Cyber Security for Next Generation Factory (SEC4FACTORY)

CHRISTIAN GEHRMANN

Contents

- Project goals
- Participating research groups
- Some research areas
- Next steps

Goals

The SEC4FACTORY has identified the need for research on a set of different Industry 4.0 security and communication research topics to create new system models and solutions:

Major computational tasks are moved to cloud resources giving high computing performance at low cost. =>

- *We shall provide highly protected computations that will not put the production itself or the production data in risk.*
- *Move of functions and usage of new wireless interfaces (5G/6G) shall not cause unacceptable performance or delays.*

Production and product data are collected during the whole production and product life-cycle in order to optimize production and reduce product fault and maintenance costs. =>

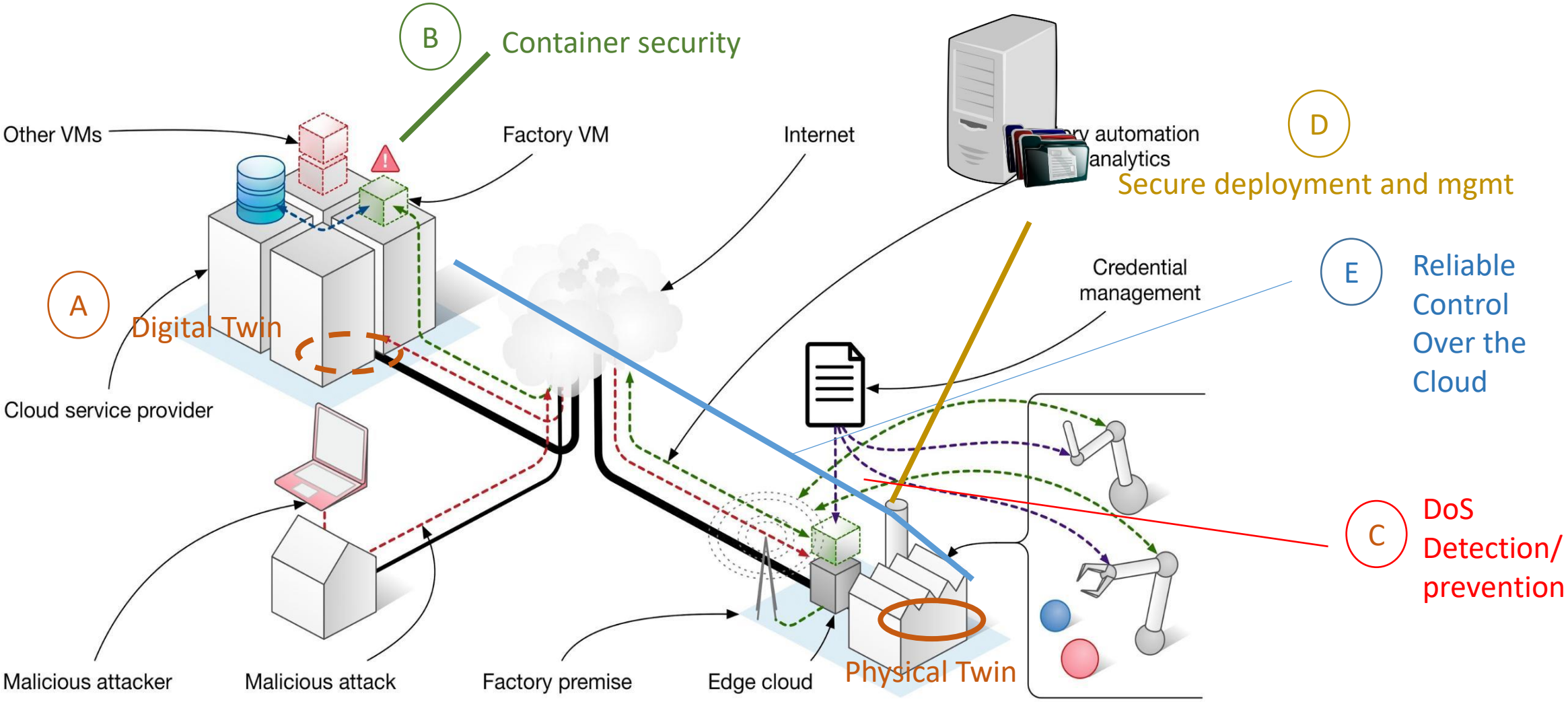
- *We shall provide efficient and secure management of production infrastructures.*
- *The systems shall offer protection of data during collection and computation and with strict access control between production and product data stakeholders.*

