ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Aspekte der Sicherheit und Privatsphäre im zukünftigen Stromnetz

Seminar Verteilte Systeme

Frühjahrssemester 2010, ETH Zürich

27. April 2010

Raphael Tawil

Übersicht

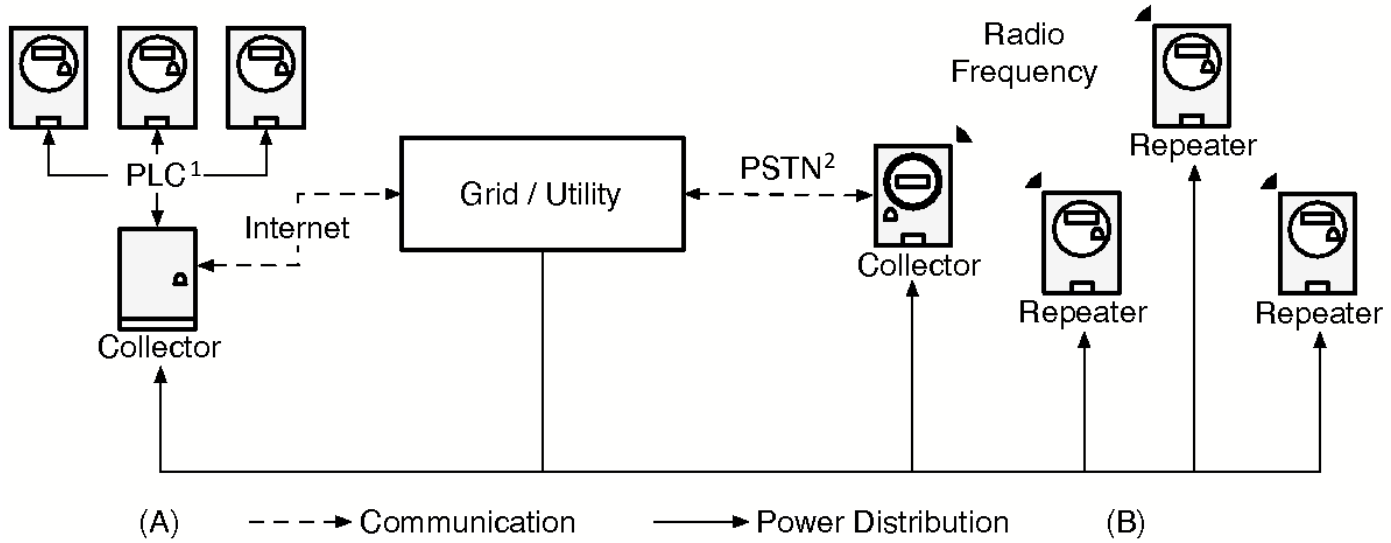
- **Einleitung**
  - Hintergrund
  - Kurzübersicht einer Advanced Metering Infrastruktur (AMI)
- **Sicherheit**
  - Sicherheit einer AMI
  - Allgemeine Sicherheit von komplexen kritischen Infrastrukturen
- **Privatsphäre**
  - Sammlung von Stromnutzungsdaten der Konsumenten
- **Schlusswort**

Hintergrund

- Dem Stromnetz steht eine grosse Transformation bevor
  - Einführung des Smart Grids
- Grundsätzlich liegt der Fokus auf positiven Aspekten
  - Kosteneffizienz
  - Umweltfreundlichkeit
- Ein grosser Nachteil sind jedoch ernstzunehmende Risiken
  - Sicherheit
  - Privatsphäre

Kurzübersicht einer AMI

- Typische Struktur einer AMI:



[1] Power Line Communication, Datenübertragung über Stromnetze

[2] Public Switched Telephone Network, Telefonnetz

Quelle: [10]

Sicherheit einer AMI

- Durch gezielte Angriffe kann Geld “verdient“ werden, was ein grosser Motivationsfaktor ist.
- Mehrere verschiedene Angreifertypen
- Sicherheit einer AMI
  - Physische Sicherheit des Smart Meters
  - Sicherheit bei der Kommunikation
- Angriffe im Grossformat (Bsp.: Denial of Service[1] (DoS) Angriffe)

