Praxistaugliche Kommunikationssicherheit in einer Smart Metering Infrastruktur

Christian Peuker [a], Dominik Engel [a]

[a] Fachhochschule Salzburg – Josef Ressel Center for User-Centric Smart Grid Privacy, Security and Control, Urstein Süd 1, A-5412 Puch/Urstein, AUSTRIA

KURZFASSUNG/ABSTRACT:
Um für zukünftige Herausforderungen, wie die flächendeckende Einbindung erneuerbarer Energien, gerüstet zu sein, müssen die klassischen Stromnetze zu sogenannten „Smart Grids“ ausgebaut werden. Da es sich bei Smart Grids um eine kritische Infrastruktur handelt, bedarf es für die aufzubauende „Advanced Metering Infrastructure“ (AMI) einer adäquaten Absicherung. Im Besonderen muss die erforderliche Kommunikationssicherheit gewährleistet sein. Eine praxistaugliche sichere Umsetzung einer AMI, die auch wirtschaftlich tragbar ist, stellt in der Energiewirtschaft eine nicht zu unterschätzende Herausforderung dar. Besonders die kostengünstige Umsetzung eines sicheren Smart Meter Gateways in der Anwenderdomäne wird als kritisch gesehen. Im vorliegenden Beitrag werden sicherheitstechnische Anforderungen an ein Smart Metering Gateway analysiert. Ausgehend von dieser Analyse wird eine Lösung vorgestellt, die diese Anforderungen, im Besonderen die wesentlichen Kernforderungen des deutschen BSI-Schutzprofils, erfüllt und durch die Verwendung günstiger ARM-basierten Prozessoren in Verbindung mit Open Source Software eine hohe Wirtschaftlichkeit erreicht.

1 EINLEITUNG

Da es sich bei einem Smart Grid um ein komplexes Gesamtsystem handelt, kann dieses als „System of Systems“ betrachtet werden. Fang gliedert dieses in die Teilsysteme *Smart Infrastructure*, *Smart Management* sowie das *Smart Protection System* [2]. In weiterer Folge sind vor allem das *Smart Communications Subsystem* als Teil der Smart Infrastructure Systems sowie das Smart Protection System von Bedeutung. Hinsichtlich einer näheren Betrachtung der Gefahren, denen ein Smart Grid ausgesetzt ist, sowie der aktuellen Herausforderungen wird auf [1] und [4] verwiesen.

Der *Smart Metering Gateway* ist ein integraler Teil des Smart Communication Subsystems. In der Literatur wird er oftmals in einen Metering und einen Management Gateway unterteilt. In seiner Funktion als Metering Gateway liest er die erforderlichen Daten verschiedenster Messgeräte (z.B. Strom, Gas, Wasser) aus und überträgt diese, nach einer optionalen Aggregation, zu den zentralen Diensten des Netzbetreibers im WAN. Darüber hinaus kontrolliert der Management Gateway sämtliche im Bereich des Kunden verbauten Komponenten zum Zwecke der Lastensteuerung. Zusätzlich kann er in Zukunft auch die Rolle eines lokalen Energiemanagers einnehmen. Grundvoraussetzung für die Wahrnehmung dieser Aufgaben ist ein sicherer, bidirektionaler Kommunikationsweg in jeden Haushalt. Da die Sicherstellung dieser Anforderung mit enormen Kosten verbunden ist, wird eine Nutzung dieser Kommunikationswege für zusätzliche artfremde Dienste, beispielsweise im Bereich des Ambient Assisted Living, angestrebt.

Aufgrund der hohen Anzahl der unterschiedlichsten im Kundenbereich verbauten Komponenten muss der Smart Metering Gateway eine Vielzahl von Kommunikationstechnologien und -protokollen unterstützen. Nicht zuletzt muss der Gateway dem Kunden ein lokales Energiefeedback zur Verfügung stellen. Dies soll der Steigerung der Motivation zur Reduzierung seines persönlichen Energieverbrauches dienen.

