(in)security in building automation – how to create dark buildings with light speed

Who I am

Present:

- Co-founder Limes Security, ICS & SDL security consultancy
- Professor for IT Security at FH St. Poelten, Austria
- Honorary Professor for Cyber Security at DeMontfort University
- SANS Community Instructor for ICS

Past:

- Former Head of Siemens ProductCERT
- Lead Stuxnet Incident Handler at Siemens

Hacking building control can have serious effects on your health

Disclaimer

Do not hack building control systems

1) without authorization
2) unless you‘re sure which part of the system you‘re messing with and what its effects are

to boldly go, where no man has gone before.

how we started hacking building automation systems for fun (and profit)

Office staff blinded by the sun unite!

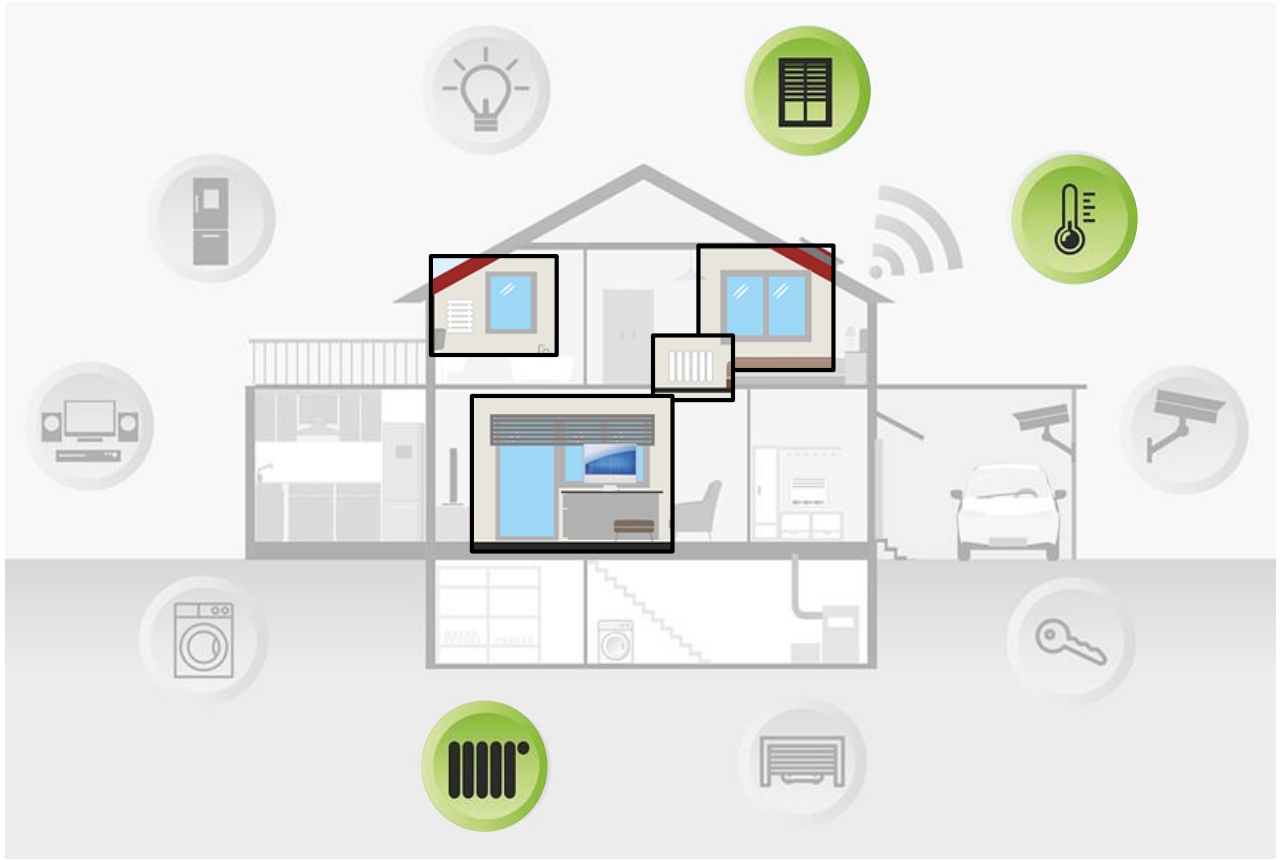
–– Outcry of an annoyed employee

there's no place like home (automation)

discussing building automation use cases

some like it hot. For the rest of us there‘s HVAC.

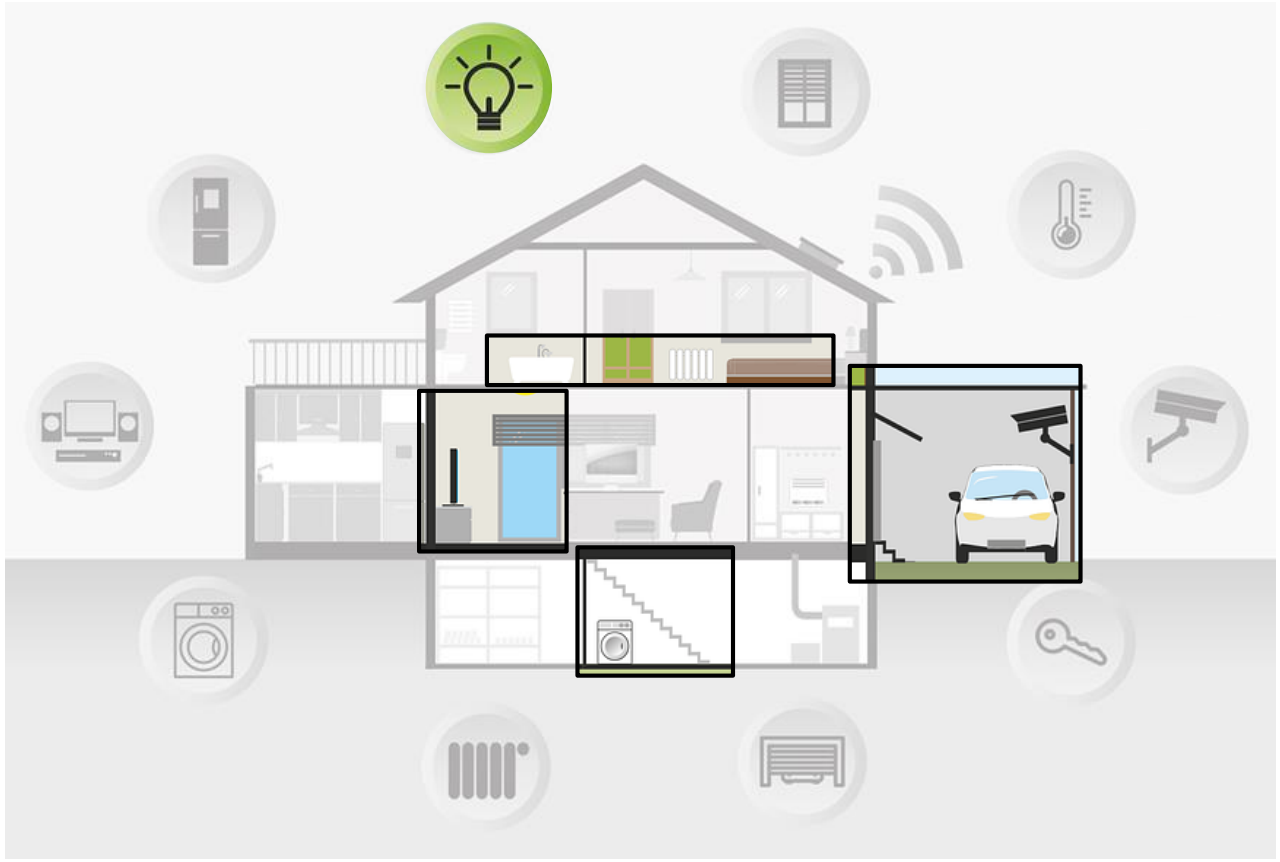
application area – heating, ventilation and air conditioning



Source: https://pixabay.com/en/smart-home-home-technology-2005993/

light switches are dead. motion detector - live long and prosper!