[1] Dienstverweigerung

Klassifizierung verschiedener Angreifer

- Es wird zwischen mehreren Angreifertypen unterschieden [10, 11]:

1. (Betrügerische) Konsumenten
   - Wollen Strom stehlen

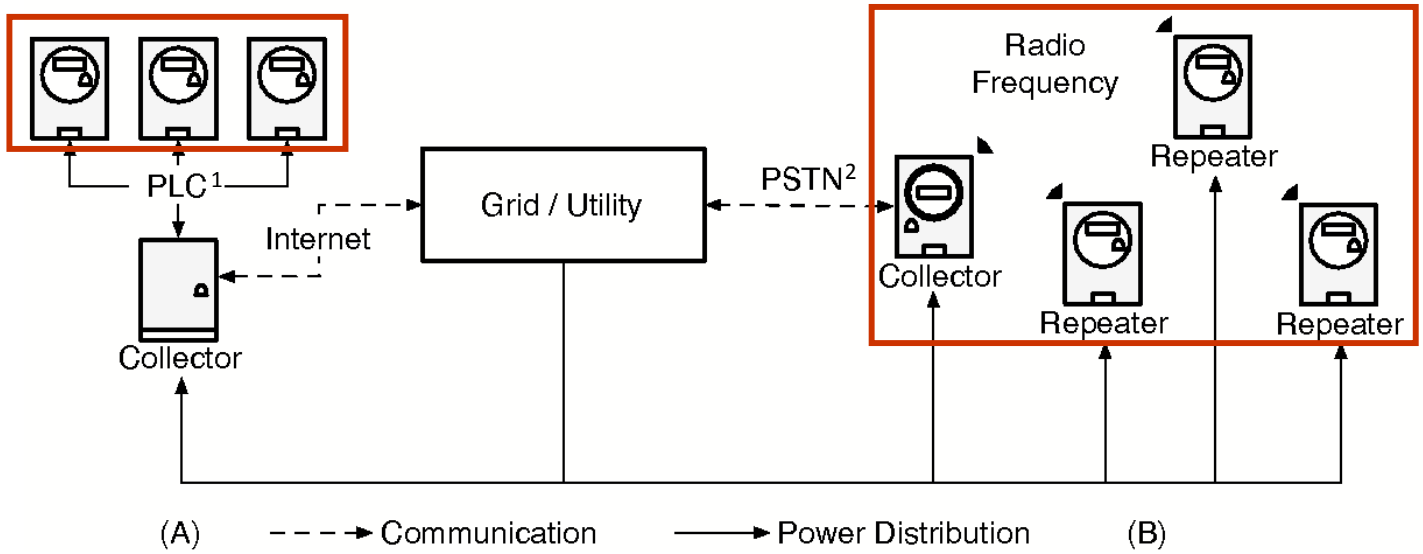
2. Organisierte Kriminalität
   - Wollen durch geeignete Sicherheitslücken Geld verdienen

3. (Betrügerische) Insider
   - Angestellter in einer AMI, der illegale Geschäfte abwickelt

