Security in Advanced Metering Infrastructure

Rikard Bodforss, Omegapoint
@rbodforss

omega point.

Commercial break!

- If you understand Swedish…
  Listen to our podcast on security:
  www.sakerhetspodcasten.se

  Also available on iTunes

omega point.

Agenda:

- Security Principles
- AMI/AMR/Smart grid etc.
- Assessing security
- Security by design

omega point.

Why do we need security?

omega point.

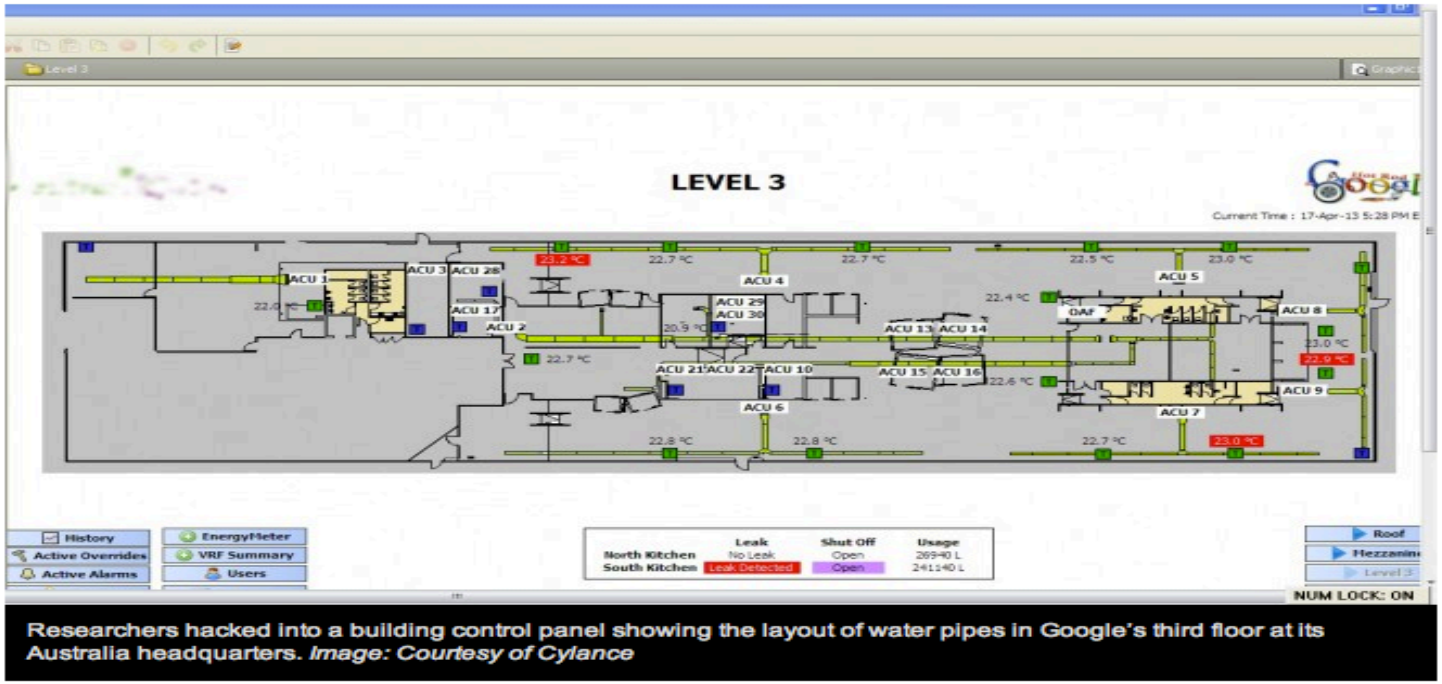
Yesterday's news:

Researchers Hack Building Control System at Google Australia Office

BY KIM ZETTER 05.06.13 6:30 AM

Follow @KimZetter

Share 214 Tweet 431 +1 17 Share 541



Researchers hacked into a building control panel showing the layout of water pipes in Google's third floor at its Australia headquarters. *Image: Courtesy of Cylance*

http://www.wired.com/threatlevel/2013/05/googles-control-system-hacked/

omega point.

Build on solid ground:

Security Principles

omega point.

Auguste Kerkhoff (1835-1903)

- The design of a system should not require secrecy and compromise of the system should not inconvenience the correspondents

omega point.

Security by obscurity

Thanks to http://xkcd.com/ for the comic!

omega point.

Risks and threat landscape

AMI/AMR/Smart grid etc…

omega point.

What is AMI?

- Automated Meter Reading
- Smart power grid that interacts with home control networks etc.

omega point.

ISC/SCADA Legacy

- Hard wired
- Physically separated
- Serial communication
- Proprietary protocols
- Under the RADAR

omega point.

