Your House knows what you did last Summer

Dr. Steffen Wendzel

Steffen.wendzel@fkie.fraunhofer.de

Internet Security Days 2015

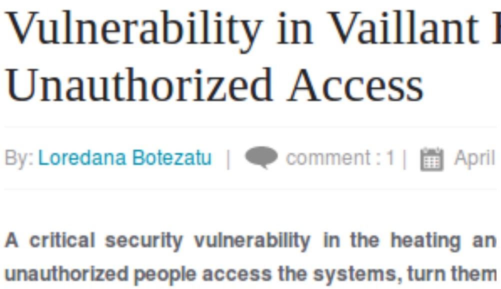
Fraunhofer
FKIE

Building Automation Systems (BAS)

- Early systems (1950‘s)
  - Pneumatic systems
- Later systems (1960’s):
  - First electric components and robust networks
- Today:
  - Smart Buildings
  - Internet of Things (IoT)

Goals of BAS

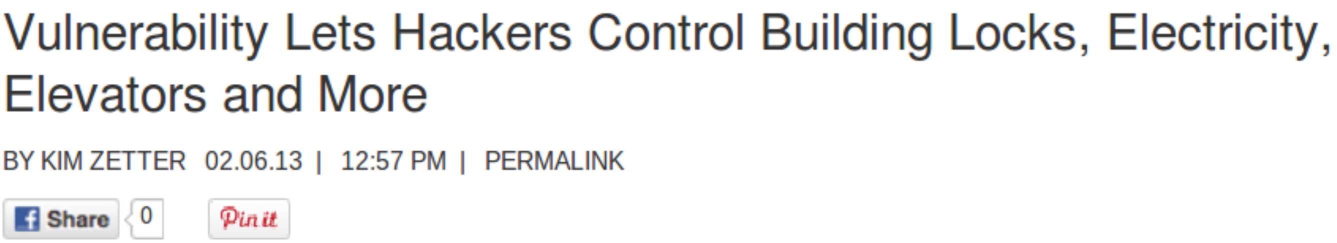
- Energy saving
- Reducing operating costs
- Enhanced life safety and security
- Fast and effective service
- Environmental friendly



Vulnerability in Vaillant Heating Systems Allows Unauthorized Access

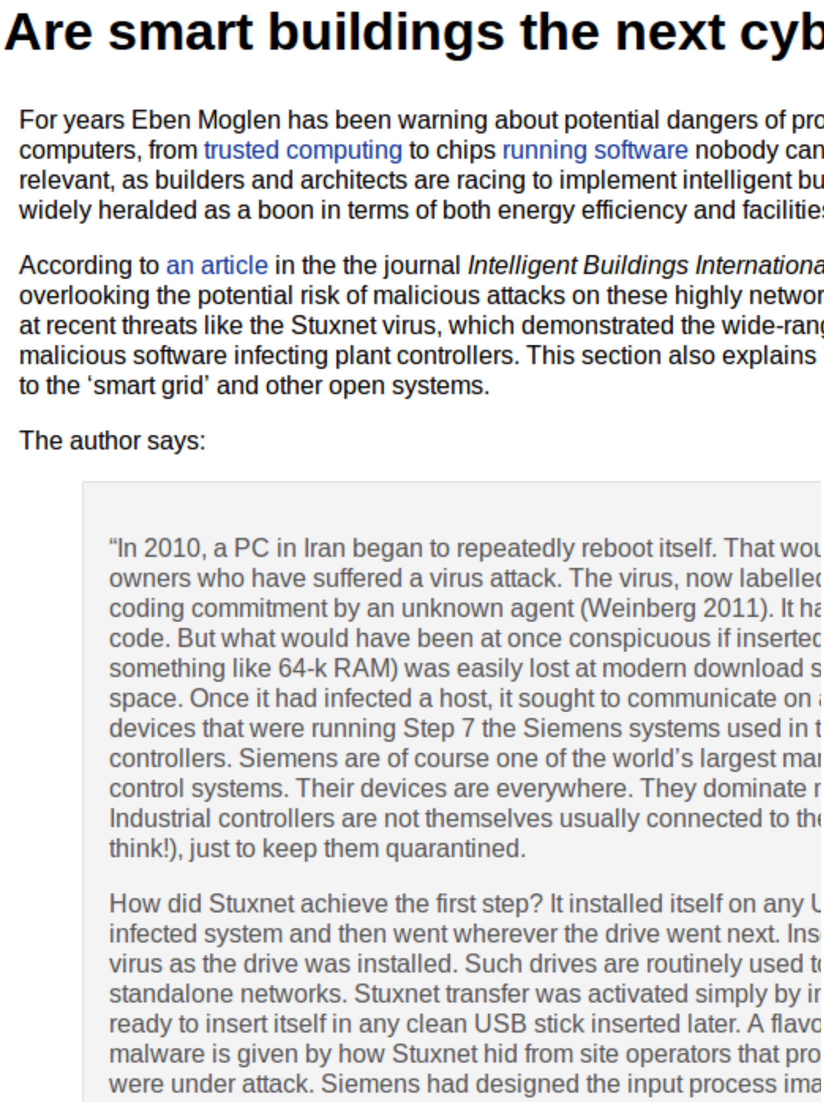
By: Loredana Botezatu | comment : 1 | April

