A Cost-efficient Building Automation Security Testbed for Educational Purposes

Jaspreet Kaur, Michael Meier, Sebastian Szlósarczyk and Steffen Wendzel

Cyber Security Department
Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), Bonn, Germany

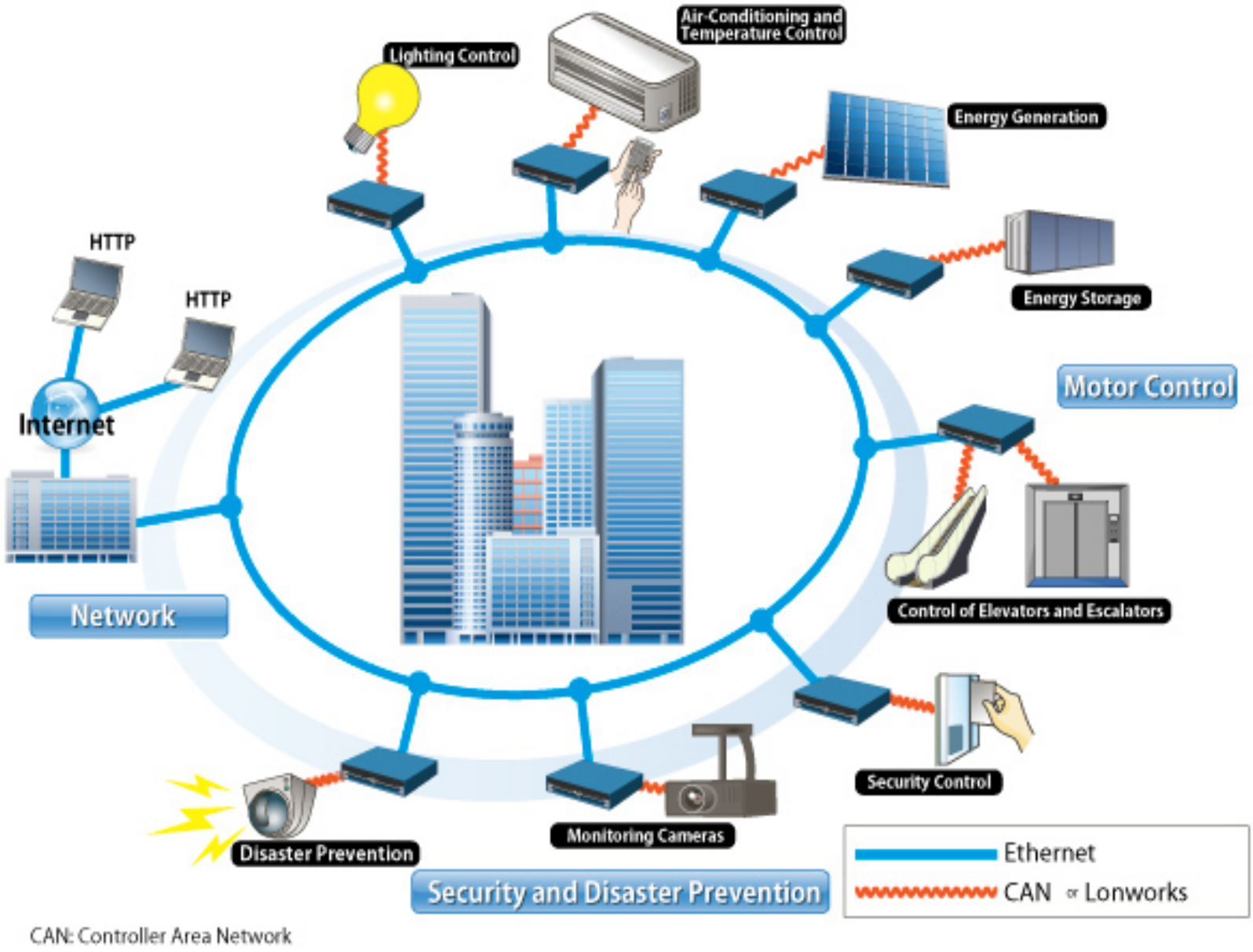
Fraunhofer FKIE

Outline

- Building Automation Systems
- Security threats in BAS
- Covert Channels in BAS
- State of security research in BAS
- Virtual testbed description
- Testbed Setup
- Benefits of Virtual Testbed

