NETWORK INFORMATION HIDING

CH. 10: STEGANOGRAPHY IN THE INTERNET OF THINGS (IOT) AND CYBER-PHYSICAL SYSTEMS (CPS)

Prof. Dr. Steffen Wendzel

https://www.wendzel.de

Information Hiding & Cyber-physical Systems

Information Hiding:
Steganography, copyright marking, anonymity, obfuscation [1]

+

Cyber Physical Systems (CPS):
integrations of computation with physical processes [2]

=

Information Hiding in Cyber-physical Systems
(specially Steganography for CPS (**CPSSteg**))

Related Work (Chronological Order)

- *Wendzel/Kahler/Rist* (2012) [3]:

  Scenario identification and description of secret data transmission in networked buildings; MLS-based protection approach

- *Tuptuk/Hailes* (2015) [4]:

  Two covert channels (relying on modulation of transmission power and of sensor data) in persuasive computing.

- *Howser (2015) [5]:*

  Data leakage in CPS and MLS-based protection (DLP)

- *Tonejc/Güttes/Kobekova/Kaur* (2016) [6]:

  Detection of selected covert channels in building automation networks using unsupervised machine learning methods.

- Wendzel/Mazurczyk/Haas (2017) [7]:

  Storage of secret data in CPS device registers and actuator states.

- *Hildebrandt/Lamshöft/Dittmann/Neubert/Vielhauer (2020) [8]*

  Pattern-based analysis of covert channels in OPC UA.

- *Neubert/Kraetzer/Vielhauer (2021) [9]*

  Study of artificial steganographic network data generation for steganographic attacks in ICS.

Covert Channels in CPS Exemplified Using Smart Buildings [1]

(Network) Covert Channel:

Intentional data exfiltration

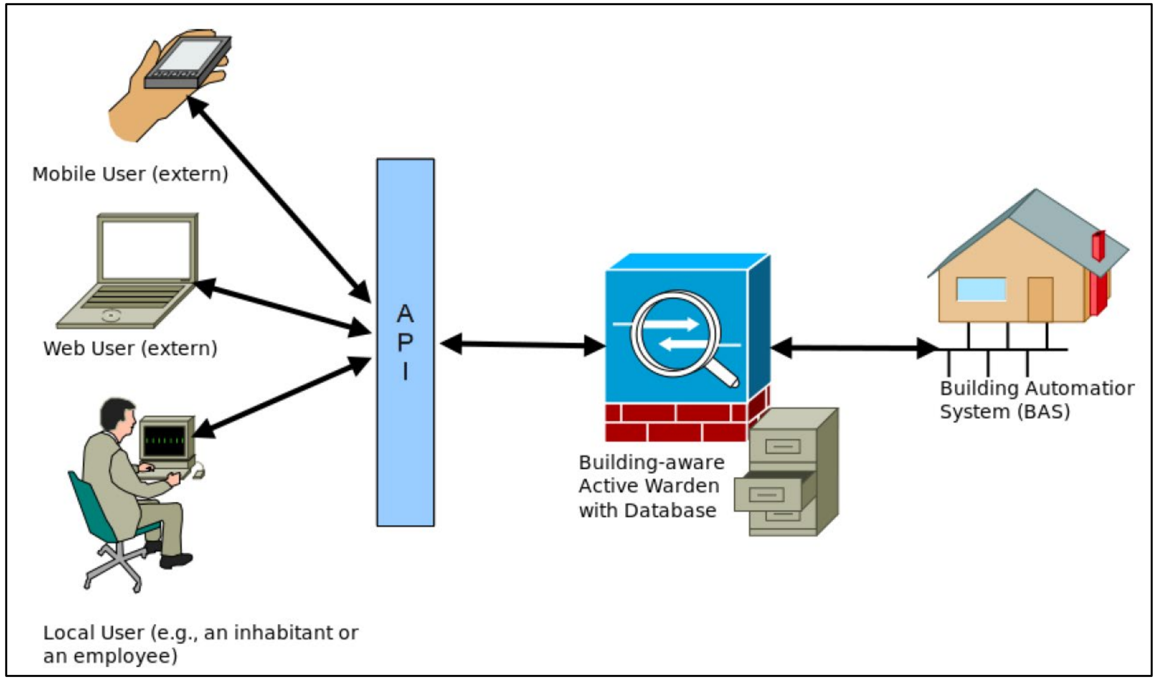
- bypassing common filter technologies of a corporate network through less secured CPS subnets, such as building automation systems.

(Network) Side Channel:

Unintentional information leakage inside the CPS (policy-breaking)

Sample scenarios:

