The 2nd IEEE International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems
11-12 September 2014, Offenburg, Germany

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

Prof. Dr. Kai-Oliver Detken[1], Carl-Heinz Genzel[2], Dr. Carsten Rudolph[3], Marcel Jahnke[1]
[1] DECOIT GmbH, Fahrenheitstr. 9, D-28359 Bremen, detken@decoit.de, www.decoit.de
[2] University of Applied Sciences of Bremen, D-28199 Bremen, carl-heinz.genzel@hs-bremen.de
[3] Fraunhofer SIT, D-64295 Darmstadt, carsten.rudolph@sit.fraunhofer.de

To meet future challenges of energy grids, secure communication between involved control systems is necessary. Therefore the German Federal Office for Information Security (BSI) has published security standards concerning a central communication unit for energy grids called Smart Meter Gateway (SMGW). The present security concept of the SPIDER project takes these standards into consideration but extends their level of information security by integrating elements from the Trusted Computing approach. Additionally, a tamper resistant grid is integrated with chosen hardware modules and a trustworthy boot process is applied. To continually measure the SMGW and smart meter (SM) integrity the approach Trusted Network Connect (TNC) from the Trusted Computing Group (TCG) is used. Hereby a Trusted Core Network (TCN) can be established to protect the smart grid components against IT based attacks. That is necessary, especially by the use of wireless connections between the SMGW and smart meter components.

Keywords: Smart Meter Gateway, Trusted Computing, Trusted Network Connect, Trusted Core Network, Smart Meters, Integrity.

I. INTRODUCTION

Future energy grids need to enable volatile and peripheral energy production without impacting the grid's stability. Additionally, different external entities and their varying interests have to be considered [4, p. 14]: Metering point operators responsible for metering systems, measurement service providers, which readout and provide data measured by metering systems, distribution grid operators, which maintain and support local energy grids, energy suppliers, which act as energy merchants using the infrastructure provided by distribution grid operators, gateway administrators (GWA), which configure, control and monitor SMGW within their lifecycle and consumers (CON), which may operate their own local power plant.

Therefore a Trusted Core Network (TCN) is necessary to protect this "Internet of things" infrastructure against IT based attacks. Among commonly known attacks, the TCN functional principle also protects network components against new threats such as the malware "chameleon", which was developed and demonstrated in the lab just recently by the University of Liverpool. The malware "chameleon" can manipulate router settings, install its own firmware and disseminate autonomously. An attack with such WLAN viruses is rather difficult to detect in current networks and the malware may disseminate over wired networks as well. In a TCN, hubs are capable of identifying each other and checking whether the software or settings have been modified. This allows the detection of infected hubs and their exclusion from communication.

TCN is based on the standardized Trusted Platform Module (TPM) as the trust anchor to reliably verify a device's condition and its identity. Each device is equipped with a TPM that stores information about the licensed software and other relevant configuration details. With this information SMGW and SM components are able to verify all the devices in their neighborhood. If the actual state deviates from the specified state, the system will detect the modification and raise an alarm. This allows for a quicker and better detection of and defense against potential attacks. If suppliers provide reference values for firmware, attacks in open networks (for example between different Wi-Fi nets) may be recognized as well which thus prevents the malware from being disseminated further.

The solution can be used for ad-hoc secure mobile networks and as Trusted Core Network (TCN) for industrial nets. Smartphones and other devices may be included in the security monitoring via additional protocols as well, for example via the standardized Trusted Network Connect (TNC).

The present security concept has been developed within the German research project SPIDER [18]. Additionally, a first TNC prototype regarding the TCN approach is described in this paper, developed by Fraunhofer SIT.

II. SCENARIO DESCRIPTION

Future challenges of energy grids may only be satisfied, if energy production and energy consumption is coordinated using secure communication between the different external entities. Therefore, two components have been introduced by the BSI to today's energy grids in Germany. They are the basic building blocks for a so called Smart Metering System. The SM describes an intelligent meter for energy commodities and the SMGW is a central communication unit for them.

Figure 1 shows the important components and areas of a Smart Metering System. This system and its security specifications are described by the BSI standards (see [4], [5], [7], and [8]).