A critical security vulnerability in the heating an unauthorized people access the systems, turn them



Vulnerability Lets Hackers Control Building Locks, Electricity, Elevators and More

BY KIM ZETTER 02.06.13 | 12:57 PM | PERMALINK



Are smart buildings the next cyber-threat?

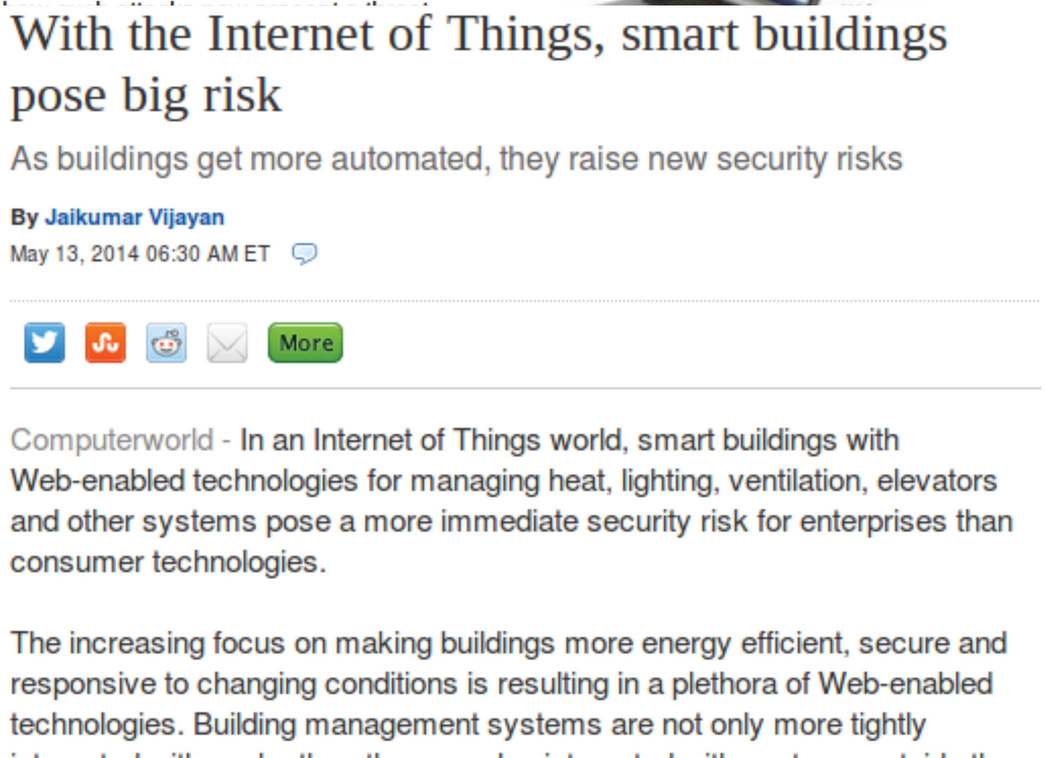
For years Eben Moglen has been warning about potential dangers of proprietary software in embedded computers, from trusted computing to chips running software nobody can access. Moglen's warnings are more relevant, as builders and architects are racing to implement intelligent buildings and smart grids, which are widely heralded as a boon in terms of both energy efficiency and facilities management.