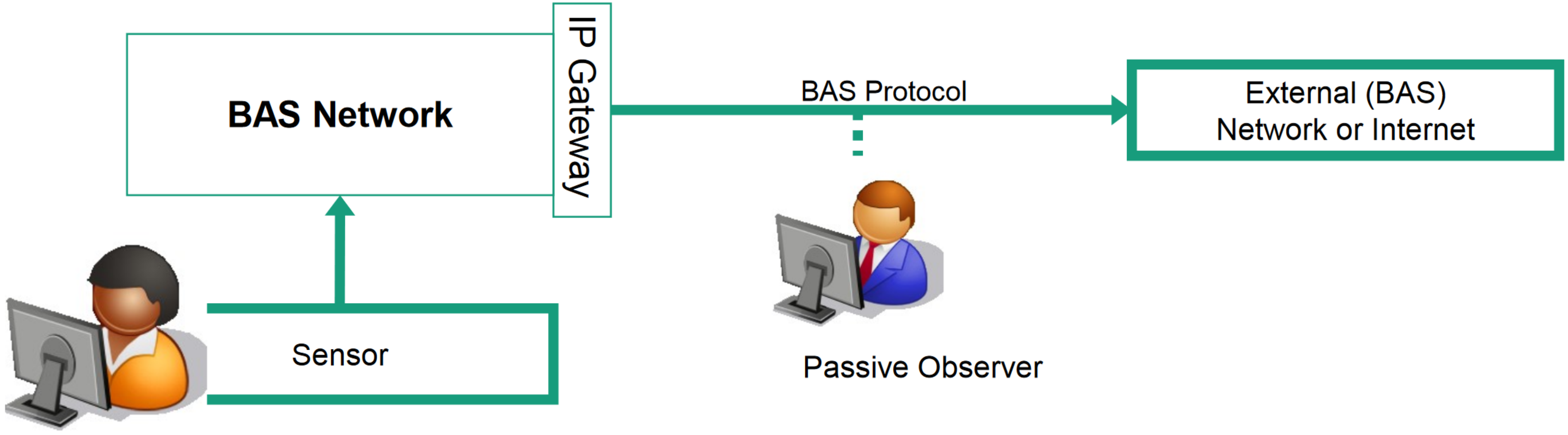
- policy-breaking observation of physical events, e.g. monitoring people inside a building (e.g. using temperature sensors, presence sensors etc.)
- planning a theft



Example: **Building-aware Active Warden** (a simple middleware using MLS)

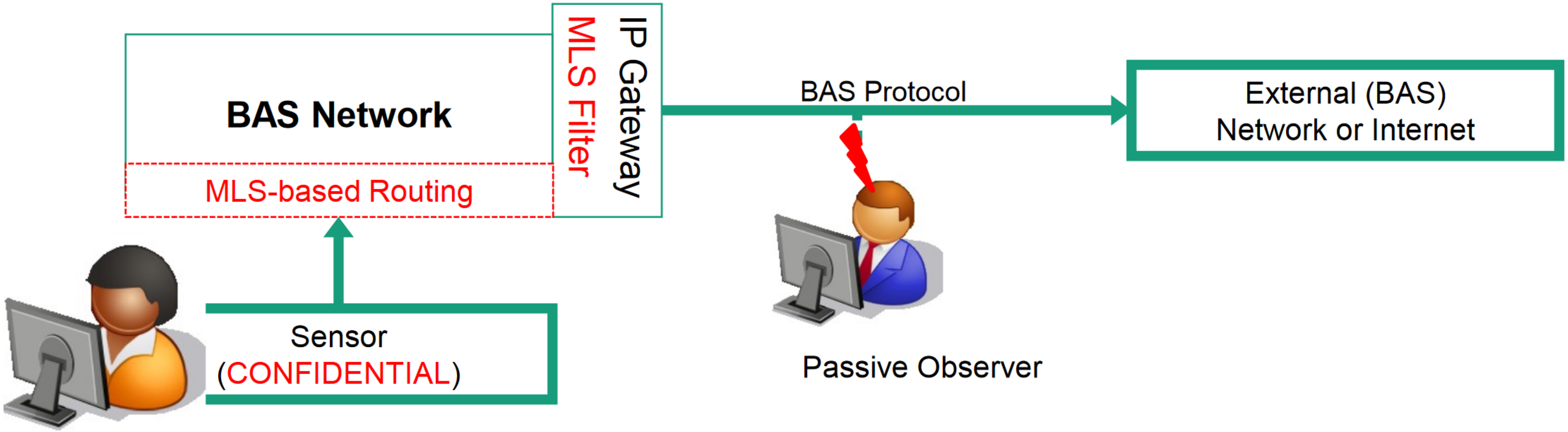
[1] Wendzel, S.: Covert and Side Channels in Buildings and the Prototype of a Building-aware Active Warden, in Proc. ICC (SFCS Workshop), IEEE, 2012.