4. Terroristen
   - Wollen dem Smart Grid Schaden hinzufügen

Angriffsstellen in einer AMI

- **Angriffsstelle 1: Smart Meter**



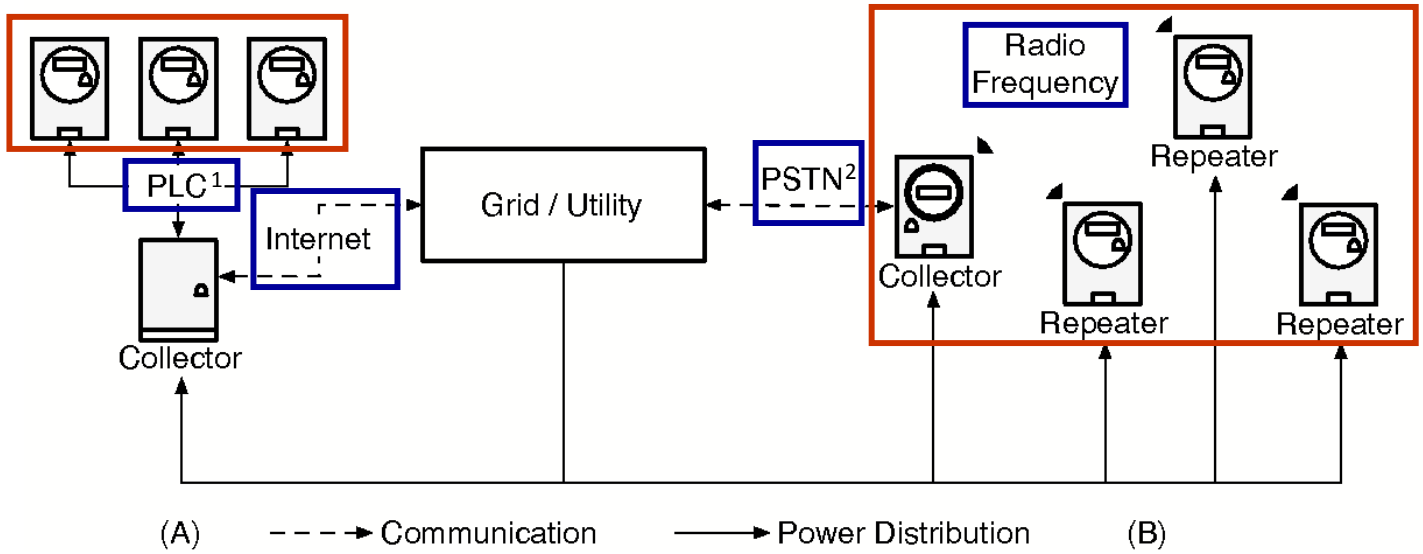
[1] Power Line Communication, Datenübertragung über Stromnetze

[2] Public Switched Telephone Network, Telefonnetz

Quelle: [10]

Angriffsstellen in einer AMI

- **Angriffsstelle 1: Smart Meter**
- **Angriffsstelle 2: Kommunikation**



[1] Power Line Communication, Datenübertragung über Stromnetze

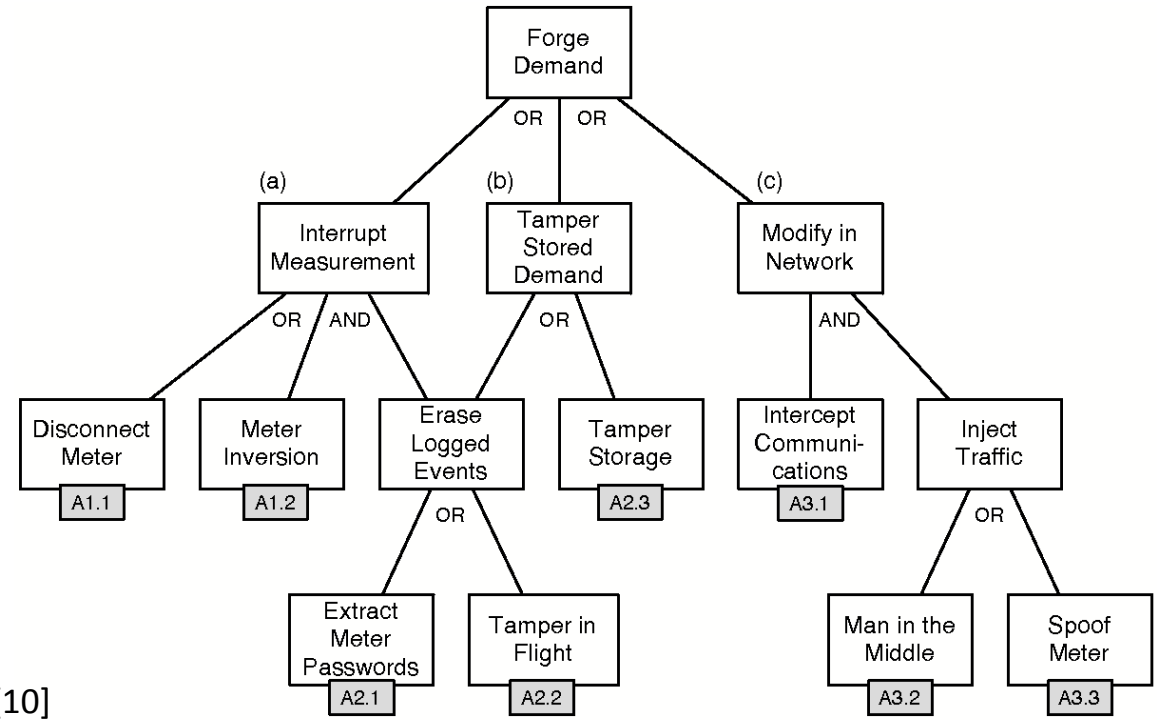
[2] Public Switched Telephone Network, Telefonnetz