2 DAS BSI-SCHUTZPROFIL

Auf der Suche nach sicherheitstechnischen Anforderungen seitens des Gesetzgebers wird man in Österreich an zwei Stellen fündig. Dies ist zum einen die „Intelligente Messgeräte Einführungsverordnung“, zum anderen die „Intelligente Messgeräte Anforderungsverordnung“. Die in diesen Verordnungen festgehaltenen Forderungen sind jedoch sehr allgemein gehalten. Neben der Anforderung eine leitungsbezogene Übertragung der Daten in Betracht zu ziehen, ist die Kommunikation nach anerkannten Stand der Technik abzusichern und zu verschlüsseln. Darüber hinaus wird die Nutzung kundenbezogener Schlüssel, die Führung eines Zugriffsprotokolls sowie eine Manipulationserkennung gefordert. Die Suche nach detaillierten Forderungen verläuft ebenso erfolglos wie jene nach der Antwort auf die Frage wie der, oftmals erwähnte, Stand der Technik zu definieren ist.

Umfassenderer Forderungen sind im Schutzprofil für die „Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen“ zu finden [2]. Dieses, vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) im Jahr 2011 veröffentlichte Schutzprofil wurde erarbeitet, um die Vertraulichkeit, Authentizität und Integrität der Daten sowie die Steuerung des Informationsflusses in einer Smart Metering Infrastruktur zu garantieren. Obwohl das BSI-Schutzprofil auf die Besonderheiten des deutschen Marktes abgestimmt ist, können die Forderungen mit einem zukünftigen Fortschritt der Liberalisierung des Strommarktes auch auf Österreich Anwendung finden.

Das Herzstück des BSI-Schutzprofils bilden die sogenannten „Access-Profile“. In diesen, für jede externe Partei separat festzulegenden Profilen wird im Detail geregelt, welche Daten, in welchem Zeitintervall, unter Verwendung welches individuellen Schlüssels bzw. Zertifikates wem in welcher Auflösung zur Verfügung gestellt werden. Dadurch soll gewährleistet werden, dass die gesamten Messdaten lediglich im Kundenbereich zur Verfügung stehen. Die Weiterübertragung ist auf das unbedingt notwendige Ausmaß zu beschränken. Zum Schutz der lokal vorhandenen Daten sind diese nach Ablauf einer nicht näher festgelegten Zeit sicher zu löschen. Zu beachten ist, dass in jedem einzelnen Verarbeitungsschritt eine Prüfung der Authentizität und Integrität der Daten gefordert wird. Zur Trennung der drei, in der BSI-Referenzarchitektur beschriebenen Netze muss der Gateway über eine Firewall-Funktionalität verfügen. Sämtliche zur Kommunikation mit externen Stellen notwendige Verbindungen müssen vom Gateway aus aufgebaut werden. Dadurch ist für den Aufbau von zur Administration des Gateways notwendigen Verbindungen ein spezieller WakeUp-Service notwendig. Besonders sicherheitskritische Funktionen, wie beispielsweise starke kryptographischen Funktionen, zuverlässige Zufallsgeneratoren sowie Möglichkeiten zur Authentifizierung von Gateway Administratoren, sollen von einem separaten Security Module wahrgenommen werden, welches in einer sicheren Umgebung, z.B. basierend auf Smart Cards, ausgeführt wird.

3 PRAXISNAHE IMPLEMENTIERUNG EINER SMART METERING INFRASTRUKTUR

Im Mittelpunkt der Umsetzung stand die Entwicklung eines Prototyps eines Smart Metering Gateways, der möglichst viele Forderungen des BSI-Schutzprofils erfüllen sollte. Um eine möglichst hohe Herstellerunabhängigkeit zu erreichen, wurde die Nutzung offener Standards angestrebt. Um die Kosten des Gateways so gering wie möglich zu halten, sowie zur Vermeidung einer Lizenzproblematik, kamen lediglich Open-Source-Software und selbst entwickelte Applikationen zum Einsatz. Zur Testung des Gateways wurde dieser in einer realitätsnahen Simulation einer Smart Metering Infrastruktur eingebettet. Hierzu wurde der Bereich des Kunden, bestehend aus den – gemäß BSI-Schutzprofil vorgegebenen – Teilnetzen *Home Area Network* (HAN) und *Local Metrological Network* (LMN) über den zu entwickelnden Gateway mit den sich im *Wide Area Network* (WAN) befindlichen zentralen Services einer externen Partei verbunden (Abbildung 1).