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

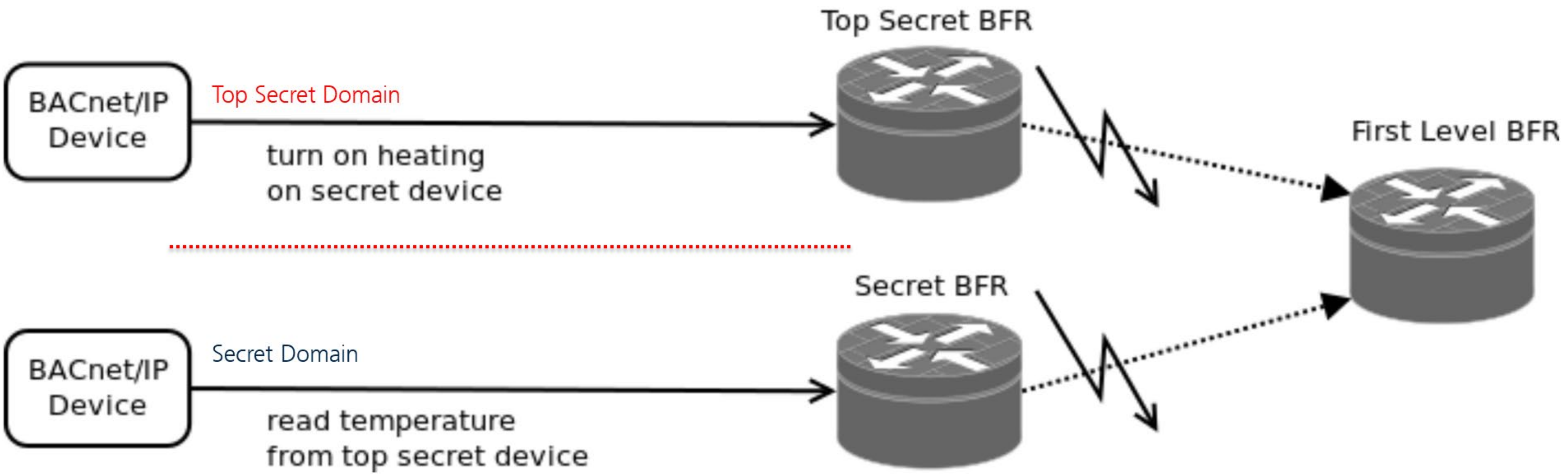


[1] Wendzel, S., Kahler, B., & Rist, T. (2012). Covert channels and their prevention in building automation protocols: A prototype exemplified using BACnet. In Proc. *Green Computing and Communications (GreenCom), 2012 IEEE International Conference on* (pp. 731-736). IEEE.

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.



[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 and MQTT regarding their vulnerability against network covert channels.
  - A. Mileva, A. Velinov, D. Stojanov: New Covert Channels in the Internet of Things, in Proc. SECURWARE, Iaria, 2018.
  - A. Velinov, A. Mileva, S: Wendzel, W. Mazurczyk: Covert Channels in the MQTT-based Internet of Things, ACCESS, IEEE, 2019.
  - A. Mileva, A. Velinov, L. Hartmann,S. Wendzel, M. Mazurczyk*: Comprehensive analysis of MQTT 5.0 susceptibility to network covert channels*. Computers & Security 104:102207. Elsevier, DOI: 10.1016/j.cose.2021.102207
  - M. Hildebrandt, K. Lamshöft, J. Dittmann, T. Neubert, C. Vielhauer*: Information Hiding in Industrial Control Systems: An OPC UA based Supply Chain Attack and its Detection*, in: Proc. IH&MMSec'20, ACM, 2020.
  - A. Mileva, L. Caviglione, A. Velinov, S. Wendzel, V. Dimitrova: *Risks and Opportunities for Information Hiding in DICOM Standard*. In: Proc. 16th International Conference on Availability, Reliability and Security (ARES 2021). Association for Computing Machinery, 2021, DOI: 10.1145/3465481.3470072
  - …
- … but the concept is always the same: take the patterns and check all protocol features/fields for these patterns.

But how can data be **stored** in a CPS?

- **Goals:**
  - Determining **how much data can be hidden** in a CPS **and for how long**.

- **Possible Benefits:**
  - Storing secret data in a location where currently nobody will search for it, e.g. embedding a cryptographic key in a smart home.
  - *Fighting product piracy* [in progress]

- Analyzed **two different strategies**:
  - <u>Register strategy</u>: utilization of unused memory registers
  - <u>Actuator strategy</u>: storing data in actuator states (e.g. heating level of a heater) in a way that it will not be recognized

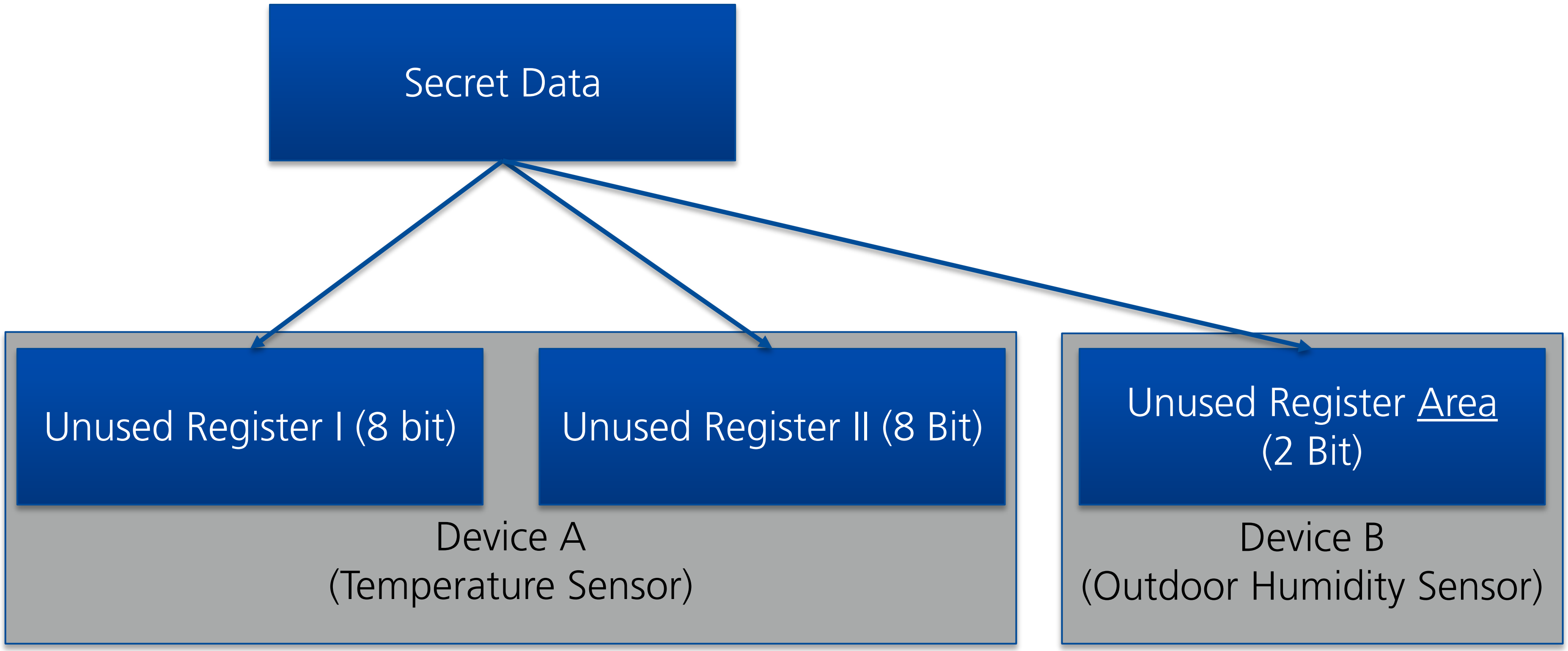
S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Option 1: Register Strategy

