Sicherheitskonzept zum Schutz der Gateway-Integrität in Smart Grids

Carl-Heinz Genzel[1], Richard Sethmann[2], Olav Hoffmann[3], Kai-Oliver Detken[4]

[1,2 und 3] Hochschule Bremen, Flughafenallee 10, 28199 Bremen
[4] DECOIT GmbH, Fahrenheitstraße 9, 28359 Bremen

carl-heinz.genzel@hs-bremen.de, sethmann@hs-bremen.de,
olavhoffmann@googlemail.com, detken@decoit.de

Abstract: Um den Herausforderungen zukünftiger Energienetze begegnen zu können, ist eine sichere Datenübertragung zwischen den Steuerkomponenten notwendig. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat hierfür Sicherheitsvorgaben in Bezug auf eine zentrale Kommunikationseinheit, das sog. Smart Meter Gateway, (SMGW) entwickelt. Das Sicherheitskonzept berücksichtigt diese Vorgaben und erhöht zusätzlich die Informationssicherheit des SMGW indem es Elemente des Trusted Computings (TC)-Ansatzes integriert. Dazu wird ein Tamper-Resistant-Grid über ausgewählte Hardwareelemente gelegt, das Secure Boot-Verfahren angewendet und eine laufende Integritätsmessung des SMGWs über den Trusted Network Connect (TNC) - Ansatz realisiert.

1 Einleitung

1.1 Zukünftige Energienetze

Zukünftige Energienetze stehen vor den Herausforderungen schwankende und dezentrale Energieerzeugung zu ermöglichen und gleichzeitig die Netzstabilität zu wahren. Weiterhin gilt es, verschiedenste Externe Marktteilnehmern (EMT) mit ihren Interessen zu berücksichtigen [Bu13a, S. 14]: Den Messstellenbetreiber (MSB), der verantwortlich für die Messsysteme ist, den Messdienstleister (MDL), der das Ab- und Auslesen von Verbrauchszähleinrichtungen übernimmt, den Verteilnetzbetreiber (VNB), der das örtliche Stromnetz unterhält und wartet, den Lieferanten, der als Handelswarenvertreter auftritt und für die Nutzung des Netzes Gebühren an den VNB zahlt sowie den SMGW-Administrator (GWA), der in viele wesentliche Prozesse des SMGW-Lebenszyklus eingebunden ist (Datenübertragung, Administration und Eichung im laufenden Betrieb) [Bu13a, S. 13], [Bu13f S. 9, 138]. Das hier vorgestellte Sicherheitskonzept wurde im Rahmen des Forschungsprojektes „**S**ichere **P**owerl**i**ne-**D**atenkommunikation im intelligenten **E**ne**r**gienetz“ (SPIDER) erarbeitet und hat sowohl eine hohe praxistaugliche als auch gesellschaftliche Relevanz. Diese Sichtweise wird von dem Energieversorger Vattenfall Europe Distribution Berlin GmbH geteilt, sie schreiben:

„…Wir sehen in den Forschungs- und Entwicklungszielen von SPIDER und der Zusammenarbeit mit dem Konsortium die Möglichkeit die eigenen Produkte und Dienstleistungen an die steigenden Sicherheitsanforderungen im Bereich der sicheren Datenübertragung in Energienetzen anzupassen und daraus wichtige Impulse für aktuelle und zukünftige Geschäftsfelder zu gewinnen…. Wir bescheinigen den Projektzielen eine hohe gesellschaftliche Relevanz und sehen in dem geplanten Vorhaben einen hohen Innovationsgrad…“

1.2 Definition und Beschreibung des Szenarios

Die neuen Anforderungen an Energienetze können nur durch die Koordination der Energieerzeugung und des Energieverbrauchs, in Verbindung mit einer sicheren Datenübertragung zwischen den Beteiligten, erreicht werden. In diesem Zusammenhang werden zwei neue Komponenten in intelligenten Energienetzen benötigt, das Smart Meter (SM) als „Intelligenter Zähler“ und das SMGW als zentrale Kommunikations-einheit. Sie bilden zusammen die Basis des Smart Metering Systems.

Die dargestellten Komponenten und Bereiche in Abb. 1 sowie die entsprechenden Sicherheitsanforderungen in einem Smart Metering System werden durch Vorgaben des BSIs im Detail beschrieben (vgl. [Bu13a], [Bu13b], [Bu13d], [Bu13e]).