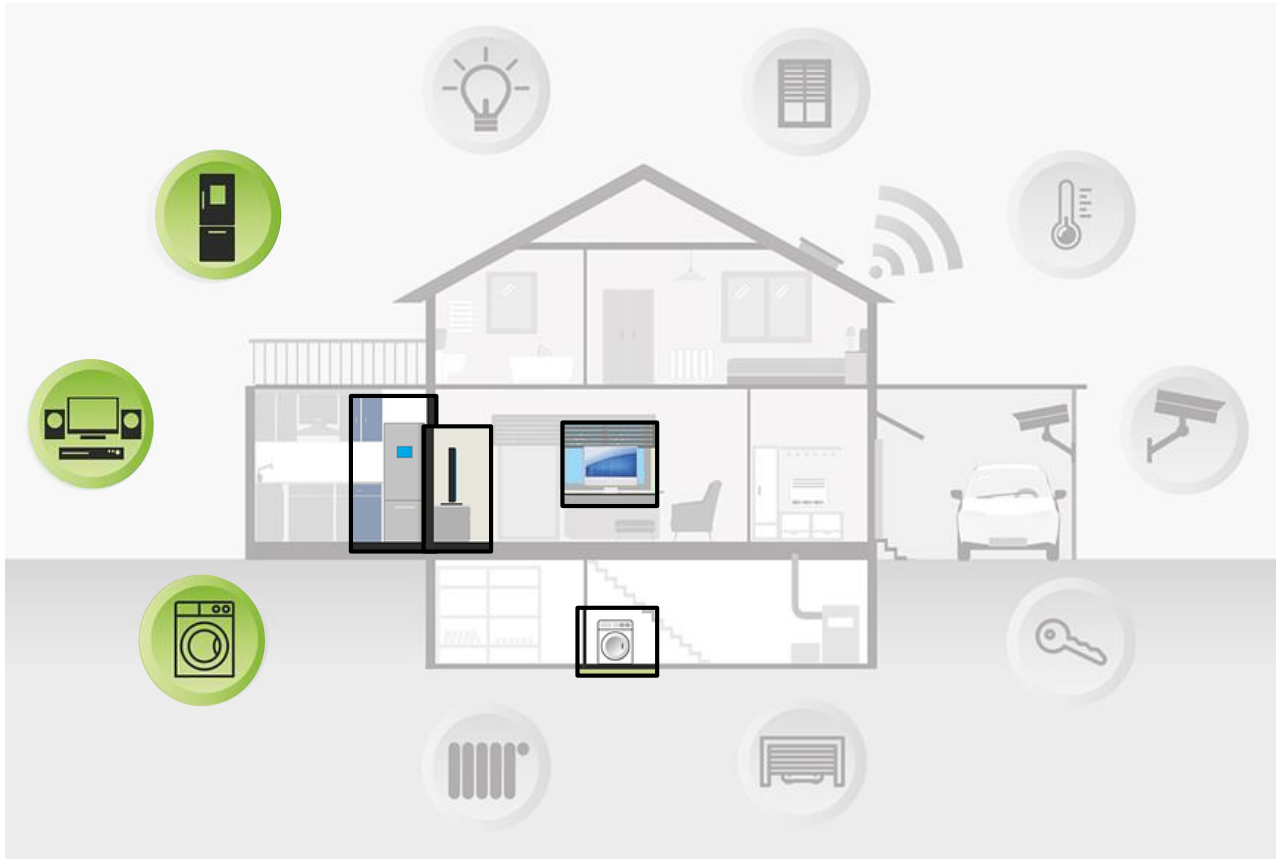
Application area – lighting



Source: https://pixabay.com/en/smart-home-home-technology-2005993/

energy flows where attention goes

application area – energy management & saving



Source: https://pixabay.com/en/smart-home-home-technology-2005993/

you shall not pass!

application area – physical access control

Source: https://pixabay.com/en/smart-home-home-technology-2005993/

with great power there must also come great responsibility

the (smart) home awakens

Source: https://pixabay.com/en/smart-home-home-technology-2005993/

try not. do, or do not. there is no try.

the state of security functions in building automation

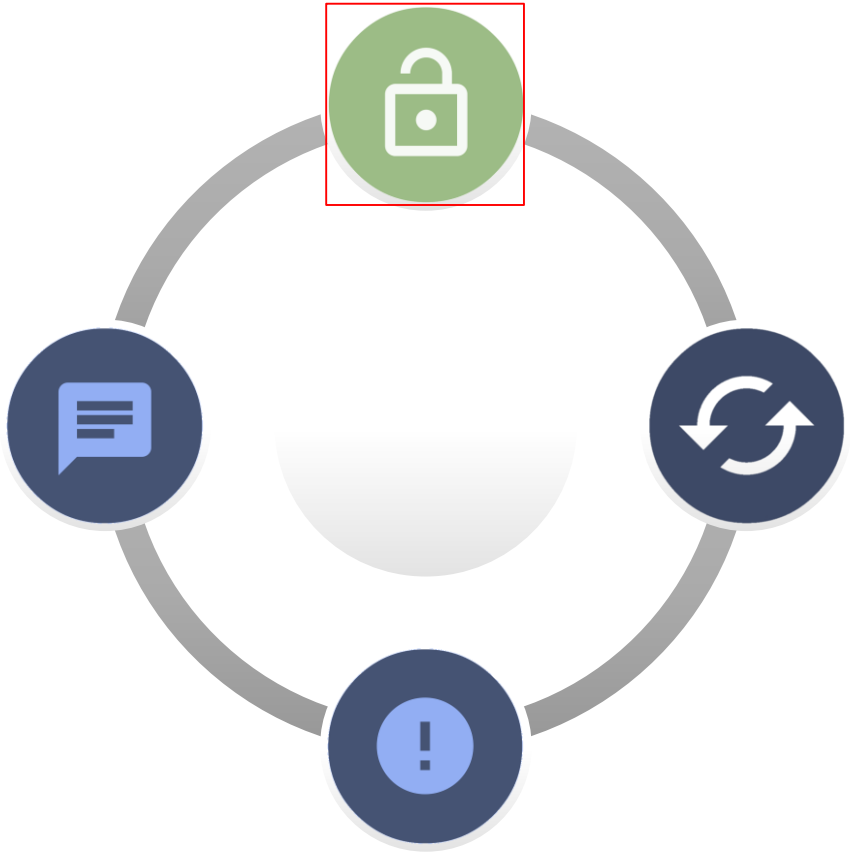
After very careful consideration, sir, I've come to the conclusion that your new defense system sucks

The state of native security functions in building automation:

