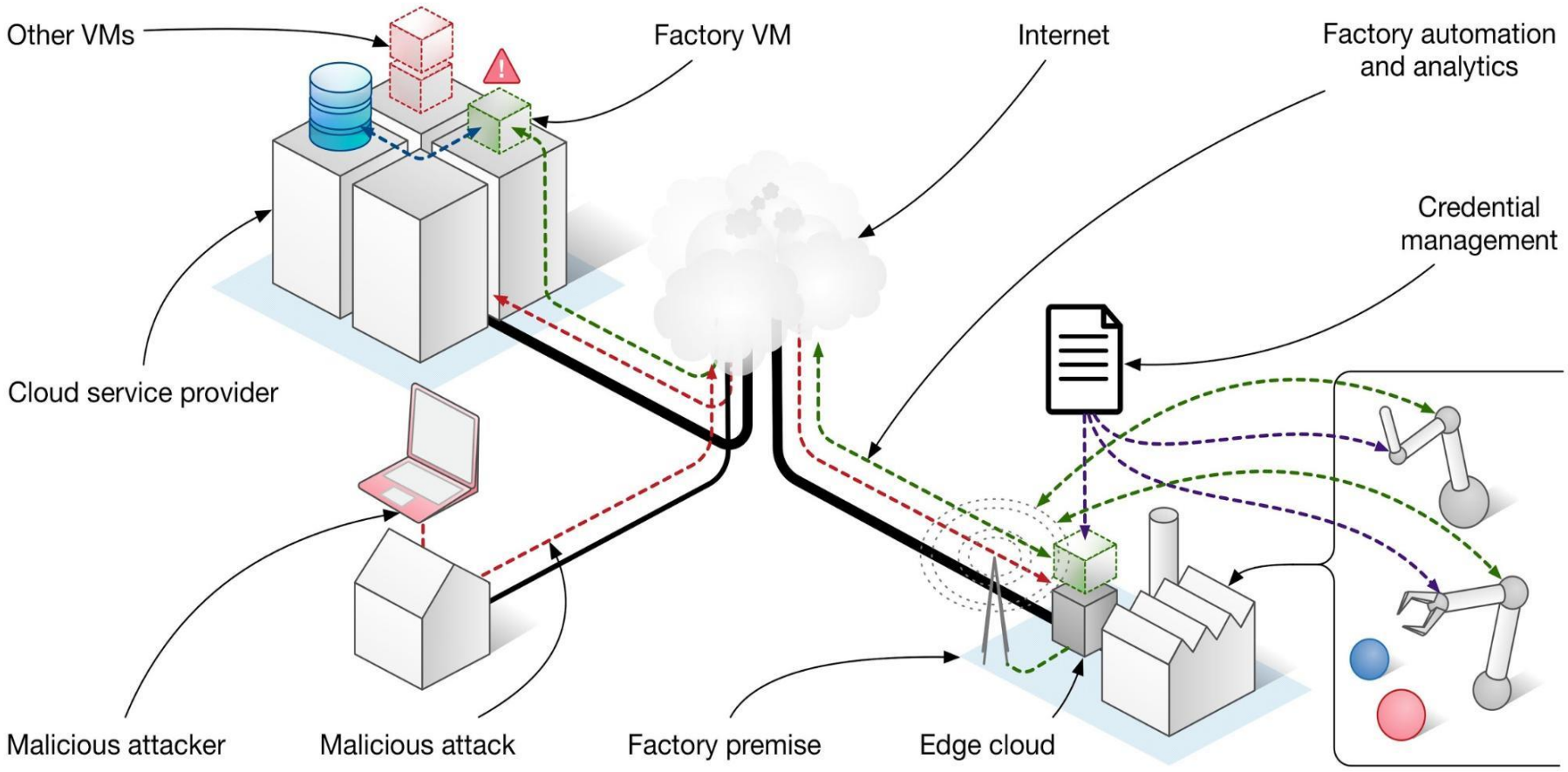
Cyber Security for Next Generation Factory (SEC4FACTORY)

