Alice´s Adventures in Smart Building Land

Steffen Wendzel & Sebastian Szlósarczyk

support: Jaspreet Kaur, Viviane Zwanger, Michael Meier ||| Art: Tobias Wendzel, Anika Schedler

steffen.wendzel@fkie.fraunhofer.de, sebastian.szlosarczyk@fkie.fraunhofer.de

Fraunhofer FKIE

Smart Buildings?

- Integrate a **Building Automation System** (BAS) for control, monitoring, management

- Early systems:
  - Pneumatic components (1950's)
  - Heating, ventilation, air-conditioning (HVAC)

- Later:
  - first electronic components (60's)
  - … and IT network components

Smart Buildings?

- Today:
  - Huge functionality spectrum
  - Integrated into “Internet of Things”
  - “Smart”
  - Respond to internal and external changes

Fraunhofer FKIE

Smart Buildings: Goals

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


Alright Humanz, me iz interested !

Down the Rabbit Hole:

Building Automation Systems

SECURITY

Fraunhofer FKIE

Vulnerability in Vaillant Heating Systems Allows Unauthorized Access

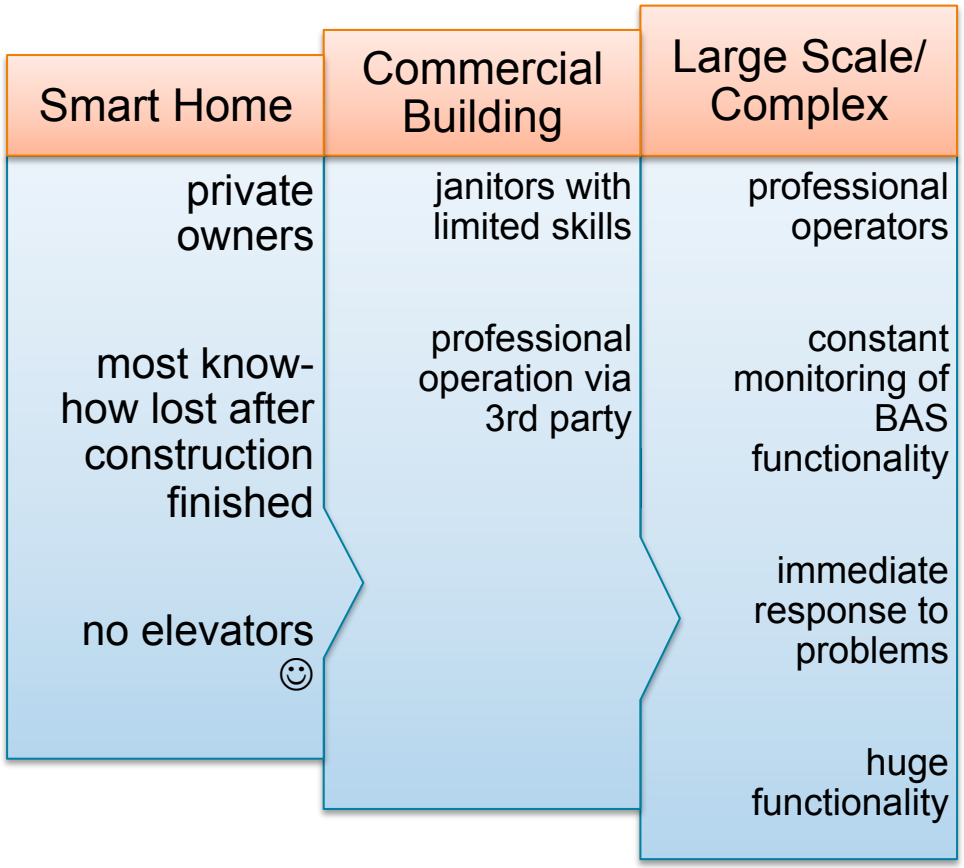
malware is given by how Stuxnet hid from site operators that pro
were under attack. Siemens had designed the input process ima

technologies. Building management systems are not only more tightly

… and the

REALITY?

There is no „THE SMART BUILDING!11!!“



How many are online accessible?

- Nobody knows!
- Estimations exist
- Malchow and Klick (2014) counted building automation environments
  - Most were found in the US (circa 15.000)
  - of the found BAS, 9% were linked to known vulnerabilities

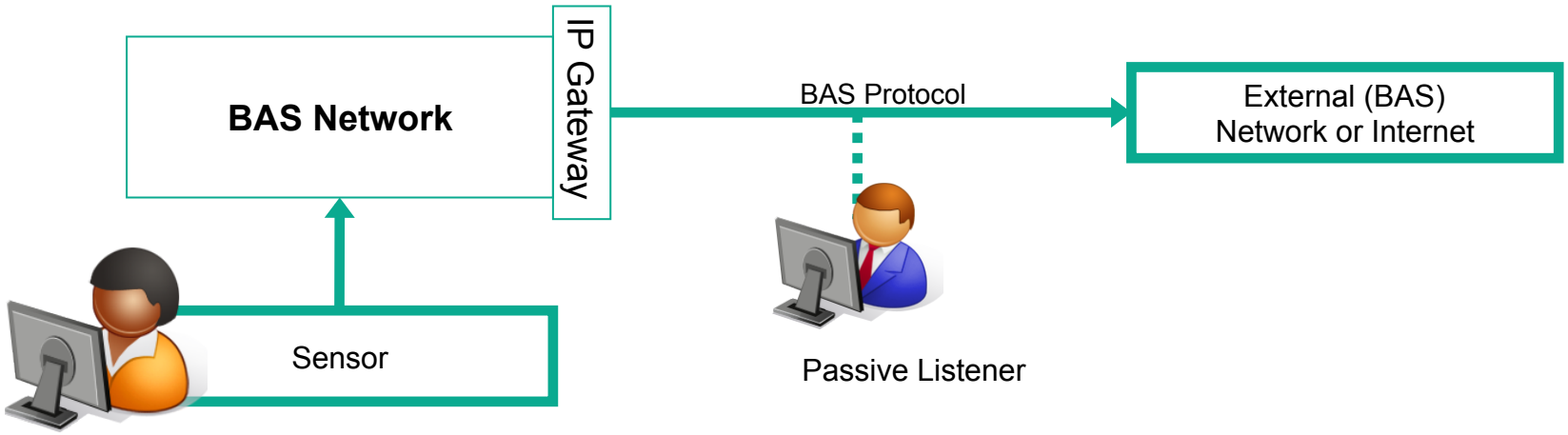
- Alternative: local/regional BAS wardriving
  - …we presented it already in 2012 ☺

