Flow-based Security Issue Detection in Building Automation and Control Networks

Pavel Čeleda, Radek Krejčí, Vojtěch Krmíček

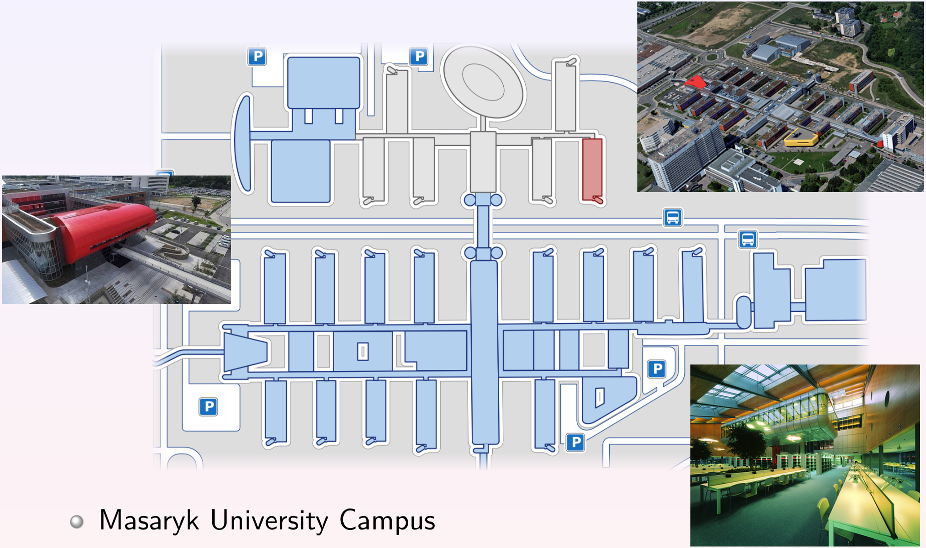
{celeda|vojtec}@ics.muni.cz, rkrejci@cesnet.cz

18th EUNICE Conference on Information and Communications Technologies
29-31 August 2012, Budapest, Hungary

Part I

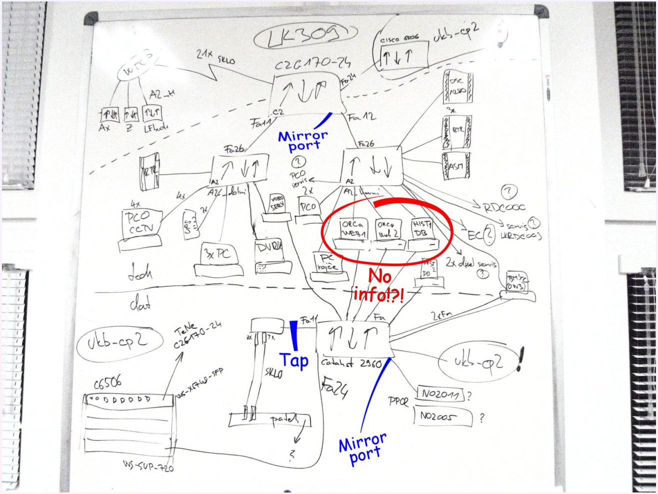
Introduction

Building Automation and Control Systems (BACS) I

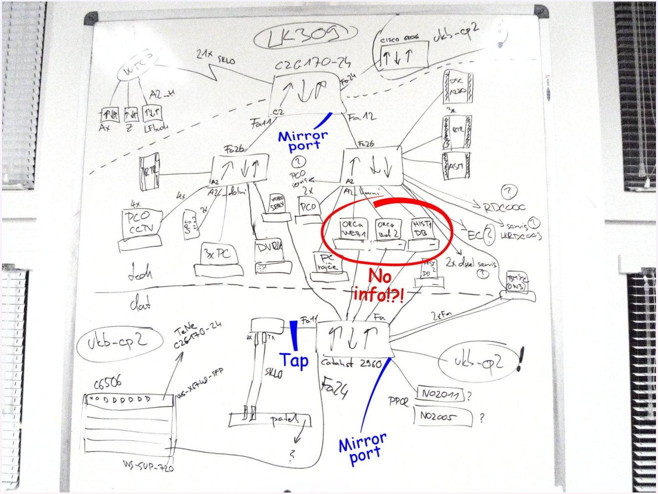


- Masaryk University Campus
- 24 teaching pavilions, over 500 controllers

Building Automation and Control Systems (BACS) II



Building Automation and Control Systems (BACS) II



Mirror port

No info!?!