This page intentionally left blank

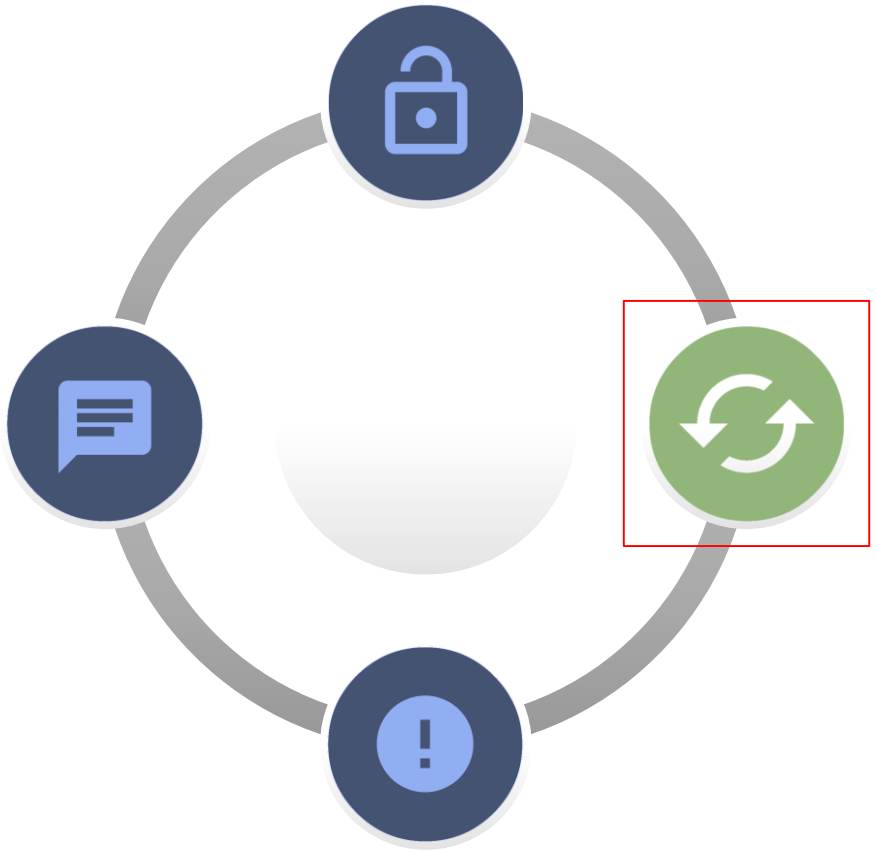
you had me at hello!

missing authentication at protocol level



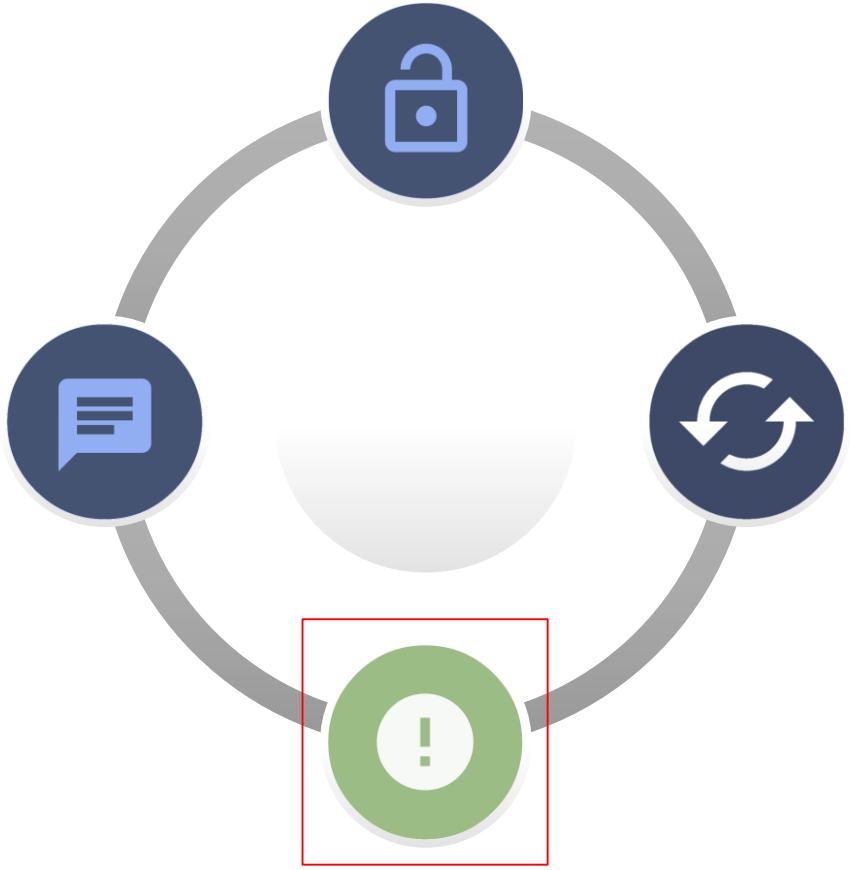
you talkin' to me?

protocols susceptible to replay/spoofing



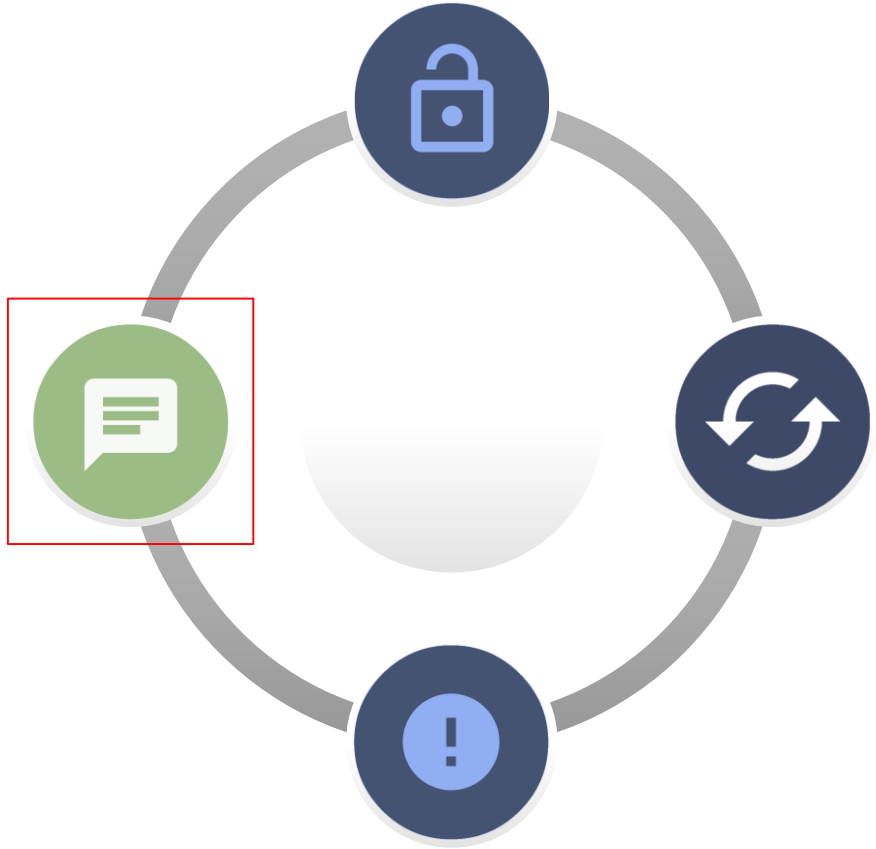
greetings, programs!

