Aspekte der Sicherheit und Privatsphäre im zukünftigen Stromnetz

Raphael Tawil

Departement für Informatik, ETH Zürich

tawilr@student.ethz.ch

Zusammenfassung

Die globale Einführung des zukünftigen Stromnetzes, auch Smart Grid genannt, ist eine der grössten Transformationen im Technologiebereich seit der Einführung von Elektrizität in Wohnhäusern. Diese Ausarbeitung gibt einen Einblick in die Problembereiche der Sicherheit und Privatsphäre, die durch die Einführung des Smart Grids aufgeworfen werden. Im Vordergrund stehen Themen wie die Diskussion von potentiellen Sicherheitslücken, die Möglichkeiten diese Schwachstellen auszunutzen, sowie eine Klassifizierung verschiedener Angreifertypen. Es werden Schwachstellen erläutert, die Stromdiebstahl, Denial of Service[1] (DoS) Angriffe und ein mögliches Eindringen in die Privatsphäre des Konsumenten zur Folge haben könnten und welche Parteien ein Motiv hätten, an solchen Angriffen beteiligt zu sein. Danach werden einige mögliche Lösungsansätze, sowie auch deren Probleme erläutert.

[1] Dienstverweigerung

1 Einführung

1.1 Hintergrund und Motivation

Dem Stromnetz wie wir es heute kennen, steht eine grössere Transformation bevor, denn die bestehende Infrastruktur wird langsam aber sicher durch ein moderneres, digitales System ersetzt. Dieses System, auch Smart Grid genannt, ermöglicht es dem Verbraucher sowie auch dem Versorger, den Stromverbrauch effektiver zu protokollieren. Damit lässt sich der Strompreis zu jedem Zeitpunkt vom Anbieter genau festlegen, was auch dem Verbraucher ermöglicht, den Strom am kosteneffizientesten zu nutzen. Zusätzlich verspricht man sich, damit die globale Erwärmung zu lindern, da der CO_2 Ausstoss verringert wird. Trotz diesen Vorteilen scheint das Smart Grid, zumindest in dessen ersten Generationen, einige Risiken in den Bereichen von Sicherheit und Privatsphäre zu bergen. Da das Smart Grid ein gigantisches Netz ist, das aus digitalen Stromzählern und verschiedensten anderen Steuerungseinheiten besteht, ergeben sich sehr effektive Angriffsmöglichkeiten, die auch im grösseren Rahmen auf eine gesamte Advanced Metering Infrastruktur (AMI) ausgeführt werden könnten. Dazu kommt noch die zu schützende Privatsphäre des Konsumenten: Da der Konsument dem Versorger Daten über seine Stromnutzung bereitstellt, muss natürlich eine angemessene Datenschutzregelung bestimmt werden. Im ersten Teil dieses Dokuments wird zuerst kurz die Struktur einer üblichen AMI dargestellt und erklärt. Im zweiten Teil werden Aspekte der Sicherheit betrachtet. Dort wird zuerst auf AMI-spezifische Sicherheitsrisiken im Smart Grid eingegangen, gefolgt von einer Fallstudie, die die generellen Sicherheitsrisiken von grösseren verteilten kritischen Infrastrukturen, zu denen das Smart Grid dazugehört, diskutiert. Im letzten Teil werden einige Risiken erläutert, die die Privatsphäre des Konsumenten in einer AMI gefährden.

1.2 Advanced Metering Infrastruktur (AMI): Kurzübersicht

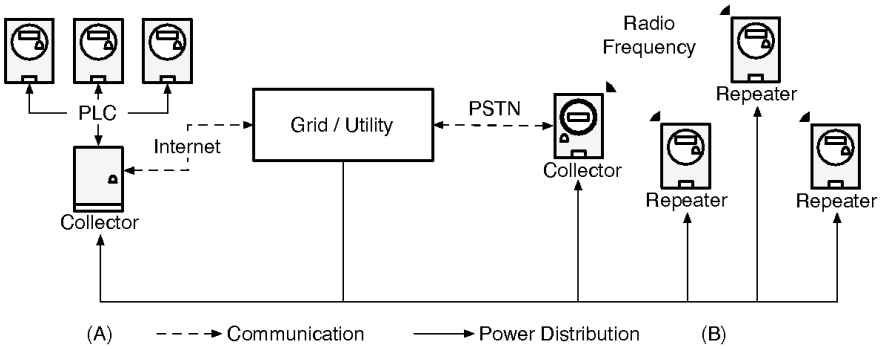

Abbildung 1: Eine typische Advanced Metering Infrastruktur [10].

Die AMI ist das Netz, das Informationen über die Stromnutzung sowohl dem Energieversorgungsunternehmen (EVU), als auch dem Konsumenten bereitstellt. Dies ermöglicht beiden Parteien bessere Entscheidungen bezüglich der Energieverwaltung zu fällen, was zu einer Kostenreduktion führt und auch das Stromnetz in Zeiten von hoher Nachfrage nicht überlastet. Diese Informationen werden von modernen digitalen

Stromzählern, im Folgenden auch Smart Meter genannt, gemessen. Solch ein Smart Meter besitzt einen Prozessor, Speicher und eine oder mehrere Kommunikationsschnittstellen.