Active research groups

1. Security research at EIT at Lund University
2. Security research at RISE, Lund and Kista
3. Broadband communication group at EIT, Lund University
4. *Reliable Wireless lab, RISE, Lund – dissolved in 2020!*

Project will run until end of 2024

SEC4FACTORY Industry 4.0 scenario



A - Security with Digital Twins

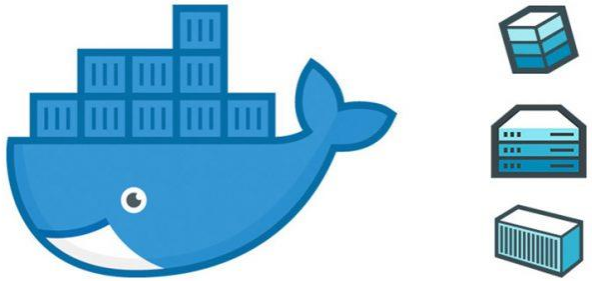
Why do we think this is interesting?

- 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

B- Container security (I)



Why do we think this is interesting?

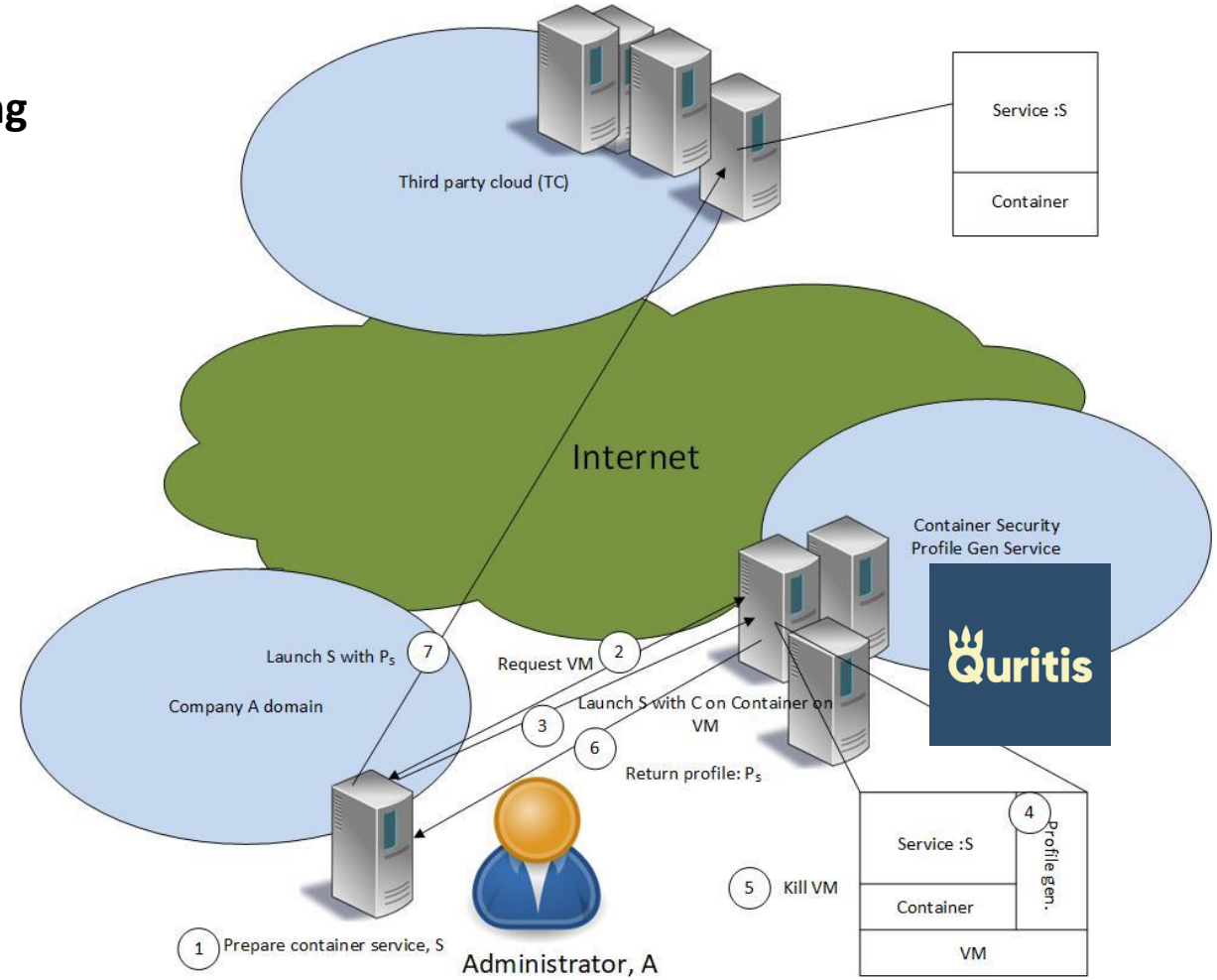
- Around 60 exploits targeting Docker environments the past 5 years
- Around 100 exploits targeting Kubernetes in the same time period

