Vorgehensweise zur Erstellung eines Smart Meter Gateways

if(is) Projekt

http://www.internet-sicherheit.de/institut/forschung/aktuelle-forschungsprojekte/security-for-smart-car-smart-grid-smart-traffic-smart-home/

21.02.2014

v1.0

Öffentlich

Autoren
Tobias Urban, B. Sc.
René Riedel, B. Sc.
Dipl.-Ing. Antonio González Robles
Prof. Dr. (TU NN) Norbert Pohlmann

Institut für Internet-Sicherheit -if(is) der Westfälischen Hochschule Gelsenkirchen

1 Einleitung

In diesem White-Paper wird eine mögliche Vorgehensweise bei der Erstellung eines Smart Metering Gateways (SMGW) beschrieben, die im Rahmen von zwei Bachelor-Arbeiten im Institut für Internet-Sicherheit erstellt worden ist. Es werden Herausforderungen thematisiert, die bei der Erstellung eines Gateways auftreten können.

In Kapitel 3 werden die Grundlagen des BSI Protection Profile (BSI-CC-PP-0077) vorgestellt, in Kapitel 4 werden die im Rahmen der Bachelorarbeiten erstellte Konzipierung und prototypische Umsetzung in Zusammenarbeit mit dem Institut für Internet-Sicherheit if(is) vorgestellt.

In Kapitel 5 werden die Erfahrungen und Herausforderungen, die das Institut für Internet-Sicherheit - if(is) bei der Erstellung eines Prototyps des SMGW gemacht hat, dargelegt. Des Weiteren werden Erfahrungen von Firmen aus dem Umfeld angerissen.

Das White Paper vereint die Erfahrungen des Instituts für Internet-Sicherheit - if(is) rund um die Entwicklung eines SMGW im Rahmen zweier Bachelor Abschlussarbeiten im Projekt SecMobil und seiner Expertise im Bereich der IT-Sicherheit mit den praktischen Erfahrungen von Firmen, die im Energiesektor, Smart Home, Smart Car und IT-Sicherheitsumfeld Erfahrungen zum SMGW gesammelt haben und weist auf, wie ein SMGW unter Vermeidung möglicher Probleme umgesetzt werden kann.

An dieser Stelle möchten wir uns ausdrücklich bei den Firmen SIRRIX AG und ESCRYPT GmbH für die Unterstützung bei der Realisierung der Bachelorarbeiten bedanken.

2 Zielgruppe dieses White Papers

Das vorliegende White-Paper richtet sich in erster Linie an Hersteller bzw. Entwickler eines Smart Metering Gateways (SMGW), welches auf den entsprechenden Technischen Richtlinien (BSI TR-03109) und dem Schutzprofil (BSI-CC-PP-0077) des BSI basiert. Hersteller von Komponenten, die mit dem SMGW interagieren (z.B. Hersteller von Smart Metern oder Hersteller eines Security Moduls), erhalten einen Überblick über das SMGW und wie eine Kommunikation mit diesem realisiert wird. Energieversorger erhalten einen Überblick über die Funktionalitäten des Gateways und wie die Kommunikation mit diesem realisiert wird.

2.1 Hersteller eines Smart Metering Gateways

Mit diesem Dokument soll den Herstellern eines Gateways ein Überblick verschafft werden, welche Herausforderungen bei der Erstellung eines SMGWs auftreten könnten. Es werden auch die Herausforderungen aus Sicht der IT-Sicherheit beleuchtet und die ergriffenen IT-Sicherheitsmaßnahmen konkret beschrieben. Letztlich wird auch der Prototyp des SMGWs, der innerhalb von Forschungsarbeiten des Instituts für Internet-Sicherheit - if(is) entstanden ist, vorgestellt.

2.2 Hersteller von Komponenten

Herstellern von Komponenten (z.B. Smart Cars, Security Modulen oder Ähnliches), die mit dem Smart Metering Gateway kommunizieren wollen, erhalten in diesem Paper eine kurze Übersicht über das SMGW. Außerdem werden Probleme thematisiert, die bei der Erstellung des Gateways auftreten können. Diese Herausforderungen könnten auch direkt oder indirekt Einfluss auf andere Komponenten haben. Ebenfalls werden die Sicherheitsmechanismen des Gateways erläutert, die ebenfalls direkten Einfluss auf die angeschlossenen Komponenten haben können.

2.3 Firmen aus dem Energiesektor und Smart Grid

Zur Zielgruppe des White Papers gehören unter anderem Firmen aus dem Energiesektor, wie es Stromanbieter jeglicher Unternehmensgröße sind, Betreiber von Industrieanlagen, für die eine verbrauchs- und lastorientierte Kommunikation mit dem Smart Home und/oder Smart Grid vorgesehen ist. Darüber hinaus auch die Betreiber bzw. die mit am Aufbau des Smart Grid beteiligten Unternehmen.

3 Das SMGW-Protection Profile

In diesem Abschnitt wird eine kurze Übersicht zu dem Gateway gegeben. Es werden die Vorteile des Einsatzes des SMGWs für private Personen und Unternehmen betrachtet.

3.1 Spezifikation

Das Schutzprofil für die *Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen*[1] wurde vom BSI nach der *Common Criteria for Information Technology Security Evaluation* entwickelt und entspricht dem Evaluation Accurance Level 4. Das Schutzprofil befasst sich mit den Sicherheitsmechanismen und daraus entstehenden Anforderungen an ein Smart Metering Gateway (SMGW), die nötig sind, um eine vertrauenswürdige zentrale Komponente entwickeln zu können.

Die Technische Richtlinie (BSI TR-03109) für die *Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems*[2] des BSI erweitert die Anforderungen, die an das SMGW innerhalb des Schutzprofils gestellt werden, hinsichtlich genutzter Protokolle, Algorithmen und der Speicherung der Messdaten.

[1] Link zu dem Schutzprofil: https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html
[2] Link zu der Technischen Richtlinie: https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html

3.2 Übersicht über das SMGW

Im Folgenden soll kurz eine Übersicht zu den wichtigsten Akteuren und Funktionalitäten des SMGW gegeben werden. Die folgende Abbildung zeigt das Umfeld des Smart Metering Gateways.