Quelle: [10]

Manipulation der Stromnutzungsdaten

- Ziel: Manipulation der Daten über die Stromnutzung

  - Repräsentation dieses Ziels als Angriffsbaum:

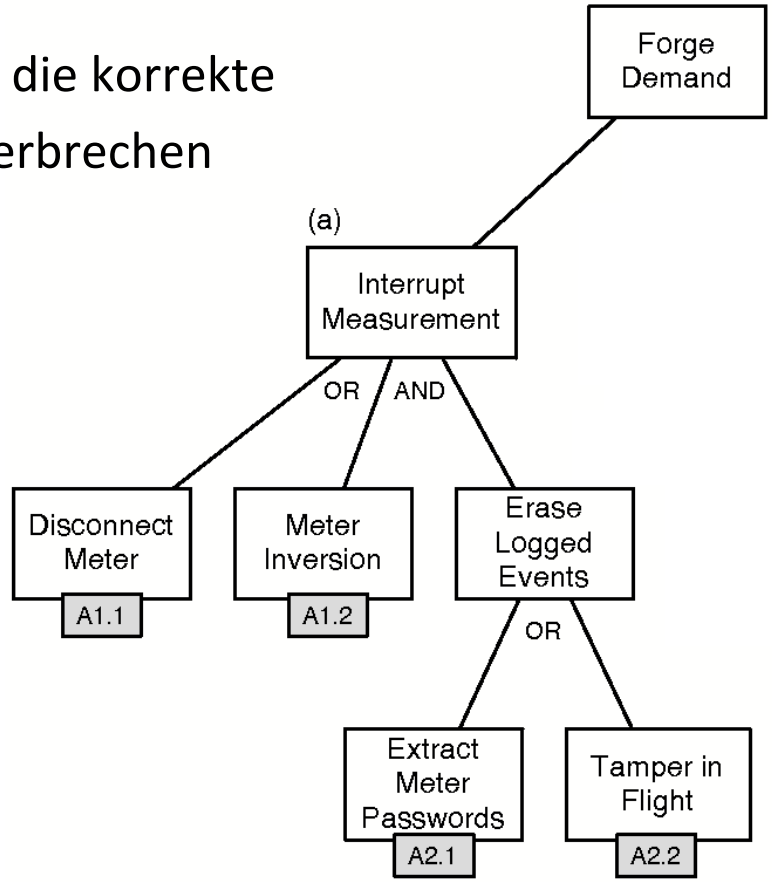


Quelle: [10]

Manipulation der Stromnutzungsdaten

- **Teilbaum (a):** Durch Veranlassung, die korrekte Messung des Smart Meters zu unterbrechen
  - Durch Abkopplung (A1.1)
  - Durch Invertierung (A1.2)

