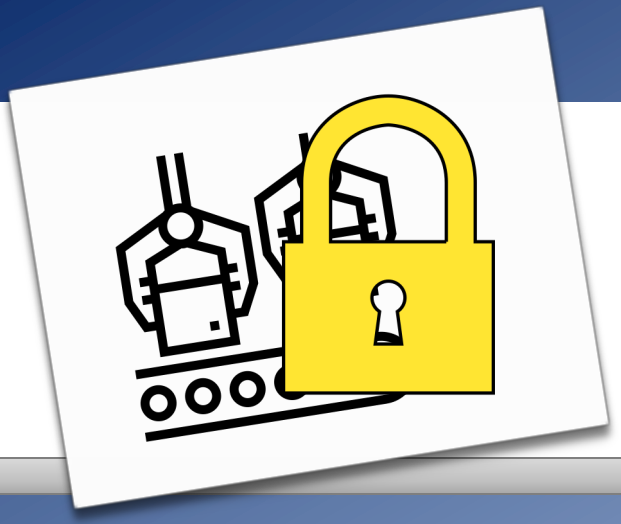


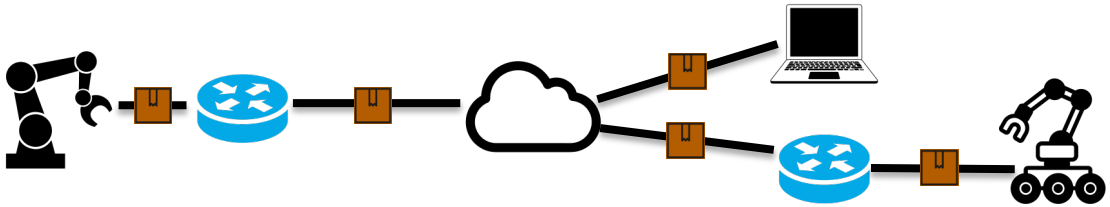
Enhancing Security and Privacy with In-Network Computing

https://www.ietf.org/id/draft-fink-coin-sec-priv-00.txt

Ina Fink, Klaus Wehrle

Security & Privacy Shortcomings in Industrial Networks

- (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

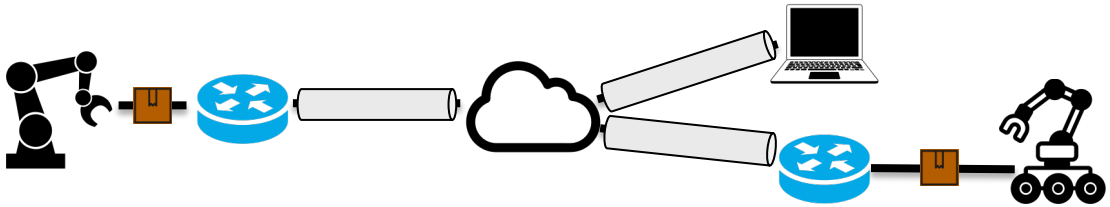


Basic protection mechanisms

Intrusion & anomaly detection

Basic Protection Mechanisms: Encryption and Integrity Checks

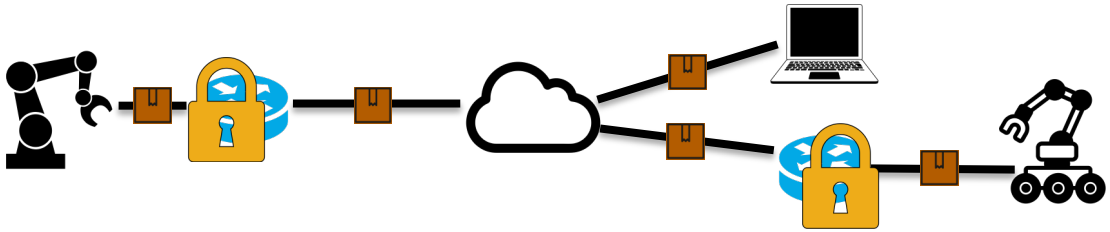
- Idea: retrofit encryption and check-sum calculation at closest networking devices
  - No additional hardware, processing overhead and attack surface
  - Problem: complex cryptographical operations impossible in existing programmable switches due to previous lack of use cases



Costs and benefits of equipping future networking hardware with elaborate cryptography chips?