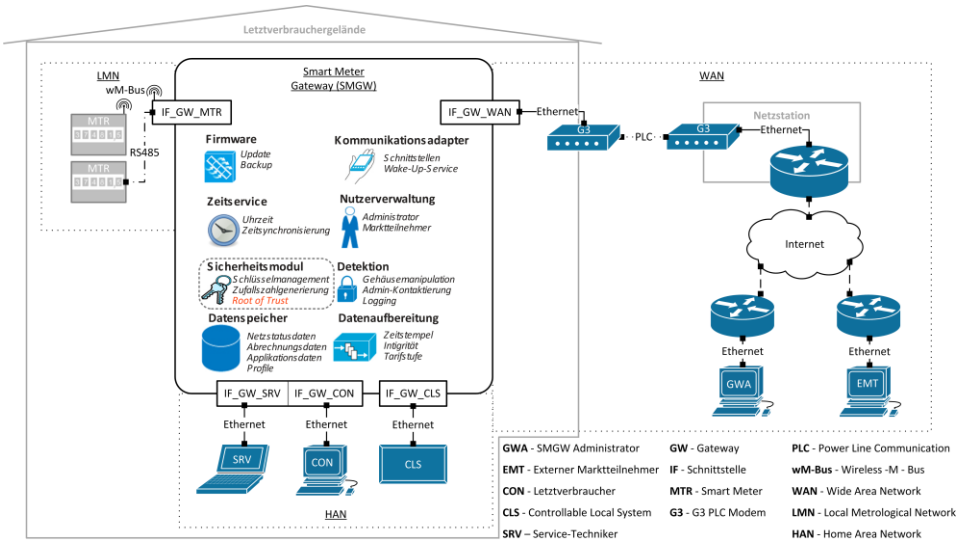

Abbildung 1: Szenario: SMGW-Kommunikation über PLC mit WAN

Das SMGW ist die zentrale Instanz in einem Smart Metering System, es besitzt die Logik zur verlässlichen Verarbeitung und sicheren Speicherung von Messdaten angeschlossener Messsysteme und soll die sichere Datenübertragung zwischen den einzelnen Teilnehmern in den angeschlossenen Netzen ermöglichen. Bei den Netzen handelt es sich gem. den Vorgaben des BSI (vgl. [Bu13a, S. 13-15]) um:

- Das Local Metrological Network (LMN), ein Netz zur lokalen Anbindung von Messgeräten (Strom-, Gas- oder Wasserzähler) der Endnutzer (Letztverbraucher (CON, LV)).

- Das Home Area Network (HAN), ein Netz zur lokalen Anbindung und Steuerung von Energieerzeugern und Energieverbrauchern (Controllable Local Systems (CLS)) der Letztverbraucher sowie zur Informationsbereitstellung für Letztverbraucher und technisches Betreiberpersonal (Service-Techniker (SRV)).

- Das Wide Area Network (WAN), zur Anbindung des GWA für die SMGW-Verwaltung und Dritter (EMT) zur Datenvermittlung.

Das SMGW erfüllt außerdem die Funktion einer Firewall zur Separierung dieser Netze und deren Teilnehmer. Neben dieser logischen Trennung sind alle Netze zusätzlich physikalisch voneinander getrennt [Bu13a, S. 13-15].

Ein Security Modul innerhalb des SMGWs stellt kryptographische Operationen für die sichere Speicherung und Übertragung von Daten zur Verfügung. Zu den Funktionen zählen unter anderem:

- Sichere Speicherung von Zertifikats- und Schlüsselmaterial

- Schlüsselgenerierung und Schlüsselaushandlung auf Basis von elliptischen Kurven

- Erzeugung und Verifikation digitaler Signaturen

- Zuverlässige Erzeugung von Zufallszahlen

[Bu13b, S. 10]

Das SMGW empfängt über das angeschlossene LMN Messwerte von Smart Metern. Smart Meter unterscheiden sich von regulären Messsystemen insbesondere dadurch, dass sie eine kryptographisch gesicherte Kommunikation zum SMGW verwenden und die Übermittlung von Messwerten durch das SMGW steuerbar ist [Bu13a, S. 15-16].

Um eine möglichst einfache Integration des Smart Meter Systems zu ermöglichen, werden zusätzliche Komponenten zur Anbindung des SMGWs an das Weitverkehrsnetz verwendet. Jedes SMGW kommuniziert mit Hilfe der G3 Power Line Communication (PLC) Technologie über die „Last Mile“ des lokalen Stromnetzes mit der nächsten Netzstation. Erst in der Netzstation wird die Kommunikation in ein vorhandenes Weitverkehrsnetz eingeleitet [SHB13 S. 333].