Security in Smart Buildings

- First issues arose in the 1990‘s
- Internet of Things increases security concerns
- Easy to apply attacks known from TCP/IP (e.g. spoofing)
- Focus of vendors: security << functionality
  - Lack of security awareness
  - Legacy hard- and software (security means are not always implementable)
  - Patchability problem
  - Insecure web-interfaces / remote access

Data Leakage via BAS

- Active / passive data leakage using remote connection of a BAS
- Used for legitimate purpose (administration of remote buildings)



Source: Wendzel, S., Kahler, B., Rist, T.: Covert Channels And Their Prevention In Building Automation Protocols: A Prototype Exemplified Using BACnet, Proc. CPSCom, IEEE, 2012.

Not enough

DRAMA!?!???!??

Smart Building Botnets (SBB)

Short Definition:

- A botnet consisting of BA systems
  - bots placed either on control units
  - … or remote-control is directly performed (no bot necessary)
- Utilize physical capabilities of BAS to perform malicious actions
  - no spamming, no DoS, …
  - novel scenarios instead!

Source: Wendzel, S., Zwanger, V., Meier, M., Szlosarczyk, S.: Envisioning Smart Building Botnets, in Proc. Sicherheit, GI, Vienna, 2014.

Smart Building Botnets (SBB)

How to build it?

- Search Shodan
- Perform BAS Wardriving
- GPS-enabled smartphones with malware

Source: Wendzel, S., Zwanger, V., Meier, M., Szlosarczyk, S.: Envisioning Smart Building Botnets, in Proc. Sicherheit, GI, Vienna, 2014.

Example 1: Mass Surveillance

Remote access to sensor data

- Monitoring of sensor values and actuator states (temperature, presence, heating levels, …)
- Who in a smart city goes so often to the bathroom each night and is probably ill?
- When can a break-in attempt to a building or whole street be performed at the optimal moment? … and where exactly?

Source: Wendzel, S., Zwanger, V., Meier, M., Szlosarczyk, S.: Envisioning Smart Building Botnets, in Proc. Sicherheit, GI, Vienna, 2014.

Scenario 2: Oil / Gas Producer

Thinkable regional attack

- Slightly increase heating levels in smart buildings over night
- … to sell more oil or gas
- Not easy to keep a low profile!
  - e.g. determining vacant rooms using observation

Source: Wendzel, S., Zwanger, V., Meier, M., Szlosarczyk, S.: Envisioning Smart Building Botnets, in Proc. Sicherheit, GI, Vienna, 2014.


WE AIL
GONNA
DIE!

Network Communication in BAS:

NETWORK PROTOCOLS

Various Protocols Exist

- Closed Protocols / Open Protocols
- EIB/KNX, LONtalk, BACnet are most widely used
- We focus on BACnet …

BACnet in a Nutshell
Overview

- Building Automation Control and Network (BACnet)
- A leading protocol in BAS
    - (remote) control and management of smart buildings
    - monitoring of buildings and according devices
- Data and communication of all devices specified in ISO-Standard 16-484-5
- Worldwide more than 730 vendors

BACnet in a Nutshell

Comparison to OSI Layer Model

- Defines four layers

OSI Layer	BACnet Stack Protocol				
Application	BACnet Application Layer				
Network	BACnet Network Layer				
Data Link	BACnet/IP over ISO 8802-2 LLC		MS/TP	LONTalk	...
Physical	Ethernet	ARCNET	RS485		...