outdated / legacy software



houston, we have a problem!

robust and purpose-built, but fragile from the network side



yippie-ki-yay, motherf—r!

building automation attack scenarios we are (NOT) looking forward to

step 1: money's only something you need in case you don't die tomorrow

the different ransom(ware) - attack outline

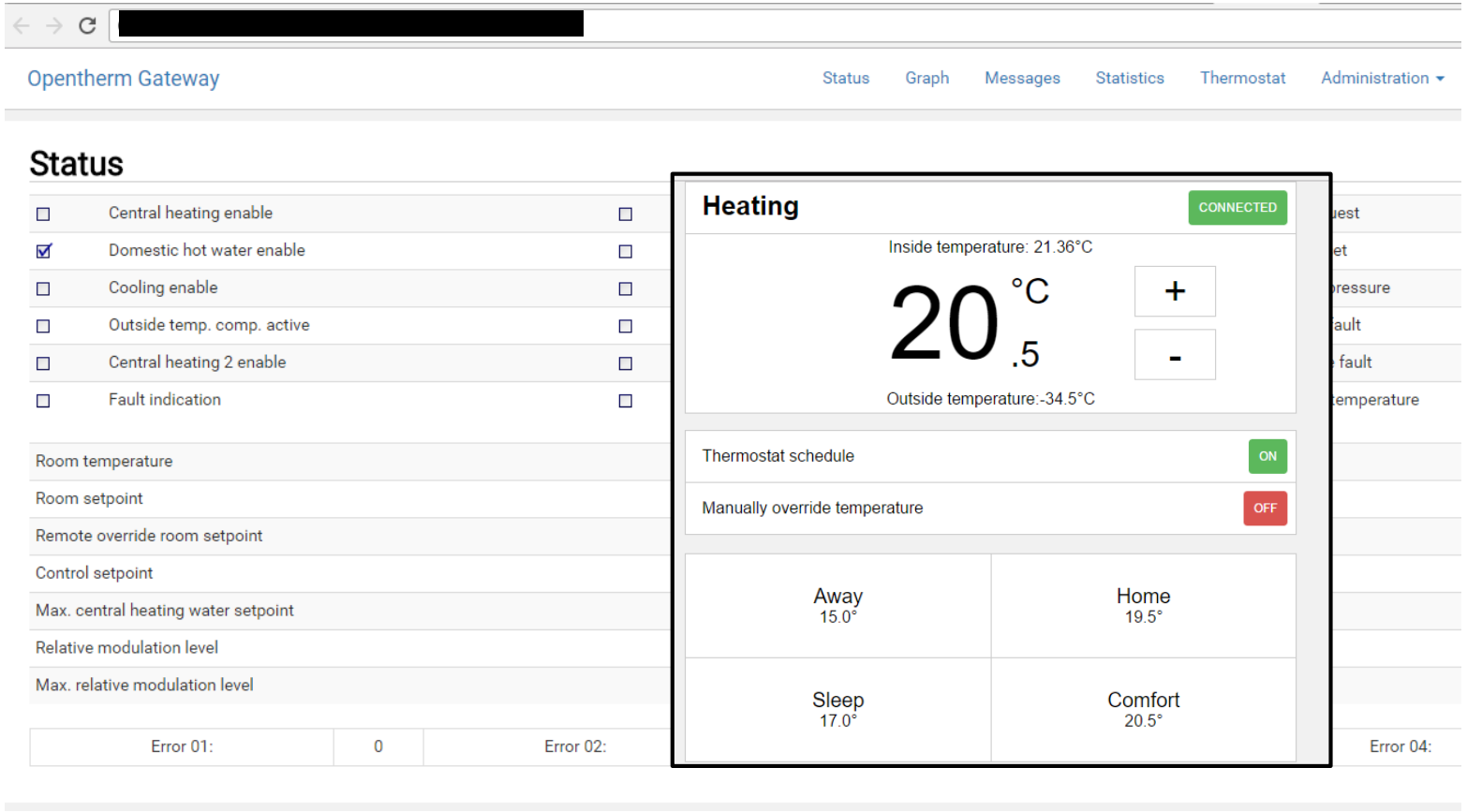
looking for hvac victims

attack preparation

attack mode: ON

step 2: you are the chosen one!

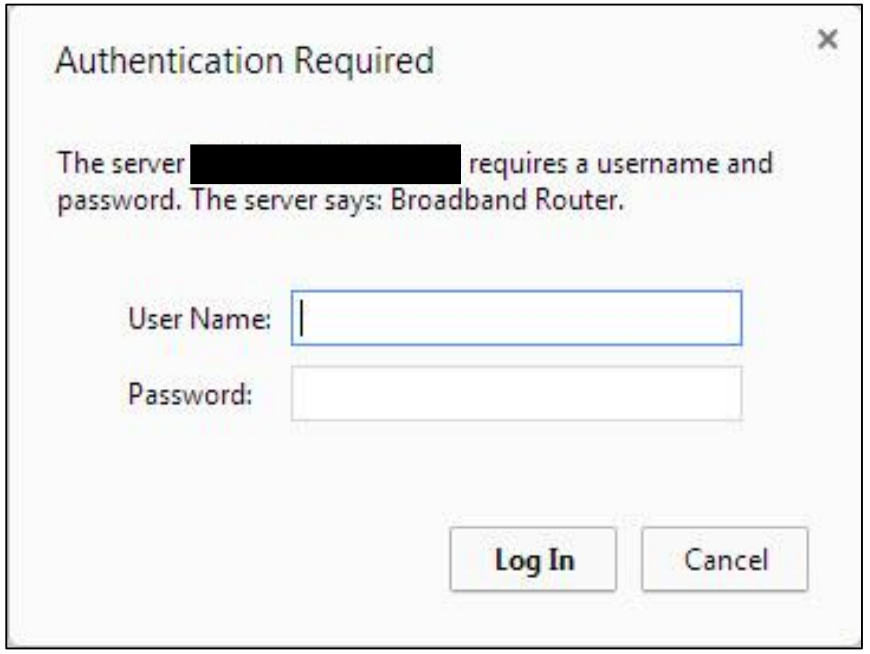
the different ransom(ware) - finding convenient victims



step 3: what's your name? who's your daddy?