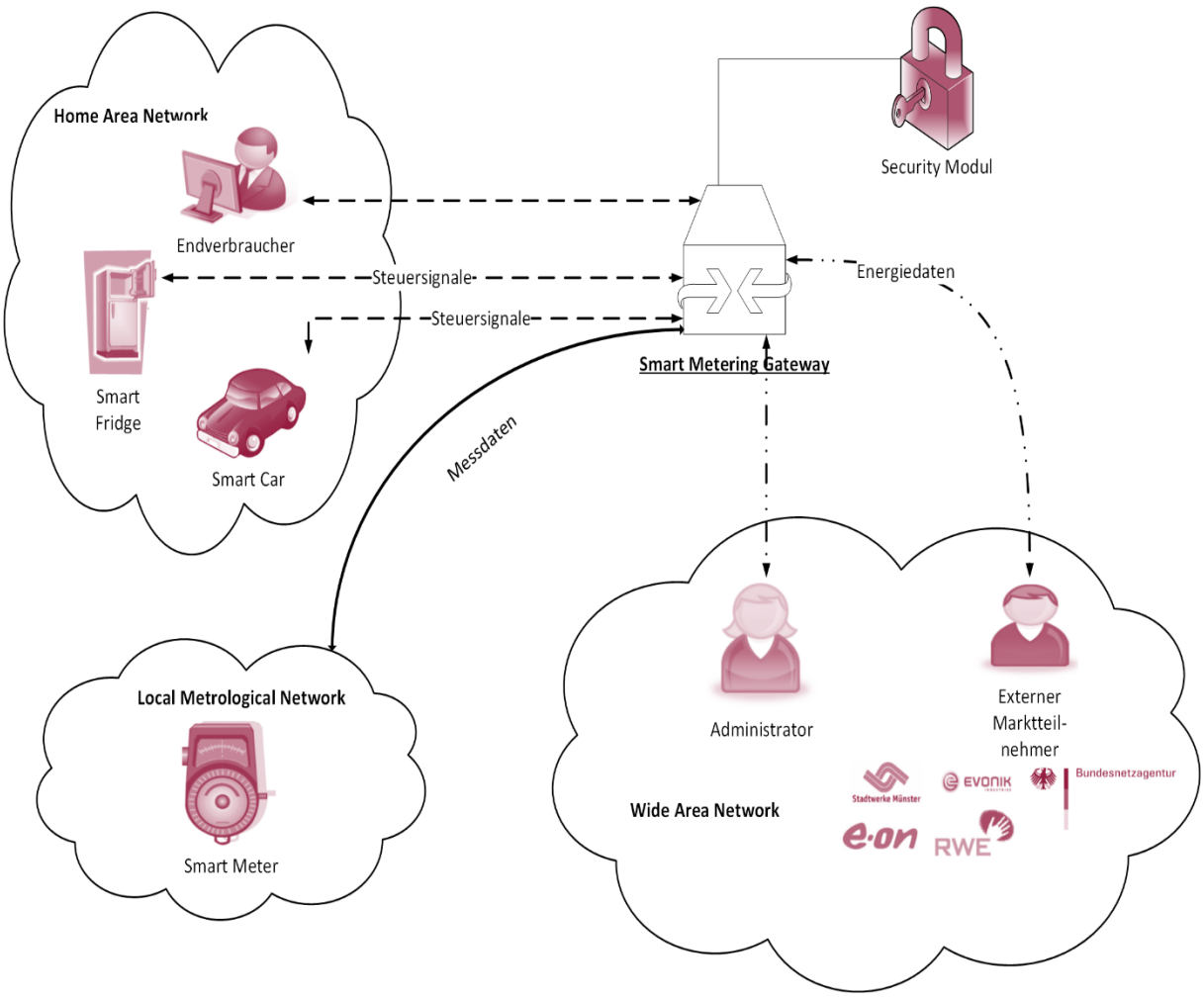

Abbildung 1: Das Umfeld des Smart Metering Gateways

3.2.1 Die wichtigsten Akteure des Smart Metering Gateways

Die folgende Auflistung beschreibt die wichtigsten Akteure die im Umfeld des SMGWs agieren.

Controllable Local System (CLS): CLS sind Komponenten im „Smart Home“ (im Bild: „Home Area Network“), die in der Lage sind mit anderen IT-Komponenten zu kommunizieren, aber nicht direkt dem intelligenten Messsystem zuzuordnen sind, beispielsweise Photovoltaikanlagen, Kühlschränke oder Waschmaschinen.

Intelligente Messgeräte (Smart Meter): Smart Meter liefern, anders als die herkömmlichen analogen Zähler, die meist jährlich ausgelesen werden, Messwerte in hoher Granularität. Technisch

ist eine minutengenaue Erfassung der Zählerstände möglich. Im Bild befinden sich die Smart Meter im „Local Metrological Network“.

Sicherheitsmodul (Security Modul): Für die kryptographischen Funktionen innerhalb des SMGWs kommt eine spezielle IT-Sicherheitshardware zum Einsatz.

Gateway-Administrator (SMGW-Administrator): Der Administrator übernimmt die Verwaltung des Gateways. Die Verwaltung beinhaltet beispielsweise das Einspielen von neuer Firmware, neuer Profile zur Tarifierung oder die Erhebung von Netzzustandsdaten.

Externe Marktteilnehmer: Externe Marktteilnehmer sind alle autorisierten Teilnehmer innerhalb des WAN, die mit dem SMGW kommunizieren dürfen. Beispiele hierfür sind Firmen, die Abrechnungen zu den Messwerten erstellen oder den Netzzustand ermitteln.

Endverbraucher: Mit Endverbraucher (oder auch Letztverbraucher) wird die Person bezeichnet, die eine Ressource (Wasser, Gas, Wärme oder Strom)[3] bezieht oder produziert.

Diese Akteure werden in drei physisch voneinander getrennten Netzen verwaltet. Diese Netze werden im Folgenden kurz beschrieben.

Local Metrological Network (LMN): In dem Lokalen Messtechnischen Netzwerk befinden sich die lokalen intelligenten Messgeräte (Smart Meter)

Home Area Network (HAN): Das Heimnetzwerk umfasst alle steuerbaren Geräte (CLS) und Benutzer (Endverbraucher), innerhalb eines Smart Home, die mit dem SMGW kommunizieren.

Wide Area Network (WAN): Im WAN befinden sich weitere Kommunikationspartner, die für die Administration des Gateways (SMGW-Admin) oder Tarifierung bzw. Netzzustandsanalyse (Externe Marktteilnehmer) zuständig sind.

3.2.2 Die grundlegenden Funktionalitäten des Smart Metering Gateways

Im Folgenden werden die wichtigsten Aufgaben des Gateways kurz dargestellt und erläutert.

Handhabung der Messwerte: Das SMGW ist für die Verarbeitung und Verbreitung der Messwerte verantwortlich. Dies umfasst das Empfangen von Messwerten von einem oder mehreren, dem Gateway bekannten und berechtigten, Smart Metern, sowie das Übermitteln der Messdaten an berechtigte externe Marktteilnehmer oder Endkunden.

Schutz von Integrität, Authentizität und Verbindlichkeit: Die Verbindlichkeit aller Daten, die das Gateway empfängt, speichert und versendet, muss sichergestellt werden. Unberechtigte Parteien müssen daran gehindert werden die Daten zu verändern, um so das Smart Metering System zu manipulieren.

[3] Im Folgenden wird nur noch von der Ressource Strom thematisiert. Die Vorgestellten Konzepte oder Probleme sind allerdings – meist 1 zu 1 – übertragbar.