S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Register Strategy: Concept

- We store data in unused registers of CPS components.



S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Register Strategy: Concept

- Drawbacks:
  - Writing registers may require direct (local bus) access to a CPS device
  - Register size (and thus steganographic storage) limited
  - Each different device model must be analyzed separately (e.g. datasheets)

- Advantages:
  - Several CPS components and CPS types contain unused registers
    - We used a temperature sensor that contains two unused registers; sensor could be embedded in several types of CPS.
  - Good reading and writing performance
  - Valuable to compare performance of **actuator strategy** (see later) – is the more sophisticated approach better?

S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Register Strategy: Experiments

- Used Maxim Integrated Products, Inc., 1-Wire DS18B20 temperature sensor
  - Communication via 1-Wire protocol

- Approach:
  - Store data in the alarm registers (2x8 bits) of up to 4 sensors.
  - Sort data by sensor-internal unique serial number (can be read via bus connection).

- In experiment, measured time consumption of 100 reading operations from 1, 2 and 4 sensors simultaneously and of 100 writing operations (0x0000 followed by 0xffff in a loop) to one sensor.

S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Register Strategy: Results

- Reading performance (avg.) per sensor increased with the number of sensors as addresses were only required to be fetched once.
- Values remained robust (0% reading errors within 180.000 operations)
- Thus, performance for steganographic operations not an issue.

Scenario	Avg. Time [µs]	Min. Time [µs]	Max. Time [µs]
Reading 1 Sensor	12.841	12.800	12.844
Reading 2 Sensors	12.804	12.784	12.806
Reading 4 Sensors	12.802	12.788	12.804
Writing 1 Sensor	71.827	71.800	71.834

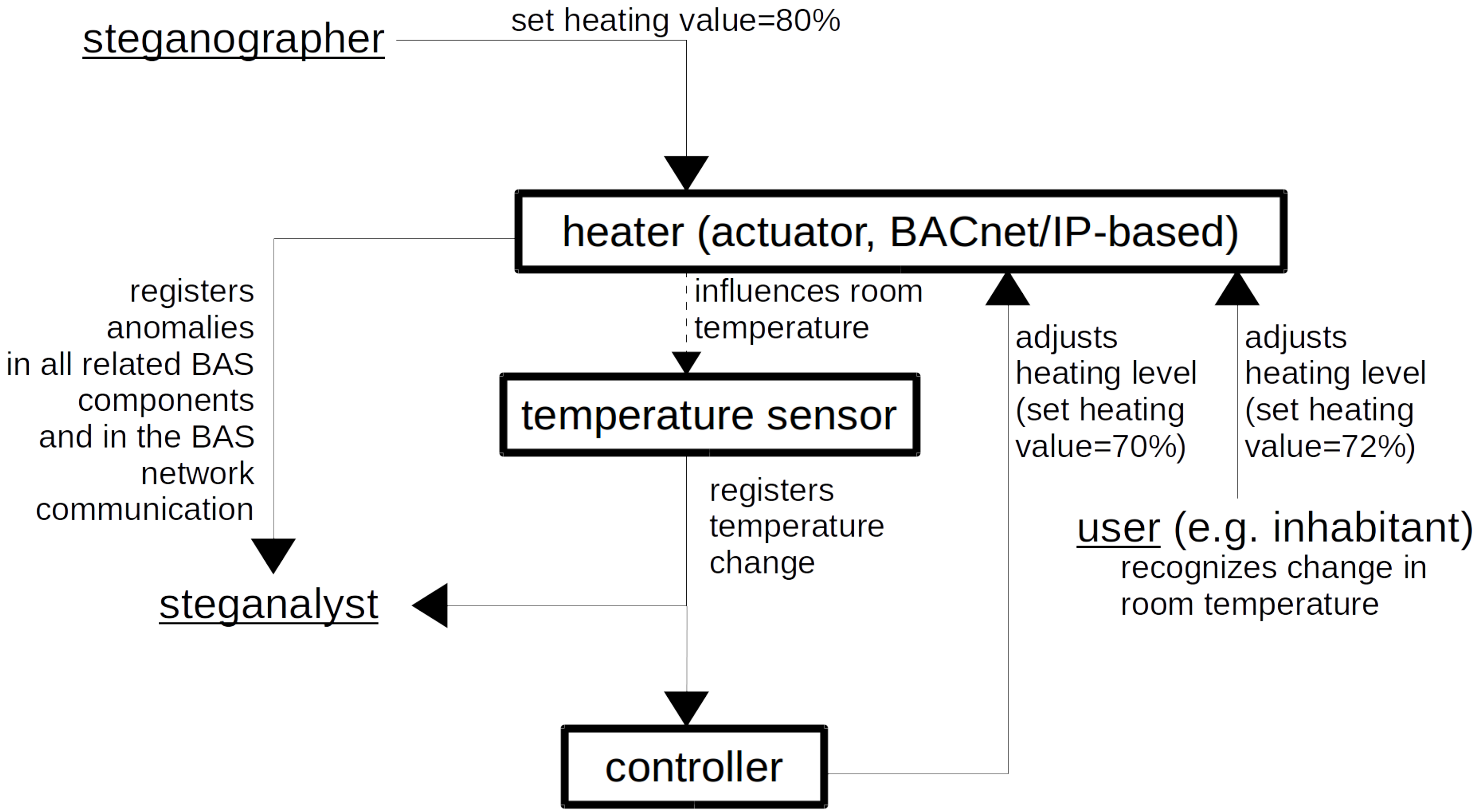
No general conclusion on storage space possible, *probably* around *#SelectedDevices * 4-8 bits* (available register bits on average).
A single 128 bit crypto key would then require 16-32 devices.