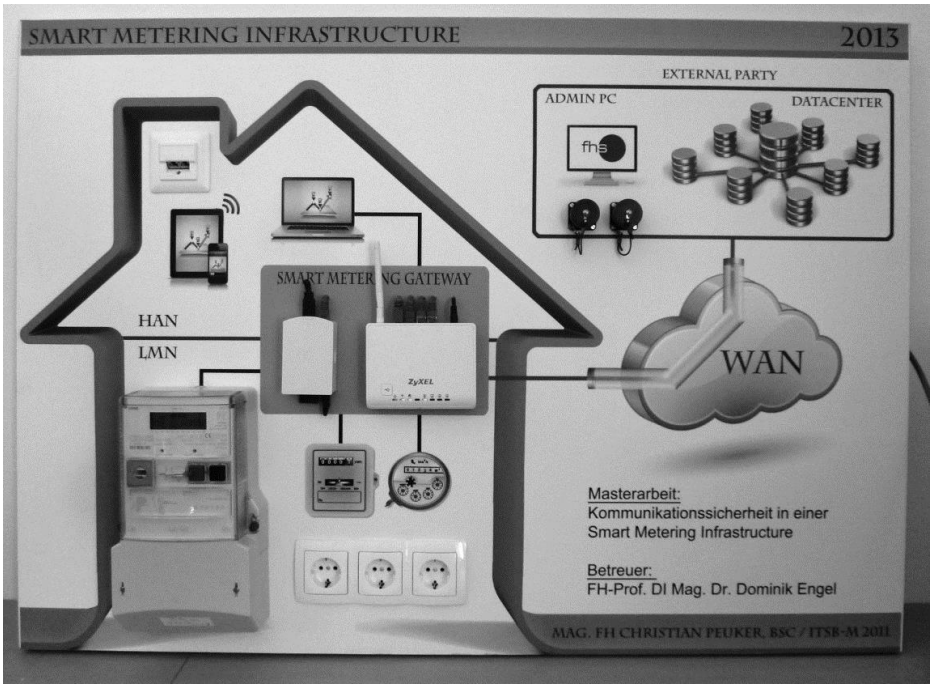

Abbildung 1: Darstellung des Testaufbaus anhand eines Präsentationsboards [5]

Als Smart Meter wird im LMN ein ISKRAEMECO MT831 Lastgangzähler verwendet. Die Kommunikation mit diesem intelligenten Stromzähler wurde mittels DIN EN 62056-21:2003 über RS-485 realisiert. Um einerseits mehrere Endgeräte im HAN anbinden, als auch um das HAN besser vom WAN trennen zu können, wurde der als Basis für den Gateway dienende Raspberry Pi um einen handelsüblichen Router ergänzt. Über das HAN des Kunden ist es diesem möglich, über eine lokale sichere Webseite sowohl das geforderte Energiefeedback zu betrachten als auch Einblick in die Logs des Gateways zu nehmen. Zur Simulation eines zentralen Servers eines Netzbetreibers wurde ein weiter Raspberry Pi als Data-Center im WAN verbaut. Im WAN befindet sich weiters ein als Gateway Administrator eingesetzter Ubuntu Rechner. Von diesem Rechner kann einerseits der Smart Metering Gateway administriert werden, andererseits dient er gleichzeitig als *Root-CA* für die aufzubauende *Public-Key-Infrastruktur* (PKI).
Für die beiden Raspberry Pis wurde Debian 7.0 „Wheezy“ als Betriebssystem gewählt. Bei beiden Pis kam zur Speicherung der notwendigen Daten ein MySQL-Server zum Einsatz. Die lokale Webseite im Kundenbereich wurde über einen Apache2 TomCat Web Server zur Verfügung gestellt. Die PKI wurde unter Abstützung auf OpenVPN realisiert. Zur Speicherung der erforderlichen Schlüssel und Zertifikate wurde das, gemäß BSI-Schutzprofil vorgesehene, PKCS #7 Format verwendet. Zur Programmierung der selbst entwickelten Applikationen wurde Java genutzt.
Der Datenkreislauf wurde wie folgt implementiert. Das Auslesen der Messwerte vom Smart Meter wird von der, auf dem Smart Metering Gateway laufenden, Applikation „Smart Reader“ übernommen (vgl. Tabelle 1). Nach einer Überprüfung der Authentizität und Integrität der Daten werden diese in die lokale Datenbank des Gateways gespeichert. Diese Daten stehen im Kundenbereich mit der maximalen Auflösung zur Verfügung. Eine weitere Übertragung dieser Messdaten wird in den sogenannten Access-Profilen geregelt (vgl. BSI-Schutzprofil) und von der Applikation „Data Processor“ wahrgenommen. Gemäß den Vorgaben des jeweiligen Access-Profiles werden die festgelegten Daten aus der lokalen Datenbank zum jeweiligen Zeitpunkt ausgelesen, zur Übertragung aufbereitet, verschlüsselt und gegebenenfalls aggregiert und / oder pseudonymisiert. Im Anschluss wird ein gegenseitig authentifizierter und mit einem individuellen Schlüssel verschlüsselter Tunnel zur Zieldestination im WAN aufgebaut. Dieser