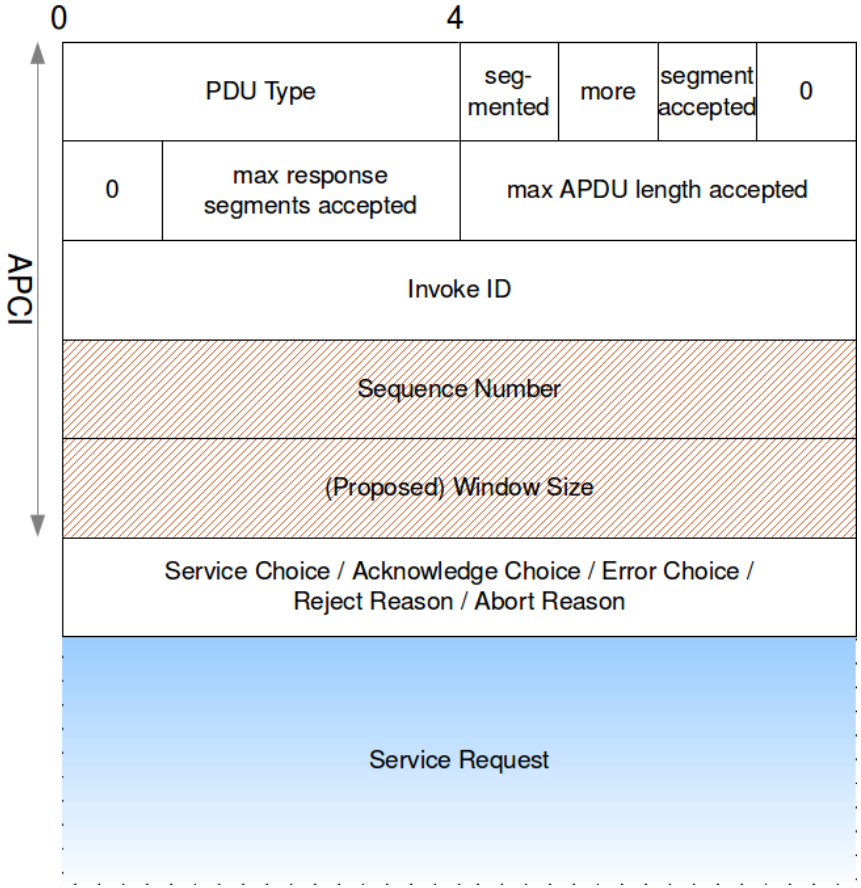
BACnet in a Nutshell
NPDU

- Network Protocol Data Unit (NPDU) serves for communication of all the devices on network layer
- Control flow and address resolution are managed with Network Protocol Control Information (NPCI)
- Opportunity to prioritize messages
- Payload depicted in Network Service Data Unit (NSDU)
  - network message, e.g. Who-Is
  - contents of application action (APDU)

	Octet	Description
NPCI	1	Version
	1	NPCI Control Octet
	2	Destination Network (DNET)
	1	Dest. Address Length (DLEN)
	Variable	Destination Address (DADR)
	2	Source Network (SNET)
	1	Source Address Length (SLEN)
	Variable	Source Address (SADR)
	1	Hop Count
NSDU	Variable	Network Layer Message or Application Layer Protocol Data Unit (APDU)

BACnet in a Nutshell
APDU

- Application Protocol Data Unit (APDU) serves for communication of all the devices on application layer
- Datagram type (PDU Type) and segmentation information are managed via Application Protocol Control Information (APCI)
- Payload depicted in Service Request field
  - Request /response for / of application action of a device
  - encoded in ASN.1



Fraunhofer FKIE

Behind the scenes

EXPLOITING BUILDING AUTOMATION PROTOCOLS

Fraunhofer FKIE

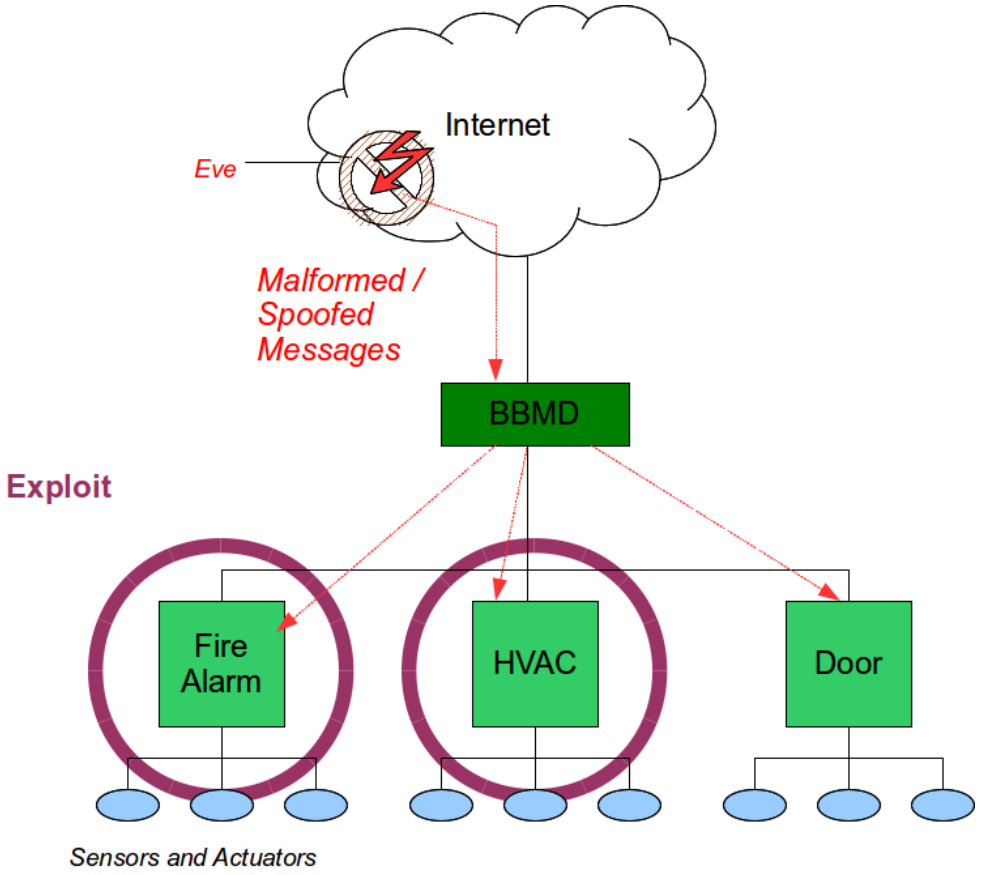
Practical security flaws in BACnet

- Authentication and encryption means are specified by the standard, nevertheless they are rarely implemented
    - Interrogation / scanning made possible
- Large attack surface (few were already known before)
    - Smurf-like attack
        - Router Adv. Flooding
    - Traffic Redirection
    - DoS Re-Routing
    - Malformed Messages
    - Inconsistent Retransmissions

