Security considerations for SmartCoDe Network

Smart Energy Management

Author: Juraj Hájek
Date: 16.11.2010
Dissemination Level: Public

Latest history – sample incidents

- 2003 – Northeast Blackout - cascading power failure in the eastern caused by software bug in energy management system (affected 55 million people in USA and Canada)
- 2007 - Goodspeed demonstrated that it was possible to write a worm that could spread among MSP 430 chips, which are used by some Smart Grid device makers
- 2008 – Cyber attack had taken out power equipment in multiple regions outside the U.S.
- 2009 – IOActive have created a worm that could quickly spread among Smart Grid devices
- 2009 – USA declared that they electricity grids have been penetrated by spies

Basic security requirements

› ***Confidentiality***: *"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…."*

A loss of confidentiality is the unauthorized disclosure of information.

› ***Integrity***: *"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…."*

A loss of integrity is the unauthorized modification or destruction of information.

› ***Availability***: *"Ensuring timely and reliable access to and use of service…."*

A loss of availability is the disruption of access to or use of service or an system.

Consumer trust and confidence

› Accenture research about customer preferences in Energy Efficiency (April 2010)

- **More than 9000 consumers**
- **17 countries**
- **About 1/3 said they would be** discouraged from using energy-management programs**, such as smart metering, if it gave utilities greater access to data about their personal energy use**

› **Trust** is fundamental to attract customers

› Potential customers have a hierarchy of needs that influences their reasoning

Privacy

› The Smart Grid opens up more opportunities for invasion of privacy
  – **Higher amount of available data**
  – **More granular form (minutes)**

› Privacy categories
  – **Privacy of personal information**
  – **Privacy of the person (e.g. required medical devices)**
  – **Privacy of personal behavior**
  – **Privacy of personal communications**

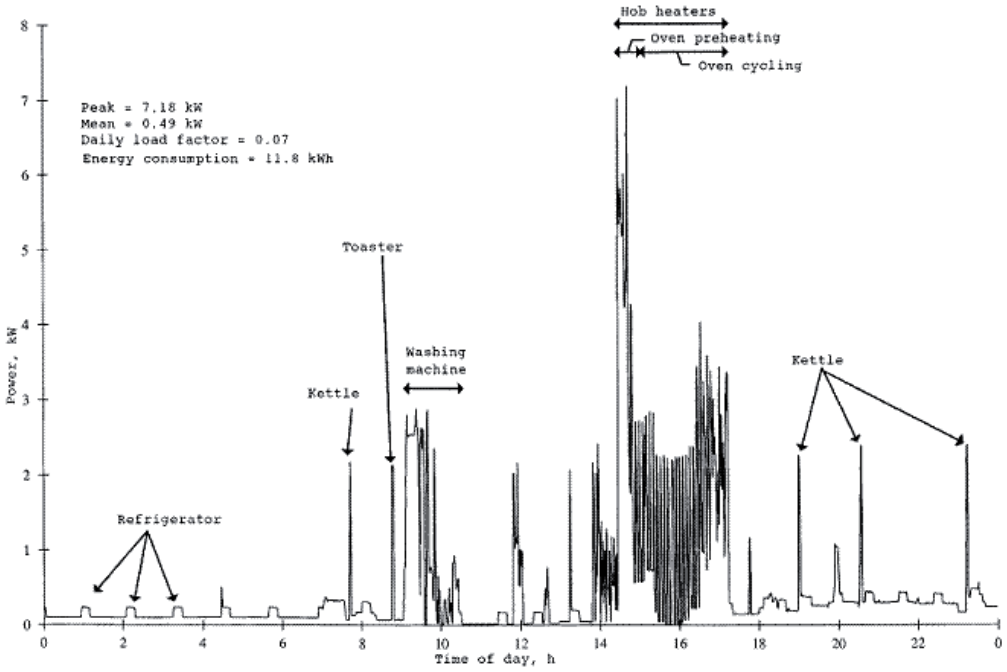
› Who owns Smard Grid Data?