Tap

Mirror port

What are the advantages of flow-based monitoring in BACS networks and how can it help to detect security issue in these networks?

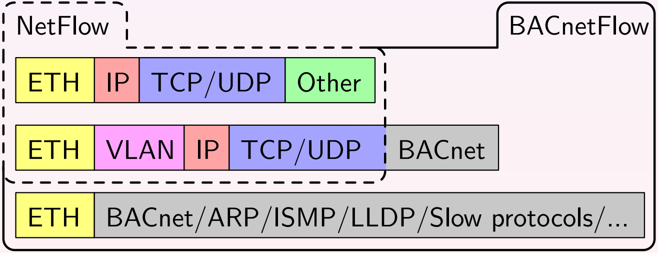
BACnetFlow

BACnet Protocol

- Communication protocol for BACS networks.
- ASHRAE standard 135 – U.S. standard, adapted by ISO, EU.
- Contains key information about BACS network traffic.

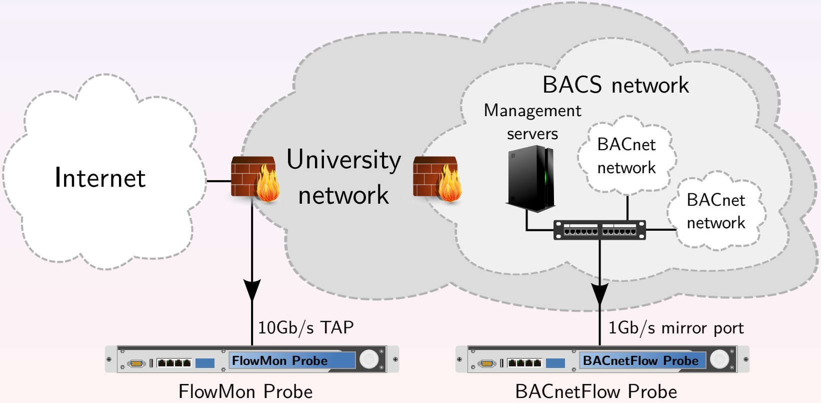
BACnetFlow

- IP flow modification for BACnet networks.



Monitored Network

- Masaryk University Network
- Including university campus BACS network



Part II

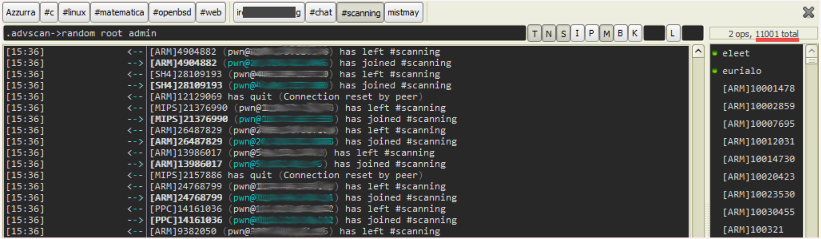
Use Case I – Intrusion Detection

Attack from Building Automation System

AIDRA Botnet in Nutshell

- **Linux malware** – IRC bots with central C&C servers.
- Based on source code of **Hydra** botnet.
- Attacks poorly-configured **ARM, MIPS, MIPSEL, PPC** and **SH4** Linux embedded devices (default Telnet credentials).
- First attacks observed at Masaryk University on 2011-12-04.

