Chapter mostly based on S. Wendzel et al.: *Don’t you touch my nuts – information hiding in cyber-physical systems*, in Proc. IEEE S&P workshops, 2017, and on a follow-up journal article in JCSM [download].

NETWORK INFORMATION HIDING

CH. 10A: STEGANOGRAPHY IN THE INTERNET OF THINGS / IN CPS

Prof. Dr. Steffen Wendzel
Worms University of Applied Sciences

https://www.wendzel.de (EN) | https://www.hs-worms.de/wendzel/ (DE) @cdp_xe (Twitter)

Online Class: https://github.com/cdpxe/Network-Covert-Channels-A-University-level-Course/

Covert Channels in CPS Exemplified Using Smart Buildings [1]

(Network) Covert Channel:

Intentional data exfiltration

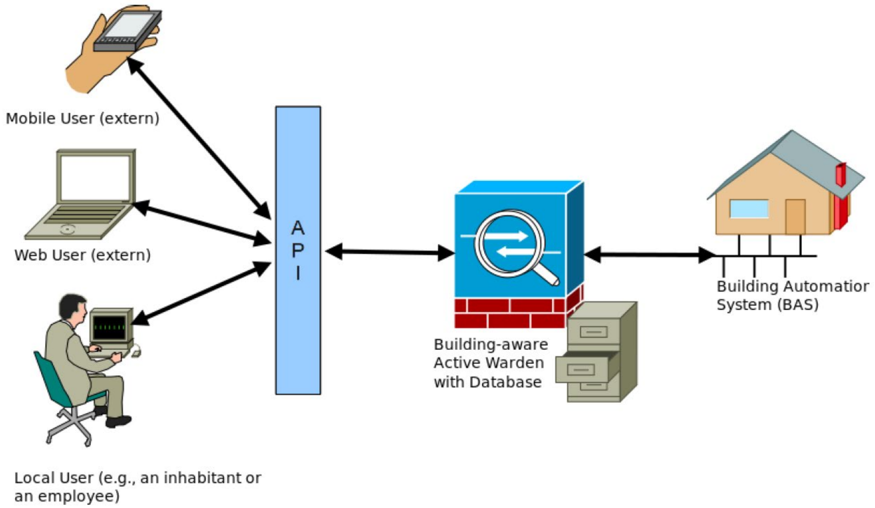
- bypassing common filter technologies of a corporate network through less secured CPS subnets, such as building automation systems.

(Network) Side Channel:

Unintentional information leakage inside the CPS (policy-breaking)

Sample scenarios:

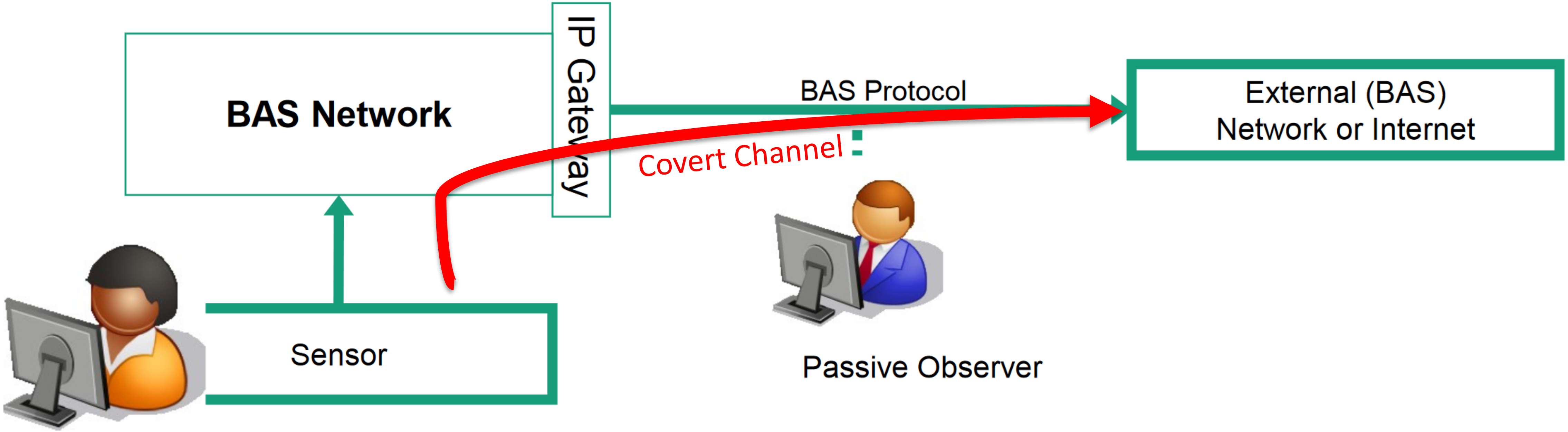
- policy-breaking observation of physical events, e.g. monitoring people inside a building (e.g. using temperature sensors, presence sensors etc.)
- planning a theft