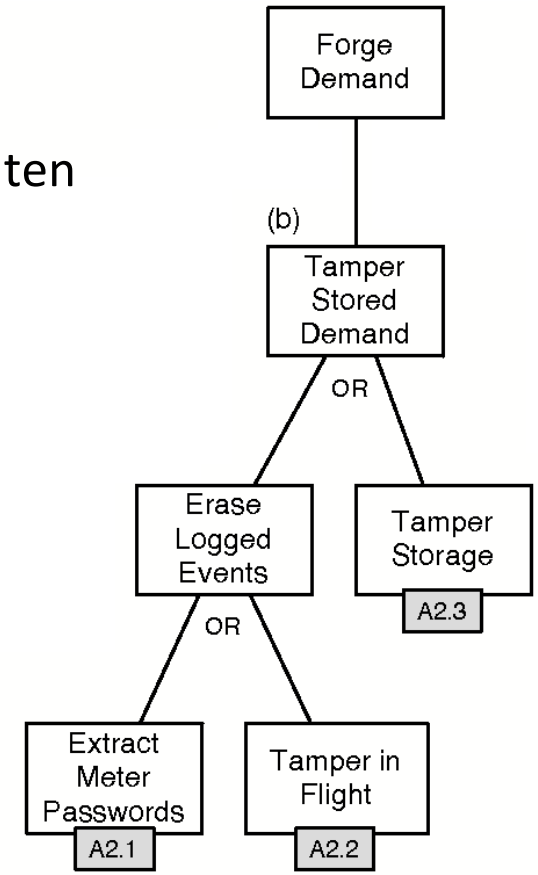
- Immer in Kombination mit dem Löschen der Logdaten (über die Smart Meter Messaktivität)



Quelle: [10]

Manipulation der Stromnutzungsdaten

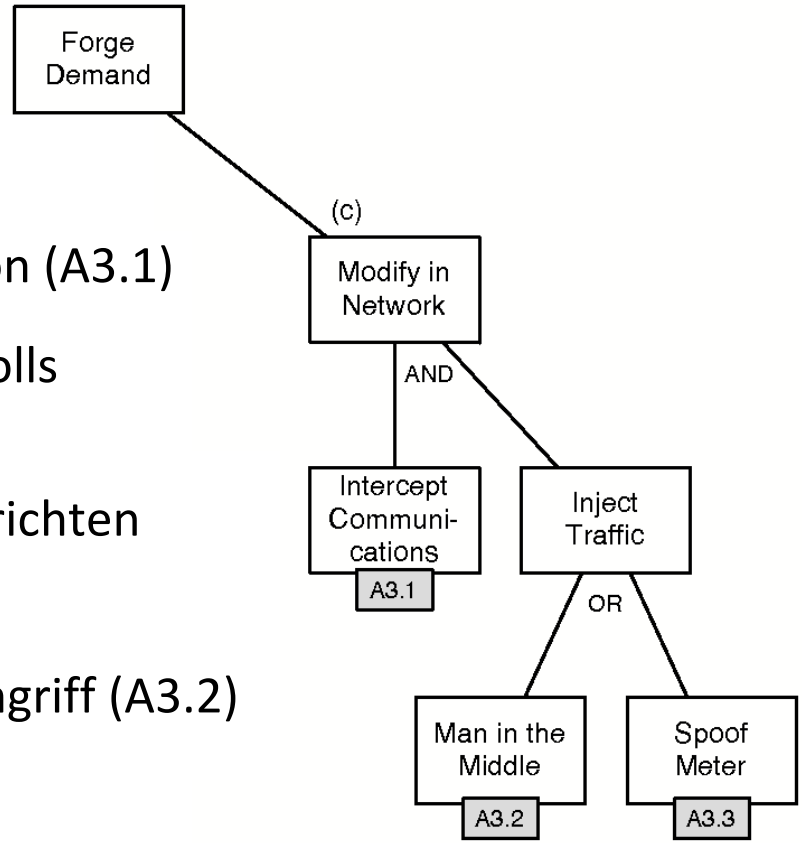
- **Teilbaum (b):** Durch Manipulation der Daten im Speicher des Smart Meters
  - Durch direktes Manipulieren der gespeicherten Daten (A2.3)
  - Durch das Löschen der Logdaten (über die Stromnutzung)