Typischerweise hat ein AMI-Netz folgende Struktur: Zentral liegt das EVU, das Daten über die Stromnutzung von einem Kollektorgerät über eine Kommunikationsschnittstelle bezieht. Diese Kollektorgeräte beziehen Messinformationen direkt von mehreren Smart Metern, die beim Konsumenten installiert sind, ebenfalls über eine geeignete Kommunikationsschnittstelle. Diese Informationen werden vom Kollektorgerät aggregiert, damit das EVU direkt die aggregierten Werte vom Kollektor beziehen kann. Eine typische Konfiguration einer AMI ist in Abbildung 1 dargestellt. Dabei werden zwei AMI-Konfigurationen dargestellt: Auf der linken Seite (A) sind die Smart Meter über ein PLC[2]-Netz mit dem Kollektorgerät verbunden, welches über das Internet mit dem EVU kommuniziert, während auf der rechten Seite (B) die Smart Meter über Funkverbindungen mit dem Kollektorgerät kommunizieren, welches mit dem EVU über das Telefonnetz (PSTN[3]) kommuniziert.

[2]Power Line Communication, Datenübertragung über Stromnetze
[3]Public Switched Telephone Network

2 Sicherheit

Smart Meter sind sehr attraktive Ziele für Manipulationen mit betrügerischer Absicht, da durch das Ausnützen einer Schwachstelle sehr leicht Geld verdient werden kann, indem Stromdiebstahl betrieben wird. Dass Geld ein guter Motivationsfaktor ist, hat sich schon bei Kabelmodems erwiesen [11]. Diese wurden so manipuliert, dass der Diebstahl von zusätzlicher Bandbreite möglich war. Sollte ein Smart Meter eine Schwachstelle aufweisen, die so ausgenutzt werden kann, dass ein Angreifer dabei Geld verdient, verliert das EVU nicht nur Geld wegen des Betrugs – es wird das EVU auch viel Geld kosten, bei zehntausenden betroffenen Smart Metern die Sicherheitslücke zu schliessen, damit der Betrug ein Ende nimmt. Dass es Versuche geben wird, Strom zu stehlen, ist keine Frage, da das schon bei herkömmlichen Stromzählern der Fall war. Diese wurden von betrügerischen Konsumenten invertiert und zählten dann einfach rückwärts. Es wird geschätzt, dass EVU alleine in den USA durch diese Art von Betrug bisher 6 Milliarden Dollar verloren haben [7]. Es wird erwartet, dass traditionelle physische Angriffe auf Stromzähler (wie z. B. deren Invertierung) mit der Einführung des Smart Grids durch fortschrittliche digitale und ferngesteuerte Angriffe ersetzt werden [9].

2.1 Klassifizierung verschiedener potentieller Angreifer

Angreifer, die ein Motiv haben, einen Angriff auf eine AMI auszuüben, können in mehrere Klassen eingeteilt werden [10, 11]:

- **Konsumenten:** Es ist im Interesse eines betrügerischen Konsumenten, den Smart Meter so zu manipulieren, dass er Strom stehlen kann. Dieses Angreifermodell ist analog zum Invertieren eines herkömmlichen Stromzählers.
- **Organisierte Kriminalität:** Eine organisierte Gruppe von Kriminellen kann für eine universell ausnutzbare Schwachstelle eines Smart Meters direkt benutzbare Gesamtpakete (z. B. Anleitungen, Software, etc.) entwickeln, mit denen die entsprechende Schwachstelle ausgenutzt wird und mit der ein durchschnittlicher Konsument Geld sparen (d. h. Strom stehlen) kann. Nach der Entwicklung eines solchen Gesamtpakets, werden diese von den Kriminellen an interessierte Konsumenten verkauft. Ähnliche Vorgehensweisen wurden bei Kabelmodems bereits beobachtet [11].
- **Insider:** Ein Insider, d. h. ein Angestellter dessen Dienst es ist, in einer AMI eine Steuerungseinheit zu steuern oder überwachen, könnte seine Position ausnutzen und die Strompreise so manipulieren, damit er mit einer anderen Organisation ein Geschäft abwickeln und dabei Geld verdienen kann. Als Beispiel sei folgendes Szenario genannt [11]: Ein EVU benutzt gewisse Server, um mit den Smart Metern ihrer Konsumenten über das Internet zu kommunizieren. Diese Server werden von einem Administrator überwacht. Das EVU selbst wird von einem anderen Unternehmen, das einen Generator betreibt, mit Strom versorgt, den es dann weiter an seine Konsumenten verkauft. Dieses Lieferantenunternehmen macht mit dem Serveradministrator des belieferten EVU nun ein Insider-Geschäft: Es bietet ihm an, den Server so zu manipulieren, dass den Smart Metern bei den Konsumenten stets ein Strompreis vorgegaukelt wird, der 2% tiefer als der normale Strompreis ist - dies soll auf eine Art und Weise geschehen, dass die Konsumenten aber trotzdem den vollen Preis bezahlen. Es wird also lediglich ein tieferer Preis angezeigt, bzw. der Smart Meter wird überlistet und glaubt fälschlicherweise, dass der Strompreis tiefer sei. Dies verursacht, dass die Nachfrage nach Strom steigt und bewirkt, dass das belieferte EVU mehr Strom von dem betrügerischen Lieferantenunternehmen kauft. Dieses

gibt dann einen Teil des Gewinns an den Serveradministrator ab. Schlussendlich wurden die Konsumenten bestohlen – diese merken es aber nicht, da ja jeder Konsument lediglich 2% mehr bezahlt als angenommen. Solch eine Betrugsmasche ist sehr effektiv und kaum bemerkbar.