Behind the scenes: Exploiting BAS

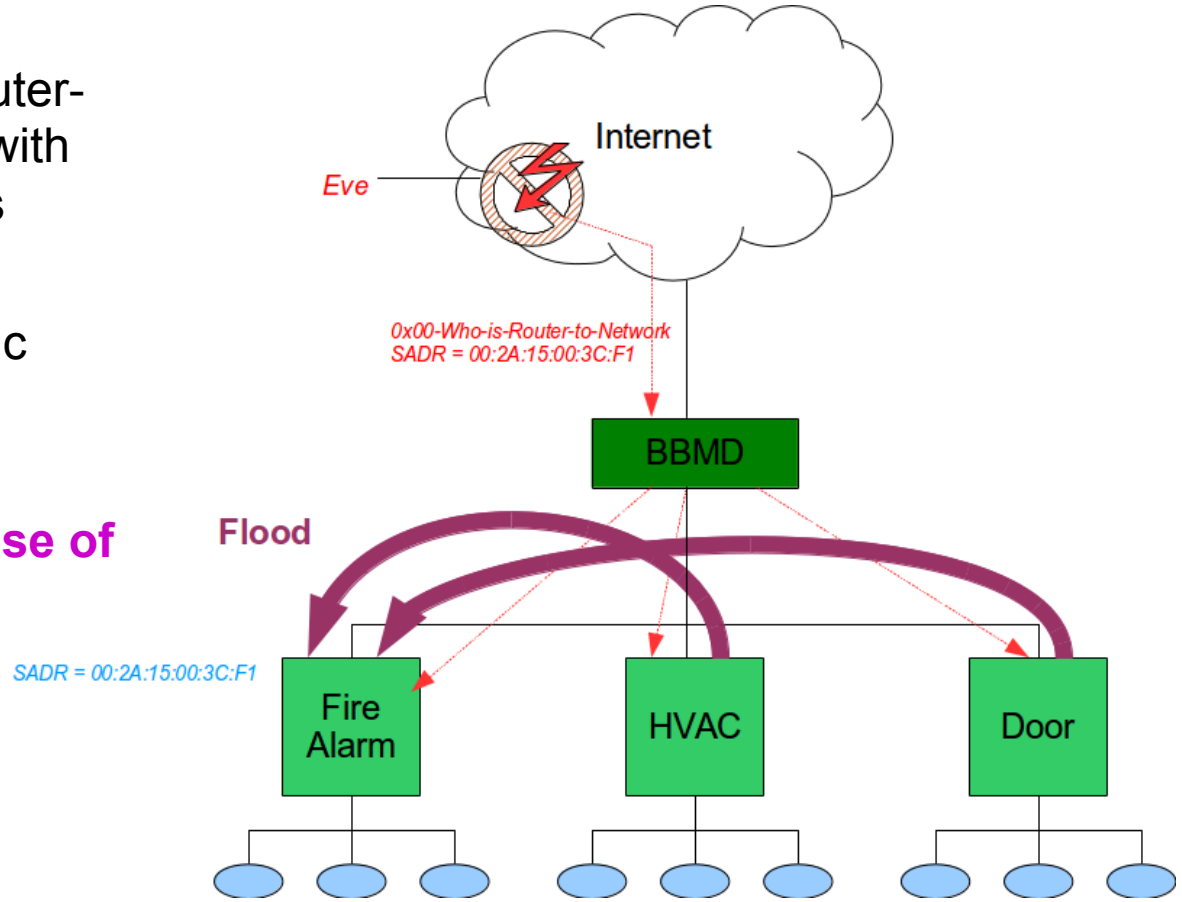
Attacking scenario

- Attacker Eve: Sends malformed or spoofed messages remotely to one or more devices in the BAS subnet
- BACnet Broadcast Management Device (BBMD) routes all the messages to the corresponding destination device
- **Exploitation of device by Eve**



Behind the scenes: Exploiting BAS
Smurf Attack

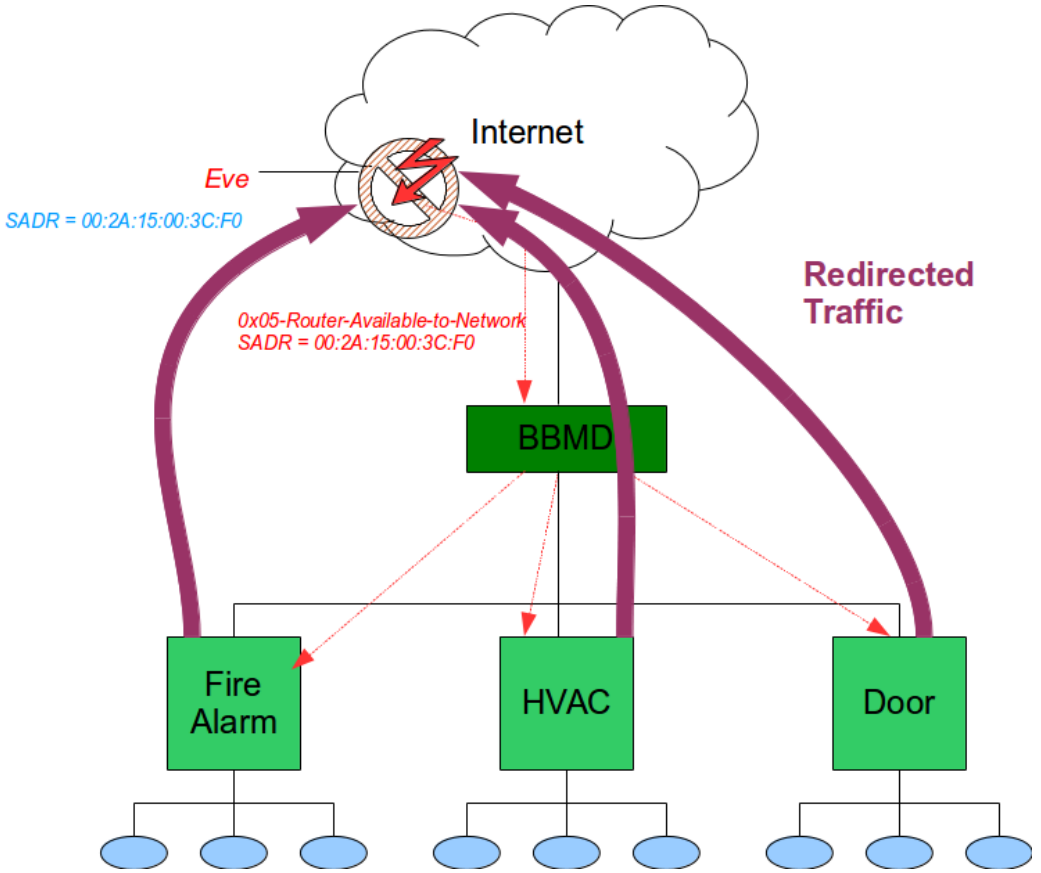
- Eve spoofs Who-is-Router-to-Network messages with victim's source address
- Victim receives all the outgoing/incoming traffic from all devices in the subnet
- **Exploit: DoS in the case of a too large amount of messages**