According to an article in the the journal *Intelligent Buildings International*, building owners and architects are overlooking the potential risk of malicious attacks on these highly networked control systems. The author looks at recent threats like the Stuxnet virus, which demonstrated the wide-ranging havoc that could be caused by malicious software infecting plant controllers. This section also explains

to the 'smart grid' and other open systems.

The author says:

> "In 2010, a PC in Iran began to repeatedly reboot itself. That wou
> owners who have suffered a virus attack. The virus, now labelle
> coding commitment by an unknown agent (Weinberg 2011). It ha
> code. But what would have been at once conspicuous if insertec
> something like 64-k RAM) was easily lost at modern download s
> space. Once it had infected a host, it sought to communicate on
> devices that were running Step 7 the Siemens systems used in t
> controllers. Siemens are of course one of the world's largest ma
> control systems. Their devices are everywhere. They dominate
> Industrial controllers are not themselves usually connected to th
> think!), just to keep them quarantined.
>
> How did Stuxnet achieve the first step? It installed itself on any U
> infected system and then went wherever the drive went next. Ins
> virus as the drive was installed. Such drives are routinely used t
> standalone networks. Stuxnet transfer was activated simply by i
> ready to insert itself in any clean USB stick inserted later. A flavo
> malware is given by how Stuxnet hid from site operators that pro
> were under attack. Siemens had designed the input process ima



With the Internet of Things, smart buildings pose big risk

As buildings get more automated, they raise new security risks

By Jaikumar Vijayan

May 13, 2014 06:30 AM ET

Computerworld - In an Internet of Things world, smart buildings with Web-enabled technologies for managing heat, lighting, ventilation, elevators and other systems pose a more immediate security risk for enterprises than consumer technologies.

The increasing focus on making buildings more energy efficient, secure and responsive to changing conditions is resulting in a plethora of Web-enabled technologies. Building management systems are not only more tightly

How many are connected to the Internet?

- Malchow and Klick (2014) counted BAS via SHODAN
  - Most systems were found in the USA (~15.000)
  - *One out of ten* systems with known vulnerabilities

- Praus and Kastner (2014):
  - USA: ~9.000 BACnet devices
  - Germany: ~120 BACnet devices and ~630 KNX devices

WHAT COULD POSSIBLY HAPPEN?

Surveillance

- Private or sensitive information can be accessed or leaked using building automation equipment.

Example:

An employee observes the presence of another employee in an office room using presence sensors (directly) or CO_2 and temperature sensors (indirectly).

Buildings as Botnets

- So-called **Smart Building Botnets** can be realized in practice.
- These botnets use buildings as ‘bots’.

Examples:

> Parallel surveillance of thousands of buildings and their inhabitants.

> Sell private data of thousands to health insurance companies.

> Increase oil consumption of a smart city to sell more oil.

Organized Thefts

- **BAS wardriving** (Kahler and Wendzel, 2012) helps to identify vulnerable smart buildings and homes.

- **How?**

Opening windows or doors allows thieves to enter a building.