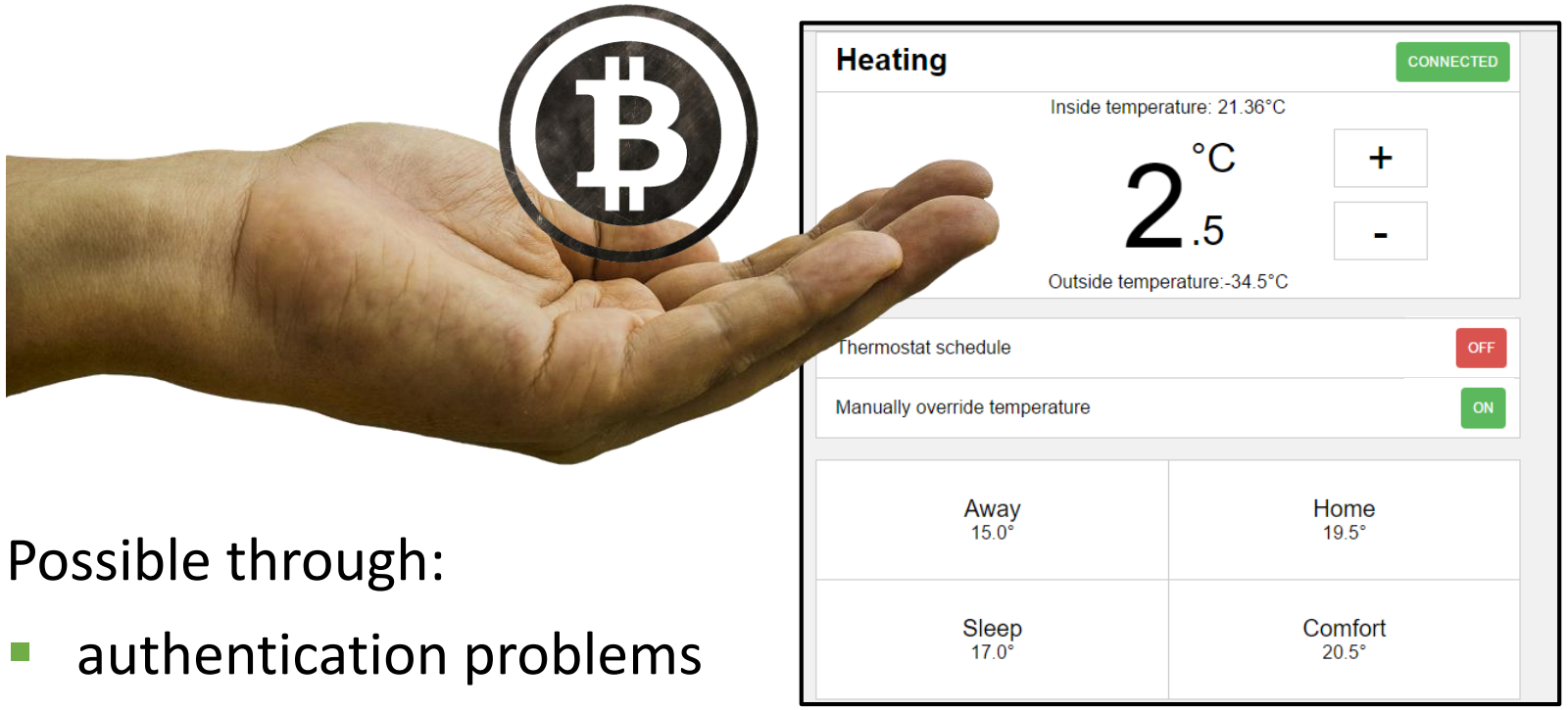
the different ransom(ware) - getting contact info for our business proposal

- Options for learning the system owner‘s email address for our ransom demand
  - Email address stored for alarming
  - Email address displayed in interface
  - Username
  - Whois
  - Imprint



step 4: i'll make him an offer he can't refuse

the different ransom(ware) - patience! you get the chicken by hatching the egg, not smashing it



Possible through:

- authentication problems
- authorization problems
- awareness issues through vendors and operators

step 1: I don’t meet the competition – I crush it

A targetted attack of a different kind - attack outline

visit sites run by competing property management

Add rogue device

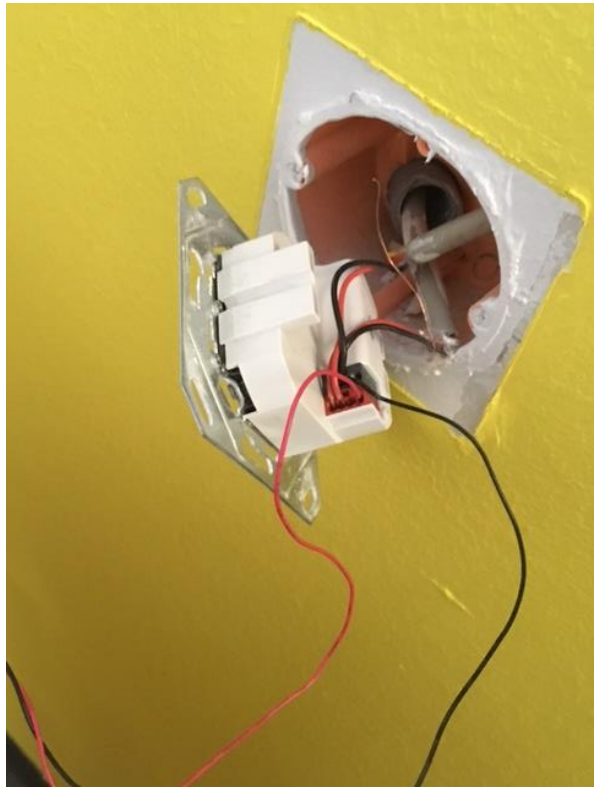
Trigger random fire / gas /security alarms

step 2: these are not the sensors you're looking for

A targeted attack of a different kind – finding appropriate entry points to the building network

step 3: pay no attention to that man behind the curtain

i'm going in – placing rogue devices for persistence on the building automation network



step 4: ooh, ahhh, that's how it always starts. Then later there's running and screaming

Sleep is for the weak– triggering alarms through spoofed messages, fake sensor readings or engineering changes

Possible through:

- access control issues (new/rogue devices)
- authentication problems
- integrity problems (changes in engineering)
- missing intelligence (sanity checks possible?)

