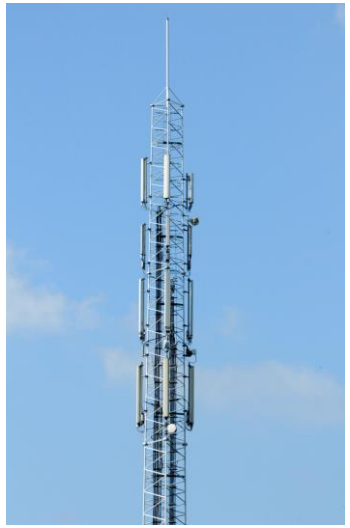
Use of Cryptography in Operational Technology



Contents

1. What is OT?
2. Cryptography in OT
3. Quantum-safe OT

Operational technology

- Software and hardware
- Detect or cause a change
- Monitoring, control of industrial equipment, assets, processes, events

- Safety and availability are key

- Industrial control systems
  - Process control
  - Integrity of data

- Programmable logic controllers (PLC)
  - Industrial computer

- Supervisory control and data acquisition systems (SCADA)
  - Control system architecture

Some differences

IT

- Dynamic
- Confidentiality, integrity
- Regular and automated patching
- Standardized
- Flexible
- Encryption on endpoints
- Regularly do pentesting
- Lifespan ~5yrs

OT

- Static
- Safety and availability
- Maybe: patching?
- Sectoral differences
- Legacy systems
- Encryption not supported on hardware
- Pentesting may lead to breakdown
- Lifespan can be >30yrs

OT: types of risks

- Make changes to target system
- Hide valid alerts
- Cause malfunction

- Gain control of management workstation
- Access to a PLC for maintenance

- IT as stepping stone
  - (Spear) phishing
  - Engineering stations

OT Malware

- Stuxnet
  - One of the first viruses to cause physical damage
- Industroyer, Industroyer2
  - Target: Ukranian energy sector
- TRITON
  - First known virus to target Safety Instrumented Systems
- Havex
  - Find and report specific types of servers
- BlackEnergy2, BlackEnergy3

Cryptography in OT

Case study: wind op zee

- Offshore wind turbines
- In 2050: we need to generate 300GWh on the North Sea

What do we want to achieve?

- Generate energy!
- Ensure availability
  - Redundant solution
- Secure environment
  - On/off remotely
- Maintenance
  - Receive sensor data
  - Push firmware updates

What do we want to achieve?

- Generate energy!
- Ensure availability
  - Redundant solution
- Secure environment
  - On/off remotely
- Maintenance
  - Receive sensor data
  - Push firmware updates

What do we want t

- Generate energy!
- Ensure availability

Quantum-safe OT

- What are the risks?
- What do you want to protect?
- Is it possible to migrate your current infrastructure?
- Very important in new security architectures!

Telecommunications security and integrity regulation

Regeling veiligheid en integriteit telecommunicatie

5. Het cryptografisch beschermen van te beschermen kritieke gegevens bij transport door technische infrastructuren.

a. Te beschermen kritieke gegevens worden bij transport met minimaal 112 bits sterkte versleuteld.

b. De cryptografische sleutels die voor de versleuteling, bedoeld in onderdeel a, worden ingezet, worden

per sessie, per vastgestelde tijdeenheid of per

vastgesteld aantal datablokken vernieuwd.

c. Gebruik van (3) TDES wordt uiterlijk 31 december 2023 uitgefaseerd en tot die tijd wordt bij dit gebruik verzekerd dat maximaal 2^20 datablokken met dezelfde sleutel worden vercijferd.

d. Met uitzondering van signaleringsverkeer ziet de netwerkaanbieder erop toe dat de versleuteling, bedoeld in onderdeel a, in alle gevallen end-to-end is.

Additional requirements for OT

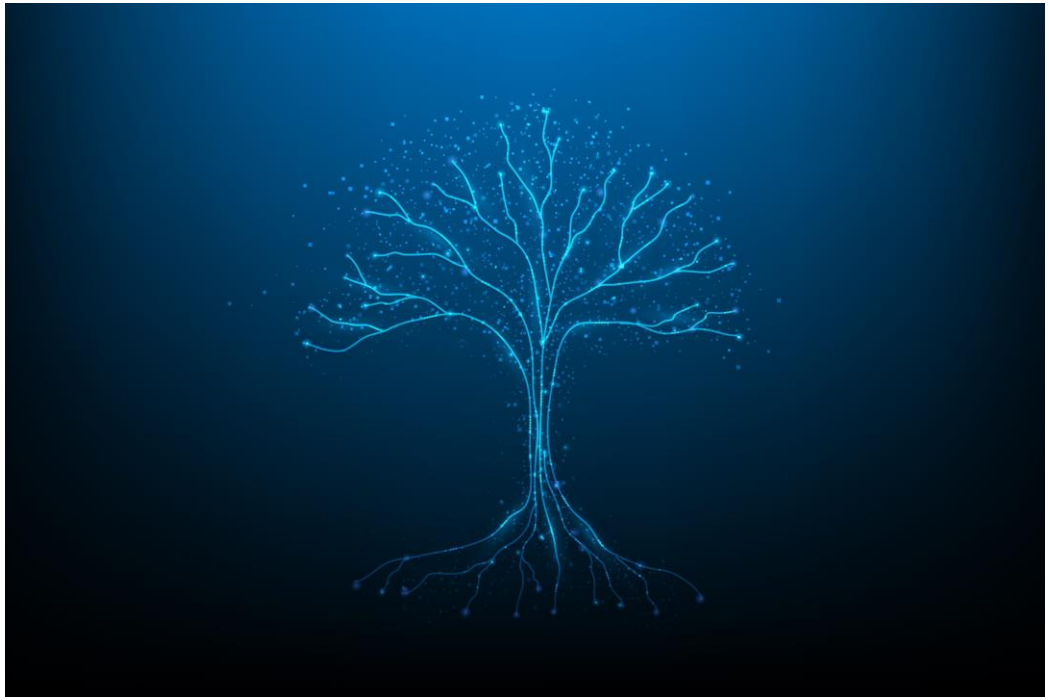
- Dealing with legacy problems
  - Life span exceeds PQC timeline
  - Hardware is not powerful enough for (heavy) cryptography
  - Complex design
- Very specific needs
  - Availability!
- Supplier and vendor management
- Consider the environment
  - Offshore energy: at sea
  - Wind, temperature changes, salt, water

Looking forward

- PQC decision trees
- Security by design for offshore energy

PQC decision trees

- How to find the most appropriate quantum-safe solution?
- All PQC solutions have pros and cons
  - Rating in a matrix
- Per use case: check matrix



Security by design for offshore energy

- Study offshore energy
  - New parks
- Architectural
- Evaluation framework
- Including quantum-safe

- Founding phase
- Public private partnership, including research organizations

Making your IT quantum safe is hard? Try OT!