AIDRA in action (screenshot of 2011.1 private version)



```
.advscan->random root admin
```

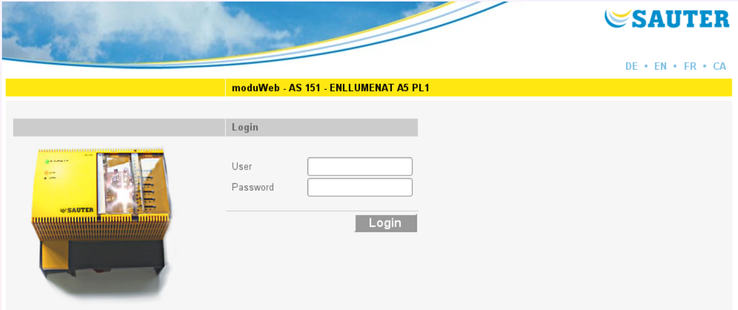
```
[15:36]            <-- [ARM]4904882 (pwn@[redacted]) has left #scanning
[15:36]            --> [ARM]4904882 (pwn@[redacted]) has joined #scanning
[15:36]            <-- [SH4]28109193 (pwn@[redacted]) has left #scanning
[15:36]            --> [SH4]28109193 (pwn@[redacted]) has joined #scanning
[15:36]            <-- [ARM]12129069 has quit (Connection reset by peer)
[15:36]            <-- [MIPS]21376990 (pwn@[redacted]) has left #scanning
[15:36]            --> [MIPS]21376990 (pwn@[redacted]) has joined #scanning
[15:36]            <-- [ARM]26487829 (pwn@[redacted]) has left #scanning
[15:36]            --> [ARM]26487829 (pwn@[redacted]) has joined #scanning
[15:36]            <-- [ARM]13986017 (pwn@[redacted]) has left #scanning
[15:36]            --> [ARM]13986017 (pwn@[redacted]) has joined #scanning
[15:36]            <-- [MIPS]2157886 has quit (Connection reset by peer)
[15:36]            <-- [ARM]24768799 (pwn@[redacted]) has left #scanning
[15:36]            --> [ARM]24768799 (pwn@[redacted]) has joined #scanning
[15:36]            <-- [PPC]14161036 (pwn@[redacted]) has left #scanning
[15:36]            --> [PPC]14161036 (pwn@[redacted]) has joined #scanning
[15:36]            <-- [ARM]9382050 (pwn@[redacted]) has left #scanning
```

```
2 ops, 11001 total
eleet
eurialo
[ARM]10001478
[ARM]10002859
[ARM]10007695
[ARM]10012031
[ARM]10014730
[ARM]10020423
[ARM]10023530
[ARM]10030455
[ARM]100321
```

source – http://www.ahacktivia.org (2011-12-08)

AIDRA Infected Device

- Modular automation station for intelligent building.
- Communication protocols – **BACnet/IP** and TCP/IP.
- Linux based (PPC) – integrated web and telnet server.



moduWeb - AS 151 - ENLLUMENAT A5 PL1

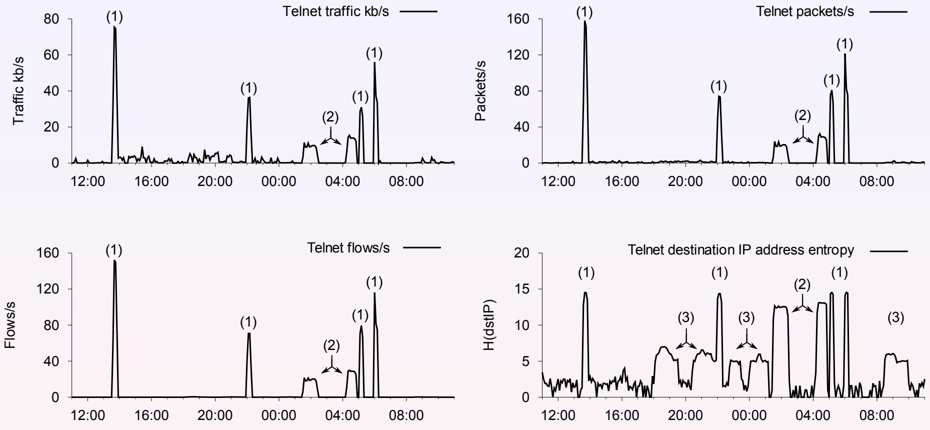
Login

User

Password

AIDRA botnet does not support any targeted attacks against intelligent buildings!