Our research

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

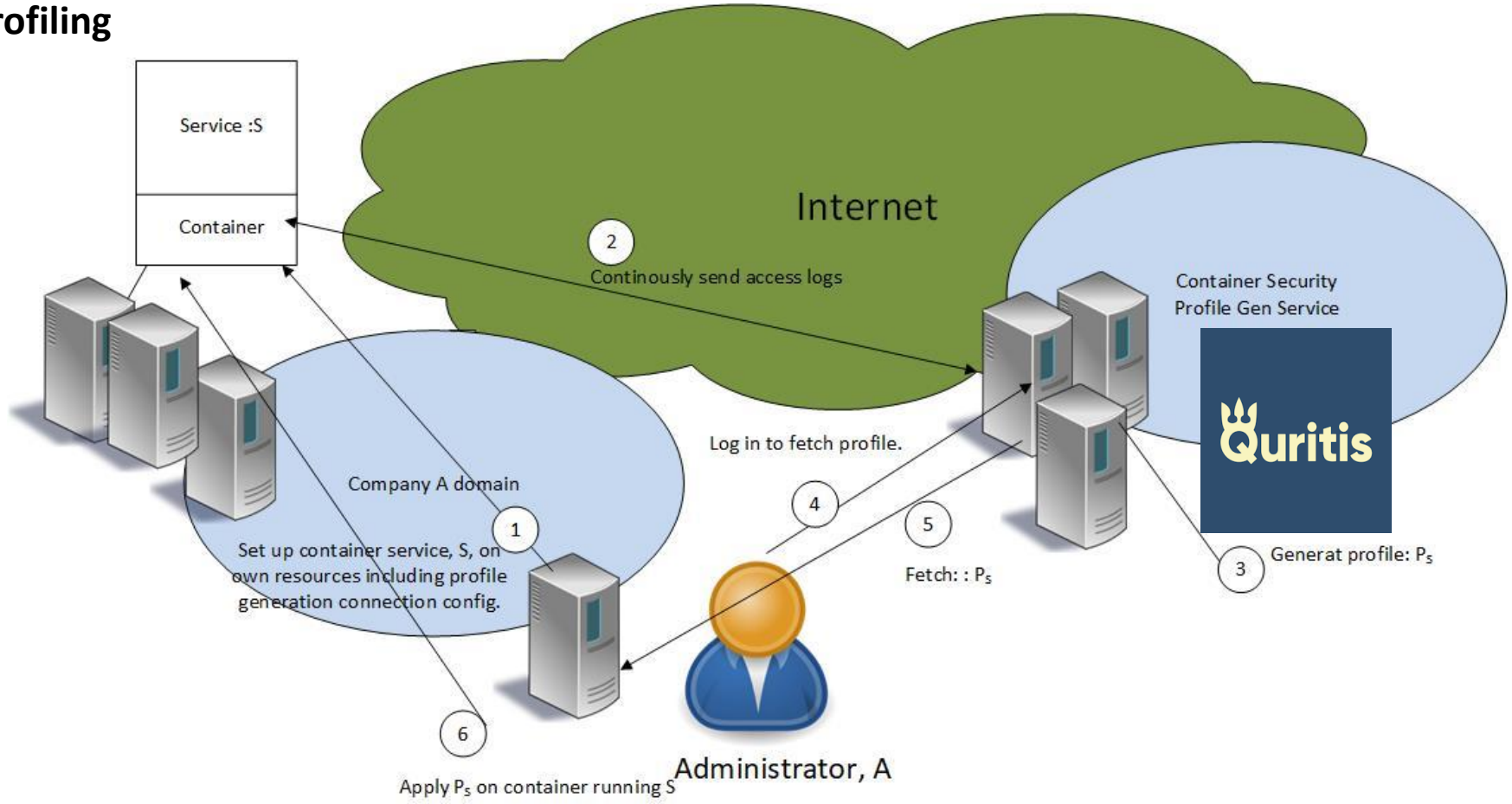
B - Container security (II)