Welche Daten in das Weitverkehrsnetz kommuniziert werden dürfen, ist ebenfalls durch das BSI in den entsprechenden Richtlinien geregelt. In diesem Zusammenhang definiert das BSI Eigentumsverhältnisse in Bezug auf die einzelnen Rollen. Der Letztverbraucher, als natürliche oder juristische Person, ist Eigentümer der Messwerte und davon

abgeleiteter Daten seiner Messsysteme. Ein EMT ist Interessent und Nutzer dieser Daten, sie ermöglichen ihm die Durchführung der Bilanzierung, Tarifierung und Netzzustandserfassung. Der GWA hat im Allgemeinen keinen Zugriff auf diese Form der Daten. Er hat im Gegenzug Zugriff auf systemrelevante Daten wie Konfigurationsdaten, System- und Eichtechnische-Logs. Der Service-Techniker hat eine Diagnosefunktion und darf daher systemrelevante Daten auslesen, sie aber im Gegensatz zum GWA nicht speichern. Der Zugriff auf das SMGW ist jedem Teilnehmer nur über das ihm zugeordnete Netz aus Abb. 1 gestattet [Bu13a, S. 118-119].

1.3 Bedrohungsanalyse

Die Bedrohungen in dem betrachteten Szenario können laut BSI (vgl. [Bu13d, S. 33]) in folgende Kategorien aufsteigend nach Tiefe der Bedrohung eingeteilt werden:

1. Aufdecken von Daten, die sich fest auf dem SMGW oder in der Verarbeitung durch das SMGW befinden (Verbrauchsdaten, Zählerstände, Profile etc.). Ziel: Informationsbeschaffung aus der Smart Meter Infrastruktur.

2. Manipulation von Daten, die sich fest auf dem SMGW oder in der Verarbeitung durch das SMGW befinden (Tarifdaten, Tarifprofile, Zählerstände etc.). Ziel: Änderungen zum eigenen Vorteil oder zur Störung des Betriebs.

3. Veränderung und Kontrolle beteiligter Systeme (CLS, SMGW etc.). Ziel: Beeinträchtigung der Infrastruktur.

Jede Bedrohung kann zusätzlich nach Angriffsort unterschieden werden. Dabei sind Angreifer aus dem WAN als höher motiviert zu betrachten, während Angreifer aus dem HAN geringer motiviert sind [Bu13d, S. 33].

Die Bedrohungen wurden durch den STRIDE-Ansatz [Mi13] analysiert. STRIDE steht für **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service und **E**levation of privilege. Die zugehörigen Sicherheitseigenschaften sowie die entsprechenden Gegenmaßnahmen in Verbindung mit Trusted Computing und den BSI-Vorgaben sind in [SHB13] und [Be13] beschrieben.

2 Stand der Technik

2.1 Vertrauenswürdiges Bootverfahren

Es ist mit vergleichsweise hohem Aufwand verbunden, Hardwarebausteine einer Plattform auszutauschen oder zu manipulieren, da sie oft mechanisch gesichert sind. Die Manipulation von Software ist dagegen verhältnismäßig einfach. Aus diesem Grund ist der Schutz der Softwareintegrität, insbesondere bei der Bereitstellung von sicherheitsrelevanten Funktionen, durch Nachweisbarkeit notwendig. Aus der

Anforderung ergibt sich jedoch eine zyklische Abhängigkeit, da für den Nachweis meist wieder Software benötigt wird [LSW10, S. 569, 570].

Zur Unterbrechung dieser Abhängigkeit wird unter anderem beim Trusted Computing das Konzept „Root of Trust“ verwendet. In der Literatur wird der „Root of Trust“ als eine unbestreitbare Charakteristik oder Eigenschaft einer einzelnen Person oder Sache, die ihre Vertrauenswürdigkeit rechtfertigt, charakterisiert (vgl. [Ki06 S. 31]). Dadurch, dass der „Root of Trust“ nicht oder nur mit sehr hohem Aufwand verändert werden kann, bildet er die Basis für die Evaluierung einer Plattform bzw. eines Systems. Die Trusted Computing Group (TCG) beschreibt hierzu die „Chain of Trust“. Sie definiert die Integrität einer Plattform als eine Vertrauenskette. Diese Kette wird ausgehend von einem zentralen Punkt, dem „Root of Trust“, über verschiedene hierarchisch angeordnete Komponenten der Plattform während des Systemstarts gebildet. Eine Komponente (N) innheralb dieser Kette kennt und prüft hierfür den unversehrten Zustand der jeweiligen Folgekomponente (N+1) anhand festgelegter Attribute und protokolliert das Ergebnis. Geht man also davon aus, dass der „Root of Trust“ nicht einfach verändert werden kann, können in Abhängigkeit dazu auch alle Folgekomponenten nicht verändert worden sein, wenn alle Prüfungen erfolgreich waren. Während des Systemstarts können hierdurch Manipulationen (z.B. durch Fremdeinwirkung) an Hard- und Software ermittelt werden [Is09, S. 4-7], [Tr07, S. 7 - 8].