- **Terroristen:** Terroristen möchten nicht unbedingt Strom stehlen, sondern einfach dem Smart Grid Schaden zufügen. Sie könnten also durch einen DoS-Angriff versuchen, das Stromnetz lahmzulegen. Dies könnte auf eine ähnliche Art und Weise geschehen, wie heutzutage DoS-Angriffe auf Webseiten ausgeführt werden, nämlich durch Botnetze. Viren- und Wurmprototypen, die sich auf Smart Metern verbreiten können, gibt es bereits [9]. Der Sprung zu einem DoS-fähigen Bot ist also extrem klein. Eine andere Möglichkeit wäre es zu versuchen, Sicherheitslücken in Stromgeneratoren auszunutzen und diese somit lahmzulegen. Dass dies möglich ist, wurde bereits experimentell bewiesen durch das Aurora-Projekt [6], das vom Departement of Energy in Idaho ausgeführt wurde. Dabei erlaubte eine Sicherheitslücke, einen Stromgenerator zu veranlassen, sich selbst zu zerstören. Leider wurden genaue Details zum Angriff geheim gehalten. Im kommenden Smart Grid könnte ein ähnlicher Angriff enormen Schaden verursachen. Ein Indikator für die Grössenordnung eines Terroristenangriffs auf eine kritische Infrastruktur liefert der Angriff auf eine Abwassersteuerungseinheit in Australien [2]: Ein Ex-Angestellter einer australischen Softwareentwicklungsfirma bewarb sich für einen Job bei der Regierung. Da er den Job nicht bekommen hatte, griff der rachesüchtige Bewerber eine Abwassersteuerungseinheit an und verursachte so, dass knappe 1 Mio. Liter Abwasser in nahegelegene Flüsse und Pärke freigesetzt wurden. Das Smart Grid, das auch eine enorme Grössenordnung aufweisen wird, könnte Angriffe mit ähnlich grossem Ausmass an resultierenden Schäden erleiden.

2.2 Angriffsbaum des Hauptangriffsziels: Manipulation der Daten über die Stromnutzung

Da das Fälschen der Informationen über die Stromnutzung das Hauptziel eines üblichen Angriffs ist (es wird im Folgenden auf die Angreifertypen “betrügerischer Konsument” und “organisierte Kriminalität” fokusiert), wird hier genauer darauf eingegangen. Die Möglichkeiten, Daten über die Stromnutzung (und somit auch die Nachfrage nach Strom) erfolgreich zu manipulieren, unterliegen dem Angriffsbaum in Abbildung 2. Dabei ist die Wurzel das Ziel des Angriffs und Pfade von den Blättern zur Wurzel stellen verschiedene Möglichkeiten dar, das Angriffsziel zu erreichen. Dabei werden die einzelnen Schritte mit AND oder OR verknüpft.

Das Hauptangriffsziel, nämlich die Manipulation der Stromnutzung (repräsentiert durch die Wurzel), kann durch drei verschiedene Massnahmen erreicht werden (Kindknoten (a), (b) und (c)) [10]:

a) Durch Veranlassung, die korrekte Messung des Smart Meters zu unterbrechen. Dies kann entweder durch Abkopplung (A1.1) oder durch Invertierung (A1.2) des Smart Meters erreicht werden. Beide dieser Handlungen sind aber mit dem Löschen bestimmter Logdateien des Smart Meters, die das Protokoll der Messaktivität beinhalten zu kombinieren, da der Angriff sonst vom EVU erkannt wird. Um diese Logdateien zu löschen, kann z. B. das Passwort für die Administrationsschnittstelle (die normalerweise nur vom EVU benutzt wird) vom Smart Meter extrahiert werden und danach können die Logdateien auf ganz “legale” Art und Weise gelöscht werden (A2.1). Eine andere Möglichkeit wäre, die geloggten Daten während der Übertragung zu manipulieren, sobald sie vom EVU angefordert werden (A2.2). Dies ist nicht zu verwechseln mit Teilbaum (c), bei dem Daten über die Stromnutzung manipuliert werden, denn hier wird nur das Aktivitätsprotokoll des Smart Meters verändert.

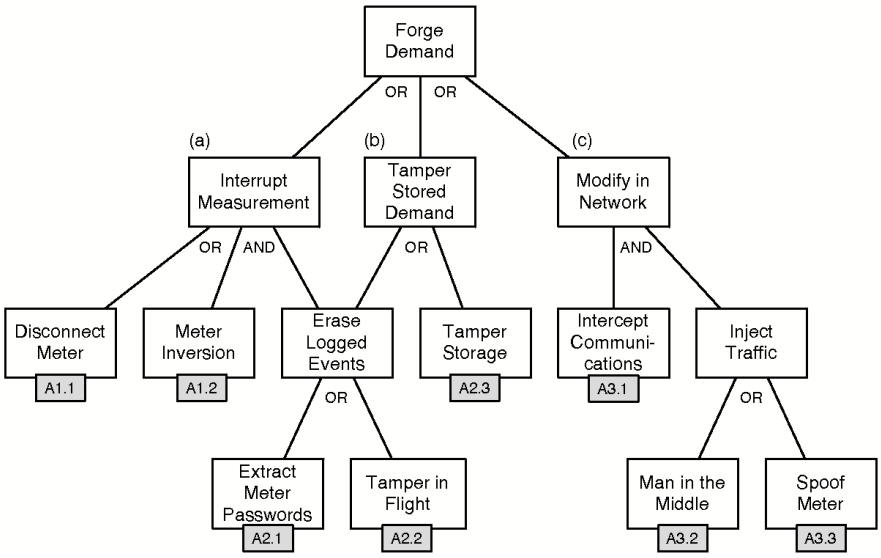

Abbildung 2: Baumstruktur der Angriffsmöglichkeiten mit dem Ziel, Informationen über die Stromnutzung zu manipulieren [10].

b) Durch Manipulation der Daten über die Stromnutzung im Speicher des Smart Meters. In die Kategorie dieses Teilbaums gehört sowohl das Löschen von Logdateien des Smart Meters (diesmal ist von Logdaten über die Stromnutzung die Rede; im Kontext von Teilbaum (b) hat dieser Knoten also die gleiche Bedeutung wie der Angriff aus Teilbaum (c)), als auch die Veränderung der schon abgespeicherten Daten (A2.3).