Power usage patterns

› Nonintrusive appliance load monitoring
› It is not required to sniff/decrypt local network communication
› Power usage can be compared with library of existing patterns

› Potential groups of interest
  – **Thieves**
  – **Annoying marketers**
  – **Police investigation (**indoor marijuana plants can be detected also with existing granularity of measurements**)**
  – **People involved in energy trading – manipulation of energy costs at the real-time energy stock market**

Power usage graph



Source: NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0

Privacy – potential solutions

- Utility company
  - **A part of energy consumption is covered from local energy sources (solar cells, electric and plug-in hybrid cars…). This changes overall power usage pattern**
  - **Data are anonymized to the level sufficient for pricing**
- Transport channels
  - **Strong cryptography**
- Local grid/network
  - **Strong cryptography**

Smart Grid Cryptography- Constraints

- General constraining issues
  - **Computational constraints (CPU,Cryptoporcessor, RAM)**
  - **Channel bandwidth**
    - Encryption - negatively influences lower layer compression algorithms
    - Integrity protection - communication overhead (could be important for limited bandwith and small messages)
  - **Connectivity**
    - access to PKI infrastructure
- General cryptography issues
  - Entropy
  - Cipher Suite (standards base, mature, preferably patent free)
  - Key Management (including certificate lifetimes)

Example - TI MSP 430 (Worm by Goodspeed)

- Parameters
  - **Devices starting at $0.25 USD in 100k units**
  - **Complete LaunchPad development kit for $4.30 USD (including compilers, debuggers)**
  - **No memory protection**
  - **Small stack space**
  - **Limited memory for program code 0.5-2 KB**
  - **Source of entropy cannot be protected**

Common SW problems

› Missing error checking (limited program memory size)
› Buffer/Integer overflows
› Small stack space – e.g. depth 7
› Programming errors in state machines (protocols, authentication schemes)

SmartCoDe – Security scope

› SmartCoDe project is focused on energy management for buildings and neighbourhoods (local grids)

› Within scope
  – **CIA (confidentiality, integrity, authenticity) of local communication**
  – **Security aspects related to commissioning of local network**
› Out of scope
  – **Security of communication between local grid and utility company**
  – **Privacy and legal aspects of data archiving outside of local grid**
  – **Authenticity and trust in the whole supply chain**
  – **Vulnerability management and traceability in the whole supply chain**

ZigBee

- Low-cost, low-power, wireless mesh networking standard
- Based on IEEE 802.15.4-2003
- Application profiles to enable interoperability
  - **Home Automation**
  - **Smart Energy**
  - **Telecommunication Services**
  - **Health Care**
  - **Remote Control**
- Security defined for the MAC, NWK and APS layers
- Security for applications is typically provided through application profiles.
- E.g. Smart Energy
  - **AES 128 encryption**
  - **ECC implicit certificates for authentication and key establishment**
- Existing commissioning cluster supports configuration ,,over the air''

SmartCoDe vs. ZigBee

- „SmartCoDe profile“ is in specification phase
- Profile is PHY/MAC layer agnostic
- Security extensions can be implemented on APS layer
- Security building blocks in ZigBee SE are mature. Higher security could be achieved e.g. by
  - **HW - smart cards available in standard low cost nodes**
  - **Well defined and standardized procedures for deploying and maintaining network, supported by specification**
- ZigBee is interoperable on protocol level, business processes affecting security could be different for each vendor (e.g. commissioning)
- High security will be available also for areas, where it is currently not supported by ZigBee (e.g. Home Automation)
- The same application profile can have several security profiles
- Fine grained approach – overhead is extremely important
- Level of compatibility will be 100% clear after specification is finished

SmartCoDe – Business Processes

- Business processes like physical deployment and configuration have impact on protocols and security
- Large constructions:
  - **Separate roles (trust in supply chain, expected skills), e.g.:**
    - Electrician – physically mounts devices
    - Commissioner – responsible for final configuration including security
  - **Output artefacts of each task should be testable**
  - **Independent commission of network parts is possible (e.g. by rooms or floors)**
- Small houses need easy solutions
- *One size fits all* approach is not realistic

Use cases – add new devices (example)

a) Home owner temporary allows join by pressing button in central device. New devices are automatically detected and joined.

b) Home owner temporary allows join by entering password to central device. New devices are automatically detected and joined.

c) Home owner or any responsible person enters password and identifiers of new devices to be joined (e.g. public key or it's part)

d) Electrician collects public keys of mounted devices by 2D bar code scanner. Commissioner creates temporary network of known devices and configures it. Building manager authorizes access to the building trust center by its personal card and joins temporary network to final. In meantime, internal auditor can check outputs of each task.

Conclusion

- New technologies usually introduce new risks and open new opportunities for attackers
- Electricity infrastructure continuously moves from supporting infrastructure to the real IT system
- There are existing standards for security in IT systems + new standards focused especially to Smart Grids
- There are several working groups still working in new standards, e.g. NIST - Guidelines for Smart Grid Cyber Security
- SmartCoDe team wants to deliver higher security also for low cost solutions

Thank you for your attention!

Any questions?

E-Mail: juraj.hajek@ardaco.com

http://www.ardaco.com