S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Option 2: Actuator Strategy

S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

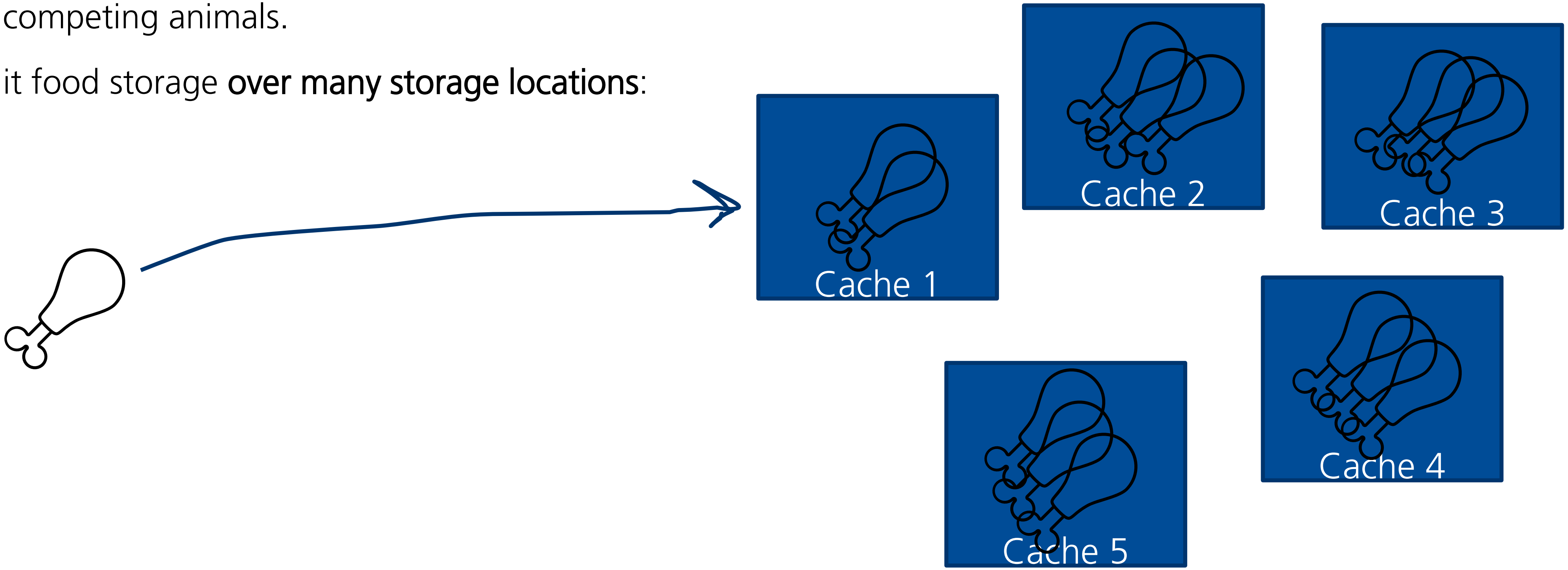
Actuator Strategy: Concept



S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Animal Scatter Hoarding

- For storing collected food, determine locations (caches) which remain mostly untouched by competing animals.
- Split food storage **over many storage locations**:



S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Adaptive Information Hiding

- How to **determine suitable actuators** for secret data storage?
  - Scan for devices in a CPS environment, e.g. BACnet: "Who-Is" broadcast to determine present devices
  - Afterwards scan these devices to determine their objects and present values
  - Monitor changes of all actuator values over time and sort out unsuitable devices (e.g. door openers or devices with frequently changed states) -> similar to Network Environment Learning (NEL)!
- Not a perfect solution:
  - Steganographer operates on the assumption that the CPS will behave as it behaved in the past (based on recordings of its historic behavior)
  - But future CPS behavior cannot be predicted with 100% accuracy based on the historic behavior
    - imagine an open house presentation: building automation system's actuators will most likely be used in different way, e.g. a previously unused room will be heated
  - Still requires use of error detecting/correcting codes, e.g. parity bits or spreading of redundant data over several devices

S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Actuator Strategy: Experiments

- Simulated scatter hoarding using the BACnet protocol
  - ISO standard for communication in automated buildings
  - **How well can we store steganographic data under different conditions?**

- **In general:** Wrote 100,000 values to an actuator (iterating through values 0°C…100°C). After each value written, the current value was read from the device.