Quelle: [10]

Manipulation der Stromnutzungsdaten

- **Teilbaum (c):** Durch Veränderung der Daten während der Übertragung



1. Belauschen der Kommunikation (A3.1)
   - Rekonstruierung des Protokolls
2. Einspeisung zusätzlicher Nachrichten
   - Durch Meter Spoofing (A3.3)
   - Durch Man-in-the-Middle Angriff (A3.2)

Quelle: [10]

Aktuelle Smart Meter: Sicherheit ungenügend

- Bisherige Schutzmassnahmen sind schwach, da die erläuterten Angriffe in der Realität (auf einem Testsystem) erfolgreich waren [10]:

  - Passwort wird im Klartext gesendet.

    → Ermöglicht Angriff aus Teilbaum (a).

  - Passwort und Schlüssel können aus dem Speicher extrahiert werden.

    → Ermöglicht Angriff aus Teilbaum (b).

Aktuelle Smart Meter: Sicherheit ungenügend

- Bisherige Schutzmassnahmen sind schwach, da die erläuterten Angriffe in der Realität (auf einem Testsystem) erfolgreich waren [10]:

  - Sogar wenn Authentifikationsmechanismen verwendet wurden, waren diese nicht korrekt implementiert.

  - Verwundbar gegen Replay-Angriff.

    → Ermöglicht Angriff aus Teilbaum (c).

Lösungsansatz

- Um angemessene Sicherheitsvorkehrungen für eine AMI zu treffen, müssen folgende Anforderungen erfüllt sein [4]:
  - Vertraulichkeit
  - Integrität
  - Authentizität
  - Verfügbarkeit
  - Nichtabstreitbarkeit
  - Zugriffskontrolle
  - Protokollierung
- Lösung (für viele dieser Anforderungen): Public Key Kryptographie [4].
- Bestehendes Problem: Physische Eingriffe.

Verhinderung physischer Eingriffe

- Passwörter und Schlüssel werden in einem manipulationssicheren Speicherbaustein gelagert [15].

  - EEPROM[1] (wird schon bei SmartCards benutzt)

  - Automatischer Löschmechanismus bei Erkennung eines physischen Eingriffs

  - Wurden erst kürzlich für Smart Meter optimiert

  Beispielprodukte [1, 13]:

  - ROHM EEPROM for Smart Meters
  - Atmel VaultIC460 128 KB EEPROM

[1] Electrically Erasable Programmable Read Only Memory,
(=Elektrisch löschbarer programmierbarer Nur-Lese-Speicher)

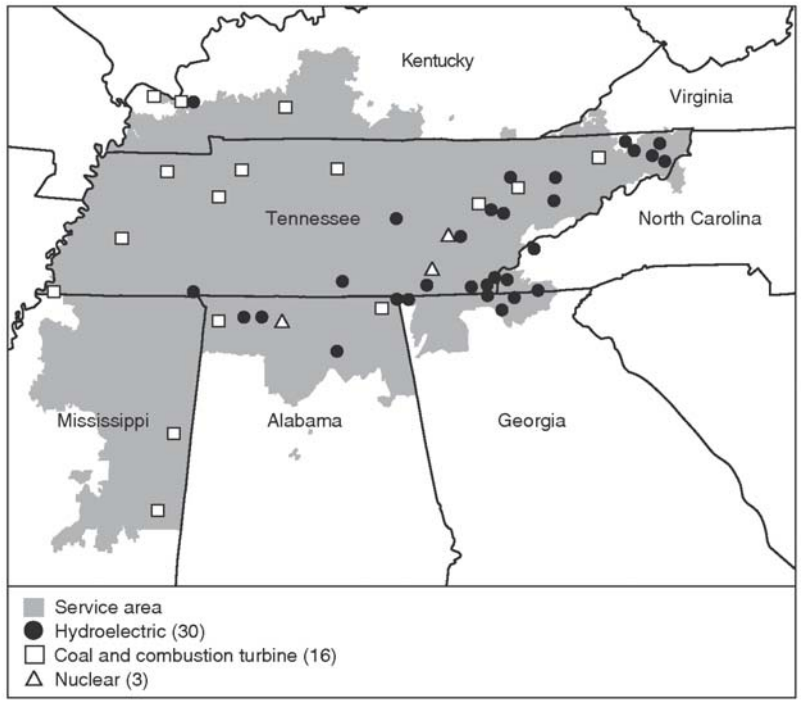
Sicherheit von kritischen Infrastrukturen