black hat USA 2017

roads? Where we're going we don't need roads

pentesting tooling for approaching building automation systems

I will find you and I will kill you

State of information gathering for building automation devices

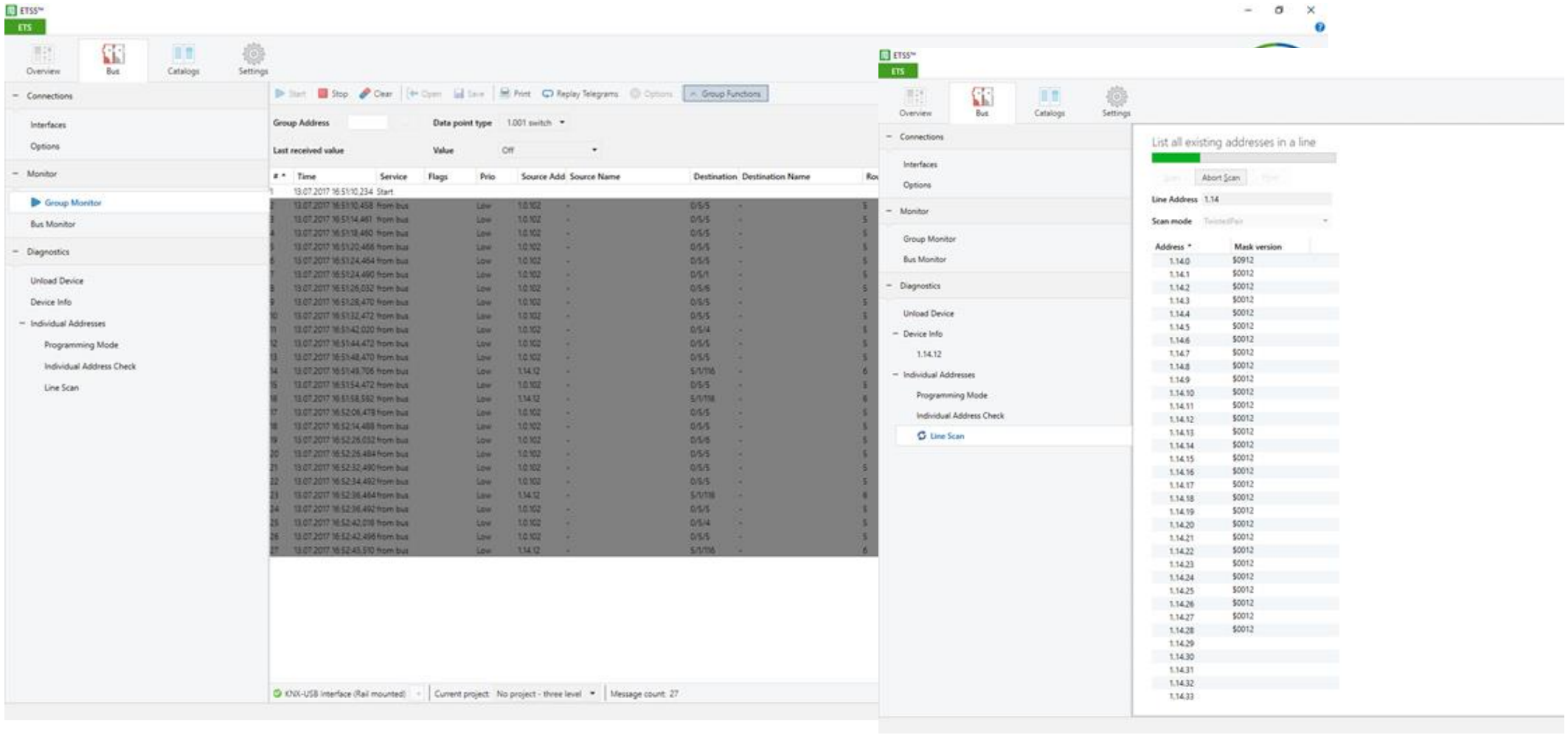
- Available projects
  - Nmap nse scripts (https://github.com/nmap/nmap/tree/master/scripts)
  - Project redpoint (https://github.com/digitalbond/Redpoint)
  - HVACScanner (https://github.com/musicmancorley/HVACScanner)
  - Nessus (https://www.tenable.com/plugins/index.php)
- Detection and enumeration of
  - BACnet/IP devices
  - KNXnet/IP devices
  - Modbus devices
  - Honeywell HVACs
  - Tridium Niagara controller

KNX protocol 101

- Designed to be independent of the used hardware platform
- Components: sensors, actuators and system devices and compontents
- Different transmission media supported
  - KNX TP (twisted pair), KNX RF (radio frequency), **KNXnet/IP (TCP/IP)**, …
- KNXnet/IP groups of services
  - Core services (locating and identifying KNXnet/IP devices)
  - Device management services (configuration)
  - Tunneling (for point-to-point communication)
  - Routing (runtime communication)
  - Remote diagnostic and configuration

i’m sorry, Dave. i’m afraid I can’t do that.

(ab)using KNX ETS for security purposes



engage!

security-relevant KNXnet/IP commands

- SEARCH_REQUEST
  - Enumerate available KNXnet/IP server
- ROUTING_INDICATION
  - Tell the router to send KNX packets via IP to a given address
- DEVICE_CONFIGURATION_REQUEST
  - Read and write the configuration of a device
  - Configuration can be protected with BCU key (0xFFFFFFFF)

gentlemen, you can't fight in here! this is the war room!

tooling for pentesting KNXnet/IP

KNXmap (https://github.com/takeshixx/knxmap/)

- Scanning
- Bus Monitoring
- Key Bruteforcing
  - Tries to bruteforce the authentication key for the configuration (BCU key)
- Group Messaging
  - Write arbitrary values to any group address on the bus
- APCI Functions
  - Interact with bus devices for retrieving information, changing configuration values or other maintenance task
  - read/write memory, restart a device, enable/disable programming mode, change authorization key for device,…

gentlemen, you can't fight in here! this is the war room!

tooling for pentesting KNXnet/IP

KNXmap

- Key Bruteforcing
  - Tries to bruteforce the authentication key for the configuration (BCU key)
- Group Messaging
  - Write arbitrary values to any group address on the bus
- APCI Functions
  - Interact with bus devices for retrieving information, changing configuration values or other maintenance task
  - read/write memory, restart a device, enable/disable programming mode, change authorization key for device,…

BACnet/IP protocol 101

- Designed for allowing communication between different building automation devices regardless of the manufacturers or service they perform
- Standard set of „objects“ with standard set of „properties“ and services
- Devices are not required to implement every service (`ReadProperty` mandatory)
- BACnet/IP Broadcast Management Devices (BBMD) & Foreign Device Registration <3
- BACnet/IP groups of services
  - Alarm and event services (monitoring objects and notifications)
  - File access services (read and write files in BACnet devices)
  - Object access services (read/write/modify properties and add/delete objects)
  - Remote device management services (special message transfer, adressing, auto-configuring)
  - Virtual terminal services (text-based connection to application program on a remote device)

use the force Luke!

Security-relevant BACnet/IP commands for discovery / information gathering

- Information gathering
  - ReadProperty
  - Read-Foreign-Device-Table/Read-Broadcast-Distribution-Table
  - Initialize-Routing-Table (Router returns it‘s routing table)
  - Who-Is

- Spoofing
  - Register-Foreign-Device
  - I-Am-Router-To-Network
  - I-am

You have chosen...wisely

Any BACnet devices exposing internal systems and networks over the internet? Nearly 2k in the US alone…

TOTAL RESULTS

2,873

TOP COUNTRIES

United States	1,917
Canada	560
Australia	45
United Kingdom	43
Finland	36

TOP ORGANIZATIONS

Comcast Business	228
AT&T Internet Services	194
Verizon Wireless	134
Telus Communications	85
Time Warner Cable	78

TOP PRODUCTS

DSM_RTR	303
NiagaraAX Station	269
DSC_1616E	189
eBMGR	183
LGR25	169

[redacted]
Added on 2017-07-17 02:46:20 GMT
United States, Los Angeles
Details
ics

```
Instance ID: 3000
Object Name: [redacted]CityPkwy ACCESS
Vendor Name: Delta Controls
Application Software: V3.40
Firmware: 493842
Model Name: eBMGR-TCH

BACnet Broadcast Management Device (BBMD):
  [redacted]:47808
```

[redacted]
Added on 2017-07-17 02:37:46 GMT
United States
Details
ics

```
Instance ID: 10000
Object Name: MAU1 Router
Vendor Name: Delta Controls
Application Software: V3.40
Firmware: 159693
Model Name: DSM_RTR

BACnet Broadcast Management Device (BBMD):
    192.168.3.5:47808
    192.168.3.3:47808
    192.168.3.2:47808
    [redacted].124:47808
```

[redacted]
Added on 2017-07-17 02:40:32 GMT
Canada, Thornhill
Details
ics

```
Instance ID: 1000
Object Name: [redacted]-Penthouse
Vendor Name: Reliable Controls Corporation
Application Software: 7.42|01,08|01,08|01,08|--,--|--,--|--,--|--,--|--,--|--,--|
Firmware: 7.42|01,08|01,08|01,08|--,--|--,--|--,--|--,--|--,--|--,--|
Model Name: MACH-ProSys

BACnet Broadcast Management Device (BBMD...
```