Dieser Vorgang wird auch als vertrauenswürdiger Bootprozess bezeichnet. Er wird in der Literatur in drei Kategorien unterteilt (vgl. [Sm05, S. 50]), die jedoch zum Teil synonym verwendet werden:

- Trusted Boot: Prüfung der Komponenten durch Analyse und Messung.
- Secure Boot: Prüfung der Komponenten durch Analyse und Messung inklusive festgelegter Aktionen bei negativem Prüfungsergebnis.
- Authenticated Boot: Prüfung der Komponenten durch Analyse und Messung abhängig von verschiedenen Szenarien. Festgelegte Aktionen bei negativem Prüfergebnis sind möglich. Die Szenarien beschreiben verschiedene valide Systemzustände.

2.2 Trusted Computing und die Anwendung des TNC-Schichtenmodells

Die TCG ist eine Standardisierungsorganisation aus der Industrie, die Spezifikationen für Trusted Computing entwickelt. Ihr Ziel ist es, einen offenen und hersteller-unabhängigen Standard für Trusted-Computing-Bausteine und Softwareschnittstellen zu spezifizieren. Sie sollen Veränderungen an IT-Plattformen erkennen und sowohl externe Softwareangriffe, als auch Veränderungen der Konfiguration, Sicherheitslücken oder schadhafte Anwendungsprogramme ausmachen [Tr12]. In der Informationssicherheit ist es häufig schwierig einem System (bspw. einem SMWG) zu vertrauen. Es ist oft nicht möglich zu erkennen, ob das Gerät (bezogen auf die Hard- und Software) manipuliert wurde. Bei der Lösung dieses Problems ist ein reiner Softwareansatz nicht zuverlässig genug, da Software leicht manipuliert werden kann.

Die TCG hat daher das Trusted Platform Modul (TPM) als ein zusätzliches Hardwaremodul spezifiziert. Als Basis des Vertrauens dient ein festes Schlüsselpaar innerhalb des Moduls. Der private Schlüssel verlässt das Modul nie und stellt seine Identität dar. Aufgrund der Annahme, dass der private Schlüssel nur dem TPM bekannt ist, kann durch den Einsatz von Signaturen der Ursprung des Inhalts zum System des TPMs zugeordnet werden. Eine nähere Beschreibung ist in [SHB13] zu finden.

TNC stellt Methoden zur Feststellung der Integrität von Endpunkten bereit, die als Basis für eine vertrauenswürdige Kommunikation dienen und kann dafür Funktionen des TPMs nutzen. Die aktuelle TNC-Architektur ist von der TCG in der Spezifikation 1.5 (Revision 3) vom Mai 2012 veröffentlicht worden. Die im Rahmen des Konzepts verwendeten Komponenten der TNC-Architektur werden in [SHB13] erläutert.

2.3 Vergleich der Trusted Computing-Technologie mit BSI-Mindestanforderungen

Das TPM ist ein zentraler Bestandteil im Trusted Computing und stellt die Identität eines Systems dar. In einem SMGW ist dagegen das Security Module ein zentraler Bestandteil der Identität. Beide Module besitzen dazu nicht auslesbare private Schlüssel (vgl. [Tr12, S. 1], [Bu13b, S. 56]) und sind fest in ihr umgebendes System integriert. Zudem müssen sie physikalischer Manipulation in Grenzen widerstehen können [Tr07, S. 47], [Ba06, S. 12, 30].

Neben einer festen Identität wird im Trusted Computing ein Integritätsnachweis in Form einer Integritätsmessung und einer davon abhängigen Attestierung im Rahmen von TNC verwendet. Dazu wird der Systemzustand anhand ausgewählter Systemattribute, meist durch ein TPM, gemessen und manipulationssicher gespeichert. Die Integritätsmessung wird beim Start des Systems oder auch zu speziellen Ereignissen während des Betriebs ausgeführt. Durch Remote Attestation kann das System aus der Ferne mit Hilfe der Messwerte auf ungewollte Veränderungen geprüft werden [Tr07, S. 8-10]. Das BSI schreibt in diesem Zusammenhang Selbsttests zur Verifizierung der Sicherheitsfunktionen und Daten vor [Bu13d, S. 38, 79]. Die Ergebnisse der Selbsttests sind ohne eine vertrauenswürdige Basis jedoch nicht vertrauenswürdig. Im Trusted Computing wird mit dem vertrauenswürdigen Bootverfahren aus Abschnitt 2.1 eine solche Basis geschaffen. Das BSI schreibt keine solche Vertrauensbeziehung vor.