c) Durch Veränderung der Daten über die Stromnutzung während der Übertragung. Dies wird in zwei Schritten erreicht: Zuerst wird die Kommunikation belauscht (A3.1). Dadurch lässt sich das Kommunikationsprotokoll rekonstruieren. Danach werden zusätzliche Nachrichten in eine bestehende Kommunikationssession eingespeist oder bestehende Nachrichten verändert. Dies ist durch Meter Spoofing (A3.3) möglich. Dabei gibt sich ein vom Angreifer gesteuertes Gerät (z. B. ein Laptop) als das Smart Meter aus und kommuniziert so mit dem EVU, das von dem Angriff nichts mitbekommt. Falls die Kommunikation verschlüsselt ist, wobei der Schlüssel zu Beginn der Session festgelegt wird (z. B. durch das Diffie-Hellman Schlüsselaustauschprotokoll) kann der Angreifer durch einen Man-in-the-Middle Angriff den Schlüssel abhören und kann so korrekt verschlüsselte Nachrichten in eine Kommunikation einspeisen oder bestehende Nachrichten verändern. Falls der Schlüssel nicht zu Beginn der Kommunikationssession vereinbart wird, sondern im Smart Meter gespeichert ist, lässt er sich durch Angriff A2.3 entnehmen. Beide dieser Angriffe gelingen nur, falls kein Authentifikationsmechanismus verwendet wird. Sollte aber einer verwendet werden, müsste der entsprechende Schlüssel (z. B. der private Schlüssel für das RSA-Signaturverfahren) ebenfalls vorher dem Speicher des Smart Meters entnommen werden (A2.3). Angriffsstellen für diese Klasse wären das Netz zwischen Smart Metern und Kollektorgeräten oder das Netz zwischen einem Kollektor und dem EVU (siehe Abbildung 1), wobei bei letzterer Angriffsstelle Daten von einer ganzen Menge von Konsumenten manipuliert werden können.

2.3 Wirksamkeit bisheriger Schutzmassnahmen

Es wird versucht, obigen Angriffen vorzubeugen, indem moderne Konzepte der Informationssicherheit angewendet werden. Leider ist dieser Schutz in diesem Fall nicht immer genügend, da der Angreifer physischen Zugriff auf die entsprechenden Geräte hat (Bsp.: Konsument hat Zugriff zum Stromzähler, Insider zu anderen Steuerungseinheiten). Teilbaum (a) des Angriffsbaums wird z. B. durch Passwortschutz zur Administrationsschnittstelle geschützt, was verhindern soll, dass der Angreifer die Logdateien löschen kann. Dies nützt aber nicht viel, denn das Passwort (oder zumindest der Hash davon) ist auf dem Smart Meter abgespeichert, zu dem der Angreifer ja physischen Zugriff hat. Er könnte also mit genügenden Kenntnissen das Passwort extrahieren oder das Passwort überschreiben und nach dem Angriff das alte Passwort wiederherstellen. Noch einfacher ist es, das Passwort abzuhören, falls es im Klartext gesendet wurde. Es wurden einige Systeme analysiert, wobei bei einem dies der Fall war [10]. Gegen physische Eingriffe war keines der getesteten Systeme ausreichend geschützt, was Teilbaum (b) des Angriffsbaum einem Angreifer auch leicht fallen lässt. Auch gegen Teilbaum (c) waren die getesteten Systeme nicht geschützt: Sogar wenn Authentifikations- und Verschlüsselungsmechanismen angewendet wurden, waren einige gegen Replay-Angriffe verwundbar. Bei bisherigen Systemen ist es also teilweise gar nicht nötig, dem Smart Meter geheime Daten wie Passwörter und Schlüssel physisch zu entnehmen, da die verwendeten Schutzmechanismen andere Lücken aufweisen, die einfacher auszunützen sind. Fazit: Die Sicherheit von heutigen Umsetzungen lässt viel zu wünschen übrig.

2.4 Lösungsansatz

Um obigen und anderen Angriffen in einer AMI vorzubeugen, müssen folgende fundamentalen Anforderungen der Informationssicherheit erfüllt sein [4]:

- Vertraulichkeit: Nur bestimmte Personen dürfen gesendete Nachrichten und gespeicherte Daten lesen können.
- Integrität: Alle Nachrichten, Daten (z. B. Verbrauchsdaten) und ausführbaren Programme (z. B. die Firmware des Smart Meters) müssen in einem legitimen Zustand erhalten bleiben.
- Authentizität: Der Ursprung einer Nachricht muss eindeutig bestimmbar sein. Nachrichten dürfen nicht mehrmals in eine Kommunikationssession eingespeist werden können (verhindert Replay-Angriffe). Zudem muss immer die Authentizität von gespeicherten Daten und ausführbaren Programmen gewährleistet werden.
- Verfügbarkeit: Knoten einer AMI können nicht (z. B. durch Überfluten mit Nachrichten) lahmgelegt werden.
- Nichtabstreitbarkeit: Der Sender einer Nachricht kann deren Sendung nicht abstreiten.
- Zugriffskontrolle: Nur berechtigte Personen können bestimmte Operationen ausführen.
- Protokollierung: Alle Befehle und physischen Eingriffe, egal ob diese erfolgreich ausgeführt wurden oder nicht, müssen umfassend protokolliert werden.