Behind the scenes: Exploiting BAS

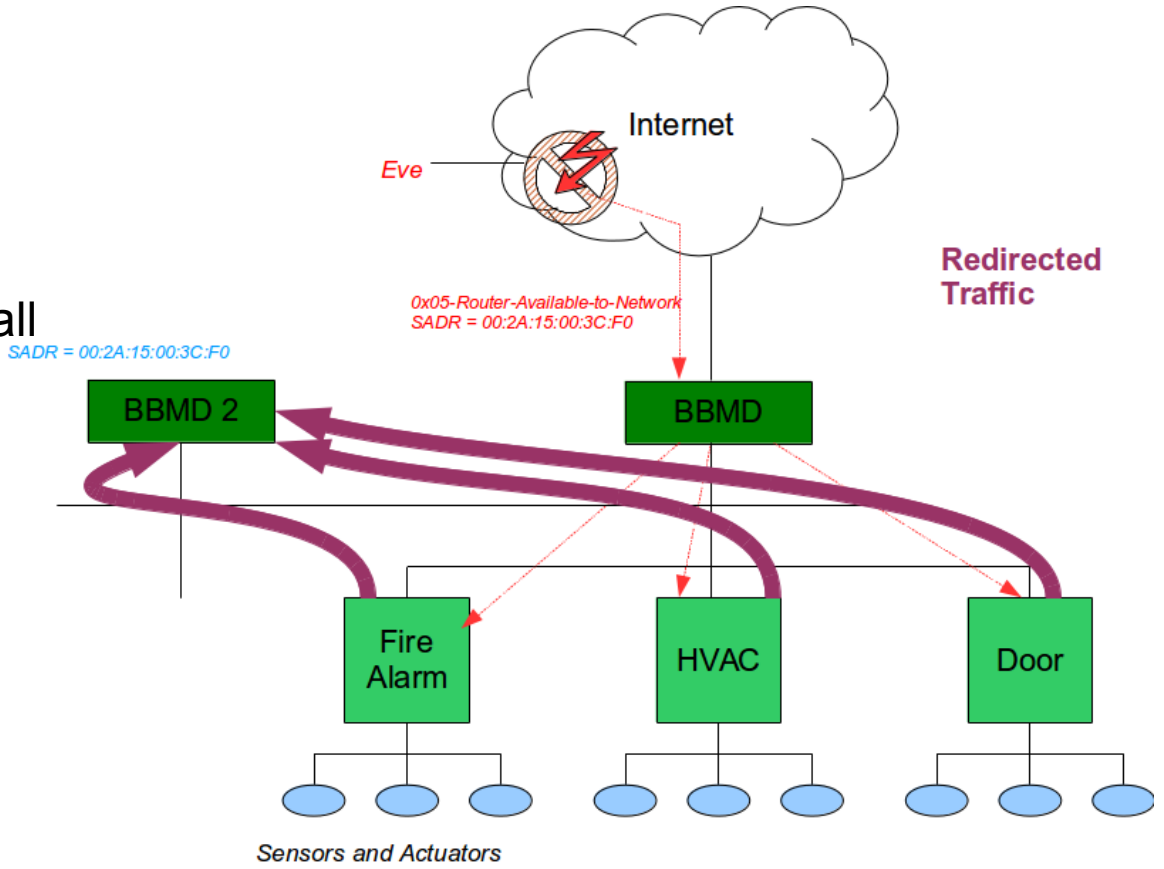
Traffic Redirection

- Eve fakes *selected* Router-Available-to-Network messages
- BBMD simply forwards all incoming and outgoing messages
- **Exploit: Eve receives ALL routed messages as the devices register her as "HOP"**



Behind the scenes: Exploiting BAS
DoS Redirection

- Eve spoofs Router-Available-to-Network messages with victim router's source address
- BBMD simply forwards all incoming and outgoing messages
- **Exploit: DoS of router**