Telnet Attacks Against Masaryk University Network



(1) AIDRA massive horizontal scan 60 to 130 thousand flows (15 minutes window).

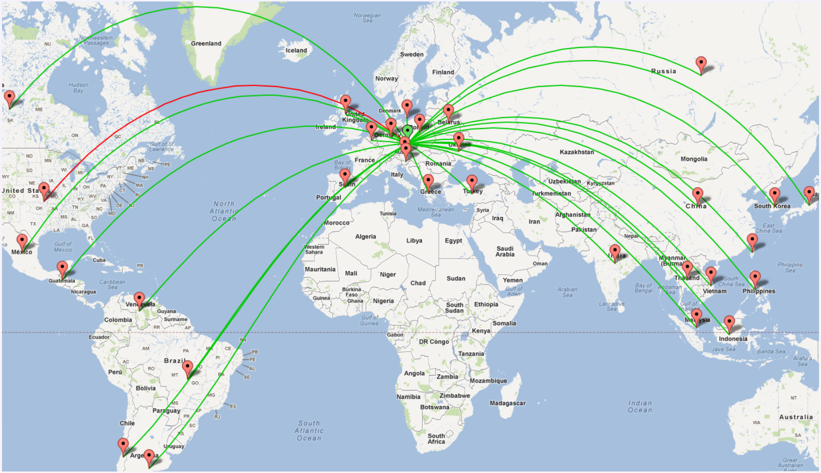
(2) AIDRA massive horizontal scan 60 to 130 thousand flows (60 minutes window).

(3) Microsoft Windows infected machines (SYN packet size is 48, 52 B).

Part III

Use Case II – Access Control

Worldwide Connection Attempts to BACS Network



Attackers' primary interests were following services - **SSH**, **TELNET**, **HTTP**, **HTTPS**, **MS-SMB**, **MSSQL**, **MSRDP** and **RADMIN**.

Week-long Access Control Validation Results

Incomming and Outgoing BACS Network Traffic

Direction	Protocol	Bytes	Packets	Flows
In	TCP	2217553	23122	323
	UDP	0	0	0
	ICMP	6812	100	96
Out	TCP	15248736	33267	287
	UDP	2068299	27396	13113
	ICMP	4202	65	65
Total		19545602	83950	13884

Found Issues

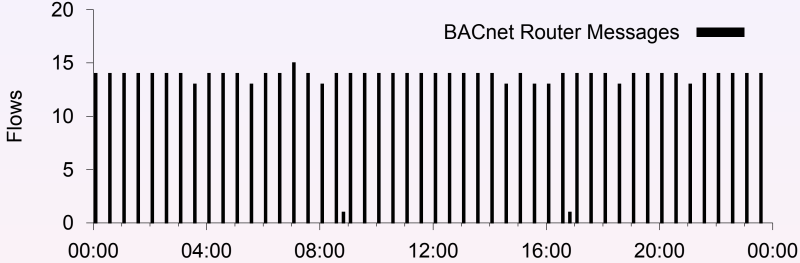
1) Foreign or public DNS servers e.g. Google Public DNS.

2) MS Windows network connectivity status indicator service.

