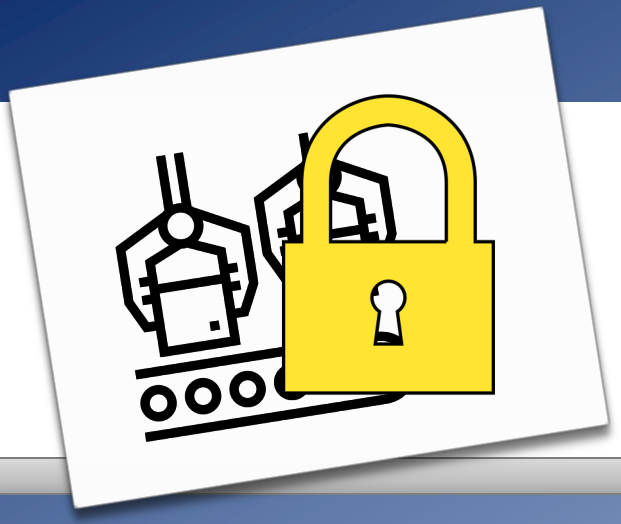


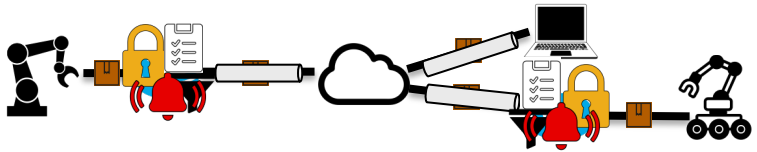
Enhancing Security and Privacy with In-Network Computing

https://www.ietf.org/id/draft-fink-coin-sec-priv-01.txt

Ina Fink, Klaus Wehrle

Enhancing Security & Privacy with INC - Recap

- (Legacy) devices are increasingly connected to the Internet
  - Sensitive data & processes
- Lack of security & privacy mechanisms on devices
  - Financial and safety threats
- Potential to retrofit functions efficiently within the network



Basic Protection Mechanisms
Encryption, integrity checks, authorization, authentication, privacy mechanisms

Efficient Enforcement of Network Policies
E.g., Manufacturer Usage Description [RFC2805]

Intrusion and Anomaly Detection
E.g., dead man switch

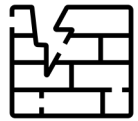
Incident Investigation
Efficient network monitoring

In-Network Vulnerability Patches

https://www.ietf.org/id/draft-fink-coin-sec-priv-01.txt

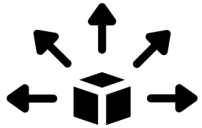
Protection Mechanism: In-Network Vulnerability Patches

- Problem: Resource-constrained devices are hard to update
  - Device vulnerabilities often cannot be fixed after deployment



- Idea: Define fine-granular rules to describe known attack patterns
  - Basically signature-based IPS
  - Efficient but flexible enforcement at switches at line-rate

- “Patches” easy to distribute
  - (Automatic) software updates of capable networking devices



Evaluation of potential and performance benefits in comparison to traditional IPS systems needed

https://www.ietf.org/id/draft-fink-coin-sec-priv-01.txt

Conclusion

- Potential of In-Network Computing for retrofitting and enhancing security & privacy
  - Protection mechanisms, anomaly detection, incident investigation
  - Update: Efficient signature-based intrusion prevention
- Reduce hardware costs and processing overhead
  - Especially beneficial for time-sensitive contexts, e.g., industrial networks, and resource-constrained devices

Ina Fink
fink@comsys.rwth-aachen.de

Current research:
- In-network policy enforcement w.r.t. industrial devices
- Enhancing incident investigation by providing efficient network monitoring

Your thoughts?!

https://www.ietf.org/id/draft-fink-coin-sec-priv-01.txt