Durch die Integritätsmessung und Attestierung können Hard- und Softwaremanipulationen erkannt werden. Das reduziert die Möglichkeiten des Angreifers, ein SMGW dauerhaft zu übernehmen. Dieser Aspekt wird in den aktuellen Spezifikationen des BSI nur pauschalisiert betrachtet. Durch die Integritätskontrolle wird zusätzlich die Authentizität der übertragenen Daten gestärkt, da unabhängig von einer PKI-basierten Authentifizierung der Zustand des SMGWs überwacht wird. Das TNC-Konzept der TCG in Verbindung mit einem vertrauenswürdigen Bootverfahren stellt daher den stärksten Sicherheitsgewinn durch Trusted Computing im Vergleich zu den BSI-Vorgaben dar. Ein aktueller TPM-Chip nach Spezifikation 1.2 kann in diesem Zusammenhang jedoch nicht verwendet werden, da die Anforderungen an die kryptographischen Algorithmen des BSIs nicht erfüllt werden. Die aktuell entstehende TPM-Spezifikation 2.0 muss diesbezüglich nach der Fertigstellung noch geprüft werden.

3 SMGW-Integrität im Smart Grid

Ausgehend von den Erkenntnissen aus Abschnitt 2 ist das folgende Konzept zur Sicherung der SMGW-Integrität im Forschungsprojekt SPIDER entwickelt worden.

3.1 Sicherstellung der Hardware

Das SMGW wird von außen wie bei aktuellen Messsystemen üblich mit einem Siegel oder einer sogenannten Plombe geschützt. Diese Komponenten dürfen während des Betriebs nicht beschädigt werden. Das SMGW besitzt zusätzlich Mechanismen, die das Öffnen des Gehäuses elektronisch erkennen. Zudem ist auf dem Hostcontroller des SMGWs ein sogenanntes „Tamper-Resistant-Grid“ aufgebracht, das eine elektronische Erkennung von Manipulationsversuchen an der Hardware ermöglicht. Alle Komponenten der Plattform sind fest fixiert und können nicht ohne weiteres entfernt werden.

3.2 Sicherstellung der Basisintegrität über Secure Boot

Für die Sicherstellung der Basisintegrität eines SMGWs soll ein Secure Boot-Verfahren verwendet werden. Ein Secure Boot-Verfahren kann, im Gegensatz zum Trusted Boot-Verfahren, ohne TPM durch vorhandene Technologien wie einen Co-Prozessor oder der aktuell in ARM-CPUs vorhandenen Trustzone [Ar13] leichter umgesetzt werden [LSW10, S. 572]. Bei der Umsetzung wird das in [LSW10, S. 570] definierte Secure Boot-Muster aus Abb. 2 angewendet.

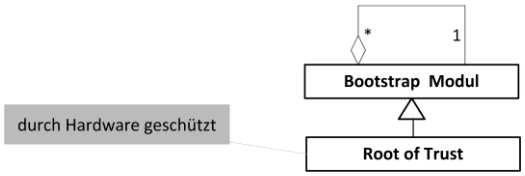

Abbildung 2: Secure Boot-Pattern gem. [LSW10, S. 570]

Der Bootprozess ist als eine Abfolge von Bootstrap Modulen gestaltet, die miteinander assoziiert sind. Das Bootstrap Modul „Root of Trust“ bildet den Ausgangspunkt des Bootprozesses und ist als eigenständiges Hardwaremodul besonders geschützt. Daraus resultiert die in Abb. 3 dargestellte Bootsequenz.

Nach dem Einschalten eines SMGWs wird zuerst das System des „Root of Trust“ aus dem Hardware-ROM geladen. Das System hat eine Referenz zum eigentlichen Bootloader (Bootstrap Modul N) und besitzt zudem eine Signatur, die den SOLL-Zustand des Bootloaders beschreibt sowie den für die Verifizierung der Signatur benötigten öffentlichen Schlüssel. Bevor das System den Bootloader lädt, wird der IST-Zustand des Bootloaders mit der SOLL-Signatur verglichen. Nur wenn die Prüfung positiv ist, wird der Bootloader geladen und die Kontrolle im Bootprozess an ihn übergeben. Der Bootloader prüft daraufhin die Hardwareintegrität (z.B. Zustand des

„Tamper-Resistant-Grid“) und das Betriebssystem (Bootstrap Modul N+1) auf dieselbe Weise mit Hilfe von Signaturen der SOLL-Zustände. Das Betriebssystem kann wiederum einzelne Applikationen (Bootstrap Modul N+M) prüfen.