Behind the scenes: Exploiting BAS

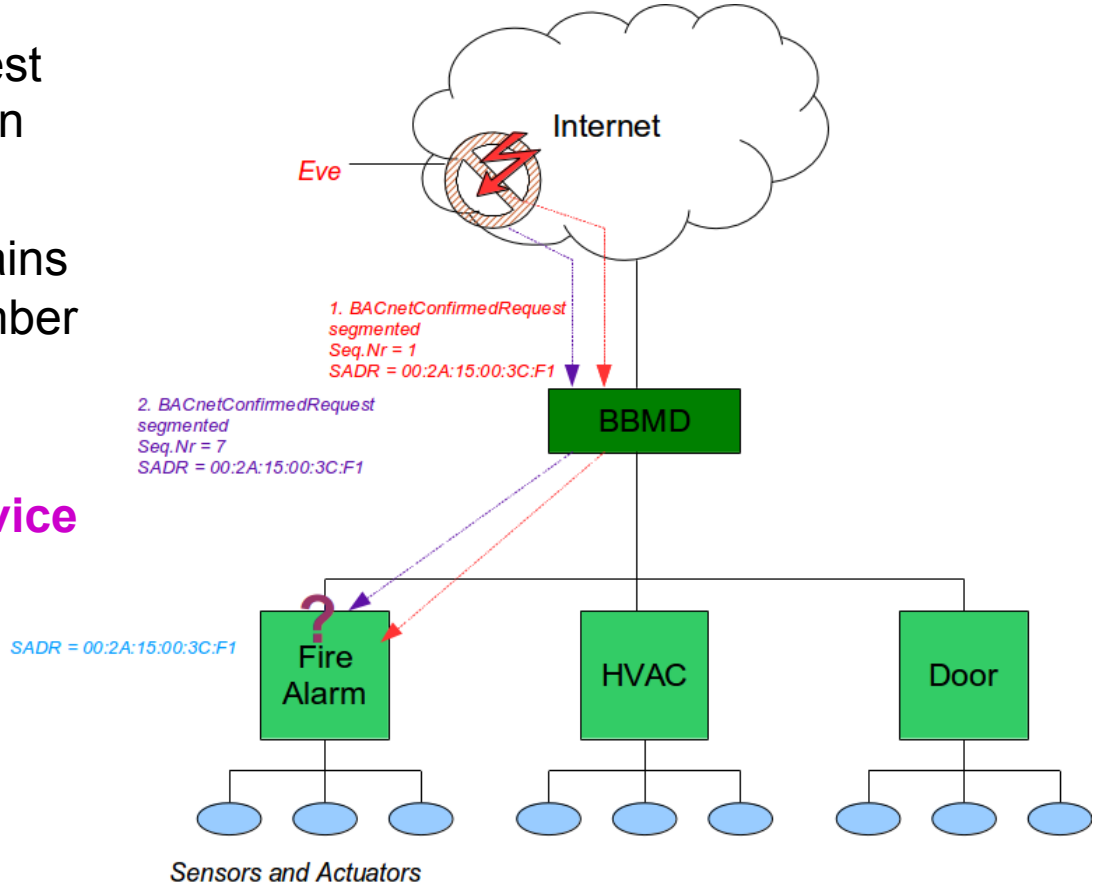
Inconsistent Retransmissions: Segmentation flaws

- Possibility of sending incorrect sequenced segments/fragments
  - Overlapping fragments
  - Replied fragments
  - Time-out fragments
- Devices cannot cope with wrong segmentation
- **Exploit: We cannot ensure inconsistent re-transmission is handled by all BACnet stack implementations of >730 vendors -> Protection required.**

Behind the scenes: Exploiting BAS

Segmentation flaws

- 1: BACnetConfirmedRequest with segmentation indication (seq.nr. = 1)
- 2: Following segment contains mismatched sequence number (seq.nr. = 7)
- **Exploit: Inconsistent Re-transmission leads to device crash**



Fraunhofer FKIE


I told you so...

Our Solution to prevent attacks

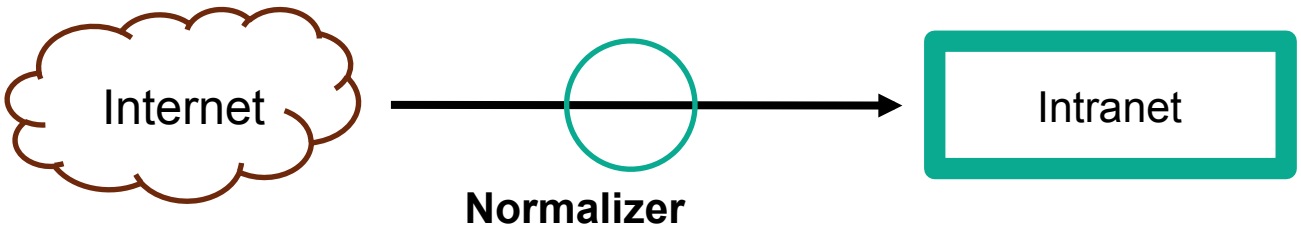
ALICE'S EVIDENCE - TRAFFIC NORMALIZATION FOR BACnet

