e.g. smart meters) to a fewer number of high-level endpoints mainly
- Furthermore, mesh networks or mobile ad-hoc networks can provide high redundancy in communication routes, highly dynamic infrastructures and fast redress processes in the case of failures
- Thus, wireless communication can be expected to be part of the new communication infrastructures for the smart grid

M-Bus possibilities for smart grids

- Within a smart grid environment the SMGW has to use the wireless M-Bus (Meter-Bus) interface
- That includes the following new possibilities:
  - The data (e.g. heat consumption) are read out electronically
  - At one single cable, which connects to a building controller, all consumption meters of a housing unit can be attached
  - All meters are individually addressable
  - Apart from the availability of the data at the controller a remote reading is possible

DECOIT

Wireless communication risks

- But dynamic wireless and ad-hoc networks include new security issues
- Additionally, for the protection of the traffic one main attack vector is the routing information, which can be manipulated
- Wireless devices in smart grids are built into places which often do not belong to and are not accessible by the company that owns them (e.g. consumer home)
- The heterogenic environment of mixed-level devices increases the security risks, because low-level devices may not be as protected as high-level devices due to lower computing capacity or energy consumption matters

Building a trust zone

- During the connection of the SMGW to the smart meters, the SMGW has to assume that the meters and connections are trustful
- With the use of the TCN approach as described before a trustworthy status of the SMGW and its smart meters can be reached
- The solution: a trusted smart grid zone can be setup from the metering point to the gateway administrator to beware manipulations and the privacy of the transmitted data

DECOIT

Conclusions

DECOIT

Conclusions

- Integrity measurement and remote attestation is important
  - Enhancement of the security of the SMGW
  - Improvement of the authenticity of data
- Secure Boot enables basis integrity
  - It is possible to setup a trust chain with TNC
  - Integrity verification is also applied at runtime
- TCN approach includes the smart meters
  - Smart Meters with TPM chip are able to check each other
  - A trusted smart grid zone can be established
- BSI specifications do not mention similar solutions!

DECOIT

Thank you for your attention!

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
http://www.decoit.de
info@decoit.de

Consultancy & Internet Technologies