The protocols

M-Bus

IEEE 802.15

ZigBee®
Control your world

Z-wave

X10®

omega point.

The trend

- “Smart”- Energy, Homes, Grid, etc…
- “Internet of things”
- Cost for PLCs/Controllers going down
- Cost for hard-wired installations going up
  Wireless to the rescue…
- Cost for analyzing (tools etc.) going down
- Tinkering is a wonderful hobby…

Still under the radar?

omega point.

- **Killerbee: Practical Zigbee Exploitation Framework**
- Joshua Wright, InGuardians
- ZigBee is a low-power, low-data wireless protocol. It uses IEEE 802.15.4 and came out in 2004. Max throughput 250Kb/s, mesh or star topology, long battery life (5-year goal), 10-100 m. range, 16 non-overlapping channels. Uses AES-CCM, but network key shared for all devices.
- ZigBee used because WiFi protocols are too bloated. Bluetooth uses too much power (frequency hopping), too complex. ZigBee low-cost, low-speed; used for lightweight embeddd technology. Security suffers because of low-cost and simplicity goals.

- **Don Bailey**
- **War Texting: Identifying and Interacting with Devices on the Telephone Network**
- Devices have been attached to the telephone network for years. Typically, we think of these devices in terms of modems, faxes, or TTY systems. Now, there is a growing shift in the nature of the devices that are accessible over the telephone network. Today, A-GPS tracking devices, 3G Security Cameras, Urban Traffic Control systems, SCADA sensors, Home Control and Automation systems, and even vehicles are now telephony enabled. These systems often receive control messages over the telephone network in the form of text messages (SMS) or GPRS data. These messages can trigger actions such as firmware updates, Are You There requests, or even solicitations for data. As a result, it is imperative for mobile researchers to understand how these systems can be detected by attackers on the global telephone network, then potentially abused…

omega point.

DEFCON

- Dave Kennedy (ReL1K) presented a talk at Defcon 19 conference demonstrating the relative insecurity of home automation devices, such as X10, HomePlug and Z-Wave modules, which communicate either locally over power lines or via RF in the ISM bands.

omega point.

Attacks

omega point.

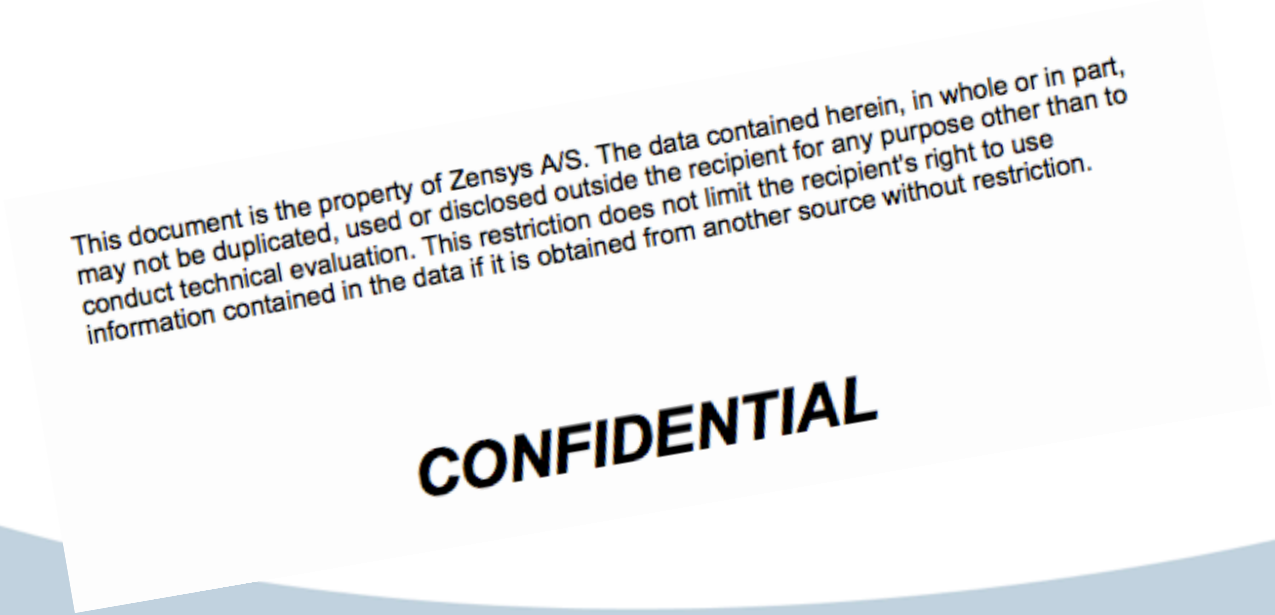
Current design principles

- Cheap to manufacture
- Optimized performance (data rates, power consumption etc.)
- Consumer experience (ease of use, deployment etc.)