Vorgang beruht nur auf den lokal gespeicherten Informationen und kann nicht von außen initiiert werden. Im WAN nimmt das „DataCenter“ als zentraler Dienst des Netzbetreibers die gesendeten Daten entgegen, überprüft nach einer erfolgreichen Entschlüsselung die Integrität und Authentizität der Daten und speichert diese in die zentrale Datenbank. Sämtliche fehlgeschlagene Prüfungen oder Fehlfunktionen werden in den an allen Stellen vorhandenen Logs protokolliert.
Die Administration des Gateways inklusive der Bereitstellung der individuellen Schlüsseln und Zertifikaten sowie der Festlegung der Access-Profile erfolgt nur durch den Gateway Administrator. Da gemäß BSI-Schutzprofil keine Verbindungen von außen zum Gateway aufgebaut werden dürfen, muss der Gateway den Aufbau des Administrationstunnels initiieren. Hierzu werden durch den Gateway Administrator spezielle WakeUp-Messages verschickt. Diese Nachrichten werden von der Applikation „GateWatcher“ entgegengenommen und wiederum auf Integrität und Authentizität überprüft. Nach einer erfolgreichen Überprüfung wird durch den Gateway ein Administrationstunnel zu einem, zuvor festgelegten und in der lokalen Datenbank gespeicherten, Ziel aufgebaut. Ein dynamischer Aufbau einer Verbindung zu einem nicht zuvor festgelegten Ziel ist aus sicherheitstechnischen Gründen nicht vorgesehen. Nach Ende der notwendigen Tätigkeiten wird der Tunnel durch das Versenden einer BreakUp-Message abgebaut.