Building Automation Systems

- Building automation systems (BAS) are concerned with the control, monitoring and management of services such as heating, ventilation and lighting in buildings
- Main aim of BAS is to meet the following goals:
  - provide safety for inhabitants (e.g. by integrating fire alarm systems or physical access control)
  - control the climate in the building/supervise and control the heating, ventilation, and air conditioning equipment
  - perform facility management (indicate problem by generating reports, graphs and annunciating alarms)
  - perform energy management strategies to reduce operating and energy costs



Source:http://www.renesas.eu/edge_ol/feature/07/index.jsp

Security Threats in BAS

- **Current security threats according to Kastner et al.**:
  - Network Attacks:
    - Attack on the network medium to access the exchanged data
    - Manipulation, fabrication or interruption in the transmitted data
  - Device Attacks:
    - On Software Level: code injection, exploiting algorithm
    - On Physical Level: component replacement

- **Emerging security threats**:
  - Covert channels and data leakage

Covert Channels in BAS

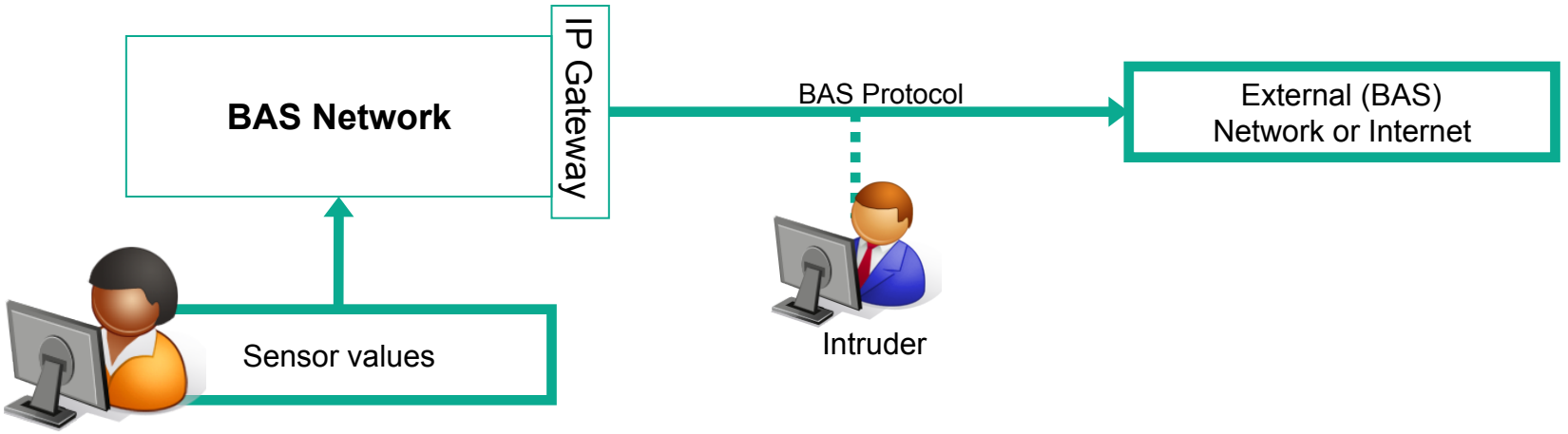
- They are used to transfer secret information in a *stealthy* manner and aim on hiding the fact that communication is taking place.

In terms of building automation systems, covert channels:

- Are one of the emerging threats in BAS.
- Realize data exfiltration over the BAS network in order to bypass sophisticated commercially available data leakage protection (DLP) means, which do not foresee data leakage protection in BAS protocols.
- Allows bypassing BAS internal protection means with policy breaking communication flows (e.g., for the undesired observation of sensor values).

Data Leakage through BAS

- (Un)intentional data leakage using remote connection of a BAS
  - via **network covert channel**
- Connection 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.

Remote access to the sensor data

- Monitoring the sensor values and actuator states (temperature, presence, heating levels, …)
- Who in a city with buildings configured with building automation infrastructures goes so often out of their homes?
- When can a break-in attempt to a region be performed at the optimal moment? Where exactly?

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

State of security research in BAS

- Educational organizations such as universities as well as small and medium sized enterprises (SMEs) are required to gain access to BAS hardware and software components for conducting research on BAS
- Time consuming to get familiar with the complicated real-world environment
- Possibility of damaging real hardware or influencing real (or even critical) BAS operations
- Linked to high costs and thus not affordable by many institutions

This work aims on sharing knowledge on the setup of low-cost BAS testbeds for universities and SMEs and educate students and employees in the field of BAS fundamentals and BAS security.