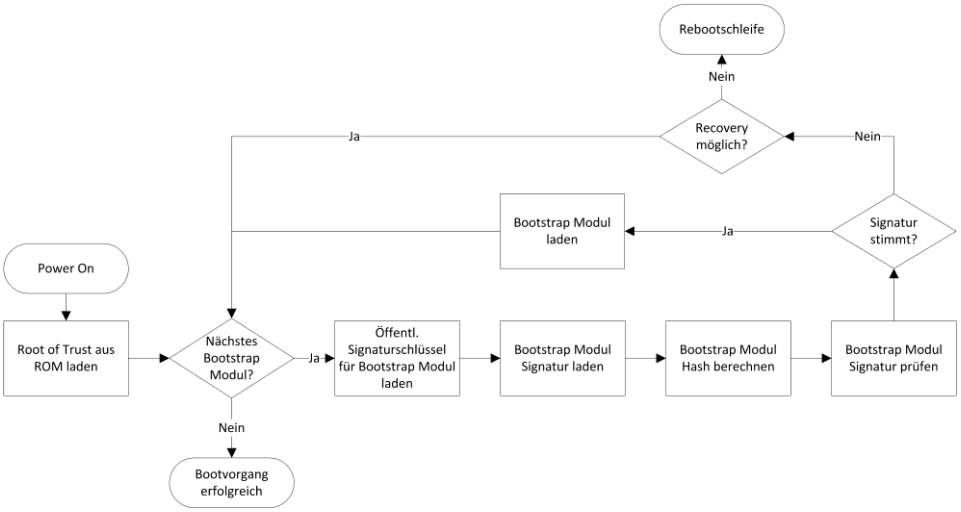

Abbildung 3: Secure Boot-Verfahren

Schlägt eine Prüfung fehl, wird der Bootvorgang unterbrochen und das System geht in einen Fehlerzustand, gekennzeichnet durch einen dauerhaften Reboot, sofern es nicht auf eine vertrauenswürdige Betriebsstufe (Recovery Möglichkeit) zurückfallen kann. Hierzu dient eine Backuppartition mit einem Duplikat der SMGW-Firmware. Sollte eine Prüfung erst oberhalb des Bootloaders fehlschlagen, ist es möglich, mit Hilfe des Bootloaders die Backuppartition für die weitere Bootsequenz zu verwenden. Erst wenn auch die Bootstrap Module auf dieser Partition nicht ihren jeweiligen SOLL-Zuständen entsprechen, bleibt das System in dem beschriebenen Fehlerzustand. Somit kann sichergestellt werden, dass es nur dann zum Betrieb eines SMGWs kommt, wenn der Initialzustand vertrauenswürdig ist.

3.3 Prüfung des SMGWs durch laufende Integritätsmessung

Es wurde festgestellt, dass der Einsatz von TNC einen signifikanten Sicherheitsgewinn darstellt. Davon ausgehend, dass die TNC-Architektur als erweiterbare Architektur beschrieben ist, kann TNC im Allgemeinen am SMGW eingesetzt werden. Der Fokus bei der Umsetzung von TNC liegt in der Ergänzung der BSI-Vorgaben durch die Integritätssicherung, während die Authentifizierung nach bestehenden BSI-Vorgaben realisiert wird.

Abb. 4 zeigt das SMGW als Network Access Requestor (NAR) und den GWA als Network Access Authority (NAA). Im Rahmen der Realisierung wird ein Integrity Measurement Collector (IMC) entwickelt. Ein TPM existiert aus den in Abschnitt 2.3 beschriebenen Gründen nicht.