Mobile User (extern)
Web User (extern)
Local User (e.g., an inhabitant or an employee)
A P I
Building-aware Active Warden with Database
Building Automation System (BAS)

<table>
<tr><td>Application 1
Energy Monitoring</td><td>Application 2
Home Control</td><td>…
…</td><td>Application n
Awareness App.</td></tr>
<tr><td colspan="4">Unified Application Programming Interface
(network I/O abstraction and multiplexing)</td></tr>
<tr><td colspan="4">Network Communication Layer
(application layer based transfer over SSL)</td></tr>
<tr><td colspan="4">Building-aware Active Warden
(hardware abstraction; contains database for RBAC, device states, users, ...)</td></tr>
<tr><td colspan="2">Building A</td><td>Building B</td><td>Building C</td></tr>
<tr><td>HomeMatic</td><td>ZigBee</td><td>EIB</td><td>HomeMatic</td></tr>
</table>

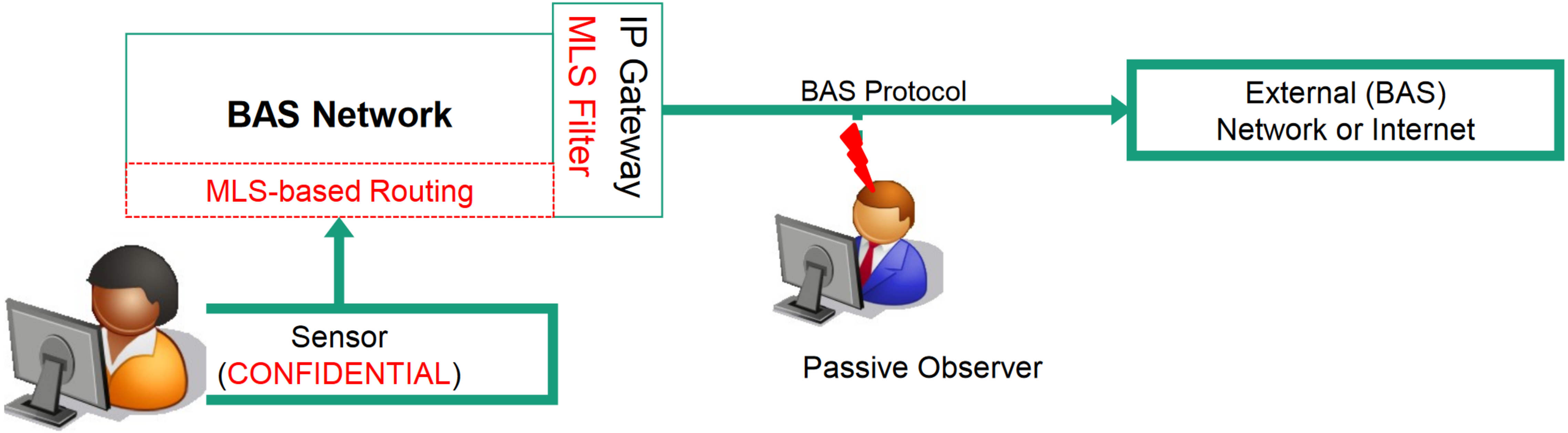
[1] Wendzel, S.: Covert and Side Channels in Buildings and the Prototype of a Building-aware Active Warden, in Proc. ICC (SFCS Workshop), IEEE, 2012.