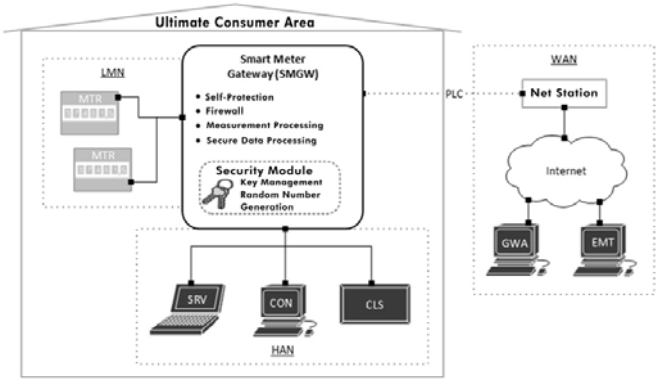

Figure 1. SMGW communication via PLC via the WAN

The SMGW is responsible for the reliable processing and secure storage of measurement data provided by various connected SM. Hereby, it facilitates a secure communication between the individual external entities. The BSI has categorized these individual entities into different networks (see [4, p. 13-15]) as listed below:

a. **Local Metrological Network (LMN):** SM for various commodities (e.g. electricity, gas and water) are connected with the SMGW through the LMN.

b. **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, CLS can be controlled by external entities (e.g. solar power plant vendors for maintenance). The consumer can connect to the SMGW across the HAN to access the measurement data gathered from its SM. A service technician is able to readout SMGW system events for troubleshooting purpose through the HAN connection.

c. **Wide Area Network:** The GWA is able to connect to a SMGW through the WAN for management purpose. Furthermore, the SMGW may communicate measurement data to authorized external entities via the WAN.

Besides that the SMGW acts as firewall, separating the described networks and their participants from each other logically and physically [4, p. 13-15].

For the secure data storage and communication, an SMGW makes use of a so called Security Module that provides cryptographic functionality such as: [5, p. 10]

a. Secure storage of certificates and keys

b. Key generation an key agreement using elliptic curves

c. Digital signature generation and verification

d. Reliable random number generation

The SMGW receives, processes and stores measurement data from SM. A SM differs from a usual metering system by being able to communicate with the SMGW in a cryptographically secured manner. Furthermore, a SM is controllable by the SMGW [4, p. 15-16].

To facilitate the integration of the described components at the customer's premises, further components are needed. Especially the WAN connection is established using the local energy grid. G3 Power Line Communication (PLC) enables the connection to a local substation across the "last mile". At the substation the communication is routed to the WAN using a common WAN technology (e.g. Ethernet, UMTS). Furthermore, to minimize constructional changes on the customer's premises to connect devices to the LMN, wireless M-Bus can be used.

For privacy reasons the data, which may be communicated into the WAN and other areas, is specified by BSI standards as well. All measurement data provided by a SM and all derived data calculated by a SMGW are owned by the consumer, who is assigned to the SM. Authorized external entities are interested in using these data (e.g. for billing or tariffing purpose). The data may also be used to manage an energy grid. The GWA has no access to these data. Instead, the GWA is able to access and store data relevant to maintain a SMGW (e.g. configuration files, system log and calibration log). The service technician is only permitted to perform system diagnosis. Therefore the technician is allowed to read data relevant to maintain the SMGW, but is not able to store such data like the GWA does. In general, every individual participant is only allowed to access the SMGW via the network it is associated with (see figure 1) [4, p. 118-119]. [3]

III. THREAT ANALYSIS

The BSI defined three categories of security threats, based on the described scenario (see [7, p. 33]). These categories are organized by their impact on a Smart Metering system, in the following list:

a. **Disclosing data**, which are stored on or processed by the SMGW (measurement data, configuration data), with the intention to gather information about the smart metering infrastructure.

b. **Manipulating data**, which are stored on or processed by the SMGW (measurement data, tariff data), with the intention to change the data in order to gain advantage or to interrupt the proper operation of components.

c. **Alteration and control of involved systems** (CLS, SMGW, etc.) with the intention to compromise the smart metering infrastructure.

Every category may be further distinguished by its origin. An attacker from the WAN side is generally characterized to be more motivated than an attacker from the HAN side. If an attack via the WAN is successful, it can be easily extended to further systems. HAN attacks may be more limited to local peculiarities instead [7, p. 33].

Based on the BSI insights, a complementary threat analysis was conducted within the research project SPIDER using the STRIDE approach by Microsoft [15]. STRIDE as shown in table 1 is an acronym, which enables the

classification of threats focusing on security aspects impaired by them, while not quantifying them.

Using STRIDE additional threats were discovered, most of them fall into the classes tampering and denial of service (DoS). The latter class may only be mitigated e.g. by supervising system resources and using prioritization. However, solutions exist in Trusted Computing to effectively recognize and control threats of the first class. The provided security concept takes these results into consideration and emphasizes on security aspects that are less cared about within the BSI standards. [3]

TABLE I. STRIDE APPROACH (THREATS AND SECURITY ASPECTS)

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

IV. CORE TRUST ELEMENTS

In the following sub-chapters the different trust elements, which are needed to build a TCN finally, will be described.