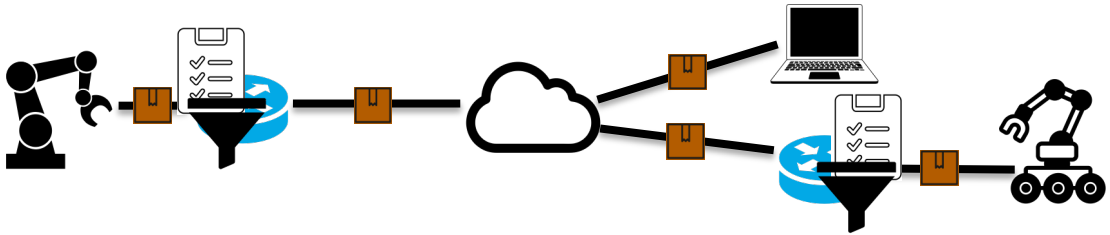
Basic Protection Mechanisms: Authorization & Authentication

- Programmable networking devices can flexibly decide if packets should be forwarded
  - Prevent unauthorized access in the first place, notify administrator in case of incident
- Ideas:
  1) Handshake with networking device at connection start, e.g., based on passwords
  2) Use of secret tokens that are verified by the networking device, e.g., using hash chains
  - Calculations can be offloaded to the control plane with enforcement at switch



Basic Protection Mechanisms: Policies

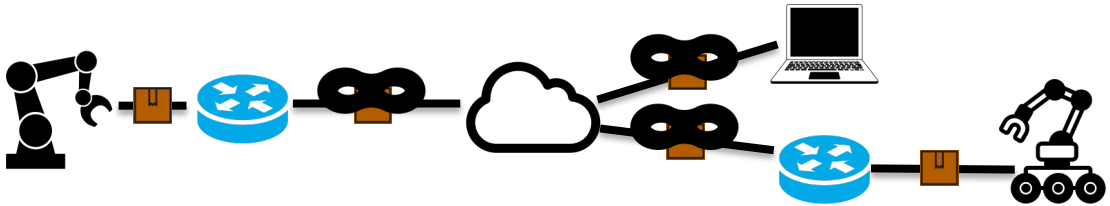
- Idea: industrial devices show function-specific behavior and restricted communication
  - Block undesired connections based on IP addresses, ports, protocols, or bandwidth
  - C.f., Manufacturer Usage Description (MUD) [RFC8520]
- Flexible policy enforcement at line-rate
  - Advanced packet filtering
  - Consideration of contextual parameters, e.g., time of day



First proofs of concept exist but full potential remains unclear

Basic Protection Mechanisms: Privacy

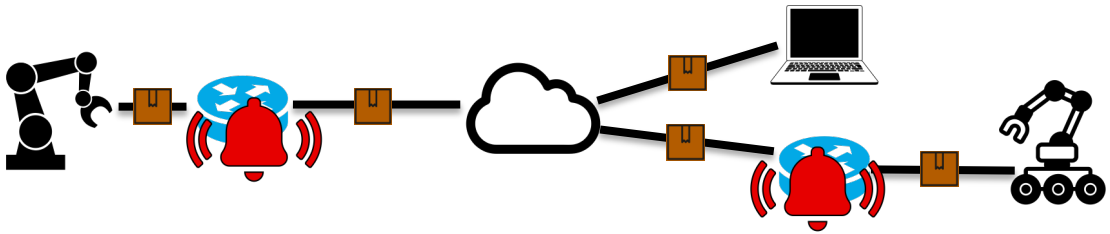
- Various sensors and entanglement with physical world
  - Sensible data increasingly shared with other entities to enhance processes
- Idea: provide simple privacy mechanisms at networking devices
  - Pseudonymization by removing or replacing critical values
  - Aggregating values of multiple packets
  - Noise addition by altering values



Further examination needed to clarify potential and feasibility

Sophisticated Protection Mechanisms: Intrusion and Anomaly Detection

- Idea: provide advanced anomaly detection at line-rate
  - Based on sensor values and traffic patterns
  - E.g., comparison of sensor values with their usual range and use of flow statistics
- Extension of dead man's switches
  - Acceleration of failure detection to support safety
  - Automatic emergency shutdowns of a system or single components



Conclusion

- Potential of In-Network Computing for retrofitting and enhancing security & privacy
  - Basic protection
  - Intrusion and anomaly detection
- 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

Future work:
- Detailed examination of potentials and challenges
- Design of architectures and interaction between networking devices
- Implementation of proofs of concept