- **Experiment 1**: Introduction of a Spurious Process [10] (**Read-only**)
  - Spurious read-only process (resulted in slow-down of steganographer's process but no data loss as BACnet protocol was able to re-send non-acknowledged packets).

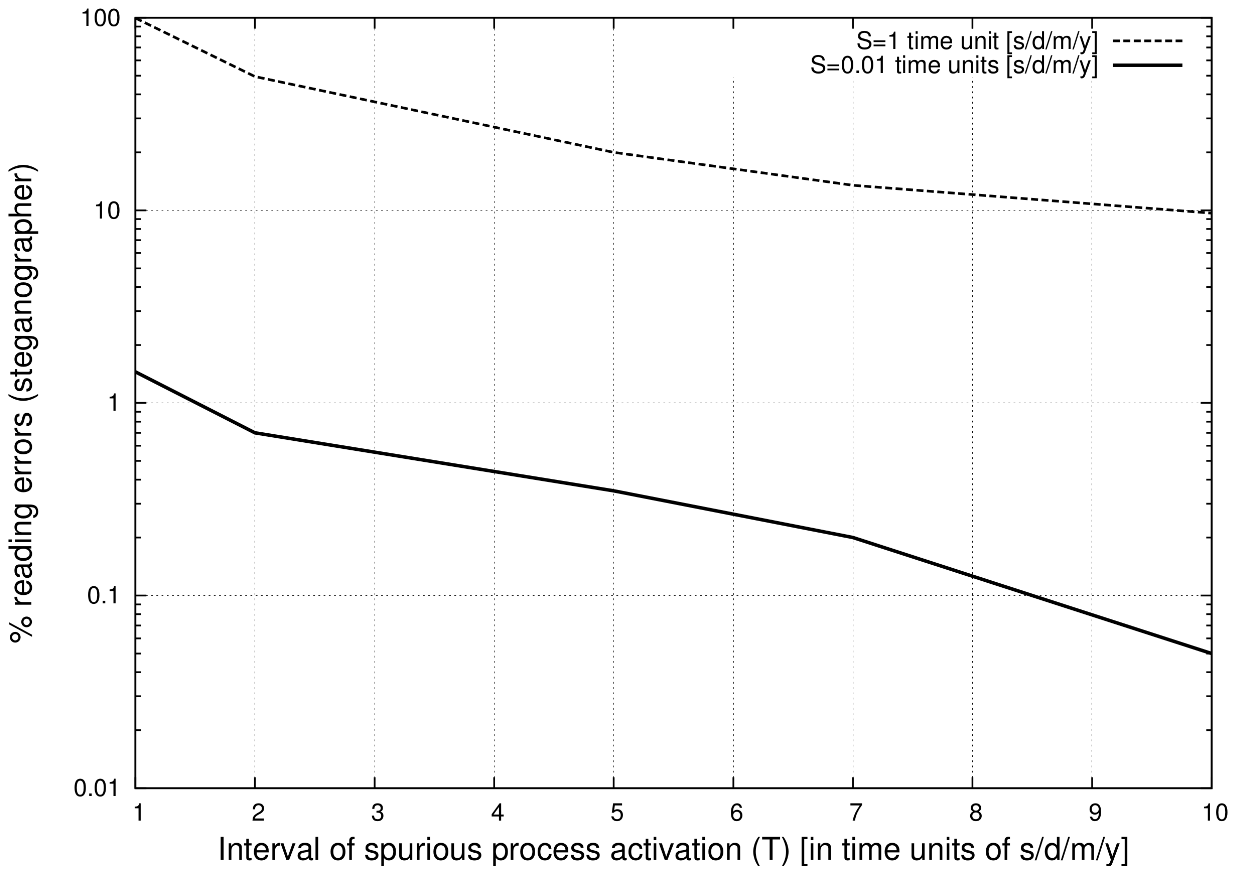
S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Actuator Strategy: Experiments

- **Experiment 2**: Spurious Process (**Read-Write**)
  - SP represents inhabitant or control logic that changes actuator states
  - Competing animal detects hoarding location (read) and steals food (replacing stored value with a random value)
  - Spurious process writes data every T seconds while the desired storage time was S seconds.
  - Simulated situations reaching from highly spurious ($T = S$) to few spurious intrusions ($S \ll T$).