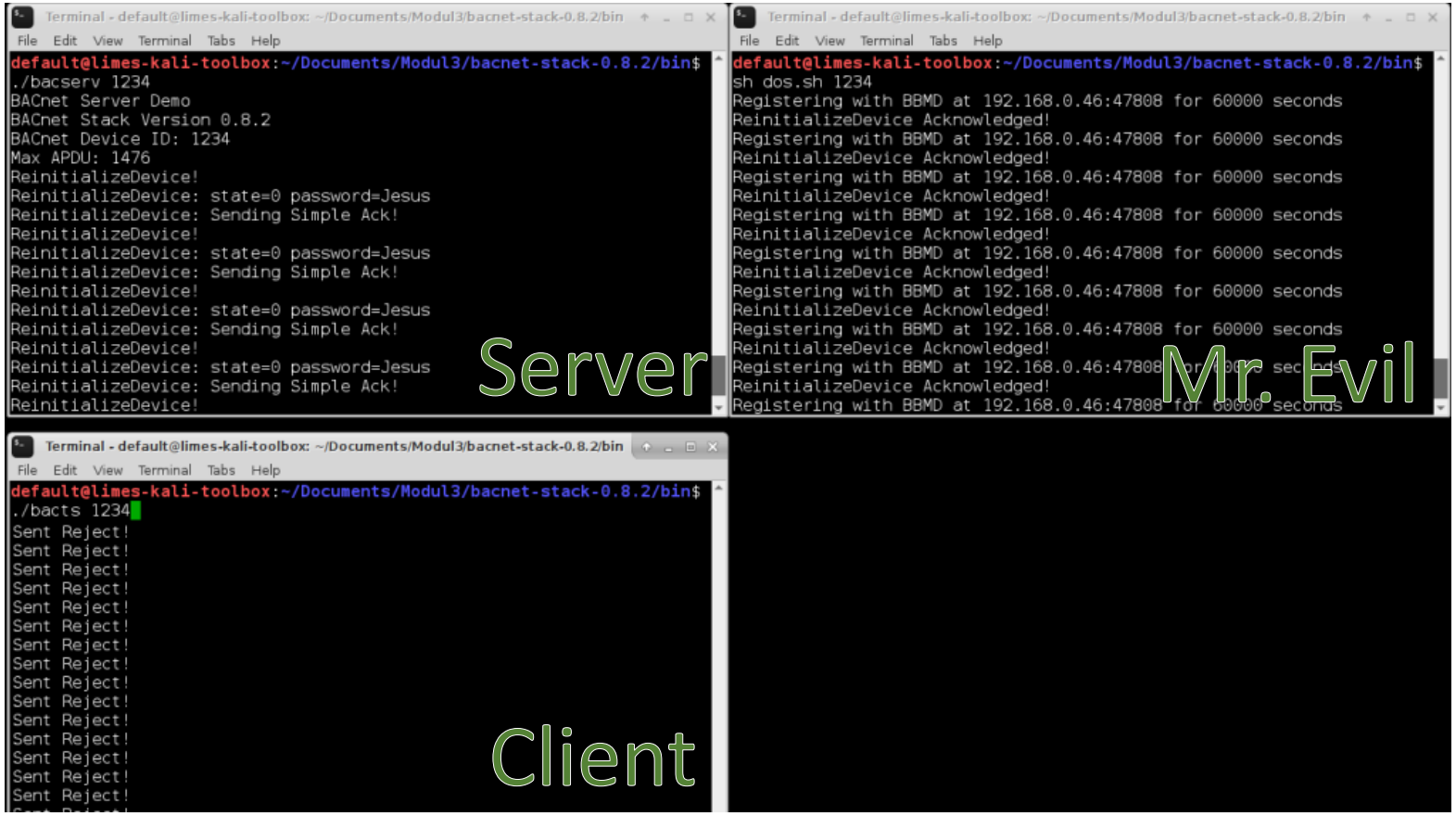
hasta la vista baby

Security-relevant BACnet/IP commands for for manipulation & sabotage purposes

- Denial of service
  - Who-is
  - Router-Busy-to-Network (tell other routers that another network can‘t be reached)
  - Initialize-Routing-Table (Routing Loop)
  - Reinitialize-Device (reboot time)
- Other useful commands
  - WriteProperty

hasta la vista baby

Constantly requesting a device to reinitialize obviously is bad for availability.
Devices password required? Go rtfm



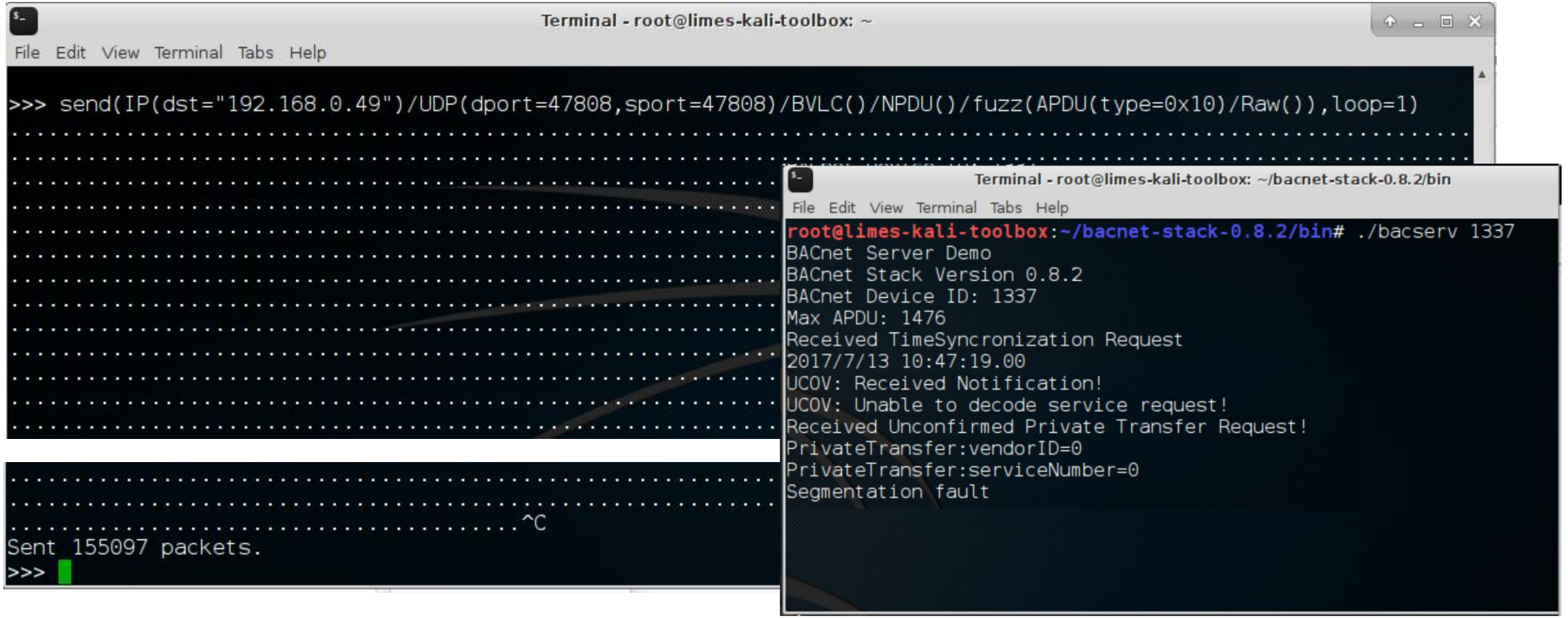
```
default@limes-kali-toolbox:~/Documents/Modul3/bacnet-stack-0.8.2/bin$
./bacserv 1234
BACnet Server Demo
BACnet Stack Version 0.8.2
BACnet Device ID: 1234
Max APDU: 1476
ReinitializeDevice!
ReinitializeDevice: state=0 password=Jesus
ReinitializeDevice: Sending Simple Ack!
ReinitializeDevice!
ReinitializeDevice: state=0 password=Jesus
ReinitializeDevice: Sending Simple Ack!
ReinitializeDevice!
ReinitializeDevice: state=0 password=Jesus
ReinitializeDevice: Sending Simple Ack!
ReinitializeDevice!
ReinitializeDevice: state=0 password=Jesus
ReinitializeDevice: Sending Simple Ack!
ReinitializeDevice!
```

```
default@limes-kali-toolbox:~/Documents/Modul3/bacnet-stack-0.8.2/bin$
sh dos.sh 1234
Registering with BBMD at 192.168.0.46:47808 for 60000 seconds
ReinitializeDevice Acknowledged!
Registering with BBMD at 192.168.0.46:47808 for 60000 seconds
ReinitializeDevice Acknowledged!
Registering with BBMD at 192.168.0.46:47808 for 60000 seconds
ReinitializeDevice Acknowledged!
Registering with BBMD at 192.168.0.46:47808 for 60000 seconds
ReinitializeDevice Acknowledged!
Registering with BBMD at 192.168.0.46:47808 for 60000 seconds
ReinitializeDevice Acknowledged!
Registering with BBMD at 192.168.0.46:47808 for 60000 seconds
ReinitializeDevice Acknowledged!
Registering with BBMD at 192.168.0.46:47808 for 60000 seconds
ReinitializeDevice Acknowledged!
Registering with BBMD at 192.168.0.46:47808 for 60000 seconds
ReinitializeDevice Acknowledged!
Registering with BBMD at 192.168.0.46:47808 for 60000 seconds
```

```
default@limes-kali-toolbox:~/Documents/Modul3/bacnet-stack-0.8.2/bin$
./bacts 1234
Sent Reject!
Sent Reject!
Sent Reject!
Sent Reject!
Sent Reject!
Sent Reject!
Sent Reject!
Sent Reject!
Sent Reject!
Sent Reject!
Sent Reject!
Sent Reject!
Sent Reject!
Sent Reject!
Sent Reject!
```