A. Trustworthy boot process

The manipulation and replacement of a system's hardware parts is considerably difficult, because in most cases they are protected by mechanical means. Instead, the manipulation of software is considerably simple. Hence, a measurable protection of the software's integrity is the key to protect a system, which provides security functionality. This requirement involves a circular dependency, because the measurement of software integrity is only possible by using software as well [12, p. 569, p. 570].

In order to overcome this dependency amongst others, a concept called "Root of Trust" is used in Trusted Computing. Literature describes the term "Root of Trust" as a non-deniable characteristic or aspect of a single person or thing, which justifies its trustworthiness (see [11 p. 31]).

Therefore, it has to resist tampering to a high degree or make it even impossible. Thus, the "Root of Trust" may form the basis for the integrity measurement of a system or platform. According to that, the Trusted Computing Group (TCG) describes the term "Chain of Trust". It expresses a system's integrity as a calculated trust chain, which is built at boot time, starting at the "Root of Trust" across various hierarchically organized components of the system. A component (n) inside this chain knows the proper integrity state of its successive component (n+1) and evaluates it against this state. Finally, it creates an evaluation record. If the evaluation is successful, the successive component (n+1) starts evaluating its next component (n+m). If the entire chain evaluation is successful, all successive components should be in an expected state, assuming that the "Root of Trust" is not changeable. Hereby, manipulations (e.g. by an attacker) on hard- and software are recognizable [10, pp. 4-7], [13, pp. 7 - 8].

This process is widely called trustworthy boot process and is distinguished in three categories (see [16, p. 50]) as follows:

a. **Trusted Boot:** Evaluation of components using analysis and measurement methods. Only one valid system state exists.

b. **Secure Boot:** Evaluation of components using analysis and measurement methods including actions, if the evaluation results in a compromised system. Only one valid system state exists.

c. **Authenticated Boot:** Evaluation of components using analysis and measurement methods including actions, if the evaluation results in a compromised system. This process knows several valid system states.

Unfortunately these categories are often used interchangeably [16, p. 50].

B. TCG's TPM and TNC approach

"The TCG is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms [14]." The published standards shall aid in the detection of alterations on IT platforms/systems including, but not limited to, software attacks, configuration changes, security flaws and faulty applications. [14]

A major challenge within the field of IT security is ensuring trustworthiness of an IT system, because in most cases it is not obvious if a system's hard- or software is tampered with. Software on its own is not able to solve this problem, as software is more prone to tampering, than hardware is (see previous section). The TCG has developed a Trusted Platform Module (TPM) standard, which describes an additional hardware component. It contains a fixed, non-public key pair, which is considered to be the modules identity. The TPM is tightly integrated inside a system and can act as a "Root of Trust", because it is not changeable. It also provides functionality to measure a system in form of a trustworthy boot process [13].

TPM is a central element in Trusted Computing providing the system's identity. However, the BSI specifies that the security module holds the identity of a SMGW. Albeit both modules use private keys, which never leave each module (see [14, p. 1], [5, p. 56]), and both are tightly integrated into their surrounding systems. Furthermore, they need to sustain physical tampering to certain extent [13, p. 47], [2, p. 12, 30].

Besides a fixed identity, Trusted Computing uses TNC to measure and certify a system's integrity. Often a TPM is used to measure and store system attributes securely, which are needed by TNC to certify the system's integrity. The measurement is typically executed on system start-up, but

may also be executed on certain system events (e.g. writing to the location containing the operating system). Remote attestation is a TNC concept, which allows certifying the integrity by sending the measured values to a remote entity for evaluation [13, S. 8-10]. According to this, the BSI requires some form of self-tests to verify security relevant functions and data [7, S. 38, 79], which is not as sophisticated as TNC and as already mentioned, these may only be trustworthy if they are secured by concepts like the "Root of Trust", as it is applied by Trusted Computing (see chapter 4, section A).

By measuring and certifying a system's integrity, hard- and software tampering is recognizable. This aids to reduce possibilities to conquer a SMGW permanently. However, this security aspect is treated only shallowly by the BSI standards. The introduction of integrity control would further strengthen the authenticity of data being communicated. A successful authentication must not certainly indicate a proper functioning SMGW, instead only if its authentication and its integrity are valid, the SMGW most certainly works as expected. This should lead in reverse to data, which is most certainly valid too.