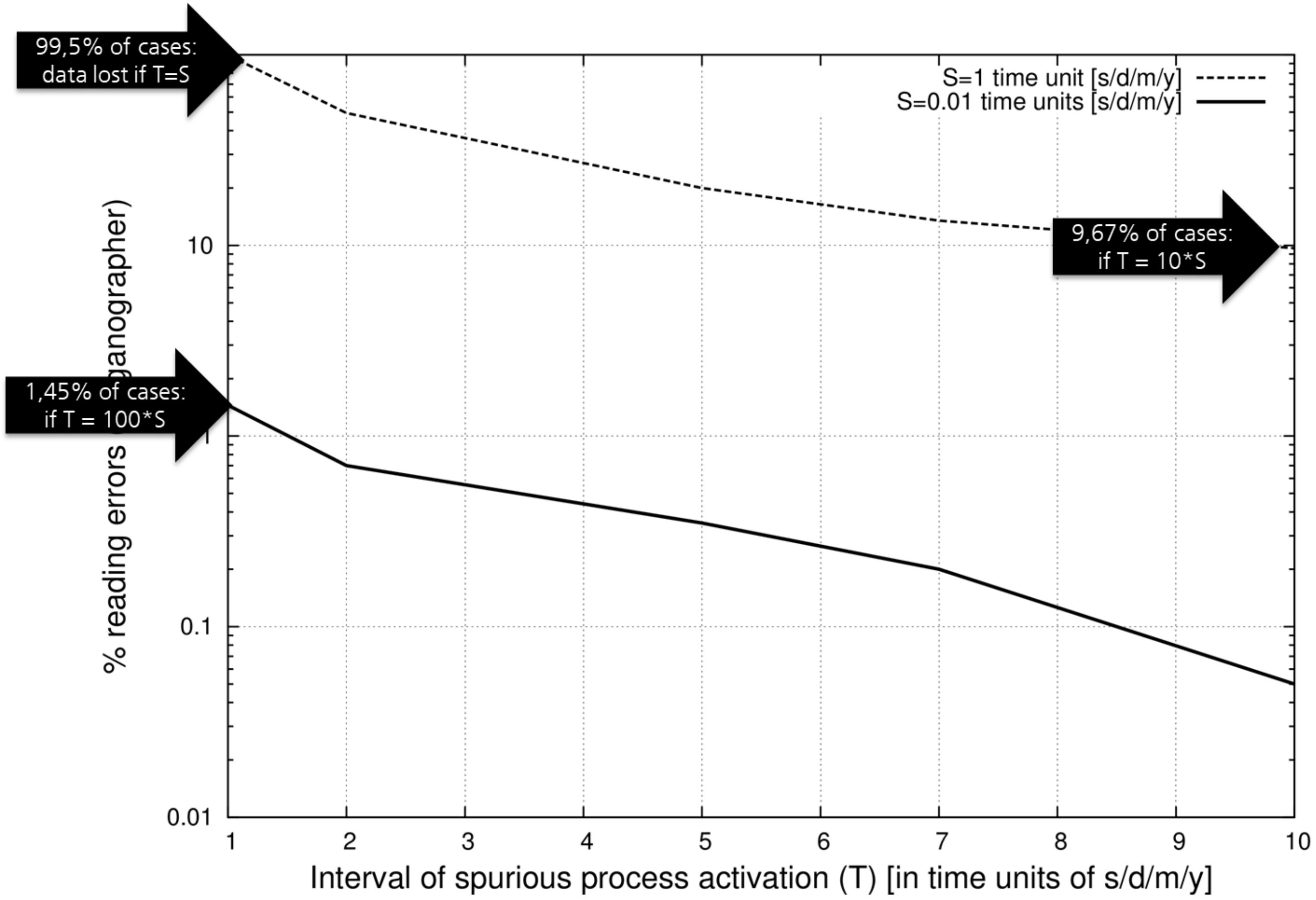
S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Actuator Strategy: Results



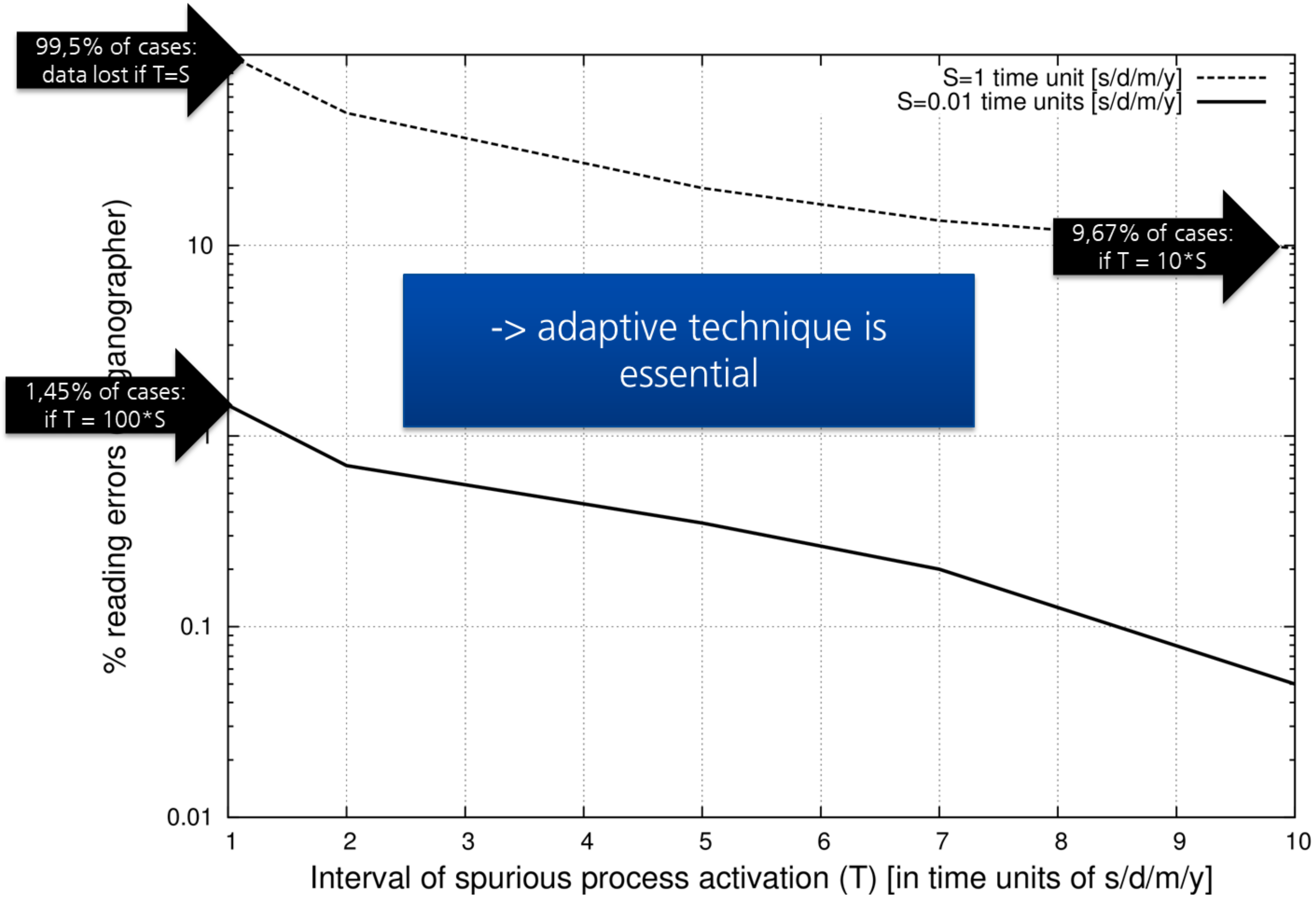
S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Actuator Strategy: Results