Firewalling und Flusskontrolle: Das Gateway verfolgt eine strikte Firewalling-Strategie. Eine grundlegende Firewalling-Policy besagt, dass *nur* das Gateway Verbindungen in das WAN aufbauen darf, also *keine* Verbindungen annimmt, die aus dem WAN aufgebaut werden. Eine Ausnahme bildet hier ein Wake-Up Service, der noch detaillierter erläutertet wird.

Wake-Up Service: Der Administrator kann das Gateway auffordern eine Verbindung zu einer fest definierten Adresse im WAN aufzubauen. Über diese Verbindung kann der Administrator das Gateway warten und konfigurieren.

Schutz der Privatsphäre: Der Schutz der Privatsphäre der Letztverbraucher ist ein wichtiger Punkt innerhalb des SMGWs. Um diese zu schützen, werden generell alle Daten der Endkunden anonymisiert übertragen. Nur falls es zwingend nötig ist die Identität des Endverbrauchers offenzulegen, beispielsweise um Abrechnungen erstellen zu können, werden die Daten pseudonymisiert übermittelt.

3.3 Vorteile des SMGW

Die Einführung des SMGW in das intelligente Stromnetz (Smart Grid) bringt einen erheblichen Aufwand mit sich. Dieser Aufwand bringt allerdings auch viele Sicherheitsvorteile mit sich. In diesem Abschnitt werden die Vorteile für die Endverbraucher und die Stromerzeuger kurz dargestellt.

3.3.1 Vorteile für die Endverbraucher

Einer der größten Vorteile für die Endverbraucher, ist die flexible und durchsichtige Tarifierung, die durch die Installation der intelligenten Zähler (Smart Meter) möglich wird. Die Endverbraucher können jederzeit ihren Stromverbrauch und die daraus resultierende Abrechnung einsehen. Ebenfalls können die Endverbraucher in quasi Echtzeit ihren Verbrauch ermitteln. Die folgende Abbildung zeigt eine Verbrauchskurve eines privaten Haushaltes, die für die Abrechnung genutzt werden könnte.

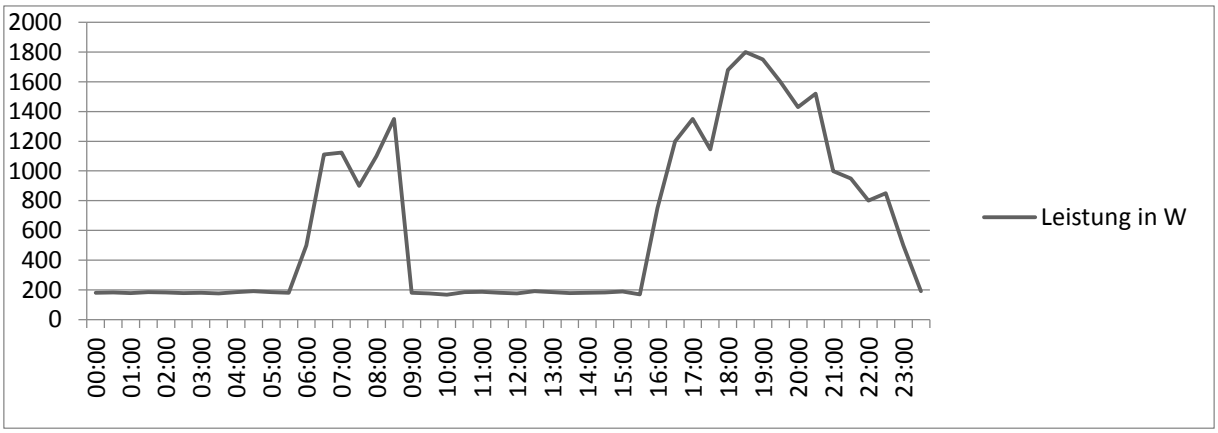

Abbildung 2: Beispielhafte Energieverbrauchskurve

Anhand der Messdaten, die in hoher Granularität vorliegen, könnten unterschiedliche Tarife umgesetzt werden. So könnten beispielweise zeitvariable Tarife oder lastvariable Tarife angeboten werden. Bei

zeitvariablen Tarifen können die Stromlieferanten unterschiedliche Preise zu unterschiedlichen Zeitpunkten definieren. Lastvariable Tarife würden den Preis an die aktuelle Last des Systems koppeln. (Wenn im gesamten System viel Strom benötigt wird, kostet dieser mehr und umgekehrt). So könnten Kunden durch die Entscheidung, wann sie den Strom verbrauchen, direkten Einfluss auf ihre eigene Stromrechnung nehmen.

3.3.2 Vorteile für die Erzeuger

Der Einsatz des Smart Metering Gateways bietet nicht nur für die Endverbraucher, sondern auch für die Stromerzeuger bzw. Netzbetreiber Vorteile. Durch die Einbindung des Gateways in das intelligente Stromnetz, ist zu jedem Zeitpunkt eine genaue Bedarfs- und Verbrauchsanalyse möglich. Das Gateway bietet auch die Möglichkeit mit intelligenten Geräten (Smart Cars, Smart Fridges, …) in den Haushalten zu kommunizieren. Steuerbefehle an diesen intelligenten Komponenten tragen dazu bei, eine bessere Lastverteilung zu ermöglichen. Ein Beispiel für eine solche Kommunikation ist das Steuern der Batterie eines Elektroautos. Liegt ein Überschuss an Strom vor kann die Batterie geladen werden, bzw. kann die Batterie Strom in das Smart Grid einspeisen, falls dieser benötigt wird.

3.4 Herausforderungen aus Sicht der IT-Sicherheit

Das Smart Metering Gateway verwaltet viele unterschiedliche Arten von Daten. Aus Sicht der IT-Sicherheit, müssen diese Daten vor Manipulationen und unberechtigten Zugriffen geschützt werden. Die schützenswerten Daten werden im Folgenden aufgelistet und möglichen Angriffsszenarien zugeordnet.

3.4.1 Messwerte

Die im SMGW anfallenden Messwerte werden zum Zwecke der Abrechnung und Netzzustandserhebung genutzt. Das SMGW muss eine Bildung von Profilen auf Basis der erhaltenden Messwerte ausschließen.

Ein potenzieller Angreifer könnte über die folgenden Angriffsszenarien versuchen, die Messwerte mitzulesen oder zu manipulieren.

Manipulation von Messdaten: Durch die Manipulation von Messdaten versucht der Angreifer seine private Stromrechnung zu beeinflussen oder eine Instabilität des intelligenten Stromnetzes hervorzurufen.

Unberechtigtes Auslesen bzw. Mitlesen von Messdaten: Für die Bildung von Profilen versucht ein motivierter Angreifer die Messdaten während der Übertragung mitzulesen. Denkbar ist auch der Versuch, die im SMGW gespeicherten Messwerte direkt auszulesen.

3.4.2 Log-Daten

Besondere Ereignisse im SMGW werden in Form von Logs protokolliert. Angriffe auf die Logs werden im Folgenden dargestellt:

Manipulation der Logs: Die Motivation für die Manipulation der Logs ist vor allem die Verschleierung eines Angriffs.