Where is security in this equation?

The problem

- As long as security is not a key priority, we will keep seeing vulnerable systems!
- The lack of public scrutiny is not helping
- Fixing usually means new hardware



omega point.

The risks


Aidon
PWR
SER
RF
Brytare
max 35 A
VID ARBETE I ELANLÄGGNINGEN TAG UR HUVUDSÄKRINGARNA.
För övrig bortkoppling använd ovanstående brytare
Brytarens ljusindikeringar :


Brytare
max 35 A
LANLÄGGNINGEN TAG UR HUVUDSÄKRINGARNA.
ig bortkoppling använd ovanstående brytare
dikeringar :
pplad
rytaren ovan
- bortkopplad
rytaren ovan
RÖTT blinkande ljus - Fjärr bortkopplad
OBS! Återkoppling kan endast ske av nätbolaget
RÖTT fast ljus - Felindikering.
Kontakta nätbolaget.
INGEN LJUSINDIKERING - Strömavbrott

Motivating vendors

- Create and share tools to assess the security of ICS/SCADA/AMI protocols
- Practice responsible disclosure

omega point.

Finding the vulnerabilities

Assessing security

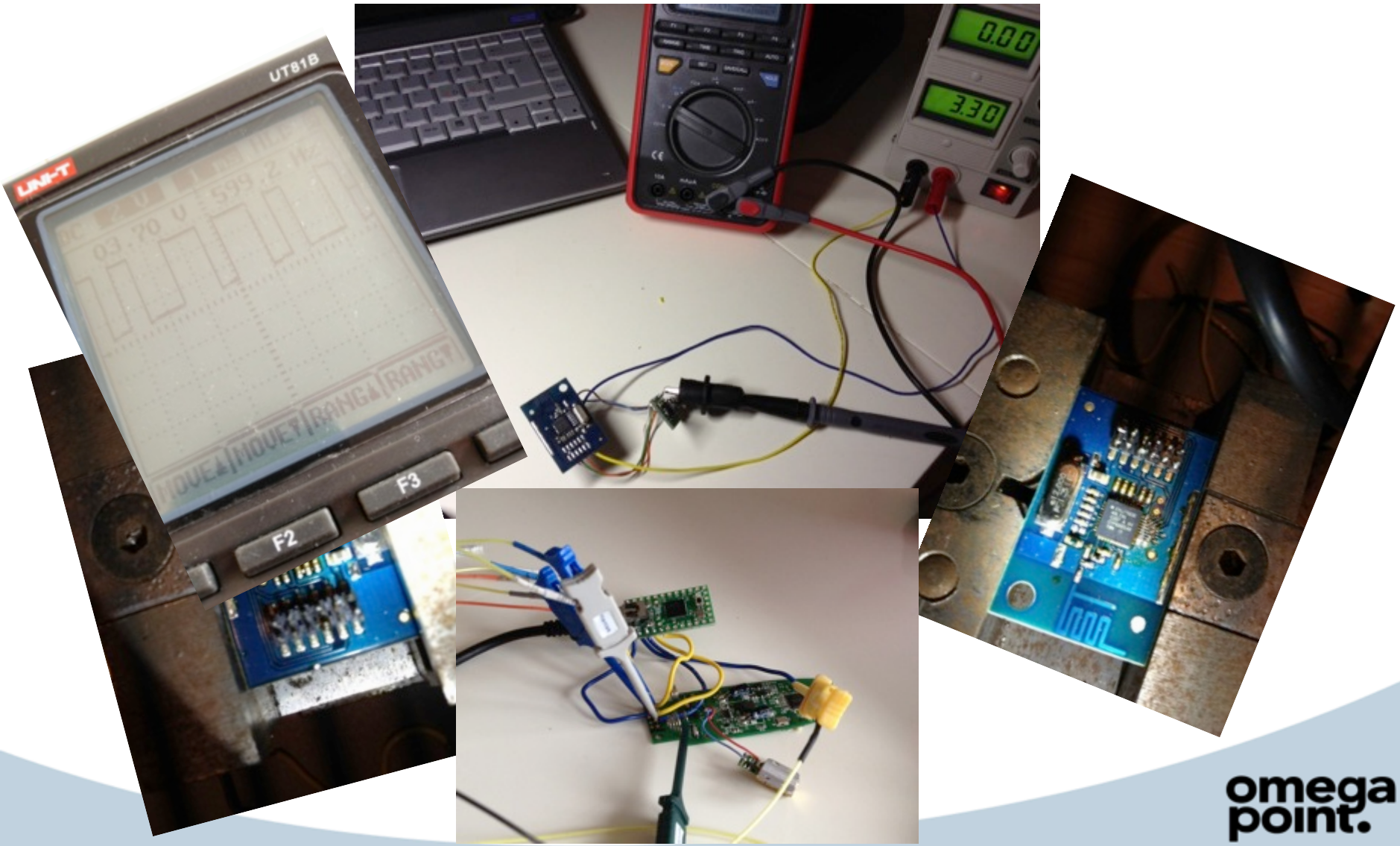
omega point.