CHRISTIAN GEHRMANN

Contents

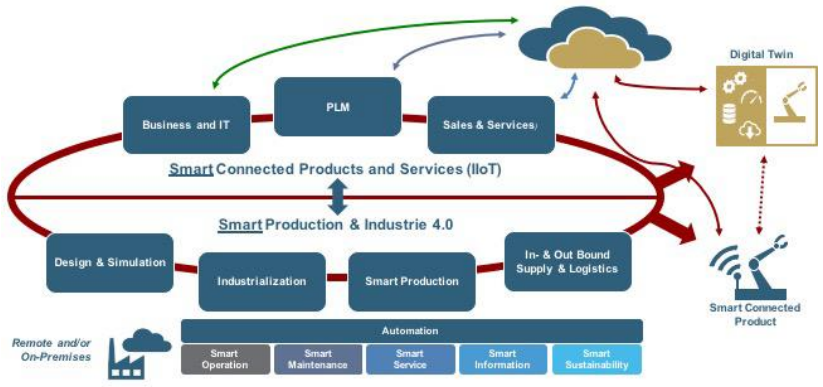
- The SEC4FACTORY scenario
- Research areas
  - Digital twins for security
  - Key management and protected analytics
  - Container security
  - DoS prevention
  - Lightweight crypto
- Next steps

SEC4FACTORY Industry 4.0 scenario



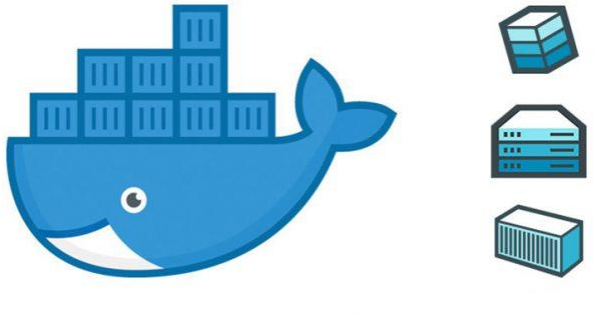
Our security research areas

1 Security with digital twins

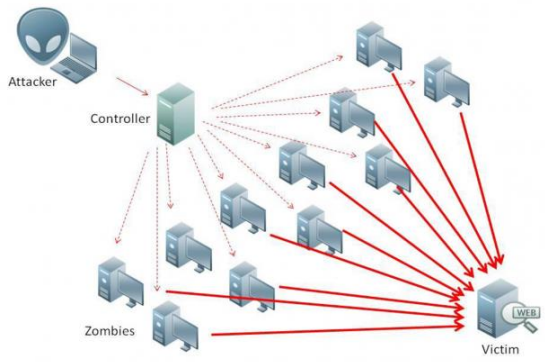


2 Key management and protected analytics

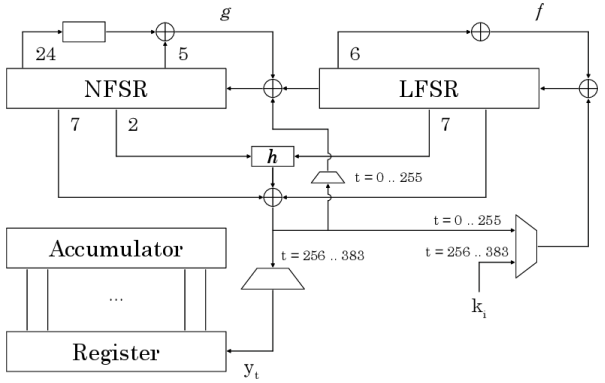
3 Container security



4 DoS Prevention



5 Lightweight crypto



Security with Digital Twins

Why do we think this is interesting?

- The Industry 4.0 paradigm shift *opens up* interfaces into sensitive industry control processes and products themselves => increased security risks
- A digital twin can move *computational loads* and *external interfaces* to cloud resources where we have better analysis and protection possibilities

Our research

- A digital twin security architecture based on secure state synchronization between physical and digital world
- Access control and intrusion detection applied on the digital twin

Key management and protected analytics

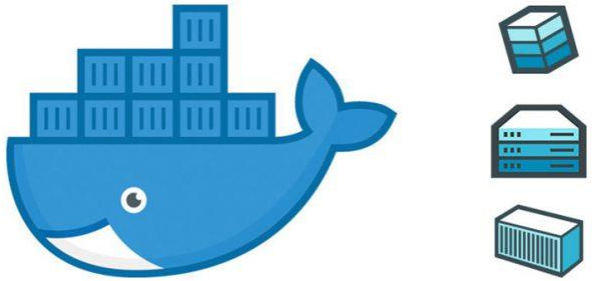
Why do we think this is interesting?

- Complete IoT infrastructures are challenging with respect to security when it comes to *management* of the a large number of units.
  - How are ownership of the infrastructure handled, i.e. when for instance transferred from one entity to another?
  - Privacy with respect to data collection and analytics?