Unberechtigtes Auslesen bzw. Mitlesen der Logs: Das unberechtigte Auslesen bzw. Mitlesen der Logs kann unterschiedlich motiviert sein. Auf der einen Seite kann ein Angreifer die privaten Informationen der Endverbraucher, zur Bildung von Profilen, nutzen. Auf der anderen Seite können die einzelnen Einträge in den Logs für die Suche weiterer Schwachstellen dienen.

3.4.3 Zeit des Gateways

Die Uhrzeit des SMGWs ist für die korrekte Tarifierung und die Verifizierung von Datenpaketen wichtig. Wenn die Uhrzeit des SMGWs von der Systemzeit des SMGW-Administrators abweicht, kommt es zu Fehlfunktionen des Gateways (Wake-Up Service, Tarifierungsroutine, Messwerterfassung, usw.). Das folgende Angriffsszenario beschreibt die Manipulation der Uhrzeit des SMGWs:

Manipulation der Uhrzeit des SMGWs: Der Hauptgrund für die Manipulation der Uhrzeit des SMGWs ist die Beeinflussung der Tarifierungsroutine. In diesem Szenario könnte ein potenzieller Angreifer versuchen, die Beziehung zwischen Verbrauch und Zeitpunkt des Verbrauches zu beeinflussen.

3.4.4 Konfigurationen

Zu den Konfigurationen des SMGWs gehören beispielsweise Zählerprofile, Auswertungsprofile, Kommunikationsprofile, CLS-Einstellungen oder Zertifikats- und Schlüsselmaterialien.

Manipulation der Konfigurationen: Gelingt es einem Angreifer uneingeschränkt und gezielt die Konfigurationen des SMGWs zu beeinflussen, kann er den gesamten Informationsfluss des Gateways steuern.

Unberechtigter Zugriff auf ein CLS: Die Übernahme eines CLS aus dem WAN heraus, kann unterschiedliche Folgen haben. Abhängig von dem jeweiligen CLS kann die Schadenskategorie eines Angriffs variieren. Handelt es sich beispielsweise um einen steuerbaren Kühlschrank, so sind die Auswirkungen eines Angriffs verhältnismäßig geringer als die Übernahme eines Elektroautos.

3.5 Lösungswege

Die folgenden Schutzmechanismen des SMGWs werden von dem SMGW (als Software Artefakt) selber umgesetzt:

- TLS-Kanal
- Digitale Signatur
- Flusskontrolle
- Inhaltsdatenverschlüsselung
- Zeitstempel
- Anonymisierung und Pseudonymisierung

Zusätzlich zu den aufgeführten Schutzmechanismen, werden die nachfolgenden Annahmen aufgestellt:

Physischer Schutz des Gateways: Es wird angenommen, dass das SMGW physisch vor jeglicher Manipulation von außen geschützt ist.

Verschlüsselung des Speichers: Die Verschlüsselung des persistenten Speichers des Gateways wird vorausgesetzt.

Unabhängig von den technischen Schutzmechanismen, muss der SMGW-Administrator für seine Aufgaben speziell geschult und ausgebildet sein. Darüber hinaus wird die Annahme getroffen, dass alle Konfigurationen ordnungsgemäß auf dem SMGW eingespielt wurden. Die folgende Abbildung zeigt vereinfacht die Zuordnung der zuvor beschriebenen Sicherheitsmechanismen zu den möglichen Angriffsszenarien.

Schutzmechanismus / Angriffsszenario	TLS-Kanal	Digitale Signatur	Flusskontrolle	Inhaltsdatenverschlüsselung	Zeitstempel	Anonymisierung u. Pseudonymisierung	Physischer Schutz	Speicherverschlüsselung
Manipulation von Messdaten	X	X		X	X	X	X	
Mitlesen von Messdaten	X			X		X		
Mitlesen bzw. Auslesen der Logs	X		X	X				
Manipulation des SMGW (Zeit, Konfigurationen, …)	X			X			X	X

Abbildung 3: Zuordnung der Sicherheitsmechanismen zu den Angriffsszenarien

4 SMGW des if(is)

Dieses Kapitel beschreibt den SMGW-Prototyp, der vom Institut für Internet-Sicherheit - if(is) innerhalb der Forschungen des Instituts und zwei Bachelorarbeiten entstanden ist. Es werden die umgesetzten Funktionalitäten, die gewählte Architektur und die eigenen Erfahrungen genauer beschrieben und betrachtet.

4.1 Umsetzung des if(is)

Die Funktionen des Prototyps, der vom Institut für Internet-Sicherheit - if(is) entwickelt wurde, werden im folgenden Abschnitt genauer diskutiert.

4.1.1 Genereller Kommunikationsfluss

Als zentrale Kommunikationseinheit ist ein Smart Metering Gateway mit zahlreichen Komponenten innerhalb eines intelligenten Stromnetzes verbunden. Zum einen sind dies weitentfernte

Kommunikationsteilnehmer im WAN (z.B. der SMGW-Administrator oder externe Marktteilnehmer) und zum anderen Komponenten (z.B. Smart Meter, Controllable Local Systems), die in unmittelbarer Nähe mit dem Smart Metering Gateway verbunden sind. Die Realisierung des generellen Kommunikationsflusses zwischen diesen Komponenten ist ein zentrales Ziel des Prototypens. Im Folgenden werden die einzelnen Bestandteile des zu realisierenden Kommunikationsflusses beschrieben.

4.1.1.1 Empfang von Messwerten

Die intelligenten Stromzähler werden direkt an das Smart Metering Gateway angeschlossen. Je nach Einstellung und Bauart verschicken diese Stromzähler entweder von alleine Messwerte an das SMGW oder nachdem das SMGW sie dazu aufgefordert hat. Diese Messwerte müssen vom SMGW entgegen genommen, gespeichert und anschließend verarbeitet werden.

Das Entgegennehmen von Messwerten ist zentraler Bestandteil des generellen Kommunikationsflusses im SMGW. Der Prototyp ist in der Lage, Messwerte von simulierten Smart Metern verarbeiten zu können.

4.1.1.2 Tarifierung

Vom SMGW empfangene Messwerte müssen vor dem Verschicken an einen Kommunikationsteilnehmer im WAN tarifiert werden. Die technische Richtlinie (BSI TR-03109) sieht für die Tarifierung von Messwerten verschiedene Modi vor. Für die Realisierung des generellen Kommunikationsflusses wurde der datensparsame Tarif umgesetzt.

4.1.1.3 Versenden von tarifierten Messwerten

Nachdem Messwerte vom SMGW tarifiert wurden, sollen diese an Kommunikationsteilnehmer im WAN verschickt werden. Die technische Richtlinie (BSI TR-03109) legt fest, dass das Versenden von Messwerten über einen vom Kommunikationsteilnehmer bereitgestellten RESTful Webservice erfolgen muss. Dieser Webservice wurde gemäß der technischen Richtlinie des BSI realisiert.