Case 1 – Cloud profiling

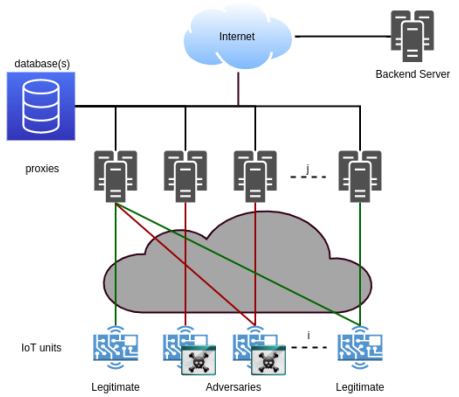


B- Container security (III)

Case 2 – Online profiling



C- DoS prevention (I)



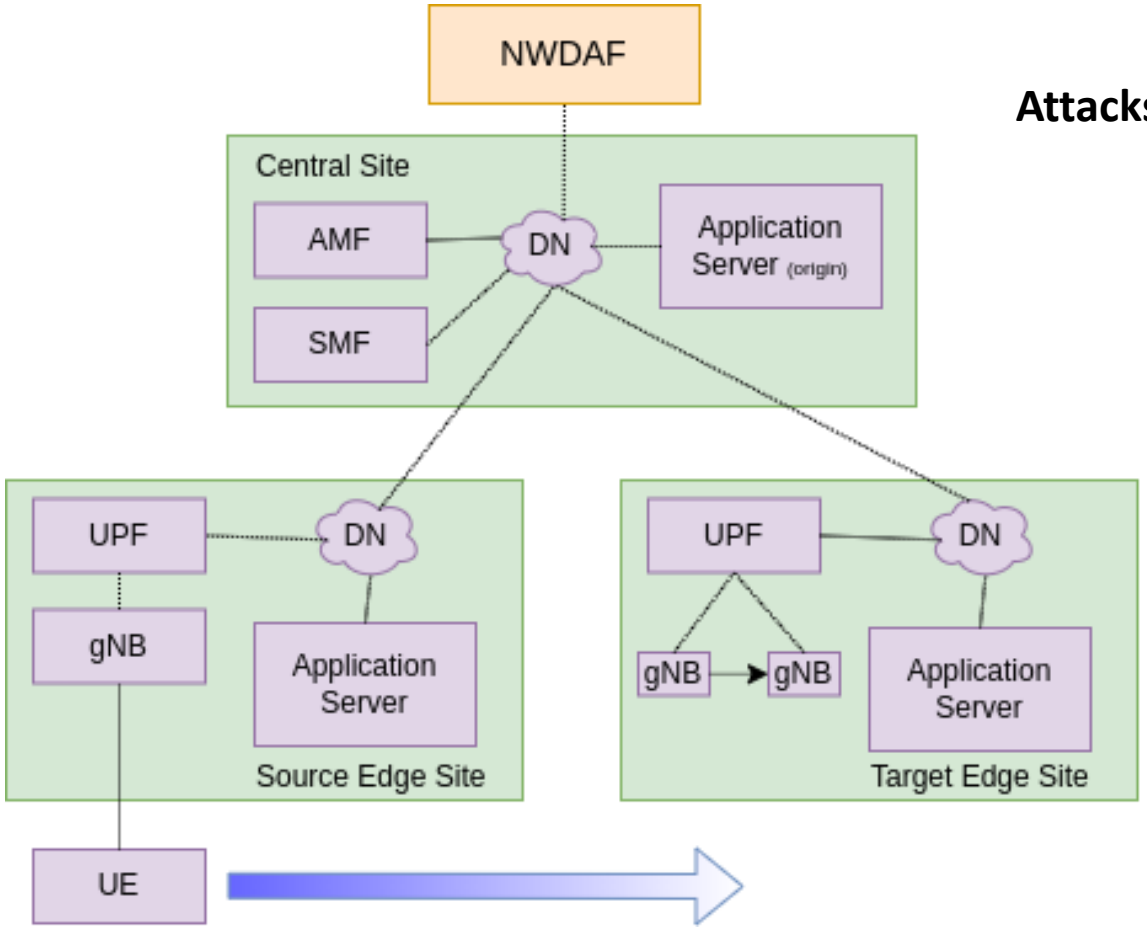
Why do we think this is interesting?

- 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

C- DoS prevention (II)

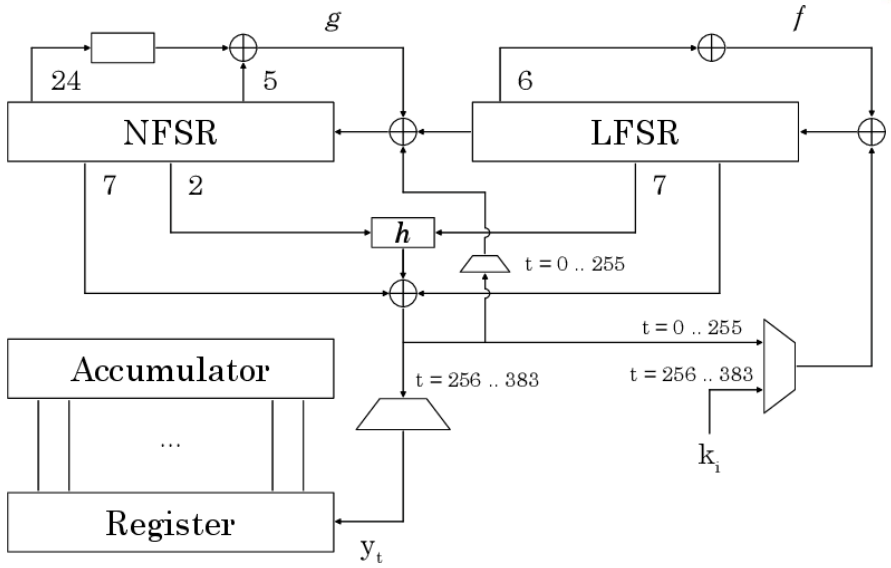


Attacks on the 5G Network Data Analytics Function (NWDAF)

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 Twins with, advanced access control and anomaly detection
- Continuous update of AppArmor profiles
- NWDAF poisoning and mobility attack detection and prevention

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