Virtual testbed description

- Allows to perform BAS security research for the *building automation control and network* (BACnet) *protocol* suite.

- Based on a defensive mechanism for eliminating covert channels in BACnet communications, so-called ***Traffic normalization***.
  - A traffic normalizer is integrated into routers that inter-connect BACnet network segments in order to monitor the traffic exchanged between the devices.
  - A normalizer drops or modifies packets containing malicious or incompliant content.
  - A normalizer uses normalization rules as a basis, which enforces the known protocol specification.

Virtual testbed description (contd.)

The principal requirements for virtual testbeds include:

- cost-efficiency,
- availability as open source, and
- easy configurability for various scenarios.

Testbed setup

The major reason of establishing the testbed is for *educational purposes*. The following components are used to fulfill the requirements (see figure below):

- **Linux machines** with the open source **BACnet stack** to act as BACnet devices; these systems are virtual Linux machines,
- a **Linux machine** running Snort with our **Snort BACnet extension** to act as a protecting traffic normalizer,
- our **protocol fuzzer** based on **Scapy**.

Testbed setup (contd.)

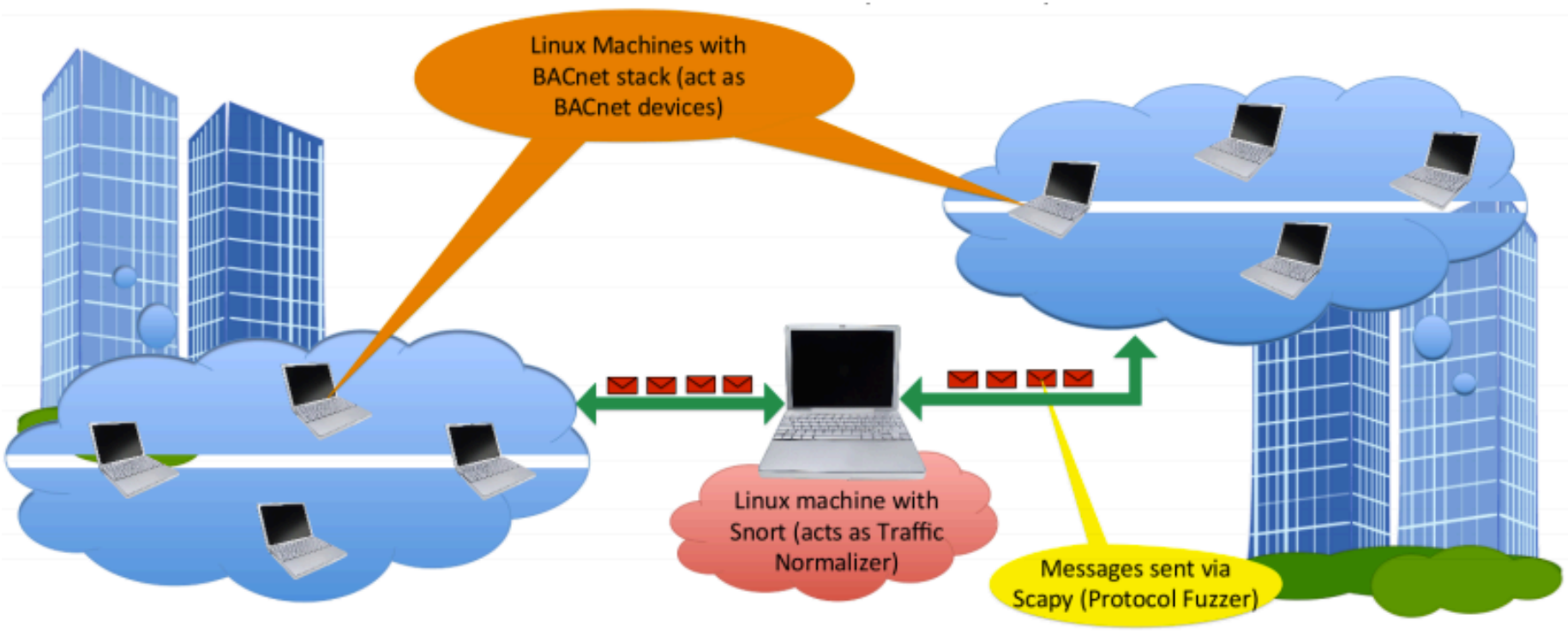
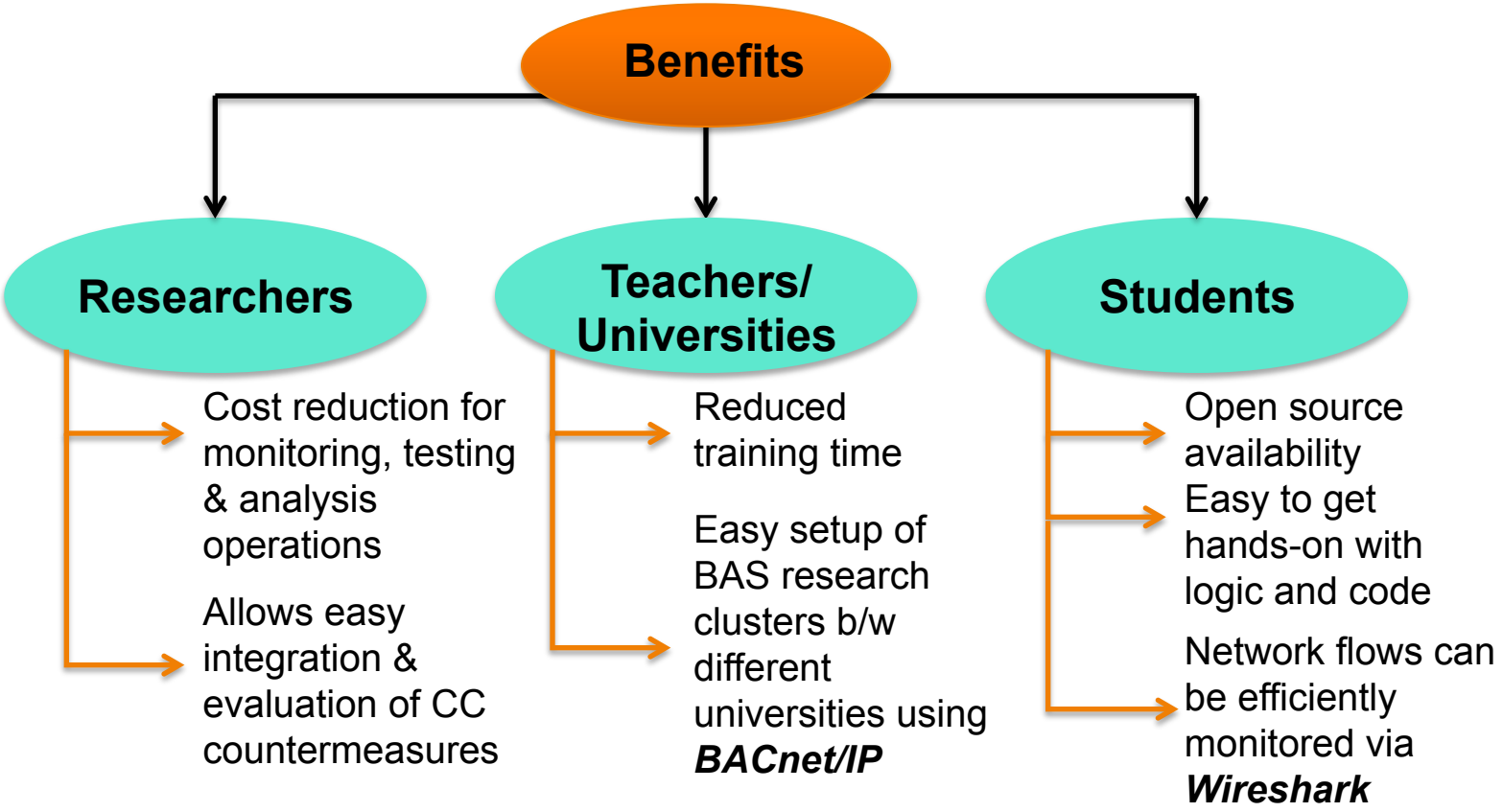


***Figure**. Virtual testbed for BACnet traffic*

Benefits of Virtual Testbed



Thank you for your attention!

Our Expertise:

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

Jaspreet Kaur
Researcher
Cyber Security Department
Fraunhofer FKIE,
Bonn Germany
jaspreet.kaur@fkie.fraunhofer.de