4.1.2 RESTful Webservices

Alle Kommunikationsszenarien im WAN müssen über einen vom Kommunikationsteilnehmer (SMGW, EMT, SMGW-Administrator) bereitgestellten RESTful Webservice, gemäß technischer Richtlinie des BSI ablaufen. Aus diesem Grund wurde der Webservice auf Seiten des SMGW umgesetzt. Für den Wirkbetrieb eines SMGW wird darüber hinaus zwingend der Webservice des SMGW-Administrators benötigt.

4.1.3 Wake-Up Service

Über einen Wake-Up Service soll der SMGW-Administrator in der Lage sein, eine verschlüsselte Verbindung mit dem SMGW anzufordern. Da der SMGW-Administrator ein Kommunikationsteilnehmer im WAN ist, darf er nicht selber eine verschlüsselte Verbindung zum SMGW aufbauen. Für die Anforderung einer verschlüsselten Verbindung muss der SMGW-Administrator ein spezielles Wake-Up-Paket an das SMGW verschicken. Ist das Wake-Up-Paket gültig, wird auf Basis eines im SMGW hinterlegten Kommunikationsprofils ein TLS-Kanal zum SMGW-Administrator aufgebaut. Der Wake-Up Service ist in der Technischen Richtlinie (BSI TR-03109) spezifiziert und wurde innerhalb des Prototypen umgesetzt.

4.1.4 Proxyfunktionalität

Gemäß der technischen Richtlinie des BSI, darf ein CLS innerhalb des HAN, nicht direkt eine verschlüsselte Verbindung mit einem Kommunikationsteilnehmer im WAN aufbauen (umgekehrt genauso). Für diesen Anwendungsfall muss das SMGW als Proxy fungieren und eine verschlüsselte Verbindung zwischen einem CLS und einem Kommunikationsteilnehmer im WAN aufbauen. Über diese Verbindung können beide Endpunkte miteinander kommunizieren. Diese Proxyfunktionalität bietet der entwickelte Prototyp an.

4.1.5 Logging

In fest definierten Situationen muss das SMGW Logeinträge erstellen. Abhängig von der auslösenden Situation muss dabei beachtet werden, dass der Eintrag in das für diese Situation vorgesehene Log (Eichtechnischer-Log, System-Log, Kunden-Log) erstellt wird. Der Logging-Mechanismus ist in der technischen Richtlinie (BSI TR-03109) spezifiziert und wurde innerhalb des Prototypen umgesetzt.

4.1.6 Bereitstellung von Informationen

Endverbraucher haben gemäß technischer Richtlinie (BSI TR-03109) die Möglichkeit, Informationen vom SMGW abzurufen. Für einen Endverbraucher ist festgelegt, welche Informationen abgerufen werden dürfen. Die für einen Endverbraucher freigegebenen Informationen können über eine spezielle Webseite abgerufen werden.

4.2 Architektur des Prototypen

Die Aufgaben des Smart Metering Gateway können, basierend auf den Schnittstellen, in fünf logische Aufgabenbereiche gegliedert werden. Der HAN-Kommunikation, der WAN-Kommunikation, der LMN-Kommunikation, der CLS–Kommunikation und der Tarifierung. Es bietet sich an, die Aufgaben logisch getrennt voneinander in einzelne Prozesse auszulagern. So ist auch beim Ausfall eines Teilprozesses die Funktionalität in den anderen Bereichen noch immer gegeben. Die Aufteilung auf mehrere

Prozesse bietet auch die Möglichkeit eine Integritätsprüfung vorzunehmen. Dies wäre auch bei einem großen Prozess möglich, würde allerdings mehr Zeit in Anspruch nehmen, in welcher das Gateway nicht verfügbar ist. Ein weiterer Vorteil der Aufteilung auf mehrere Prozesse ist die Möglichkeit auf Betriebssystemebene die Kommunikation zwischen den Prozessen beeinflussen zu können. Dies könnte bedeuten, dass schon auf Betriebssystemebene geregelt wird, wie die Prozesse untereinander kommunizieren dürfen. Auch die Austauschbarkeit einzelner Komponenten ist so sehr einfach und schnell möglich.

Ein Nachteil bei der Aufteilung auf mehre Prozesse liegt darin, dass die Prozesse über geeignete IPC-Mechanismen miteinander kommunizieren müssen. Dies ist aufwendiger und langsamer als eine direkte Kommunikation.

Die folgende Abbildung zeigt die Aufteilung des SMGWs in die unterschiedlichen Prozesse.

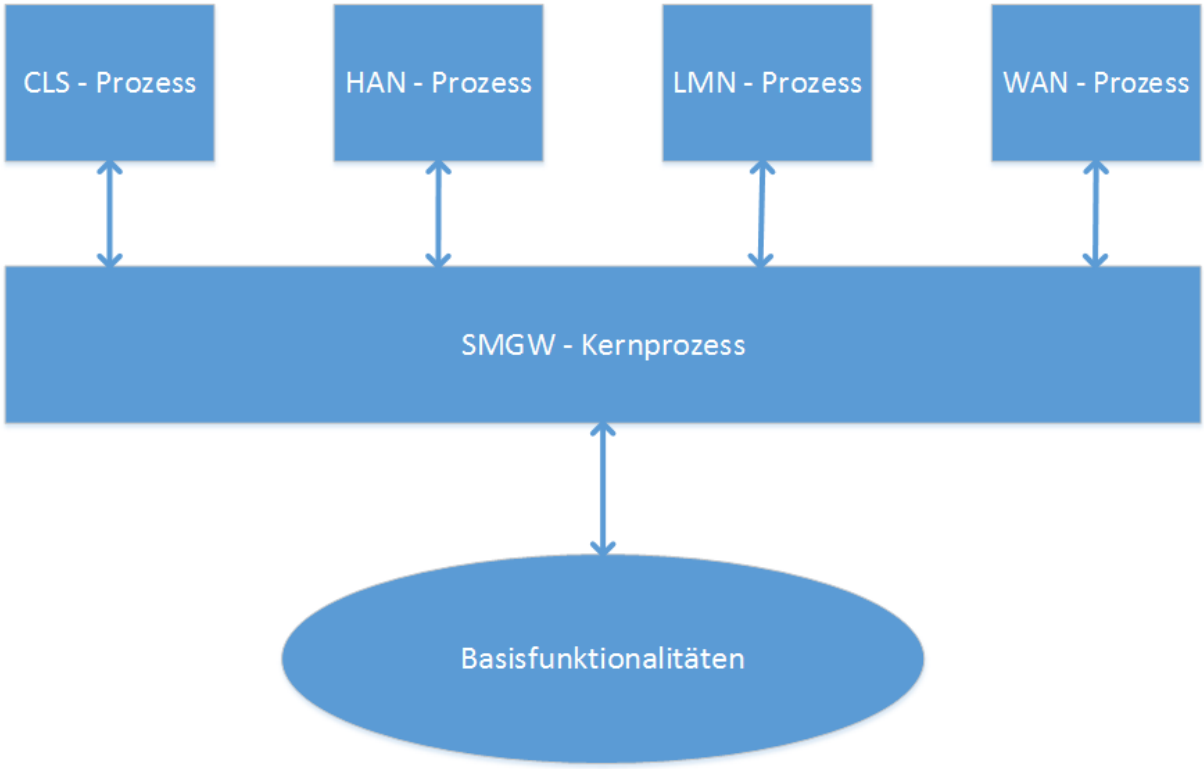

Abbildung 4: Prozessaufteilung des SMGWs

SMGW-Kernprozess: Der Kernprozess des SMGWs beinhaltet die Geschäftslogik des Gateways. Er ist für die Verwaltung und sichere Speicherung aller Einstellungsprofile und der empfangenen Messdaten zuständig. Die Tarifierung der originären Messwerte findet ebenfalls im Kernprozess statt.