He‘s dead Jim!

Sneak peak into BACnet protocol stack quality: A rudimentary fuzzer‘s results on OSS implementations…



help me, Obi-Wan Kenobi. you're my only hope

Outlook on how this can be fixed

make building automation control security great (again)!

Integrators / operators must evaluate their current posture. Make use of ASHRAE et al.'s retro-fit proposals.

holistic measures

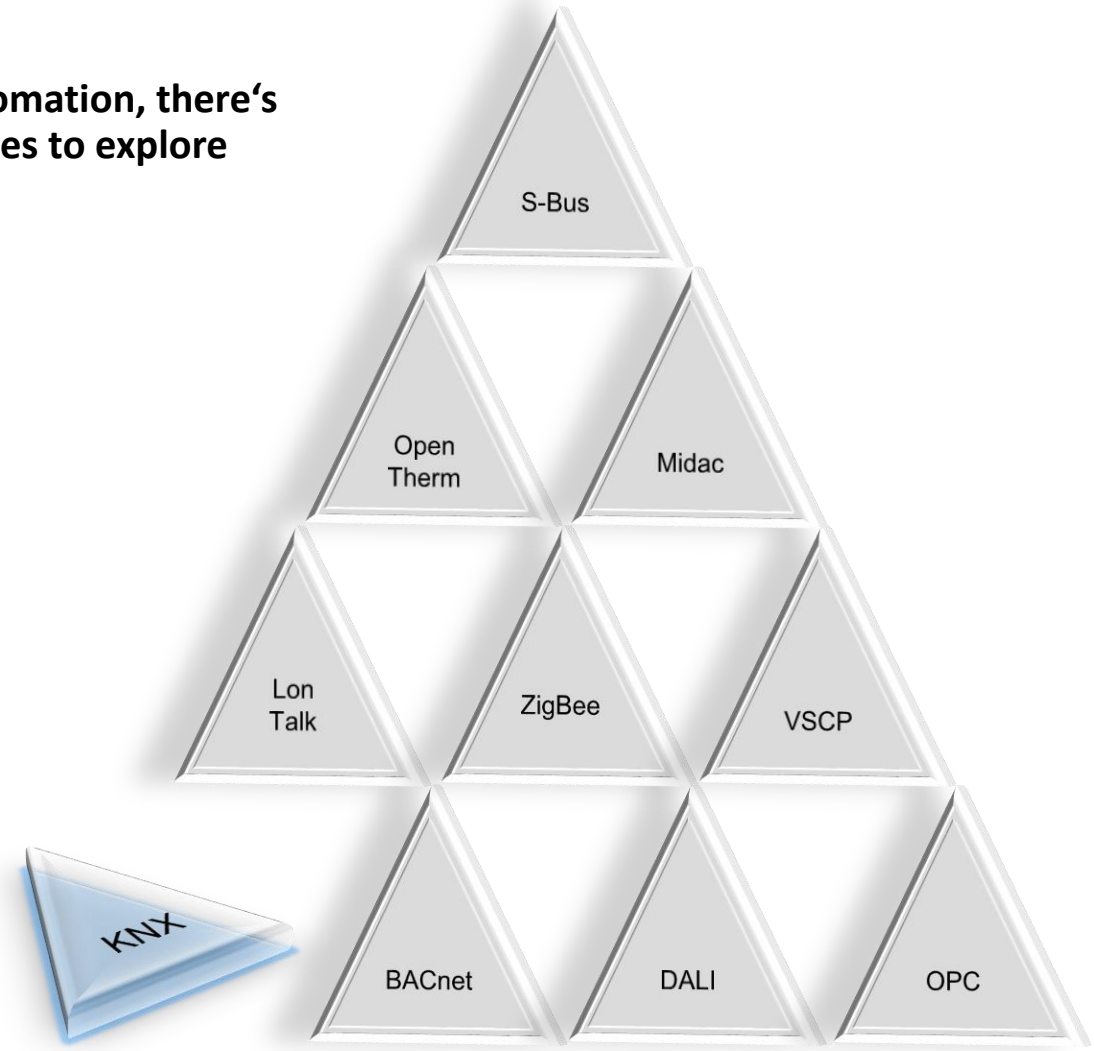
- physical separation
- reducing external access points
- securing interfaces with other systems
- actually apply proposed network architectures

protocol-specific measures

- deploy security proxies
- restrict communication paths
- guard configurations
- protect communication

To infinitiy … and beyond!

A house of cards – in building automation, there‘s many more protocols / technologies to explore



end of line

thanks & kudos for awesome quotes / ideas / research / support go to

K. Reisinger, M. Fuchssteiner, D. Haslinger, R. Seyer, M. Wieser

Contact info:

tbr@limessecurity.com