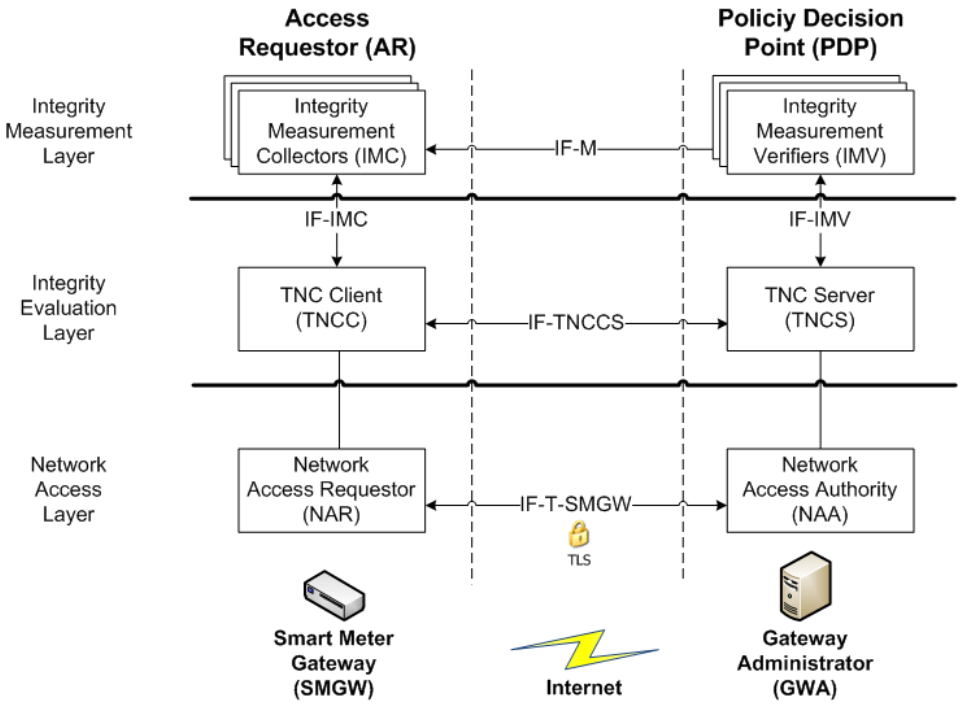

Abbildung 4: TNC-Schichtenmodell mit relevanten Komponenten des Systemkonzepts (in Anlehnung an [Tr12, S. 13] und [SHB13] Abb. 2)

Der IMC wertet Sicherheitsaspekte aus, die die Integrität des SMGWs messbar machen. Hierfür sind Hash-Summen vorgesehen, die periodisch über ausgesuchte Komponenten (z.B. eingesetzte Firmware-Komponenten, Konfigurationsdateien, Hardware-komponenten etc.) gebildet werden. Die Messwerte werden auf Dateiebene gespeichert und mit Hilfe der Mehrbenutzerfähigkeit und der granularen Dateisystemberechtigungen von Linux vor Veränderungen geschützt. Da die Dateisystemrechte auf Kernelebene geprüft werden, sind die Zugangsrechte nur schwer auszuhebeln. Im Sinne von TNC übermittelt der IMC die Messwerte zur Attestierung an den Integrity Measurement Verifier (IMV), der sich auf der Seite des GWA befindet. Dementsprechend, wird auf der Seite des GWAs ein IMV umgesetzt, der die Werte des IMCs interpretieren kann. TNC-Client (TNCC) und TNC-Server (TNCS) sind für die Kommunikation und die Reaktion auf die Ergebnisse der Attestierung zuständig. Sie liegen als standardisierte Komponenten bereits in entsprechenden Bibliotheken vor. Bei negativen Ergebnissen muss zusätzlich der GWA eingreifen. Durch die softwarebasierte Umsetzung kommt es in besonderem Maße darauf an ein System zu nutzen, dass die Integrität der Software bereits beim Systemstart verifizieren kann, um das Vertrauen in die Messwerte zu sichern.

In Abb. 4 wird der Vermittlungskanal zwischen NAA und NAR als IF-T-SMGW dargestellt, da an diesem Punkt keine bestehenden Spezifikationen der TCG für IF-T

verwendet werden kann. Die Bezeichnung IF-T-SMGW soll deutlich machen, dass die Möglichkeit besteht, an dieser Stelle eine neue Spezifikation zu erwirken. Für die Übertragung der Integritätsmesswerte vom SMGW zum GWA zur Verifizierung der Integrität, wird ein Webservice verwendet, der im Rahmen der BSI-Vorgaben für die Alarmierung und Ereignisvermittlung in Verbindung mit dem Systemzustand eines SMGWs verwendet werden soll. Alle weiteren Vorgaben zur Kommunikation über die WAN-Schnittstelle (vgl. [Bu13a, S. 22]) haben weiterhin Bestand. Um reguläre Ereignisse und Alarmierungen von TNC-Nachrichten zu unterscheiden, werden letztere speziell gekennzeichnet. Dieses Vorgehen, ermöglicht die Interoperabilität zu nicht TNC-fähigen Endpunkten. TNC-Nachrichten sind für diese Endpunkte normale Ereignisse, während TNC-fähige Geräte die Nachrichten gesondert interpretieren können. Die darüber liegenden Ebenen sind vollständig in Software umgesetzt und von den BSI-Vorgaben kaum beeinflusst, daher können auch die vorhandenen Spezifikationen verwendet werden.