Viele dieser Anforderungen können durch korrekte Anwendung von Public-Key Kryptographie (PKK) erfüllt werden [4]. An dieser Stelle soll nicht auf die Funktionsweise von Public-Key Kryptographie eingegangen werden – es wird auf die Literatur verwiesen [5]. PKK erlaubt es, Nachrichten und Daten zu verschlüsseln, so dass nur eine bestimmte Zielperson diese wieder entschlüsseln kann. Zudem ermöglicht sie, Nachrichten, Daten und ausführbaren Code (hier wird auf den Begriff 'Trusted Computing' verwiesen) digital zu signieren. Durch diese Methoden werden die Anforderungen Vertraulichkeit, Authentizität, Integrität und Nichtabstreitbarkeit erfüllt. Um Replay-Angriffen vorzubeugen, kann z. B. in jede versendete Nachricht ein Zeitstempel eingebunden werden, was in obigem verwundbaren System offensichtlich nicht der Fall war. Wie schon weiter oben erwähnt, wird die Zugriffskontrolle bei Smart Metern durch Passwortschutz erreicht und das Befehlsprotokoll wird in einer Logdatei auf dem Dateisystem im Speicher des Smart Meters abgespeichert. Dies klingt alles schön und gut, doch nützt es nichts, wenn ein Angreifer (wie z. B. ein betrügerischer Konsument) physischen Zugriff zum Smart Meter hat.

2.5 Verhinderung physischer Eingriffe

Wie schon oben gesehen, ist das Lesen und/oder Manipulieren des Speichers des Smart Meters eine gute Angriffsstelle. Dadurch wäre es möglich, Passwörter und Schlüssel aus dem Smart Meter zu extrahieren, was zur Nichterfüllung von obigen Sicherheitsanforderungen führt. Auch ist dieser Eingriff enthalten in Teilbaum (a) und (b) in obigem Angriffsbaum (Abbildung 2) (und wäre auch nützlich in Teilbaum (c), falls Authentifikations- und/oder Verschlüsselungsverfahren angewendet werden). Eine Möglichkeit diese Angriffe zu vermeiden, wäre heikle Daten wie Passwörter und Schlüssel in einem manipulationssicheren Speicherbaustein zu lagern [14]. Für solche Zwecke benützt man üblicherweise einen EEPROM[4]-Speicherbaustein: Ein Speicherbaustein dieser Art wird auch bei Smart-Cards benutzt. Die darauf gespeicherten Daten werden gegen physische Eingriffe wie folgt geschützt: Der EEPROM-Chip ist mit einem Baustein verbunden, der Sensoren besitzt, die bei einem physischen Eingriff (erkannt durch umgebungsbedingte Veränderungen) einen automatischen Löschmechanismus aktiviert, indem eine hohe Spannung über dem EEPROM-Chip angelegt wird. Dies führt dazu, dass die heiklen Daten gelöscht werden und der Smart Meter somit unbrauchbar gemacht wird, was dazu führt, dass das EVU den versuchten Angriff erkennt. EEPROM-Speicherbausteine, die speziell für Smart Meter optimiert wurden, kamen erst kürzlich auf den Markt und werden sicherlich zu den zukünftigen Entwicklungen in diesem Bereich gehören. Beispielprodukte sind in der Quellenangabe zu finden [1, 13].

2.6 Allgemeine Sicherheit von kritischen Infrastrukturen

Wie schon erwähnt, ist das Smart Grid ein verteiltes System, dessen Grösse ein gigantisches Ausmass aufweisen wird. Es ist klar, dass eine solche kritische Infrastruktur gute Sicherheitsvorkehrungen treffen muss. Hier liegt der Fokus jedoch nicht auf Stromdiebstahl, sondern auf den allgemeinen Sicherheitsvorkehrungen, die beim Betrieb einer solchen kritischen Infrastruktur getroffen werden müssen. Auch werden hier nicht die unzähligen Sicherheitsforderungen aufgelistet, sondern eine konkrete Fallstudie analysiert, von der man für das zukünftige Stromnetz einiges lernen kann. Diese wird in folgendem Abschnitt präsentiert.

[4]Electrically Erasable Programmable Read Only Memory, elektrisch löschbarer programmierbarer Nur-Lese-Speicher

2.6.1 Fallstudie der Tennesse Valley Authority

Die TVA, Tennesse Valley Authority, ist das grösste EVU in den USA. Die Fläche, die von TVA mit Energie versorgt wird erstreckt sich auf über 207'200 km^2 und ist verteilt über sieben Bundesstaaten. Die TVA versorgt ca. 8,7 Mio. Menschen mit Energie und betreibt elf Verbrennungsanlagen für fossile Energieträger, acht Gasturbinen, mehrere Atomkraftwerke, 29 Staudämme und ein Pumpspeicherwerk. Die grafische Darstellung dieser Daten ist in Abbildung 3 zu sehen.