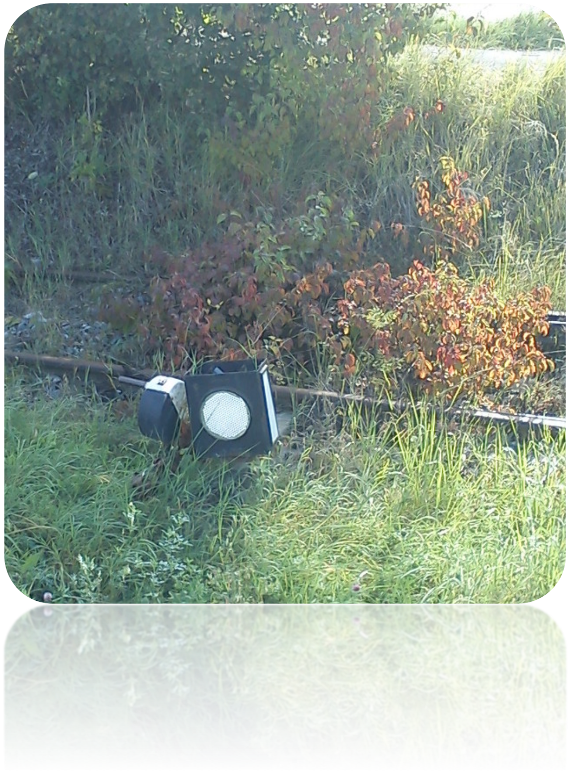
Sensor information can be used to see whether someone is actually at home, or not, reducing the risk for thieves.

Disrupting Organizational Processes

- Several organizational processes rely on building automation systems.
- If attackers stop a BAS from working, they also influence organizational processes.

- **Example:**

Heating, air-conditioning and lightening in a greenhouse.

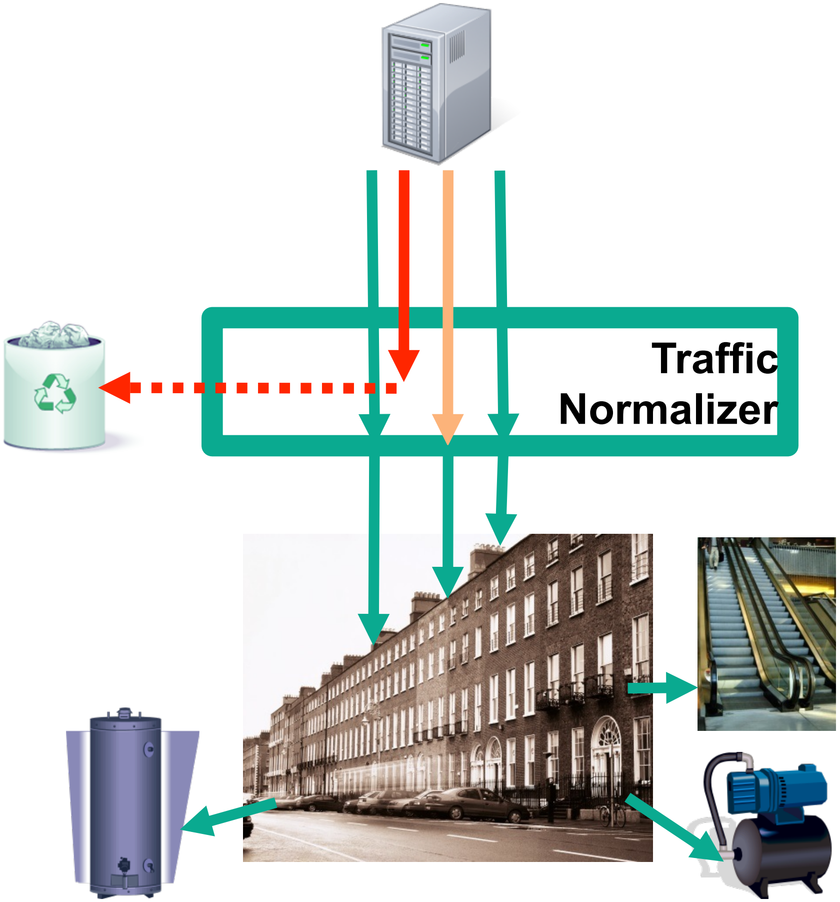


Building Automation Systems Protection:

SELECTED SOLUTIONS FROM OUR OWN RESEARCH

Traffic Normalization

- Traffic sent within building automation networks is monitored by a **traffic normalizer**.
- To evaluate traffic, the normalizer is `**aware**' of the building's setup and typical behavior. Normalization can provide high-quality analysis results of all events.