Der Kernprozess nutzt Basisfunktionalitäten, die beispielsweise von dem Betriebssystem angeboten werden. Dazu zählen unter anderem, das Logging, die interne Uhrzeit des SMGWs oder der Aufbau von TLS-gesicherten Kanälen.

Der Kernprozess bietet den übergeordneten Prozessen Funktionalitäten an, die diese für die Erfüllung der einzelnen Aufgaben benötigen.

Basisfunktionalitäten: Die Basisfunktionalitäten entsprechen Funktionalitäten, die nicht direkt von der Anwendung umgesetzt, sondern von unteren Schichten (zum Beispiel vom Betriebssystem) bereitgestellt werden. Nur der Kernprozess des SMGWs soll direkt auf diese Funktionen zugreifen, um den darüber liegenden Schichten eine Abstraktion zu ermöglichen.

CLS-Prozess: Der CLS-Prozess realisiert die Aufgabe des Aufbaus eines transparenten TLS-gesicherten Kanals zwischen einem externen Marktteilnehmer und einem CLS im privaten Haushalt. Dazu nutzt der CLS-Prozess den Kernprozess, um die entsprechenden Profile und angeschlossenen CLS zu ermitteln.

HAN-Prozess: Die Bereitstellung von Daten für den Letztverbraucher wird im HAN-Prozess realisiert. Der Prozess bezieht die Informationen, die dem jeweiligen Kommunikationspartner angezeigt werden sollen und dürfen, von dem Kernprozess.

LMN-Prozess: Die Messdaten werden innerhalb des LMN-Prozess empfangen und geprüft. Anschließend werden die Messdaten an den Kernprozess übertragen, um dort gespeichert, verarbeitet und an EMT im WAN übertragen zu werden.

WAN-Prozess: Der WAN-Prozess ermöglicht die Kommunikation des Gateways mit den externen Marktteilnehmern und dem SMGW-Administrator. Außerdem übernimmt der Prozess die Verarbeitung des Wake-Up Paketes. Der Kernprozess wird von dem WAN-Prozess zum Aufbauen der TLS-gesicherten Verbindungen und zum Aufbringen der Konfigurationsprofile, Zertifikate und Ähnlichem verwendet.

4.3 Verwendete Technologien

Der Abschnitt befasst sich mit den Technologien die bei der Entwicklung des Prototypens eingesetzt wurden.

4.3.1 Programmiersprache Java

Für die Entwicklung des Prototypens wurde JAVA als Programmiersprache gewählt. JAVA wurde C++ oder C# aufgrund der fast vollkommenen Plattformunabhängigkeit vorgezogen. Da für JAVA zusätzlich viele Frameworks bzw. APIs existieren[4], die eine schnelle Entwicklung des Prototypens ermöglicht haben. Die Wahl von JAVA als Programmiersprache hat auch einige Herausforderungen mit sich gebracht.

[4] GuruxDLMS for Java, Java Architecture for XML Binding, Oracle GlassFish Webserver, …

4.3.2 Wahl eines geeigneten Betriebssystems

Unterschiedliche Linux Derivate wurden als Plattform für das Gateway in Betracht gezogen. Da der Prototyp des Gateways auf einem PandaBoard ausgeführt werden sollte, musste beachtet werden, dass die Betriebssysteme für den Einsatz auf dieser Hardware geeignet sind. Im Folgenden werden zwei, von vielen möglichen Betriebssystemen kurz dargestellt

Gentoo-Linux: Gentoo-Linux (kurz Gentoo) ist ein frei verfügbares Betriebssystem, welches auf Linux basiert. Das besondere an Gentoo ist, dass es komplett quellbasierend aufgebaut ist und dem Nutzer die Möglichkeit gibt, das System komplett nach seinen Wünschen zu gestalten.

Aufgrund dieser Individualisierbarkeit kann Gentoo in vielen Bereichen eingesetzt werden und auf den jeweiligen Einsatzzweck perfekt abgestimmt werden. Beispiele für die Einsatzbereiche von Gentooo sind klassische Desktopsysteme, Serversysteme und Embedded-Systems.

Ubuntu: Ubuntu ist eine freie Linux Distribution, die auf Debian basiert. Ubuntu ist eine der weit verbreitetsten und bekanntesten Linux Derivate. Aufgrund der einfachen Handhabung und simplen Installation ist Ubuntu besonders für Einsteiger sehr gut geeignet. Ubuntu bietet allerdings nicht ohne weiteres die Möglichkeit das System – genau wie bei Gentoo-Linux – komplett nach seinen Wünschen zu gestallten.

Da JAVA als Programmiersprache gewählt wurde, kann letztlich jedes Betriebssystem, auf dem eine Java Virtual Maschine lauffähig ist, gewählt werden. Zwar eignet sich Gentoo prinzipiell besser für die Umsetzung des Gateways, allerdings wurde für den Prototypen aus Zeitgründen Ubuntu gewählt.

4.3.3 Verwendete Hardware

4.3.3.1 PandaBoard

Das PandaBoard wird von einer OpenSource-Community entwickelt und steht unter der Creative Commons Attribution-Share Alike 3.0 Lizenz. Das PandaBaord wurde in erster Linie für die Entwicklung von mobilen Anwendungen und Geräten entwickelt.

Die wichtigsten Eigenschaften des PandaBoard ES für das SMGW werden kurz dargestellt.

CPU	Dual-core mit jeweils 1.2 GHz
Netzwerk	1x 10/100 MBit Ethernet-Controller 1x 802.11 b/g/n W-LAN Adapter
Echtzeituhr	Ja, nicht Batterie unterstützt
Arbeitsspeicher	1024 MB DDR2
Festplatte	SD (SDHC SDXC) / MMC / SDIO-Kartenleser
Preis	Ca. 169,00€ (inkl. Steuern)

Abbildung 5: Technische Eigenschaften des PandaBoards ES

Das PandaBoard ist von Haus aus nicht mit ausreichend physischen Schnittstellen ausgestattet. Daher wird zusätzliche Hardware benötigt, um diese bereitzustellen. Positiv ist, dass bereits eine drahtlose Schnittstelle von dem Board bereitgestellt wird. Die Tatsache, dass die Uhr nicht Batterie gestützt wird, wirkt zunächst nachteilig. Da das SMGW im Normalfall immer läuft, muss diese nur bei dem Start des Gerätes initial gestellt werden. Der Preis des Bordes fällt allerdings sehr hoch aus, dies ist aber vor allem auf die hohe Leistungsfähigkeit zurückzuführen. Auch bei diesem Board muss eine SD-Karte zusätzlich erworben werden.