Challenges with assessing proprietary protocols

- Requires specific hardware
- Few or no tools purpose built
- Lack of available documentation

omega point.

Hardware hacking



omega point.

Sniffing internal communication

```
------------------------------------------------------------------------------
 Bus Pirate binary mode SPI SNIFFER utility v0.3 (CC-0)
 http://dangerousprototypes.com
------------------------------------------------------------------------------
 Parameters used:
 Device = COM12,  Speed = 115200, Clock Edge= 1, Polarity= 0 RawData= 1
 Opening Bus Pirate on COM12 at 115200bps…
 Starting SPI sniffer…
 Entering binary mode…
 Switching to SPI mode
 Setting Clockedge/Polarity ..... CKE=1OK
. . .
5B [5C 0F 0x0F(FF 0xFF)5C A5 0xA5(85 0x85)5D ]
5B [5C 80 0x80(FF 0xFF)5C 42 0x42(FF 0xFF)5D ]
5B [5C C1 0xC1(FF 0xFF)5C 05 0x05(FF 0xFF)5D ]
5B [5C C3 0xC3(FF 0xFF)5C A0 0xA0(FF 0xFF)5C 14 0x14(FF 0xFF)5C 2E 0x2E(FF 0xFF)5C 15 0x15(FF 0xFF)5C 4A
0x4A(FF 0xFF)5C 04 0x04(FF 0xFF)5D ]
. . .
5B [5C 0F 0x0F(FF 0xFF)5C A1 0xA1(81 0x81)5D ]
5B [5C A2 0xA2(FF 0xFF)5C 66 0x66(FF 0xFF)5D ]
5B [5C A2 0xA2(FF 0xFF)5C CD 0xCD(FF 0xFF)5D ]
5B [5C A2 0xA2(FF 0xFF)5C 7C 0x7C(FF 0xFF)5D ]
5B [5C A2 0xA2(FF 0xFF)5C 50 0x50(FF 0xFF)5D ]
5B [5C A2 0xA2(FF 0xFF)5C DD 0xDD(FF 0xFF)5D ]
5B [5C A2 0xA2(FF 0xFF)5C 26 0x26(FF 0xFF)5D ]
5B [5C A2 0xA2(FF 0xFF)5C 7C 0x7C(FF 0xFF)5D ]
5B [5C A2 0xA2(FF 0xFF)5C 50 0x50(FF 0xFF)5D ]
5B [5C 8F 0x8F(FF 0xFF)5C A5 0xA5(FF 0xFF)5D ]
. . .
```

Channel 0x42
(2466MHz)

SOP code:
66CD7C50DD267C50

omega point.

Dumping memory

omega point.

How to do it right

Security by design

omega point.

What can be done to minimize the attack surface?

omega point.

A holistic view

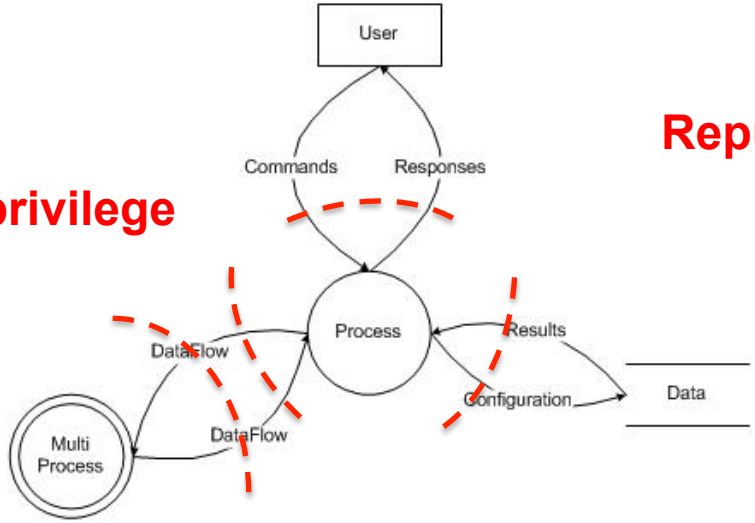
omega point.

Understand the threats

Spoofing

Repudiation

Elevation of privilege



Tampering

Denial of service

Information disclosure

omega point.

Questions?

Rikard.Bodforss@omegapoint.se
Twitter: @rbodforss
www.sakerhetspodcasten.se
securityblog.omegapoint.se

omega point.