The TNC specification by TCG describes an architecture, which provides instruments to validate the system integrity of endpoints in a network to facilitate trustworthy communication. TNC defines two scenarios: [13], [14]

a. The first scenario describes an **authentication process** which evaluates a system's integrity in addition to any provided credentials.

b. The second scenario describes the **monitoring of a system's integrity** continuously.

Finally, the TNC standard in combination with some sort of trustworthy boot processes represents the most valuable security enhancement in contrast to BSI standards. However, the current TPM version 1.2 is not suitable because it does not fulfil the cryptographic requirements of the BSI standards. For example, the BSI requires elliptic curve based algorithms, which are not part of the TPM version 1.2. Future TPM versions like 2.0 may include stronger cryptographic algorithms. But that has to be evaluated, once such modules are available and the specification is final. [3]

C. Concept of a Trusted Core Network

The novel concept for security realized in the so-called Trusted Core Network (TCN) is motivated by the following requirements. Instead of the standard approach of access control and authenticity and confidentiality for all traffic, this approach bases security on individual network nodes. Each network node is safeguarded as sensitive constituent. Thus, all network nodes provide a distributed basis for implementing a secure information and communication infrastructure. All nodes regularly check the health of other nodes in their vicinity. The concept can be seen as "neighborhood watch" for IT networks. Current solutions for anomaly detection in industrial environment are mostly software-only based as for example the framework described in [19]. These mechanisms fail in the case of successful attacks that change the status of devices e.g. by exchanging the firmware. The core of TCN is the Trusted Neighborhood Discovery (TND) protocol. It provides an extended link-layer network discovery protocol for anomaly detection in industrial systems.

TND uses Trusted Computing technology for secure identification of devices and to distribute reliable status information via remote attestation as defined by the Trusted Computing Group (TCG). Using these security functions, each node reliably assesses the identity and the trusted state of all directly adjacent nodes and reports the result to a monitoring server that can correlate these reports, raise alerts and induce reactions.

1) Security requirements motivating TCN

One very relevant threat in critical infrastructures is the manipulation of devices by either corrupting software running on the device or by changing configuration data. Devices in such infrastructures usually have a clearly defined role. Therefore, the correct software status should be known. Furthermore, configurations are relatively stable or change within clearly defined boundaries. However, experience shows that one needs to assume that in most devices software can be changed and success probabilities for attacks are very high, much higher than failure rates in safety considerations.

Thus, one goal of security mechanisms in infrastructures is to continuously monitor the status of all devices. This monitoring should not depend on communication links to central control entities. Instead, distributed infrastructures require fast and self-contained distributed security monitoring for early detection and fast containment of attacks. Reactions need to be a mix of automated reactions and reactions induced by humans. Fast automated reactions should always aim at maintaining essential core functionality while preventing the spread of attacks to other parts of the infrastructure. More far-reaching defence and redress actions should be controlled by operators knowing the context learned from aggregated information.

2) The Trusted Core Network Architecture

This section introduces the TCN architecture using Trusted Network Discovery (TND) that enables the verification of the integrity of software and hardware states of adjacent devices within critical network segments. Using a TPM, remote attestation is initiated from all devices in the neighborhood of each network component. Thus, each device or node can autonomously detect and react to changes in software and hardware of the others. This attestation includes the TPM-signed measurements of executed software, hardware settings and application configuration of a node since last boot. Whitelists of software and hardware conditions are used to verify the status.

The protocol developed for this process is a variant of the link-layer discovery protocol LLDP. All routers use link-layer discovery to find nodes in the neighborhood. All nodes found in a single hop distance are then requested to answer an attestation challenge. The verification process can either use pre-installed identities and reference values for nodes,

use public-key cryptography for certified identities and reference values, or rely on a central entity to confirm the validity of the attestation results.

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 as shown in figure 2. Additionally, periodically re-launching the attestation procedure with all devices in the neighborhood provides fresh information. To avoid Denial-of-Service (DoS) attacks (targeting the protocol integration and expensive TPM operation), the network components, which are able to trigger the attestation, are restricted to a valid identity key and a minimum timeout, which is verified before any incoming message is further processed.