Bei dem Testen des Prototypen wurde festgestellt, dass die CPU des PandaBoards, bei ‚Volllast', zu ca. 95% ausgelastet wurde. Dies liegt vor allem, an dem Betrieb der zwei Webserver (WAN und HAN Kommunikation) sowie der Tatsache, dass das Security Modul nicht vollständig eingebunden werden konnte und somit die kryptographischen Berechnungen von der CPU durchgeführt werden mussten.

4.3.3.2 Sicherheitsmodul

Für die eigenständige Realisierung des Security Moduls werden die SmartMX Karten der P5Cx145 Familie empfohlen. Dies ist die einzige Smart Card der gängigen Hersteller von Smart Cards, die alle geforderten kryptographischen Eigenschaften des SMGWs unterstützt, mit Ausnahme des PACE-Protokolls.

Das SMGW nutzt das Security Modul für drei Aufgaben der CMS-Inhaltsdatenverschlüsselung, während des TLS-Handshakes und zum Erstellen bzw. Prüfen von digitalen Signaturen. Daher wird das Security Modul im Rahmen des Prototypens zu großen Teilen softwareseitig simuliert.

Bei der Realisierung des SM sollte auch die Möglichkeit in Betracht gezogen werden, das SM durch eine Kooperation mit einer in diesem Bereich operierenden Firma zu erhalten.

4.3.3.3 Betriebskosten des Prototyps

Die Umsetzung der Energiewende ist in Deutschland gesetzlich beschlossen, somit ist auch die Einführung des Smart Metering Gateways in den privaten Haushalten unvermeidlich.

Für den Betrieb des SMGWs ist eine permanente Stromversorgung nötig. Dies bedeutet, dass Stromkosten für den Betrieb des Gateways anfallen.

Um eine Einschätzung des Verbrauchs eines Gateways zu erhalten, wurde der Stromverbrauch des Prototyps und eines handelsüblichen Switches innerhalb der Testumgebung eine Stunde lang gemessen. Die folgende Tabelle zeigt die Ergebnisse der Messung.

Verbrauch pro Stunde	0,013 kWh

⇒

Verbrauch pro Tag	0,312 kWh
Verbrauch pro Jahr	113,88 kWh

Abbildung 6: Stromverbrauch des Prototyps

Bei einem durchschnittlichen Strompreis von 28,73 Cent pro kWh ergibt sich daraus ein Gesamtwert von 32,72 € pro Jahr. Ausgehend von dem durchschnittlichen Verbrauch eines drei Personen Haushaltes innerhalb eines Jahres (3.500 kWh), entspricht dieser Gesamtwert einer prozentualen Erhöhung von 3,25 %.

Durch die Überdimensionierung der Bauteile (PandaBoard, Switch, SmartCard-Reader) sind die hier vorgestellten Messwerte als Obergrenze zu verstehen. Bei einer für das SMGW optimierten Hardware ist mit einem geringeren Stromverbrauch zu rechnen. Die zusätzlichen Stromkosten sind zu vernachlässigen, wenn durch den geplanten Einsatz von speziellen Tarifen (deren Umsetzung nur durch das Gateway möglich ist), die Stromkosten der Endverbraucher reduziert werden können.

5 Mögliche Herausforderungen bei der Entwicklung

Dieser Abschnitt zeigt einige mögliche Herausforderungen bzw. „Stolpersteine“ auf, die unter anderem bereits im Vorfeld der Implementierung eines Gateways die Entwicklung und Umsetzung nachhaltig beinträchtigen können.

Im ersten Teil dieses Kapitels werden die konkret während der Bachelorarbeiten aufgetretenen Hindernisse gestrafft beschrieben und die Quintessenz daraus unter „Erfahrungen aus den Bachelorarbeiten“ dargestellt. Der nächste Teil des Kapitels beschreibt die Herausforderungen, die sehr wahrscheinlich auftreten können, da seitens der Standardisierung (Spezifizierung) noch nicht alle notwendigen Spezifikationen verabschiedet worden sind, bzw. notwendige Infrastrukturen wie die zugehörigen notwendigen PKIn noch nicht aufgesetzt worden sind. Der dritte Teil des Kapitels beschreibt die praktischen Erfahrungen von Firmen bei der Entwicklung und/oder Roll-out eines SMGW.

5.1 TLS-Handshake und CMS Inhaltsdatenverschlüsselung

Die Technische Richtlinie TR-03109-1 schreibt genau vor, wie der TLS-Handshake in Kombination mit dem Security Modul umgesetzt werden muss. Die „Standard“ JAVA-Klassen zum Aufbau von TLS-

verschlüsselten Kanälen bietet allerdings nicht die Möglichkeit, den Handshake so zu beeinflussen, dass beispielsweise die Generierung des EC-Schlüsselpaars von dem Security Modul übernommen wird. Hier müsste eine eigenständige Umsetzung des TLS-Handshake Protokolls implementiert werden. Zwar könnte man versuchen den Aufbau des TLS-Kanals aus dem Programm an eine untere Ebene auszulagern (z.B. an ein VPN-System). Dies würde aber die Problematik der Einbindung des Security Moduls nicht umgehen. Ähnlich verhält es sich mit der CMS Inhaltsdatenverschlüsselung.

Der Entwickelte Prototyp nutzt das Security Modul zurzeit lediglich für die Erzeugung der Zufallszahlen.

Generell ist anzumerken, dass im Rahmen des Smart Metering Gateways sehr viele unterschiedliche Protokolle genutzt werden, welche in einigen Fällen nicht standardmäßig von der JAVA-API[5] unterstützt werden (z.B. COSEM). Hier muss bedacht werden, dass eine zumindest Teilweise Umsetzung der Protokolle nötig ist.

5.2 Herausforderungen durch fehlende Spezifikationen und nicht vorhandener Infrastruktur

Noch nicht abgeschlossene Standardisierung: Der Prozess der Spezifizierung rund um das Smart Metering Gateway ist zwar schon sehr weit fortgeschritten aber noch nicht vollständig abgeschlossen. In diesem Abschnitt werden einige noch nicht vollständig spezifizierte Teile dargestellt.