4 EVALUIERUNG

Im Zuge des Testaufbaus konnte ein typisches Smart Metering Szenario gemäß der BSI-Referenzarchitektur nachgebaut werden. Aufgrund der Tatsache, dass für den Prototypen eines Smart Metering Gateways lediglich Open Source Software sowie selbst entwickelte Software benutzt wurde konnten die Kosten gering gehalten werden (die Kosten eines Raspberry Pi belaufen sich aktuell auf $25).
In der Evaluierung des Testaufbaus zeigte sich, dass mit Ausnahme der Nutzung eines separaten Security Modules alle Forderungen des BSI- Schutzprofils erfüllt werden konnten. Kernstück der Kommunikationssicherheit in diesem Projekt ist die Nutzung einer Public Key Infrastructure für sämtliche Verbindungen ins WAN. Eine zentrale Voraussetzung hierfür ist allerdings, dass diese Verbindungen über IP-basierende Kommunikationsmittel realisiert werden. In Hinblick auf die notwendige Root-CA ist durch die Netzbetreiber zu beurteilen, ob diese durch die Netzbetreiber selbst betrieben werden kann oder ob auf öffentliche Zertifikate zurückgegriffen werden muss.
Bezüglich der Kommunikationssicherheit besteht die größte Problematik bei der Kommunikation zwischen dem Smart Meter und dem Metering Gateway. Grund hierfür ist, dass diese Schnittstelle vom Hersteller des Messgerätes abhängig ist und diese in der Regel nicht den sicherheitstechnischen Anforderungen entspricht. Abhilfe kann die gemeinsame Verbauung der beiden Komponenten sowie die Gewährleistung der erforderlichen Sicherheit durch physische, bauliche Maßnahmen schaffen.
Bezüglich der Überprüfung der Eignung eines Raspberry Pis als Basis für einen Smart Metering Gateway haben über mehrere Monate dauernde Performance-Test ergeben, dass mit diesem für den vorliegenden Testaufbau vollkommen das Auslangen gefunden werden kann. Im Zuge des Projekts wurden der Smart Meter im 30 Sekunden Takt ausgelesen und diese Daten im Minutenintervall an das Data Center übermittelt. Das Auslesen und die Übertragung der Messdaten verlaufen sehr stabil. Obwohl die durch den Programmteil „SmartReader“ verursachte durchschnittliche Prozessorauslastung von ca. 20% derzeit kein Problem darstellt, kann diese durch eine Überarbeitung des Programmcodes mit großer Wahrscheinlichkeit nochmals reduziert werden (vgl. Tabelle 1).

Tabelle 1. Durchschnittliche Auslastung des Gateways.

Applikation	Auslastung Prozessor	Auslastung Speicher
Smart Reader	13,8 %	5,7 %
Data Processor	1,8 %	5,9 %
Gate Watcher	0,2 %	3,7 %
OpenVPN Client	0 %	0 %
MySQL Server	0,8 %	9,7 %
Apache Tomcat 2	3,5 %	27,2 %

5 FAZIT

Abschließend kann festgehalten werden, dass es im Zuge des Testaufbaus gelungen ist, zu beweisen, dass es mit relativ geringen Kosten möglich ist, den Prototypen eines auf offenen Komponenten und Schnittstellen basierenden Smart Metering Gateways zu entwickeln. Neben dem großen Vorteil der Herstellerunabhängigkeit bietet ein solcher Gateway die Möglichkeit, die zählerseitigen Schnittstellen beliebig zu erweitern bzw. anzupassen, um danach auf eine einheitliche, durch den Netzbetreiber vorgegebene Art und Weise, mit den zentralen Diensten zu kommunizieren. Weiters besteht die Möglichkeit den Gateway laufend an die Herausforderungen der Zukunft anzupassen, ohne die restliche Infrastruktur ändern zu müssen.
Da die Kernforderungen des BSI-Schutzprofiles mit überschaubarem Aufwand umgesetzt werden können, sind die österreichischen Netzbetreiber nach Meinung der Autoren jedenfalls gut beraten, diese Forderungen von Beginn an zu berücksichtigen.

DANKSAGUNG

Die Autoren bedanken sich für die finanzielle Unterstützung des Bundesministeriums für Wissenschaft, Forschung und Wirtschaft und der Nationalstiftung für Forschung, Technologie und Entwicklung.

LITERATURVERWEISE

[1] C. Eckert, *Sicherheit im Smart Grid: Eckpunkte für ein Energieinformationsnetz*, Alcatel-Lucent Stiftung für Kommunikationsforschung, 2011.

[2] Bundesamt für Sicherheit in der Informationstechnologie, *Protection Profile for the Gateway of a Smart Metering System Version 1.2*, 2013. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf.

[3] X. Fang, S. Misra, G. Xue und D. Yang, “Smart Grid - The New and Improved Power Grid: A Survey,” *IEEE Communications Surveys & Tutorials*, 14, S. 944-980, 2012.

[4] Z.Fan, P.Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan und W. Chin, “Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities,” *IEEE Communications Surveys & Tutorials*, vol. 99, S. 1-18, 2011. Early Access.

[5] C. Peuker, „Kommunikationssicherheit in einer Smart Metering Infrastructure“. Masterarbeit, Fachhochschule Salzburg, Puch/Salzburg, Österreich, 2013.