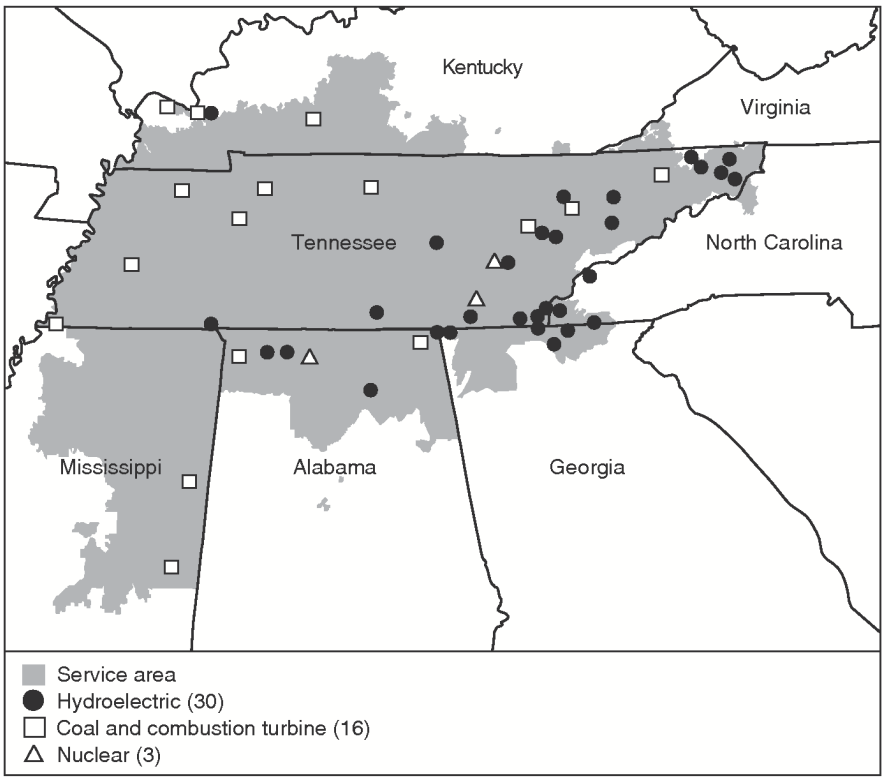

Abbildung 3: Die Generatoranlagen der TVA und die durch sie mit Energie versorgte Fläche [2].

Die GAO[5] hat zwischen März 2007 und April 2008 geprüft, ob die TVA angemessene Sicherheitsvorkehrungen getroffen hat. Diese Prüfung war ausgelegt, um zu prüfen, ob die drei Eigenschaften Vertraulichkeit, Integrität und Verfügbarkeit von Information und Steuerungseinheiten sichergestellt waren. Es wurden sechs Einrichtungen der TVA geprüft, die eine Stichprobe aller Bereiche, in der die TVA tätig ist, darstellt, da sowohl Generatoren verschiedenster Art, als auch funktionelle Einheiten (die z. B. für die Verteilung von Energie zuständig sind) in dieser Testmenge enthalten waren. Leider musste die GAO feststellen, dass die Sicherheitsvorkehrungen der TVA mangelhaft waren und deshalb extreme Sicherheitsrisiken bestanden. Da das kommende Smart Grid eine ähnliche Grössenordnung aufweisen wird, wenn nicht sogar eine grössere, ist es interessant, die Fehler zu analysieren, die die TVA gemacht hat, um diese beim moderneren Smart Grid zu vermeiden. Die folgende Liste zeigt einige der wichtigsten Sicherheitsschwachstellen auf, die bei

[5]Government Accountability Office

der Prüfung aufgefallen sind [2]:

- Sicherheitsschwachstellen im internen Rechnernetz:
  - Fast auf allen der geprüften Arbeitsstationen und Server waren wichtige Sicherheitsupdates und Antivirensoftware nicht installiert oder wiesen mangelhafte Sicherheitskonfigurationen auf.
  - Es wurden Firewalls verwendet, um das Eindringen aus Rechnernetzen mit tieferen Sicherheitsstufen in Rechnernetze höherer Sicherheitsstufen zu vermeiden. Bei drei der sechs geprüften Einrichtungen konnte die Firewall entweder umgangen werden, oder deren Konfiguration war anderswie mangelhaft.
  - Es wurden nicht genügend Massnahmen getroffen, mögliche Eindringlinge zu erkennen.
  - Viele der benutzten Passwörter, die Zugriff zu kritischen Kontrolleinheiten ermöglichen, wiesen nur schwachen Schutz auf.
  - Zugriffe auf eine kritische Kontrolleinheit wurden nirgendwo protokolliert.

  Mögliche Folgen von solchen Sicherheitsschwachstellen sind unbefugter Zugriff auf Information mit höherer Geheimhaltungsstufe, Kompromittierung von internen Computersystemen und DoS-Angriffe. Ein Beispiel für einen DoS-Angriff hat sich im Januar 2003 ereignet: Der 'Slammer'-Wurm, der sich auf verwundbaren Microsoft SQL Servern verbreitete, infizierte Maschinen des internen Rechnernetzes des Davis-Besse Atomkraftwerks [2]. Dies führte zu einem fünfstündigen Ausfall des Sicherheitsüberwachungssystems und einem sechsstündigen Ausfall des Kraftwerks, da dessen Hauptsteuerungscomputer auch infiziert wurde.

- Sicherheitsschwachstellen bezüglich physischem Zugriff
  - Wichtige Netzwerkbuchsen waren nicht vor unbefugtem Zugriff geschützt.
  - Ein Serverraum hatte keine Rauchmelder und in einem Steuerungsraum war sogar eine Küche zu finden (Feuer- und Wassergefahr).
  - Die Zugriffskontrolle war ungenügend segmentiert. In einer Einrichtung konnten 75% der Angestellten durch Benutzung ihrer Dienstmarke problemlos in kritische Räume gelangen, obwohl nur eine Teilmenge von ihnen diese Räume wirklich benötigten.

Mögliche Folgen von solchen Sicherheitsschwachstellen sind physische Angriffe aller Art, die in erfolgreichen DoS-Angriffen resultieren können. Auch könnte die Kommunikation belauscht werden. Dass in einem Serverraum eine Küche nichts zu suchen hat, sollte jedem klar sein.