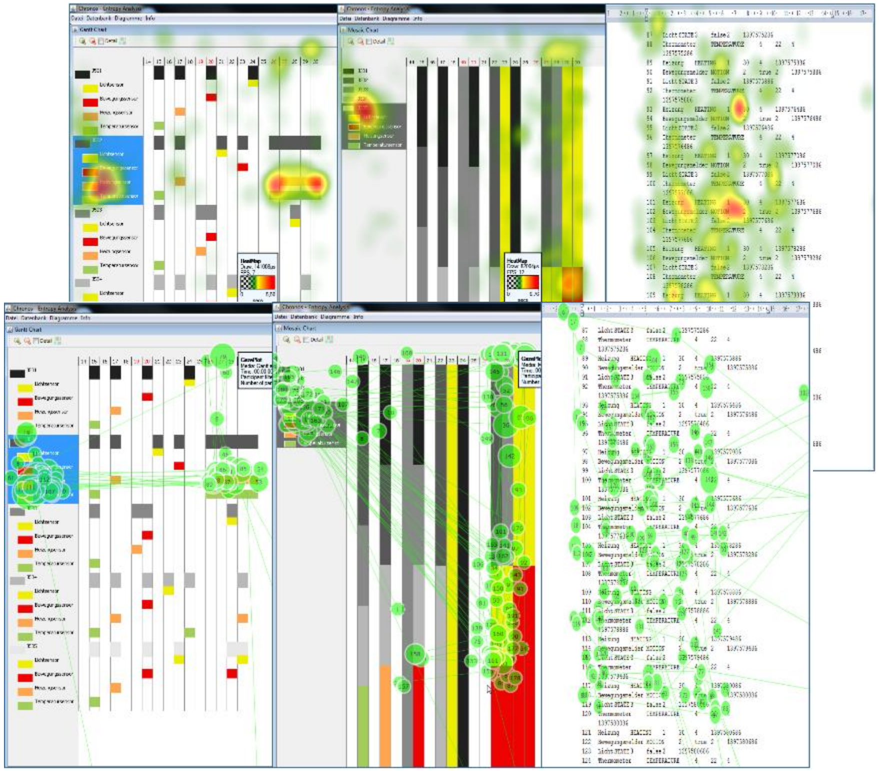


GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Building Automation Reliable Network Infrastructure

Situational Awareness

- BAS are complex distributed systems with a large number of parallel events to monitor.
- Studying visualization methods helps to determine the optimal method to present events of the BAS to an operator.

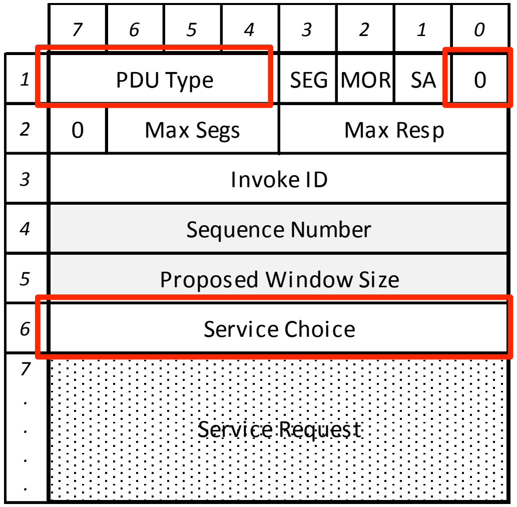


GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Building Automation Reliable Network Infrastructure

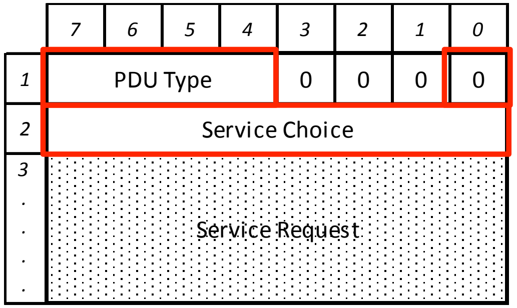
Tagging of Sensitive Data

- Ensuring that sensitive data is not distributed to all nodes of a network. This solution was designed for easy implementation in practice.