4 Fazit und Ausblick

Die relevanten Aspekte zur Verbesserung der Sicherheit durch Trusted Computing sind die Integritätsmessung am SMGW und die damit verbundene Attestierung der Messwerte beim GWA in Verbindung mit TNC, da solche Überlegungen bei den aktuellen BSI-Spezifikationen bisher keine Rolle spielen. Es ist hierbei besonders wichtig die Integritätsmessung sicher durchzuführen, da sonst kein Vertrauen in die Messwerte möglich ist. Das beschriebene Sicherheitskonzept erfüllt diese Anforderung, indem eine Vertrauenskette erzeugt wird. Hierzu werden Integritätsmessungen während des Bootvorgangs (Secure Boot) und zur Laufzeit eingesetzt und die Messwerte zu den Hard- und Softwarekomponenten manipulationssicher gespeichert. Die Einbettung von Trusted Computing stellt daher einen wirklichen Mehrwert dar, um Smart Grid-Infrastrukturen wirkungsvoll absichern zu können.

Zukünftig kann der Einsatz eines Monitoring-Systems die Informationssicherheit im Smart Grid weiter erhöhen. Der Metadata Access Point (MAP) aus den TNC-Spezifikationen definiert hierfür bereits Schnittstellen, die zur zentralen Informations-sammlung eingesetzt werden können. Ein Ansatz für weitere Forschung zu dem aktuellen Thema der ganzheitlichen IT-Sicherheit im Smart Grid-Umfeld.

Danksagung

Die Autoren danken dem BMWi-ZIM [Bu13g] für die Förderung und allen SPIDER-Projektpartnern [Sp13] für die gute Zusammenarbeit.

Literaturverzeichnis

[Ar13] ARM Ltd: TrustZone. http://www.arm.com/products/processors/technologies/trustzone/index.php, Nov. 2013; zuletzt aufgerufen am 22.11.13.

[Ba06] Bare, J. C.: Attestation and Trusted Computing. University of Washington, Washington, 2006.

[Be13] Becker, C: Bedrohungsanalyse für Smart Grids und Anpassung des Sicherheitskonzeptes. Hochschule Bremen, Bremen, 2013.

[Bu13a] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2013.

[Bu13b] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109-2 Smart Meter Gateway Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2013.

[Bu13c] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109-4 Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2013.

[Bu13d] Bundesamt für Sicherheit in der Informationstechnik: Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP). Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2013

[Bu13e] Bundesamt für Sicherheit in der Informationstechnik: Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP). Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2013.

[Bu13f] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109-1 Anlage VI : Betriebsprozesse. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2013.

[Bu13g] Bundesamt für Wirtschaft und Technologie: Zentrales Innovationsprogramm Mittelstand (ZIM). http://www.zim-bmwi.de/, Nov. 2013; zuletzt aufgerufen am 22.11.13.

[Is09] ISO/IEC: ISO/IEC 11889-1 Information technology — Trusted Platform Module — Part 1: Overview. ISO copyright office, Genf, 2009.

[Ki06] Kinney, S.: Trusted platform module basics : using TPM in embedded systems. Elsevier, Amsterdam [u.a], 2006.

[LSW10] Löhr, H.; Sadeghi, A.-R.; Winandy, M: Patterns for Secure Boot and Secure Storage in Computer Systems. Availability, In IEEE: ARES '10 International Conference on Reliability, and Security, Krakow, 2010; S.569-573.

[Mi13] Microsoft: Threat Modeling Uncover Security Design Flaws Using The STRIDE Approach. http://msdn.microsoft.com/en-us/magazine/cc163519.aspx, Jan. 2013; zuletzt aufgerufen am 6.11.13.

[SHB13] Sethmann, R.; Hoffmann, O.; Busch, S.: Sichere Datenübertragung in Smart Grids mit Trusted Computing. DACH-Security, Nürnberg, 2013; S.332-343.

[Sm05] Smith, S. W: Trusted Computing Platforms : Design and Applications. Springer, New York, 2005.

[Sp13] SPIDER: Partner. http://www.spider-smartmetergateway.de/cms/front_content.php?idcat=3&lang=1, Nov. 2013; zuletzt aufgerufen am 22.11.13.

[Tr07] Trusted Computing Group: TCG Specification Architecture Overview. TCG PUBLISHED, Beaverton, 2007.

[Tr11] Trusted Computing Group: TPM Main - Part1 Design Principles. TCG PUBLISHED, Beaverton, 2011.

[Tr12] Trusted Computing Group: TCG Trusted Network Connect TNC Architecture for Interoperability. TCG PUBLISHED, Beaverton, 2012.