Fraunhofer
FKIE

FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE FKIE

A Cost-Efficient Building Automation Security Testbed for Educational Purposes

Jaspreet Kaur, Michael Meier, Sebastian Szlósarczyk and Steffen Wendzel
{jaspreet.kaur, michael.meier, sebastian.szlosarczyk, steffen.wendzel}@fkie.fraunhofer.de

BUILDING AUTOMATION SYSTEMS

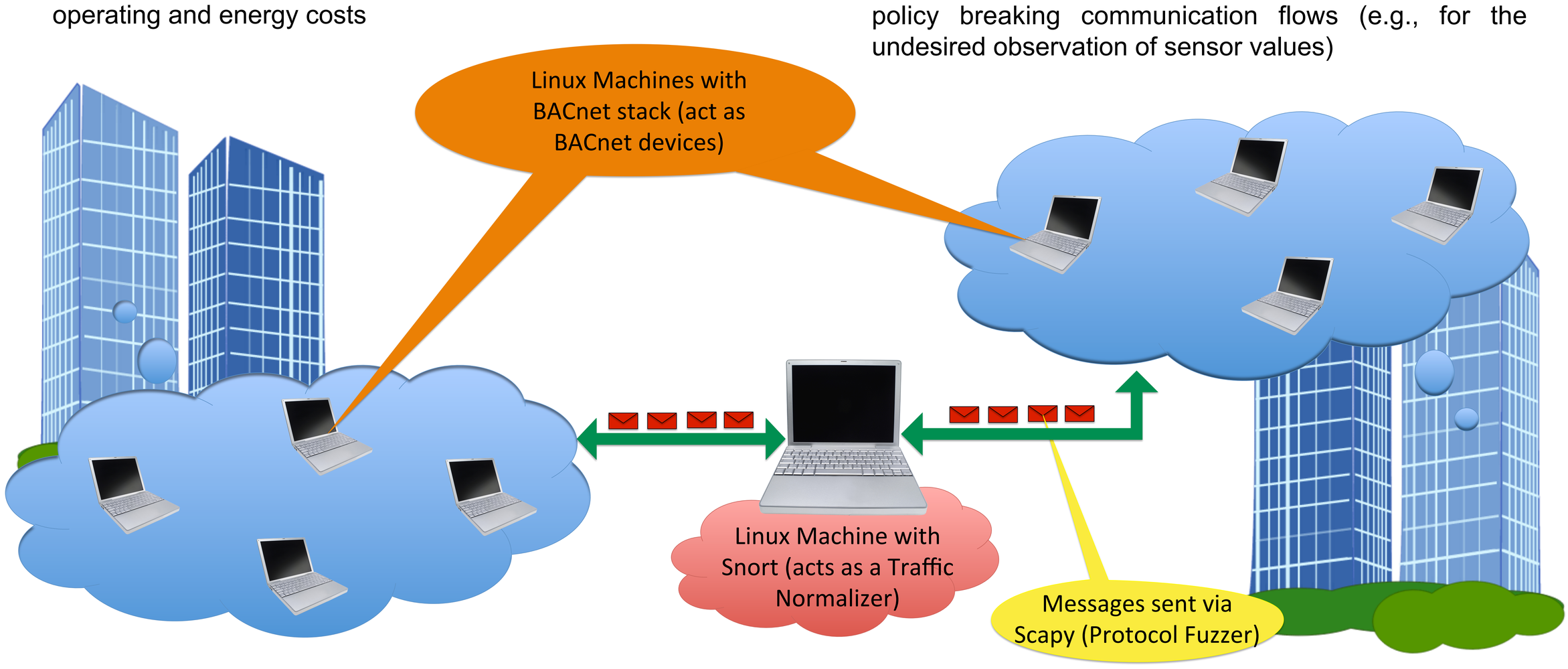
Building automation systems (BAS) are concerned with the control and monitoring of buildings, while aiming to achieve different goals such as:

- 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

COVERT CHANNELS IN BAS

Covert channels are hidden communication channels not foreseen by a system's design. These channels are used to transfer secret information in a stealthy manner and aim to hide the fact that communication is taking place. Covert channels in BAS can be used for the following purposes:

- perform 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
- allow bypassing BAS internal protection means with policy breaking communication flows (e.g., for the undesired observation of sensor values)



Structure of the virtual testbed for traffic normalization between BACnet devices

VIRTUAL TESTBED

Major goal: Allow teaching of BAS fundamentals and BAS security for students and employees in a highly configurable way without requiring expensive BAS hardware.

Defensive mechanism: *Traffic Normalization*

We implemented traffic normalization as a protection measure for one of the widely used BAS protocols *BACnet.*

1. Sits on the communication path between the BACnet devices and monitors the traffic exchanged between the devices in order to detect anomalies.
2. Reports malicious activity and perform actions (drop/ modify) as per normalization rules.

Benefits:

- very simple, cheap solution and available as open source
- easy to get hands-on with the logic and code
- dynamically show the behavior and relationship of the components involved
- comprehensive testing can be done effectively without damaging the real hardware
- results in reduced training time
- efficient monitoring of network flow with the help of Wireshark