Alle diese Sicherheitsschwachstellen, die in allen drei Bereichen, Vertraulichkeit, Integrität und Verfügbarkeit, Risiken herbeiführen, kommen unter anderem daher, dass die TVA ihrerseits keine genügende Sicherheitseinschätzung durchgeführt hat und damit sogar das US Gesetz verletzt hat. Von dieser Fallstudie kann man lernen, Sicherheitseinschätzungen frühzeitig durchzuführen, damit diese und ähnliche Schwachstellen bei neuen Systemen wie z. B. dem Smart Grid, nicht zu finden sein werden. Dies wurde für das Smart Grid auch schon teilweise gemacht: Das NIST[6] hat dazu ein 237-seitiges Dokument veröffentlicht [8]. Auch zum Schutz der Privatsphäre des Konsumenten in einer AMI, auf die im nächsten Teil genauer eingegangen wird, gibt es ein ähnliches Dokument [3].

[6] National Institute of Standards and Technology

3 Privatsphäre

Mangelhafte Sicherheit ist nur ein Teil der Probleme, die die Einführung des Smart Grids mit sich bringen kann, denn die Privatsphäre des Konsumenten wird dadurch auch ziemlich gefährdet. Dies ist der Fall, da der Konsument dem EVU viele Informationen über die Art seines Stromverbrauchs preisgeben muss. Hier wird auf die Gefährdung der Privatsphäre des Konsumenten eingegangen, wobei der Konsument selbständig keine Daten über seinen Stromverbrauch veröffentlicht. Dass die Privatsphäre noch weiter gefährdet ist, wenn ein Konsument Daten über seinen Stromverbrauch auf Webportalen veröffentlicht, sollte jedem klar sein.

In Zukunft könnten Systeme anstehen, die Geräteerkennung anhand der Lastkurve ausführen, welche direkt in den Smart Meter integriert werden. Dies bedeutet, dass ein EVU, das Zugriff auf die Daten des Smart Meters hat, herausfinden kann, welche Geräte zu welchem Zeitpunkt betrieben werden. Es ist klar, dass diese Informationen wertvoll sind, da sie gut dafür geeignet sind, dem Konsumenten massgenschneiderte Werbung zu schicken. Deshalb sollte jede Institution, die Teil einer AMI ist und Zugriff auf solche sensiblen Daten hat, den Konsumenten im voraus genauestens informieren, wie sie diese Daten verwendet. Ein Vorschlag wäre, eine Regierungsbehörde zum Schutz des Konsumenten zu gründen [9]. Diese sollte Gesetze festlegen, in welcher Art Daten über die Konsumenten gesammelt werden, wer genau auf diese Daten Zugriff hat und was die Konsequenzen sind bei widerrechtlichem Umgang mit diesen Daten. Ein anderes realistisches Szenario wäre, dass Schadsoftware entwickelt wird, die sich auf Smart Metern verbreiten und diese heiklen Daten sammeln, sollten diese nicht genügend geschützt sein. Diese können von den Urhebern der Schadsoftware dann verkauft werden und schlussendlich wiederum illegalerweise für Werbezwecke verwendet werden.

Um zu veranschaulichen, welche Informationen über den Konsumenten von den Daten des Speichers eines Smart Meters mit Geräteerkennung durch Analyse der Lastkurve herauslesbar sind, sollte Abbildung 4 betrachtet werden.

Aus solchen Daten könnte man z. B. folgendes über einen Konsumenten folgern [12]:

- Hat der Konsument Kinder?
- Wann ist der Konsument bei der Arbeit?
- Benutzt der Konsument oft eine Mikrowelle oder bevorzugt er den Herd?
- Wie oft wäscht der Konsument seine Kleider?
- Wie oft benutzt der Konsument den Wasserkocher?
- Wie oft benutzt der Konsument den Toaster?

Es ist also klar ersichtlich, dass mit der Einführung des Smart Grids auch Massnahmen getroffen werden müssen, die bestimmen, wie ein EVU mit den gesammelten Daten umzugehen hat. Man stelle sich vor, was geschehen würde, wenn eine EVU gesammelte Daten dieser Art ohne Einverständnis des Konsumenten an Drittanbeiter verkaufen würde oder diese anderswie in falsche Hände gerieten: Die betroffenen Konsumenten würden mit massgeschneiderter Werbung aller Art überschwemmt werden. Ein guter Indikator für eine solche Entwicklung wären die steigende Anzahl von verschickten massgeschneiderten Werbeemails, die aus der Datensammlung über das Surfverhalten von Personen resultieren. Auch können für den Konsumenten