COSEM-Objekte: Die Spezifikation der COSEM-Objekte, die innerhalb des Gateways eingesetzt werden sollen, ist noch nicht abgeschlossen. Der Spezifizierungsprozess hat aber bereits begonnen. Erste Ergebnisse dieses Prozesses sind 2014 zu erwarten. Die Ergebnisse oder Teilergebnisse können über die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (DKE) eingeholt werden. Hier ist der Fachbereich 4 insbesondere das Sachgebiet 4.6 innerhalb des DKE für die Normierung der Objekte zuständig (DKE/AK 461.0.142).

Testspezifikation: Zu jeder Technischen Richtlinie bzw. zu jedem Schutzprofil, das vom BSI herausgegeben wird, gehört in aller Regel auch eine Testspezifikation. Diese definiert, wie das Produkt, welches durch die Spezifikation definiert ist, zu testen ist. Für das Smart Metering Gateway besteht zurzeit noch keine solche Testspezifikation. Diese wird zurzeit aber erarbeitet. Wann diese Spezifikation veröffentlicht wird, ist allerdings nicht bekannt.

Viele physische Komponenten: Problematisch gestaltet sich bei der Entwicklung eines Smart Metering Gateways, dass viele unterschiedliche, zum Teil physische Komponenten miteinander kommunizieren. All diese Komponenten (Security Modul, Smart Meter, CLS, SMGW-Admin, usw.) müssen zum Entwicklungszeitpunkt entweder vorliegen oder es müssen entsprechende Simulatoren entwickelt werden. Die Entwicklung dieser Simulatoren führt zu einem erheblichen Mehraufwand.

[5] Diese Protokolle werden, in der Regel, auch nicht von den APIs anderer Hochsprachen direkt unterstützt.

Vor allem ist die korrekte Einbindung des Security Moduls in das SMGW mit sehr hohem Aufwand verbunden.

Public Key Infrastruktur (PKI): Die Technische Richtlinie TR03109-4 beschriebt den Aufbau einer Smart Metering – PKI, die speziell für den Betrieb des Smart Metering Systems eingeführt werden soll. Diese PKI ist zurzeit noch nicht aufgebaut. Da ein großer Teil dieser PKI[6] allerdings von den Marktteilnehmern (Betreibern/Entwicklern des SMGW) umgesetzt wird, ist davon auszugehen, dass die PKI erst im Laufe der Zeit entstehen wird.

5.3 Praktische Erfahrungen von Unternehmen

Im Zuge der Konzipierung und Umsetzung des SMGW Prototypen sind wir in Kontakt mit Unternehmen, aus den Bereichen die das SMGW tangieren, getreten.

In einem regen direkten Austausch mit Unternehmen, die an einer Entwicklung des SMGW interessiert sind oder dabei sind eines zu konzipieren, konnten wir feststellen, dass diese Unternehmen unabhängig vom Institut für Internet-Sicherheit – if(is) im Großen und Ganzen auch auf die unter Kapitel 5.1 und 5.2 aufgeführten Herausforderungen gestoßen sind.

Eine wichtige noch zu lösende Herausforderung ist die noch nicht vollständig abgeschlossene Standardisierung, die besonders Unternehmen eine betriebswirtschaftlich auf Investitionsschutz orientierte Entwicklung erschwert.

An dieser Stelle hätten wir Ihnen gerne jetzt schon Unternehmen, Ihre Herausforderungen und möglichen Lösungen bei der Entwicklung eines SMGW genannt, sodass Sie sich mit diesen hätten austauschen können. Das ist uns zum jetzigen Zeitpunkt aus Gründen der zu wahrenden Vertraulichkeit noch nicht möglich gewesen.

Im Nachgang zum Erscheinen dieses White Papers hoffen wir auf noch mehr Kontakte mit entsprechenden Unternehmen und auf die sich daraus für alle ergebende Synergie, so dass wir Ihnen dann entsprechende Unternehmen bereitstellen können.

Sie könnten an einer weiteren Auflage des White Papers teilnehmen.

6 Ausblick

Abschließend wird ein mögliches Zusammenspiel des Smart Metering Gateways mit weiteren Komponenten des intelligenten Stromnetzes, die sich in anderen Domänen außerhalb des Smart Home befinden, betrachtet.

Denkbar wäre eine Kommunikation des SMGWs, über eine weitere Instanz im WAN, mit Elektroautos bzw. den Ladesäulen an Tankstellen. So könnte nicht mehr wichtig sein, wo der Strom genutzt wird, sondern von wem dieser genutzt wird. Dies könnte bedeuten, dass sich ein Endverbraucher

[6] Mit Ausnahme des ROOT-CA.

gegenüber einer Ladestation für Elektroautos authentifiziert und der anfallende Betrag automatisch auf dem heimischen Stromanschluss, also auch auf der Stromrechnung des Letztverbrauchers verbucht wird. Die Ladesäule ermittelt und überträgt Informationen zu dem Fahrzeug, dem Letztverbraucher und der geladenen ‚Menge' Strom. Aus dieser Interaktion ergeben sich neue Herausforderungen, die den Datenschutz der Endverbraucher betreffen. So könnten anhand der Daten, wo der Letztverbraucher den Strom bezogen hat, ein Bewegungsprofil des Kunden erstellt werden.

Das White Paper vereint die Erfahrungen des Instituts für Internet-Sicherheit - if(is) rund um die Entwicklung eines SMGW im Rahmen zweier Bachelor-Abschlussarbeiten im Projekt SecMobil und seiner Expertise im Bereich der IT-Sicherheit mit den praktischen Erfahrungen von Firmen, die im Energiesektor, Smart Home, Smart Car und IT-Sicherheitsumfeld Erfahrungen zum SMGW gesammelt haben und weist auf, wie ein SMGW unter Vermeidung möglicher Probleme umgesetzt werden kann.

7 Kontakt

Wenn Sie weitere Fragen zu dem entwickelten Prototypen oder dem SMGW haben, würden wir uns freuen, wenn Sie mit uns in Kontakt treten!

Prof. Dr. (TU NN) Norbert Pohlmann, Institutsleiter if(is)
Dipl.-Ing. Antonio González Robles, Projektleiter Secure eMobility

Institut für Internet-Sicherheit - **if(is)**
Westfälische Hochschule
Fachbereich Informatik und Kommunikation
Neidenburgerstr. 43
45887 Gelsenkirchen
E-Mail: gonzalezrobles@internet-sicherheit.de

Tel.: +49 (0) 209 95 96 746

A Acknowledgments

This work was supported by the German Federal Ministry of Economics and Technology (Grant 01ME12024 Secure eMobility (SecMobil)).

B Literaturverzeichnis

[1] T. Urban and R. Riedel, Konzeption und prototypische Entwicklung eines Smart Metering Gateways, basierend auf dem Schutzprofil des BSI, Gelsenkirchen, 2013.

[2] T. Urban, R. Riedel, N. Pohlmann and A. González Robles, "Gefahrenpotenzial intelligenter Stromnetze aus Sicht der IT-Sicherheit: Anforderungen an IT-Systeme in kritischen Infrastrukturen," *IT-Sicherheit,* no. 4/2013, 2013.

C Abbildungsverzeichnis