Our research

- Pure symmetric key based solutions (quantum computing safe):
  - Ownership transfer
  - Identity protected analytics

Container security



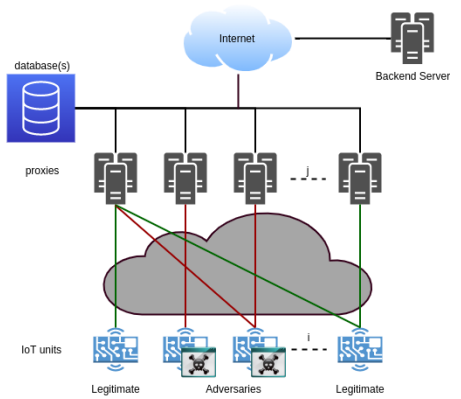
Why do we think this is interesting?

- Around 60 exploits targeting Docker environments the past 5 years
- Around 100 exploits targeting Kubernetes in the same time period

Our research

- Automatic generation of Mandatory Access Control profiles for containers
- Focusing on AppAmor profiles and complete system solutions

DoS prevention in an IIoT setting



Why do we think this is interesting?

- DoS has been a major security issue since the rise of the Internet
- Even if we have lots of protection mechanism, there are still much to be done trying to reduce the risks

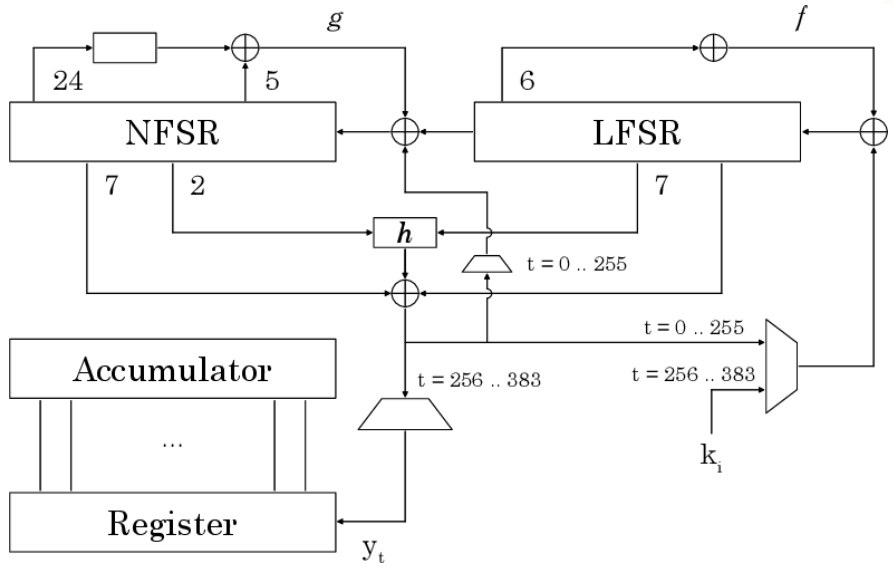
Our research

- DoS mitigation through detection and IoT side in combination with filtering at boarder routers
- DoS mitigation through source based detection and filtering using

Lightweight stream ciphers

Lightweight Cryptography Standardization: Finalists

- ASCON
- Elephant
- GIFT-COFB
- Grain128-AEAD
- ISAP
- Photon-Beetle
- Romulus
- Sparkle
- TinyJambu
- Xoodyak



Size, power, speed at 100kHz

Parallelization	Area	Power	Throughput
1	4934 μm^2	313 nW	50 kbit/s
2	5336 μm^2	368 nW	100 kbit/s
32	16853 μm^2	574 nW	1600 kbit/s

- M. Hell, T. Johansson, W. Meier, J. Sönnerup and Y. Hirotaka, ” An AEAD Variant of the Grain Stream Cipher”, Codes, Cryptology and Information Security, Rabat, April, 2019.

Next steps >>

- Digital Twin enhanced synchronization, advanced access control and anomaly detection
- IIoT recovery with trusted execution
- DDoS prevention with XPO and automatically generated blocking thresholds
- Advanced Kubernets cluster automatic AppArmor profile generation

- Extended industry collaboration in all our research areas
- Extended academic collaboration in all our research areas

Contact

- Christian Gehrmann – christian.gehrmann@eit.lth.se
- Maria Kihl – maria.kihl@eit.lth.se
- Marco Tiloca – marco.tiloca@ri.se
- Martin Hell – martin.hell@eit.lth.se