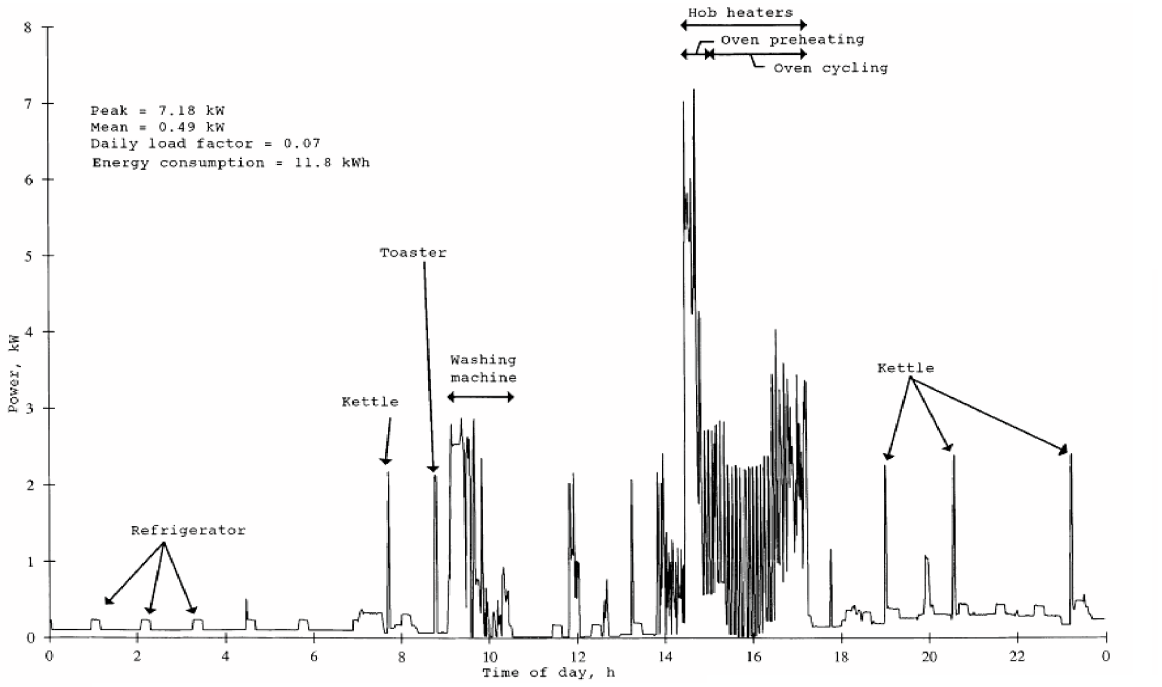

Abbildung 4: Stromnutzung, gemessen in 1-Minuten-Intervallen [15]. Die Geräte haben eindeutige Leistungscharakteristiken, die von einem Smart Meter zur Geräteerkennung verwendet werden können, gleichzeitig aber auch für andere Zwecke missbraucht werden können.

andere finanzielle Verluste Realität werden: Einbrecher würden sich sicherlich für diese Daten interessieren: Es lässt sich nämlich leicht herauslesen, zu welcher Tages- oder Nachtzeit sich der betroffene Konsument gerade nicht zu Hause befindet.

4 Schlussfolgerungen

Zusammengefasst können wir von dieser Ausarbeitung folgendes sehen: Das langsam aber sicher kommende Smart Grid birgt einige Risiken im Bereich der Sicherheit und Privatsphäre. Die bisherige Situation sieht nicht allzu gut aus, da viele der oben aufgeführten Angriffe in der Realität auf getesteten Systemen auch wirklich ausführbar waren. Man kann in erster Linie also erwarten, dass in der ersten Generation des Smart Grids, sollten keine besseren Sicherheitsvorkehrungen getroffen werden oder verwendete Sicherheitsvorkehrungen nicht korrekt implementiert werden, der Diebstahl von Strom und Geld eine leichte Arbeit sein wird. Es könnte sogar Realität werden, dass man auf dem Schwarzmarkt Gesamtpakete kaufen kann, die es einem Durchschnittskonsumenten erlauben, einfach per Anleitung (und unerkannt) Stromdiebstahl zu begehen. Gegen diese Probleme wurde ein Lösungsansatz aufgezeigt, der die Erfüllung der wichtigsten Sicherheitsanforderungen garantiert. Auch wurde aufgezeigt, dass die kommende Infrastruktur möglicherweise gegen grossangelegte Angriffe (z. B. DoS-Angriffe) nicht genügend geschützt ist. Aus der Fallstudie der TVA konnte man schliessen, dass es wichtig ist, frühzeitig Sicherheitseinschätzungen durchzuführen, damit die Schutzvorkehrungen der ganzen Infrastruktur auch wirklich wasserdicht sind. Zum Schluss wurde gezeigt, dass die Privatsphäre der Konsumenten im Smart Grid gefährdet sein wird, wenn das Gesetz nicht genau vorschreibt, wer was mit gesammelten Daten anstellen darf. Auch könnten Daten über die Stromnutzung eines Konsumenten per Schadsoftware in falsche Hände geraten. Auch gegen diese Probleme müssen entsprechende Schutzmassnahmen entwickelt werden.

Literatur

[1] Atmel. http://www.smartgridnews.com/artman/uploads/1/atmel.pdf. 2009.

[2] N. Barkakati and G. C. Wilshusen. Deficient ICT Controls Jeopardize Systems Supporting the Electric Grid: A Case Study. *Securing Electricity Supply in the Cyber Age*, pages 129–142, 2010.

[3] A. Cavoukian, J. Polonetsky, and C. Wolf. SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation. November 2009.

[4] Certicom. Securing Smart Meters and the Home Area Network. *EDIST Conference*, 2009.

[5] CGI. www.cgi.com. Public Key Encryption and Digital Signature: How do they work? 2004.

[6] CNN. http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html. 2009.

[7] Electric Light and Power Magazine. Reducing Revenue Leakage. http://uaelp.pennnet.com/. 2009.

[8] A. Lee and T. Brewer. Smart Grid Cyber Security: Strategy and Requirements. *NIST*, December 2009.

[9] P. McDaniel and S. McLaughlin. Security and Privacy Challenges in the Smart Grid. *IEEE Security & Privacy Magazine*, 7(3):75–77, May/June 2009.

[10] S. McLaughlin, D. Podkuiko, and P. McDaniel. Energy Theft in the Advanced Metering Infrastructure. September 2009.

[11] R. C. Parks. Advanced Metering Infrastructure Security Considerations. November 2007.

[12] J. Polonetsky. Privacy and the Smart Grid: New Frontiers, New Challenges. www.futureofprivacy.org.

[13] ROHM. http://www.rohm.com/ad/smartmeter/index.html. 2010.

[14] USEA. The Smart Grid: Lunch and Learn (Session 5). http://www.usea.org. 2009.

[15] G. Wood and M. Newborough. Dynamic Energy-Consumption Indicators for Domestic Appliances: Environment, Behavior, and Design. 2003.