- Das Smart Grid
  - ist ein verteiltes System
  - hat eine enorme Grössenordnung
  - beinhaltet sehr kritische Knoten im Netz (z. B. Generatoren)

- Es müssen angemessene Sicherheitsvorkehrungen getroffen werden.
  - Fokus nun nicht mehr auf Stromdiebstahl
  - Sondern auf allgemeinen Sicherheitsanforderungen
  - Das gesamte Stromnetz muss sicher sein, nicht nur die AMI

Fallstudie: Tennesse Valley Authority

- Die TVA ist das grösste EVU[1] in den USA.
  - Versorgte Fläche: 207‘200 km^2 mit ca. 8,7 Mio. Einwohnern
  - Verteilt auf sieben Bundesstaaten



[1] Energieversorgungs-unternehmen

Quelle: [2]

Fallstudie: Tennesse Valley Authority

- Die GAO[1] prüfte (März 2007 – April 2008), ob die TVA angemessene Sicherheitsvorkehrungen getroffen hatte.

  - Es wurde auf Vertraulichkeit, Integrität und Verfügbarkeit von Information und Steuerungseinheiten geachtet.

  - Das Resultat war enttäuschend.

  - Die TVA hat nie selbst eine Sicherheitseinschätzung durchgeführt (Verletzung des US Gesetzes).

  - Wir sollten aus Fehlern lernen (mit Blick auf das Smart Grid).

[1] Government Accountability Office

Quelle: [2]

Fallstudie (TVA): Resultat der GAO

- Sicherheitsschwachstellen im internen Rechnernetz:
  - Auf fast allen Arbeitsstationen und Servern
    - waren wichtige Sicherheitsupdates nicht installiert.
    - war keine Antivirensoftware installiert.
  - Firewalls waren mangelhaft konfiguriert.
  - Kein Intrusion Detection[1] System wurde verwendet.
  - Passwörter wiesen nur schwachen Schutz auf.
  - Zugriffe wurden nirgendwo protokolliert.

- **Folgen:** Unbefugter Zugriff auf Information, DoS Angriffe, Kompromittierung von internen Computersystemen

[1] Erkennung von Eindringlingen

Quelle: [2]

Fallstudie (TVA): Resultat der GAO

- Sicherheitsschwachstellen bezüglich physischen Aspekten:
  - Wichtige Netzwerkbuchsen waren nicht vor unbefugtem Zugriff geschützt.
  - Die Zugriffskontrolle war ungenügend segmentiert.
  - Ein Steuerungsraum hatte eine Küche (Feuer- und Wassergefahr)

- **Folgen:** Physische Angriffe verschiedenster Natur, Unbefugter Zugriff auf Information.

Quelle: [2]

Privatsphäre

- Konsumenten stellen dem EVU Daten über ihren Stromverbrauch zur Verfügung.

- Datensammlung:

  - Durch das EVU
  - Durch andere Parteien (Bsp.: mittels Schadsoftware)

- Natur der Daten:

  - Was sagen diese Daten über den Konsumenten aus?
  - Was geschieht, wenn diese Daten in falsche Hände geraten?

Leistungscharakteristik von Geräten

- Es stehen Smart Meter an, die Geräteerkennung anhand der Leistungskurve durchführen.
- Das EVU, das Zugriff auf diese Daten hat muss eine angemessene Privacy Policy festlegen.