	7	6	5	4	3	2	1	0
1	PDU Type				SEG	MOR	SA	0
2	0	Max Segs			Max Resp			
3	Invoke ID							
4	Sequence Number							
5	Proposed Window Size							
6	Service Choice							
7	Service Request							

Confirmed-Request-PDU

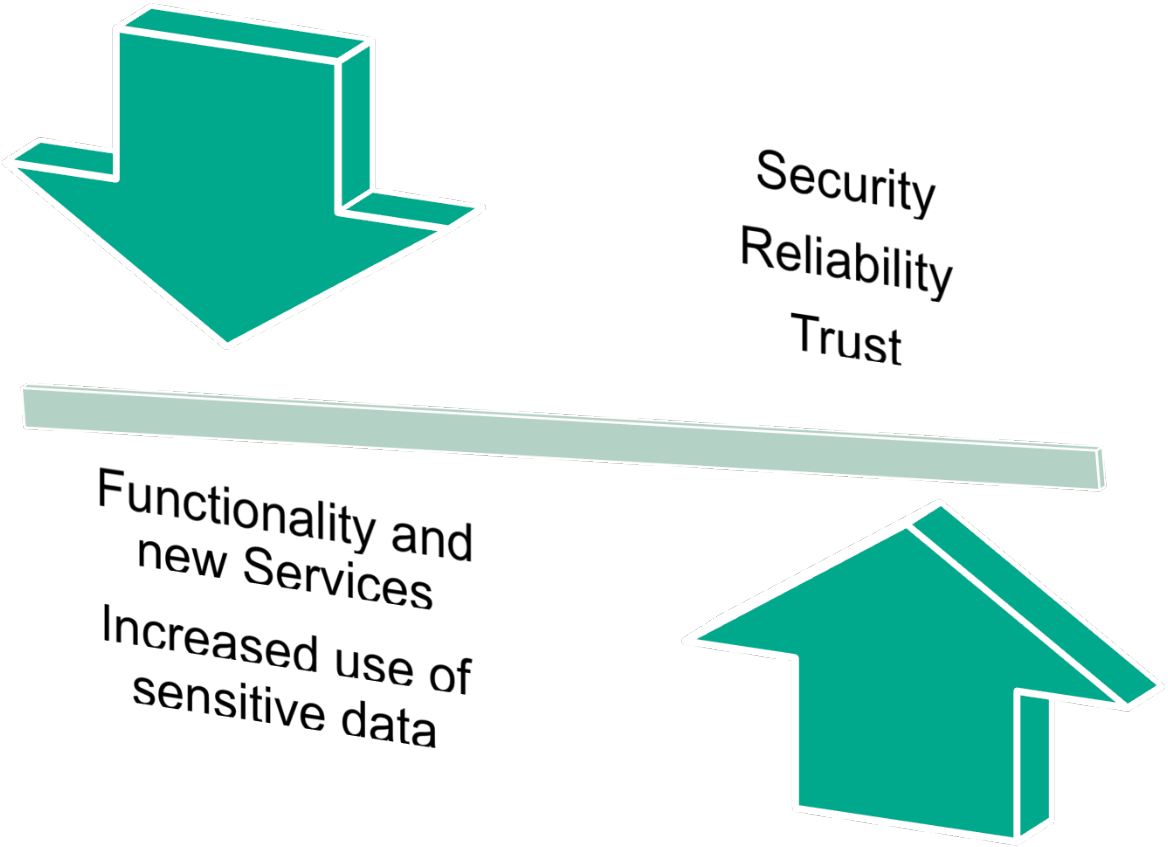


	7	6	5	4	3	2	1	0
1	PDU Type				0	0	0	0
2	Service Choice							
3	Service Request							

Unconfirmed-Request-PDU

CONCLUSION

Balance Between Functionality and Security



Security

Reliability

Trust

Functionality and new Services

Increased use of sensitive data

Thank you for your attention!

What we do:

Security Analysis of Building Automation Systems

Prototype Development

Consulting and Training

Dr. Steffen Wendzel
Head of Secure Building
Automation Systems
Dep. Cyber Security
Fraunhofer FKIE, Bonn
steffen.wendzel@fkie.fraunhofer.de