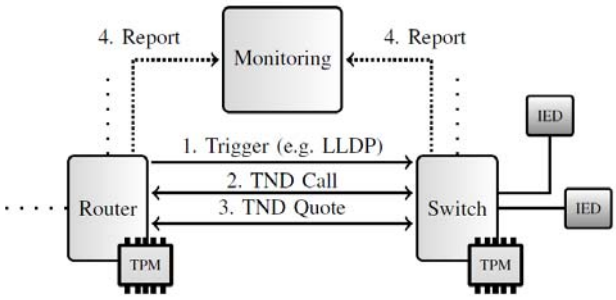

Figure 2. Overview of the Trusted Core Network (TCN)

3) TCN summary

The TCN architecture establishes secure device identities and is a basal technology for an anomaly monitoring framework. It enables the mutual verification of software states of neighboring devices. Thus, trust is established on device level in the network in a peer-to-peer manner. The decentralized attestation saves network resources, is independent from connectivity and is scalable in contrast to attesting each device from a central monitoring entity. With TND, reliable statements of the current running firmware on a device can be made since the verification is entangled with the device's hardware by using a TPM as trust anchor. This is impossible with purely software-based security technology. Implementing TND on a low level network layer like ISO/OSI layer 2 shows a negligible influence on the existing network traffic and enables to fulfill many requirements for real-time and availability. Also the fact that the attestation is limited to neighboring devices reduces the effort of the trust establishment. In critical real-time environments TND traffic can be relocated to a separate physical communication channel to prevent any interference with real-time traffic.

In general, TND can be applied to various scenarios where health checks for interconnected devices are useful. One possible application is to build a trusted core network in an industrial context in which the neighboring network devices, such as switches and routers, check each other and report anomalies to a security event management system or to support security automation. That way the operator of the network can be sure that network devices do not maliciously reroute traffic, manipulate the forwarded traffic, or violate safety requirements. Another exemplary use case is the establishment of trust between substations in power grids. Here, manipulations of the devices could cause instability of the power distribution because Intelligent Embedded Devices (IED) directly perform critical tasks such as control voltage regulation or sending sensible information of the current workload to operation and control centers. In this context the TCN enables the verification of the IED within and between substations to ensure their proper behavior.

Once established, trusted computing technology in the devices can support additional security solutions. First steps on the area of TC-based solutions for industrial security are presented in [20] and [21]. Furthermore, [22] proposes a central approach for interoperable and secure TC-based device authentication in smart grids using TPMs and TNC.

TND is one module of a systemic approach to anomaly monitoring in industrial applications that will be developed in an upcoming research project. Besides the protection on device level, which is done by TND, an end-to-end message verification is needed to detect manipulated or injected messages within the network. Furthermore, the meta-data of the anomaly reports must be gathered, analyzed and aggregated to defer information on the state of the complete infrastructure from these distributed events. Further, this information can be related to other security-relevant events, e.g. on application level, or from physical surveillance. This information can then support adequate reaction, mitigation and redress processes.

V. LOW-LEVEL DEVICE INTEGRITY IN SMART GRIDS

While high-level devices mostly support a trustworthy boot process and TPM is at least available for most laptops and servers, low-level devices lack such approaches. The following concept describes how a SMGW's integrity can be secured based on the insights of chapter 2 in respect of other low-level devices in smart grids:

1. **Hardware integrity protection:** Basically, all hardware parts are tightly integrated into a SMGW chassis. The chassis is protected by a visible, physical, permanent seal, which is destroyed, if the chassis is opened and the opening is signaled to the SMGW software by an electronic switch. Additionally, certain hardware parts (e.g. CPU and security module) are protected by an electronic tamper resistant grid, which shall detect hardware tampering attempts and signal them to the SMGW software.
2. **Basic integrity protection at system startup** is realized by a trustworthy boot process. Secure Boot does not rely on a TPM and defines actions to be taken if the system's integrity is compromised. Technologies like co-processors or the Trustzone [1] used in ARM-CPU may aid in the implementation of a secure boot process [12, p. 572]. Figure 3 shows the pattern of Secure Boot (see [12, p. 570]), which has been applied to this concept. The boot process is organized as list of bootstrap modules. The first module in this list is the

"Root of Trust", which is protected by hardware (see figure 3).

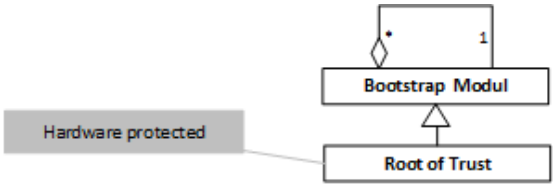

Figure 3. Secure Boot pattern [13, p. 570]

According to this pattern, you can see the boot sequence in figure 4 completely. After powering up the system, the "Root of Trust" is loaded from the hardware ROM. 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).