S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Actuator Strategy: Results



S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Actuator Strategy: Results

- Storage capacity of actuators highly depends on actuator type (e.g. boolean on-off switches or heaters that provide a fine distinction between heating levels).
- We can assume storage capacity of *2-7* bits per *useful* actuator
  - *18-64* actuators for a 128 bit AES key (**more than in case of register approach!**)
- If we further assume *5-10%* of actuators could be utilized in medium-sized BACnet environments (e.g. 1,000-20,000 actuators), we could store approx. *350* bits - *1.7* Kbytes if *7* secret bits/device can be stored.
- **Advantage: unified accessibility** of actuator approach using common protocol (BACnet) over register approach (individual register access needed!)
  - Especially in larger installations
- Performance: ~0.0055 sec per value that must be written/read
  - some actuators much slower
  - some bus systems much slower
  - 0% reading errors without RW spurious process

S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Limitations and Future Work

- Structure, environments and capabilities of CPS can vary strongly between different CPS types (e.g. smart building vs. wearable).
  - Further studies needed for other CPS types.
  - Caused influence of steganographer on CPS (and its physical environment) not necessarily clear -> CPSSteg considered risky.
    - Probably not suitable for ICS.

- Novel approaches for information hiding in CPS can be expected.
  - One could use **BACnet COV Subscription** relationships to encode steganographic data.
  - Embedding data for copyright marking, e.g. DRM for smart buildings to fight piracy of products (e.g. using CPS traffic obfuscation or covert channels).

S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.

Conclusion

- Covert data exfiltration over CPS is a promising practical approach.

- The amount of data we can store in a CPS highly depends on
  - How we embed data (hiding method)
  - How many devices are available (e.g. #actuators)

- Similarly, these factors influence the robustness of the embedded data.

References

1. W. Mazurczyk, S. Wendzel, S. Zander, A. Houmansadr, K. Szczypiorski: **Information hiding in communication networks**, Wiley-IEEE, 2016.
2. E. A. Lee: **Cyber physical systems: design challenges**, Proc. 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC), IEEE, 2008.
3. S. Wendzel, B. Kahler, T. Rist: **Covert channels and their prevention in building automation protocols: a prototype exemplified using BACnet**, Proc. IEEE CPSCom Workshop on Security of Systems and Software Resiliency, IEEE, 2012.
4. N. Tuptuk, S. Hailes: **Covert channel attacks in pervasive computing**, Int. Conf. on Pervasive Computing and Communications (PerCom), IEEE; 2015.
5. G. Howser: **Using information flow methods to secure cyber-physical systems**, in: Critical Infrastructure Protection IX, Springer, 2015.
6. J. Tonejc, S. Güttes, A. Kobekova, J. Kaur: **Machine learning methods for anomaly detection in BACnet networks**, Journal of Universal Computer Science (J.UCS), Vol. 22(9), 2016.
7. S. Wendzel, W. Mazurczyk, G. Haas: **Steganography for Cyber-physical Systems**, Journal of Cyber Security and Mobility (JCSM), River Publishers, 2017.
8. M. Hildebrandt, K. Lamshöft, J. Dittmann, T. Neubert, C. Vielhauer: **Information Hiding in Industrial Control Systems: An OPC UA based Supply Chain Attack and its Detection**, in: Proc. IH&MMSec'20, ACM, 2020.
9. T. Neubert, C. Kraetzer, C. Vielhauer: **Artificial Steganographic Network Data Generation Concept and Evaluation of Detection Approaches to Secure Industrial Control Systems Against Steganographic Attacks**, in Proc. ARES, ACM, 2021.
10. Y. Fadlalla: **Approaches to Resolving Covert Storage Channels in Multilevel Secure Systems**, Ph.D. Thesis, University of New Brunswick, 1996.