Part IV

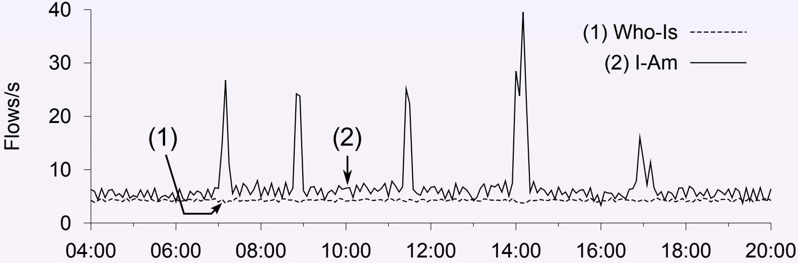
Use Case III – BACnet Attacks

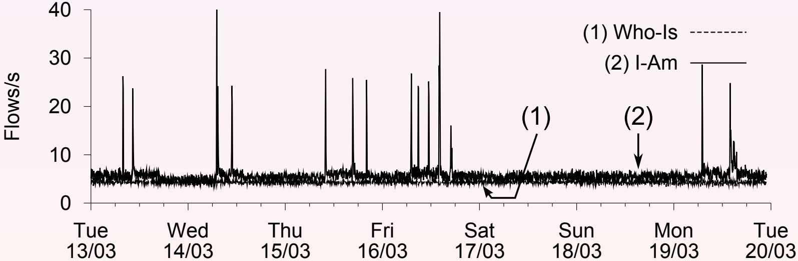
BACnet Router Spoofing Attack



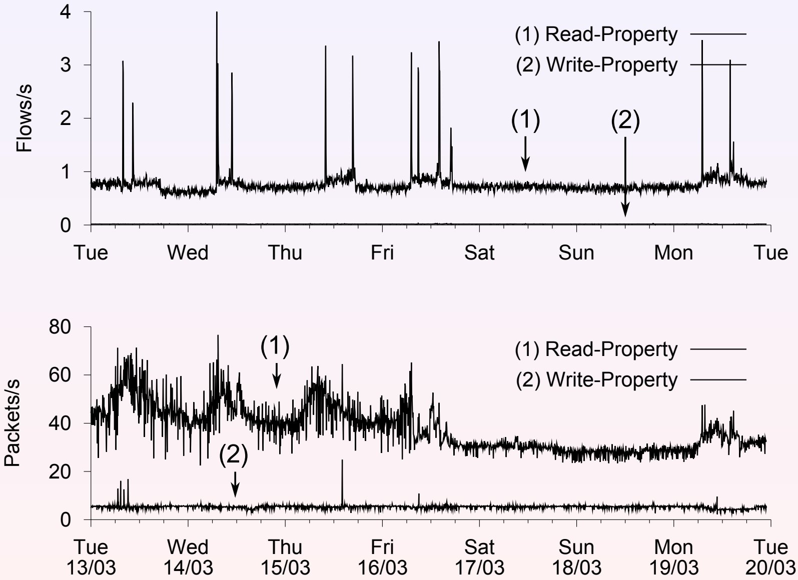
BACnet over IP routers broadcasting ***I-Am-Router-To-Network*** and ***I-Could-Be-Router-To-Network*** messages to the BACS network.

BACnet Device Discovery DoS Attack





BACnet Write-Property Attack



Part V

Conclusion

Conclusion

Summary

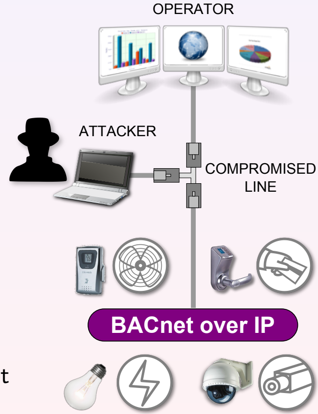
- Any embedded device can threaten others.
- Flow-based monitoring in BACS networks is valuable source of information.
- Even an application protocol specific attacks can be detected using flow approach.

Future Work

- Detect malfunction/misconfiguration of BACnet devices.

Thank You For Your Attention!

Flow-based Security Issue Detection in BACnet



Pavel Čeleda et al.
celeda@ics.muni.cz

BACnet Toolset
http://dior.ics.muni.cz/∼celeda/bacnet