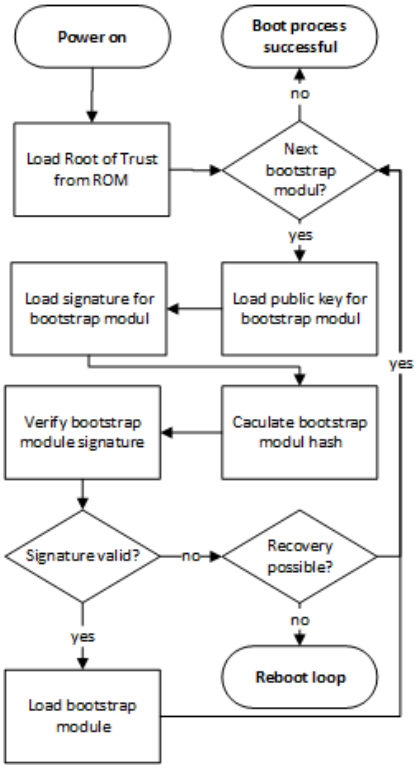

Figure 4. Secure Boot process [3]

Additionally, it verifies the operating system software (bootstrap module n+1) using a known signature and the corresponding public key. If the signature is correct, the operating system is loaded and in turn may verify additional software (bootstrap module n+m) the same way, 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. 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.

3. **TNC integrity assessment capabilities** are realized by the application of one or both described TNC scenarios. TNC is an open architecture and therefore extendable to fit into different IT infrastructures. For instance, for the SMGW the monitoring scenario will be implemented, using a custom BSI compliant communication channel to report integrity information on certain events as stated in [3].

VI. WIRELESS SECURITY IN SMART GRIDS

The use of wireless communication in smart grids differs from the common use of Wireless Local Area Networks (WLAN) in office environments, private homes, or public hotspots. In these environments, WLAN are mainly used to provide connectivity between high-level endpoints, such as laptops, tablets or smartphones. Regarding the smart grid, the goal of using wireless communication is to connect a large number of low-level endpoints such as sensors (e.g. SM) to a fewer number of high-level endpoints mainly. Furthermore, especially on the WAN, 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 [23]. Thus, wireless communication can be expected to be part of the new communication infrastructures for the smart grid. However, very heterogenic endpoints, dynamic wireless networks, and ad-hoc networks also introduce new security issues. In fact, while in today's WLAN important devices are protected or at least built into controlled environments, such as company premises, devices in the smart grid are built into places which often do not belong to and are not accessible by the company which 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. This increases the security risks for higher level and lower level devices significantly.

In addition to the protection of the actual devices and the traffic between them, a main attack vector is the routing information distributed via network nodes. By manipulating routing information, attackers can gain control over all traffic in the network and can violate availability for the complete

network from one single manipulated node (see [24] for examples of routing-based attacks).

One approach to prevent routing-based attacks is to use a mechanism similar to the Trusted Core Network (TCN) described before. All nodes in the network request attestation from nodes in their neighborhood and only accept routing information from nodes that are known, securely identified and not manipulated. Recently, Trusted Computing technology was integrated into existing protocols for mobile ad-hoc networks within the EU FP7 project SecFutur [21], [25].

While WLAN technology is not yet used within the SPIDER project, the SMGW uses a wireless M-Bus interface to communicate with the SM. M-Bus (Meter-Bus) is an European standard (EN13757-2 physical and link layer, EN13757-3 application layer) for the remote reading of gas or electricity meters. M-Bus is also usable for other types of consumption meters. The M-Bus interface is made for communication on two wires. A radio variant of M-Bus (Wireless M-Bus) is also specified in EN13757-4. The M-Bus has been developed to fulfill the need for a system for networking and remote reading of utility meters, for example to measure the consumption of gas or water in the home. This bus fulfills the special requirements of remotely powered or battery-driven systems, including consumer utility meters. When interrogated, the meters deliver the data they have collected to a common master, such as a hand-held computer, connected at periodic intervals to read all utility meters of a building.

Some substantial characteristics of this interface include the following new possibilities:

a. The data (e.g. heat consumption) are read out electronically.

b. At one single cable, which connects to a building controller, all consumption meters of a housing unit can be attached.

c. All meters are individually addressable.

d. Apart from the availability of the data at the controller a remote reading is possible.

e. Numerically encoding together with numerically indexed data structure makes data transfer efficient.

But in the M-Bus environment, there are some connectivity troubles foreseeable. Because of the SMGW's placement into a metal chassis the wireless connection can be too weak to get connectivity to the smart meters. Additionally, the smart meters are distributed to a house or shared apartment and can be out of reach for the wireless M-Bus from the SMGW. Those are problems regarding the normal operation and are not relevant for IT security, but should also be mentioned and be solved in the near future.