Data Exfiltration through a CPS (e.g. a Building Automation System, BAS) [1]



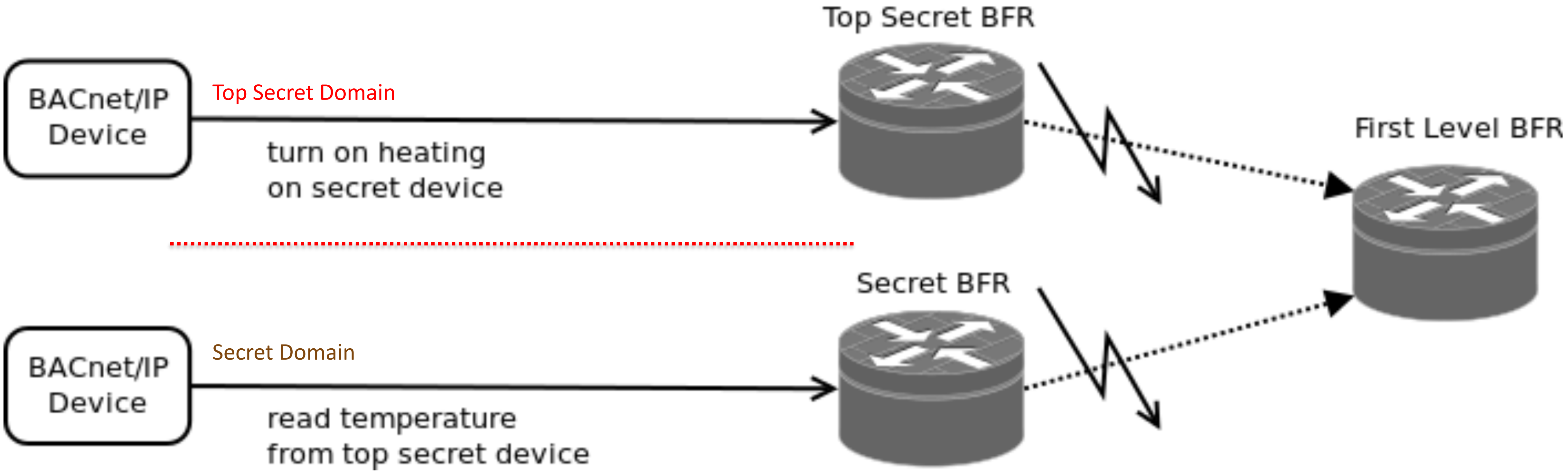
[1] Wendzel, S., Kahler, B., & Rist, T. (2012). Covert channels and their prevention in building automation protocols: A prototype exemplified using BACnet. In Proc. *Green Computing and Communications (GreenCom), 2012 IEEE International Conference on* (pp. 731-736). IEEE.

Countermeasure: MLS-Gateway [1]



[1] Wendzel, S., Kahler, B., & Rist, T. (2012). Covert channels and their prevention in building automation protocols: A prototype exemplified using BACnet. In Proc. *Green Computing and Communications (GreenCom), 2012 IEEE International Conference on* (pp. 731-736). IEEE.

Countermeasure: MLS-Gateway [1]



[1] Wendzel, S., Kahler, B., & Rist, T. (2012). Covert channels and their prevention in building automation protocols: A prototype exemplified using BACnet. In Proc. *Green Computing and Communications (GreenCom), 2012 IEEE International Conference on* (pp. 731-736). IEEE.

Newer work is available as well …

- My work was limited to the BACnet protocol and middleware solutions.
- However, other IoT/CPS protocols exist.
  - For instance, A. Mileva et al. analyzed several IoT protocols such as CoAP [1] and MQTT [2] regarding their vulnerability against network covert channels.

[1] A. Mileva et al.: New Covert Channels in the Internet of Things, Securware 2018.

[2] A. Mileva et al.: Covert Channels in the MQTT-based Internet of Things, IEEE Access, 2019.

But how can data be stored in a CPS?

I will discuss this in Chapter 10**b**!