Fraunhofer FKIE

Traffic Normalization

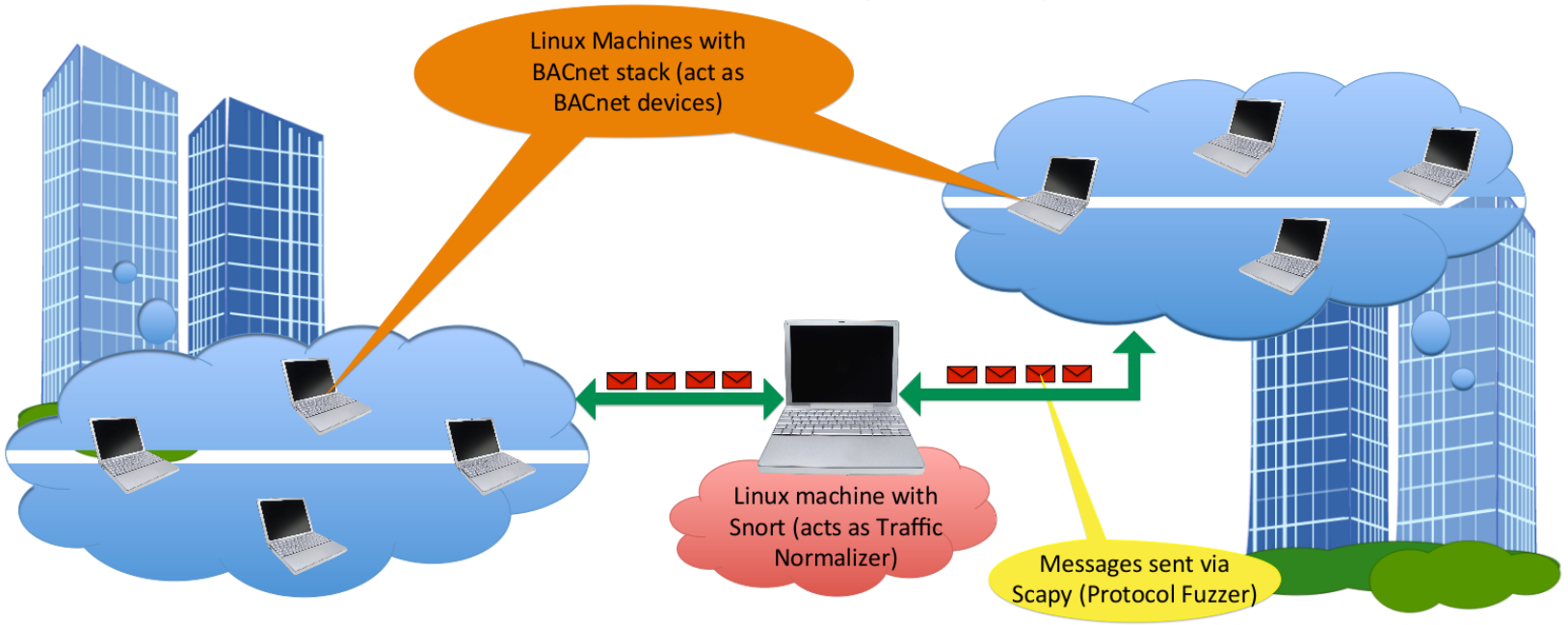
Methodology

- Eliminates ambiguities and prevents devices of proposed attacks, e.g. several types of Denial of Service (DoS) on network layer
- Limits address spoofing
- Can ensure standard conforming network traffic
- **Ability to secure legacy systems which are not patchable**
  - independent of any platform
- can be integrated into each network protocol



Traffic Normalization
Solution for BACnet

- Integration into Snort's Traffic Normalizer
  - as extension with own BACnet stack!
- Testbed:



Fraunhofer FKIE

Potential
Intrusion Prevention

- Prevention of a subset of presented attacks
- Traffic Normalization as preliminary *Intrusion Prevention*
- Implementation of *stateful context-filter* made possible
  - Caching application payload
  - Matching requests to corresponding responses
  - Application-related threats are prevented
- Forensic purposes

Potential

Anomaly Detection – Example on basis of heating device

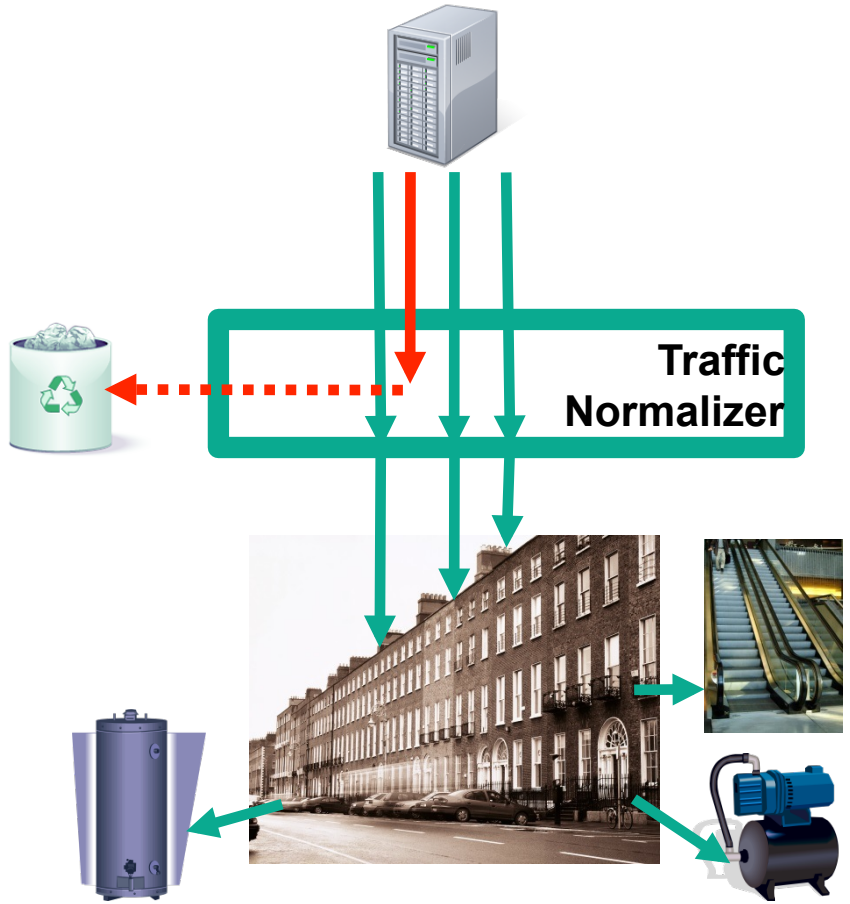
- Collection of state samples
- Learning of discrete states
- Modelling state-based anomaly recognition
- Modelling n-grams

- Heating time and temperature
- Interaction with temperature measurement device
- Winter (if it is cold) -> heating is turned on
- Summer (if it is warm) -> heating is turned off
- e.g. Midsummer (~35°C, but heating „burns“)
- Modelling n-grams, to detect abnormal state
- *Prevention*