From the security point of view, the M-Bus protocol does not specify mechanisms to evaluate the integrity of the communicating endpoints. At present, a SMGW has to assume that the meter and its connections are trustworthy. This behavior can provoke a chain of aberrations based on one compromised single SM, because the SMGW cannot prove the integrity of a SM and its measured data, but uses this data to calculate energy consumption and production as well as to deduce the current condition of its managed infrastructure. With the use of the TCN approach in combination with TNC and TPM, as described before, a trustworthy status can be reached throughout the infrastructure. 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.

Hence, a SM should integrate a "Root of Trust" like a TPM or another co-processor as described in chapter 5. To enable the integrity control of a SM, TNC can be integrated using a custom communication channel between the SM and the SMGW. Therefore, the numerically indexed data structure of the M-Bus protocol must be extended. New Value and Data Information Fields (VIF/DIF) have to be specified to communicate integrity information data via the protocol. The SMGW can examine these data for integrity issues by itself or by means of another party (e.g. the GWA), as specified by TNC, before gathering any measured energy related data. After a successful evaluation of the data against known values, the SMGW can begin to retrieve measured energy related data from a SM. In case of an evaluation failure the SMGW may report an integrity evaluation error to a gateway administrator to induce further actions, instead. Together with the data and transport encryption methods specified by the BSI [26 pp. 14-20] the reliability and integrity of the measured data is strengthened at its first occurrence providing a more reliable infrastructure in total. Finally, this approach enables a converged TCN scenario in smart grids, where low-level devices report and measure their own integrity.

VII. CONCLUSIONS AND PROSPECTS

The relevant aspect of Trusted Computing to enhance the security of low-level devices such as the SMGW is the measurement and verification of its integrity using the TNC approach of the TCG. If using TNC, it is especially important to protect the measurement logic to ensure the trustworthiness of the measured values. This concept complies with this requirement by generating a trusted chain. Integrity verification is first applied at boot time utilizing Secure Boot and establishing the trusted chain including the TNC software. Integrity verification is also applied at runtime, utilizing the (at boot time) verified TNC software. The measured values of hard- and software components are stored tamper safe in the file system. This leads to an advanced gateway security, which affects all adjacent components.

The next step of this paper describes how the trusted platform of the SMGW can be extended to a Trusted Core Network (TCN), which also includes the SM components. The TCN architecture is able to review a node's identity and to guarantee the node's desired state. For a smart grid scenario a distributed, redundant node control is needed, checking the identity and state of neighboring nodes in a peer-to-peer manner. A Trusted Network Discovery (TND) protocol facilitates locating all active devices within the direct environment. Using the TPM the system identifies the node

and compares the current state to the target state. Modifications or manipulations can thus be detected in a fast and distributed manner. Alerts will be sent directly to central monitoring and the spread of attacks and malware can be prevented. Besides the device's identity, the TCN reviews downloaded executable software and configuration data. If changes are found, appropriate countermeasures can then be taken, so that essential functions may be maintained (resiliency), even in the case of manipulations or successful attacks on individual components.

The use of a TPM chip can be recommended, but it is not available today on the market. Only in high-level devices like laptops or client-/server-systems a TPM is integrated. Low-level devices like SM do not have TPM chips inside. Additionally, the SM components are not very smart today and have to be improved to support necessary security functionality, especially on the wireless interface. Furthermore, not all problems regarding M-Bus connectivity and IT security are solved in the area of smart grids. But as described Trusted Computing approaches and specifications can help to establish a trustworthy platform for smart grids, including wireless components and interfaces. Therefore, the BSI specifications should extend their definitions with such security features from our point of view. Otherwise, manufactures and vendors will not implement these kinds of security solutions in their smart grid components.

Acknowledgment

The authors give thank to the BMWi-ZIM [9] for the financial support as well as to all other partners involved into the research project SPIDER for their great collaboration. The project consists of the industrial partners devolo AG and DECOIT GmbH, and the research partners University of Siegen, Fraunhofer FOKUS, and University of Applied Sciences of Bremen. Further associated partners are the energy provider Vattenfall and RWE, the hardware vendor Maxime, and the certification expert datenschutz cert. [18]

Additionally, the project would like to give thanks to Fraunhofer SIT, who developed as external partner an extended security concept in the field of "Internet of things" to create a TCN platform. This solution is a result of BMBF project ANSII [27] to provide a secure foundation for anomaly detection in industrial networks and the project SecFutur [25] from the European Union's 7th Framework Program for research, technological development, and demonstration to use the TCN concept in mobile ad-hoc networks.