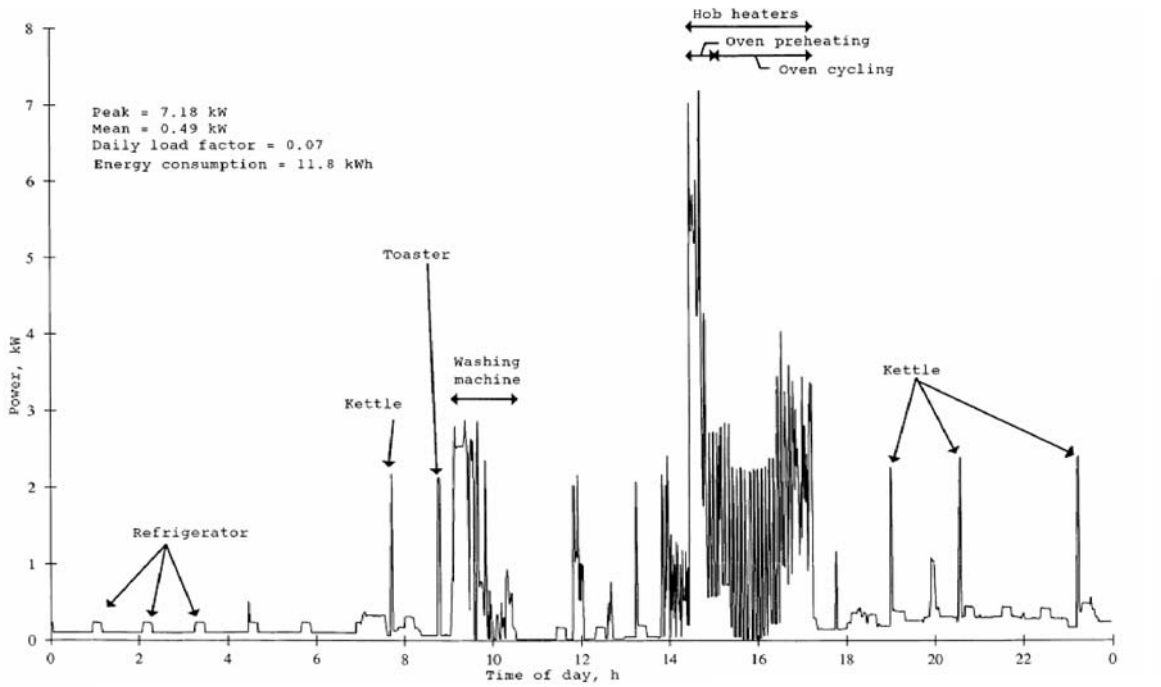


Abbildung: [14]

Konsequenz der Datensammlung

- Aus solchen Daten könnte man folgendes über einen Konsumenten folgern [12]:
  - Wie oft wäscht der Konsument Kleider?
  - Hat der Konsument Kinder?
  - Wann ist der Konsument bei der Arbeit?
  - Benutzt der Konsument oft eine Mikrowelle?
  - Wie oft benutzt der Konsument den Toaster/Wasserkocher?

- Sollten Stromnutzungsdaten in falsche Hände geraten, drohen folgende Konsequenzen:
  - Überflutung mit massgeschneiderter Werbung
  - Einbrecher wissen, wann das Haus leer steht...

Schlusswort

- Das kommende Smart Grid birgt einige Risiken im Bereich Sicherheit:
  - Smart Meter sind noch nicht sicher...
  - ...aber auf dem richtigen Weg.
  - Smart Grid hoffentlich sicherer als TVA.

- Auch im Bereich Privatsphäre gibt es noch einiges zu klären:
  - Wie wird die Privacy Policy eines EVU aussehen?
  - Generelles Misstrauen der Konsumenten.

Fragen?


OH YEAH, THE METER GOT HACKED...
VIRUS
WORM
SPYWARE
VIRUS
©2008 Maaike Hartjes.nl
Don't forget security!

Referenzen

[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] G. Wood and M. Newborough. Dynamic Energy-Consumption Indicators for Domestic Appliances: Environment, Behavior, and Design. 2003.
[15] USEA. The Smart Grid: Lunch and Learn (Session 5). www.usea.org. 2009.