Summary

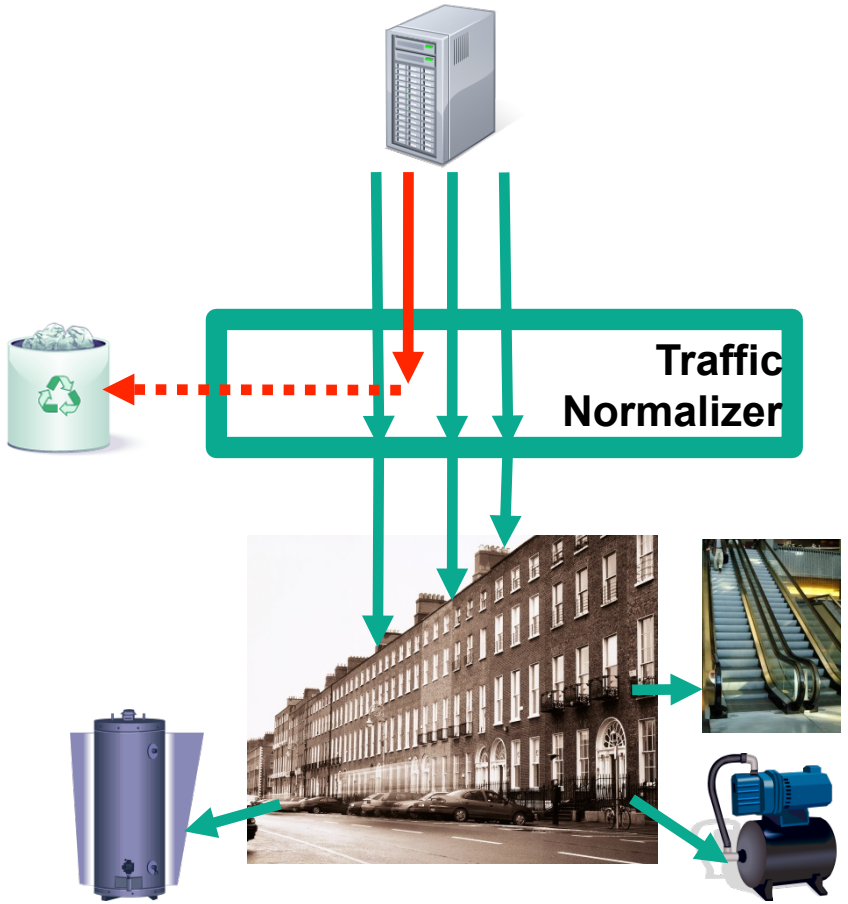
Summary: IT Security for BAS

- **Main concerns:** Prone to many current and future security attacks such as
  - Network attacks: Manipulation, fabrication or interruption of the transmitted data over the network
  - Overlay Networks
  - Botnets: Utilize physical capabilities (like sensors, actuators) of buildings and enable to novel attacks



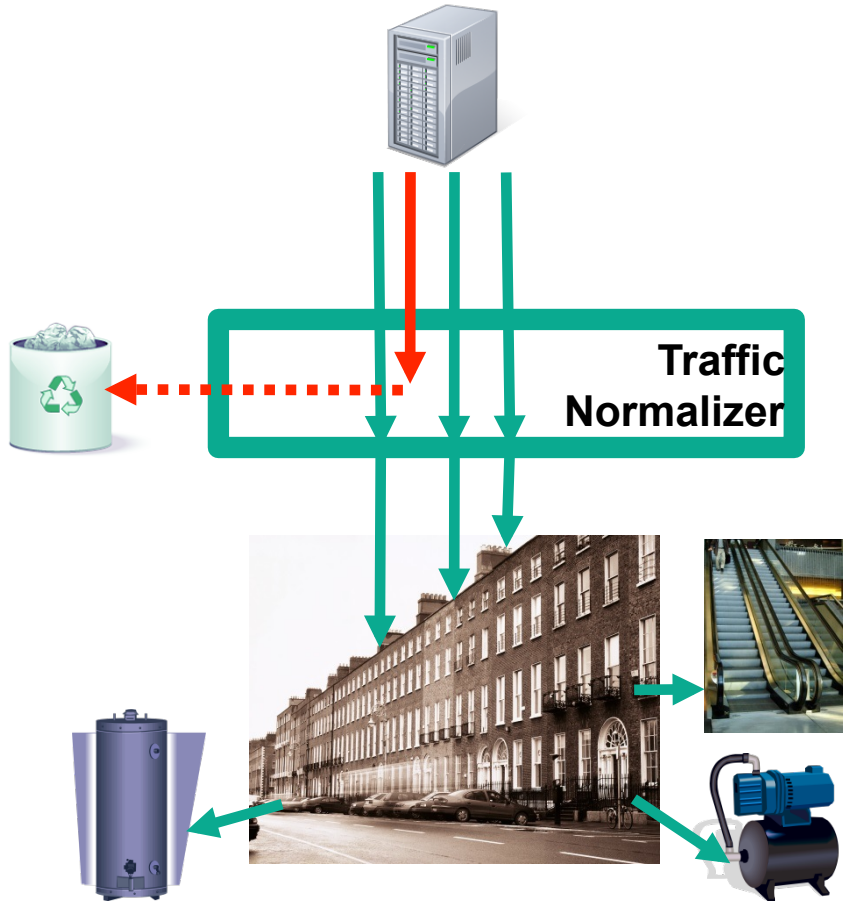
Summary: IT Security for BAS

- **Main concerns:** Prone to many current and future security attacks such as
  - Device attacks:
  - i) Physical level: component replacement, microprobing
  - ii) Software level: code injection, exploiting algorithm



Summary: IT Security for BAS

- Our Contribution: **FKIE Traffic Normalizer**
  - Eliminates an attack before it reaches the building equipment
  - Drops/modifies the network traffic using normalization rules based on protocol specification
  - Can be used between organizational sites, buildings and floors



Thank you for your attention!

Our Expertise:

- Secure Building Automation
- Data Leakage Protection
- Network Steganography/
  Network Covert Channels

Steffen Wendzel
Head of Secure Building Automation
Cyber Defense Research Group
Fraunhofer FKIE
steffen.wendzel@fkie.fraunhofer.de

http://www.wendzel.de

Sebastian Szlósarczyk
Researcher
Cyber Defense Research Group
Fraunhofer FKIE
sebastian.szlosarczyk@fkie.fraunhofer.de

Fraunhofer FKIE