References

[1] ARM Ltd: TrustZone, „http://www.arm.com/products/processors/technologies/trustzone/index.php", last access: 22.06.14, Nov. 2013

[2] J. C. Bare, "Attestation and Trusted Computing", University of Washington, Washington, 2006

[3] K.-O. Detken, C.-H. Genzel, R. Sethmann, and O. Hoffmann, "Security concept for gateway integrity protection within German smart grids", 3rd ASE International Conference on Cyber Security, ASE (Academy of Science and Engineering) 2014, 27.-31. Mai, ECSaR - International Workshop on Engineering Cyber Security and Resilience, Stanford University, Stanford (USA) 2014

[4] Federal Office for Information Security (BSI), „Technical Guideline BSI TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems", BSI, Bonn 2013

[5] Federal Office for Information Security (BSI), „Technical Guideline BSI TR-03109-2 Smart Meter Gateway Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls", BSI, Bonn 2013

[6] Federal Office for Information Security (BSI), "Technical Guideline BSI TR-03109-4 Smart Metering PKI – Public Key Infrastruktur für Smart Meter Gateways", BSI, Bonn 2013

[7] Federal Office for Information Security (BSI), "Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)", BSI, Bonn 2013

[8] Federal Office for Information Security (BSI), "Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP)", BSI, Bonn 2013

[9] Federal Ministry for Economic Affairs and Energy, "Central Innovation Program SME: http://www.zim-bmwi.de", May 2014, last access at 21.06.2014

[10] ISO/IEC, "ISO/IEC 11889-1 Information technology – Trusted Platform Module – Part 1: Overview", ISO copyright office, Genf, 2009

[11] S. Kinney, "Trusted platform module basics : using TPM in embedded systems", Elsevier, Amsterdam [u.a], 2006

[12] H. Löhr, A.-R. Sadeghi, and M. Winandy, "Patterns for Secure Boot and Secure Storage in Computer Systems", availability, in IEEE: ARES '10 International Conference on Reliability, and Security, Krakow, 2010; p.569-573

[13] Trusted Computing Group, "TCG Specification Architecture Overview", TCG PUBLISHED, Beaverton 2007

[14] Trusted Computing Group, "TCG Trusted Network Connect TNC Architecture for Interoperability", TCG PUBLISHED, Beaverton 2012

[15] Microsoft, "Threat Modeling Uncover Security Design Flaws Using The STRIDE Approach", available from: http://msdn.microsoft.com /en-us/magazine/cc163519.aspx, May 2014, last access at 21.06.2014

[16] S.W. Smith, "Trusted Computing Platforms: Design and Applications", publishing house Springer, New York 2005

[17] Trusted Computing Group, "TPM Main – Part1 Design Principles", Specification Version 1.2, Revision 116, 1st March, 2011

[18] SPIDER project website, "http://www.spider-smartmetergateway.de", May 2014, last access at 21.06.2014

[19] J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations", Smart Grid, IEEE Transactions on, vol. PP, no. 99, pp. 1–11, 2014

[20] N. Kuntze, C. Rudolph, S. Leivesley, D. Manz, and B. Endicott-Popovsky, "Resilient core networks for energy distribution," in Power and Energy Society General Meeting, IEEE, 2014, pp. 1–5.

[21] A. Oberle, A. Rein, N. Kuntze, C. Rudolph, J. Paatero, A. Lunn, and P. Racz, "Integrating Trust Establishment into Routing Protocols of Today's MANETs," in Proceedings of the 11th IEEE Wireless Communications and Networking Conference (WCNC). Shanghai, China: IEEE Press, April 2013, pp. 1403–1408

[22] N. Kuntze, C. Rudolph, I. Bente, J. Vieweg, and J. von Helden, "Interoperable device identification in smart-grid environments," in Power and Energy Society General Meeting, 2011 IEEE, July 2011

[23] Y. Zhang, W. Sun, L. Wang, H. Wang, R.C. Green, M. Alam, "A multi-level communication architecture of smart grid based on congestion aware wireless mesh network", North American Power Symposium (NAPS), 2011 , vol., no., pp.1,6, 4-6 Aug. 2011

[24] C. Gottron, P. Larbig, A. Konig, M. Hollick, R. Steinmetz, "The rise and fall of the AODV protocol: A testbed study on practical routing attacks", Local Computer Networks (LCN), 2010 IEEE 35th Conference on , vol., no., pp.316,319, 10-14 Oct. 2010

[25] SecFutur project website, "http://www.secfutur.eu", June 2014, last access at 30.06.2014

[26] Federal Office for Information Security (BSI), „Technical Guideline BSI TR-03116-3: Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3 - Intelligente Messsysteme", BSI, Bonn 2014

[27] ANSII project website, „http://www.ansii-projekt.de", June 2014, last access at 30.06.2014