NOKIA

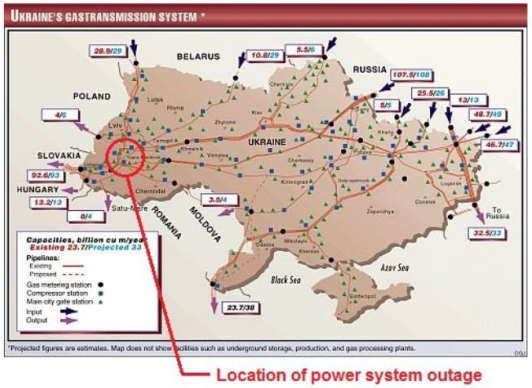
Use of Trusted Computing Technologies in Railways

Ian Oliver

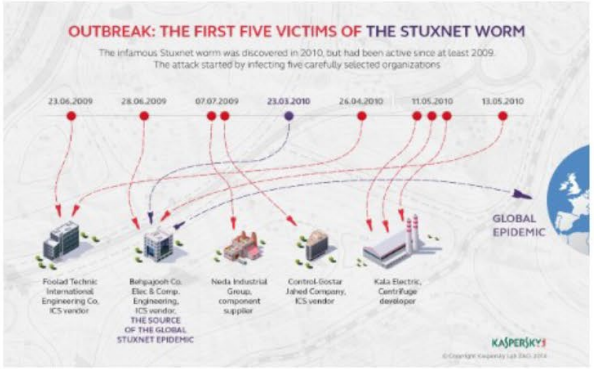
17 January 2023

NOKIA Bell Labs

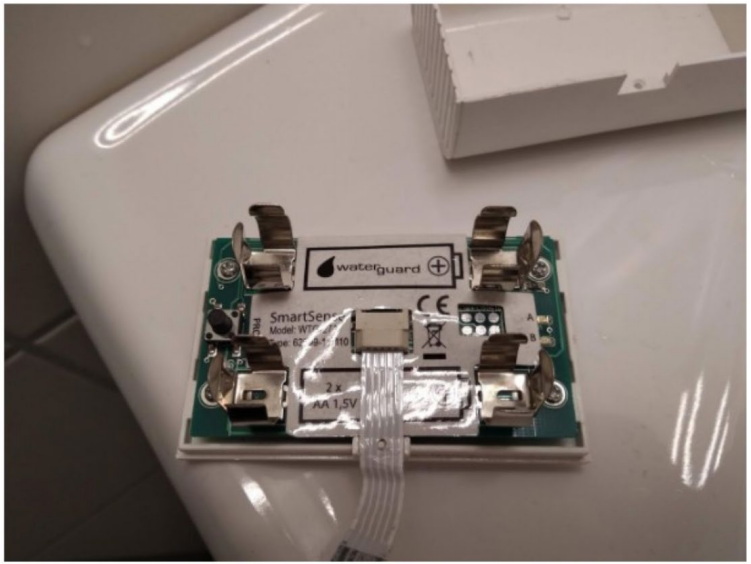
Threat Landscape



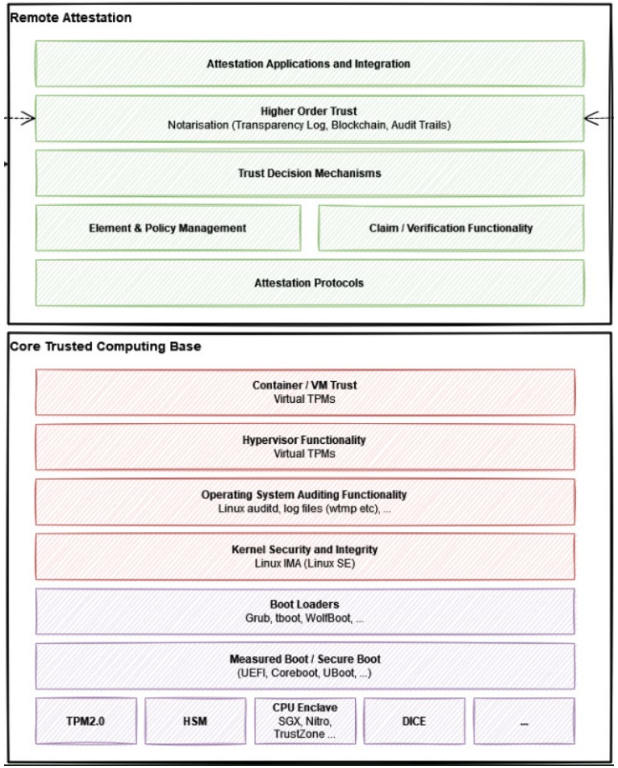
https://www.emptywheel.net/2016/01/11/ukraines-system-company-hacking-coordinated-in-more-than-one-way/



Threat Landscape

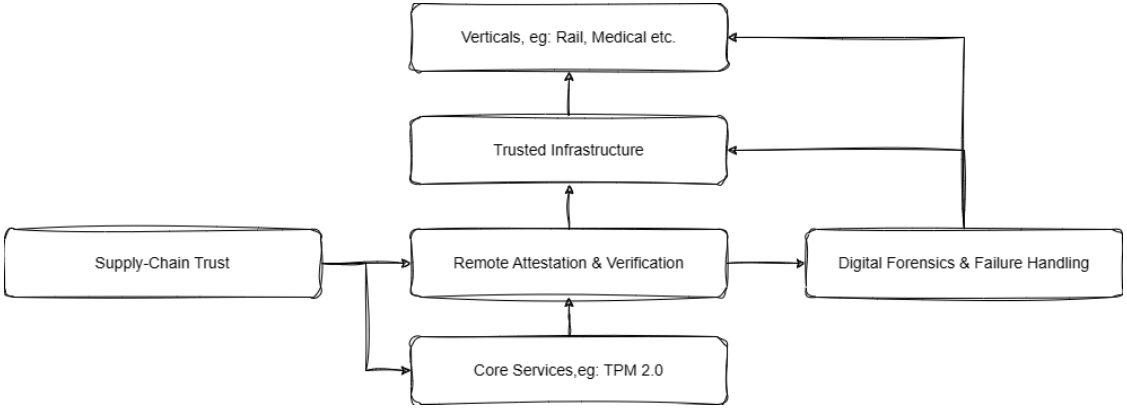


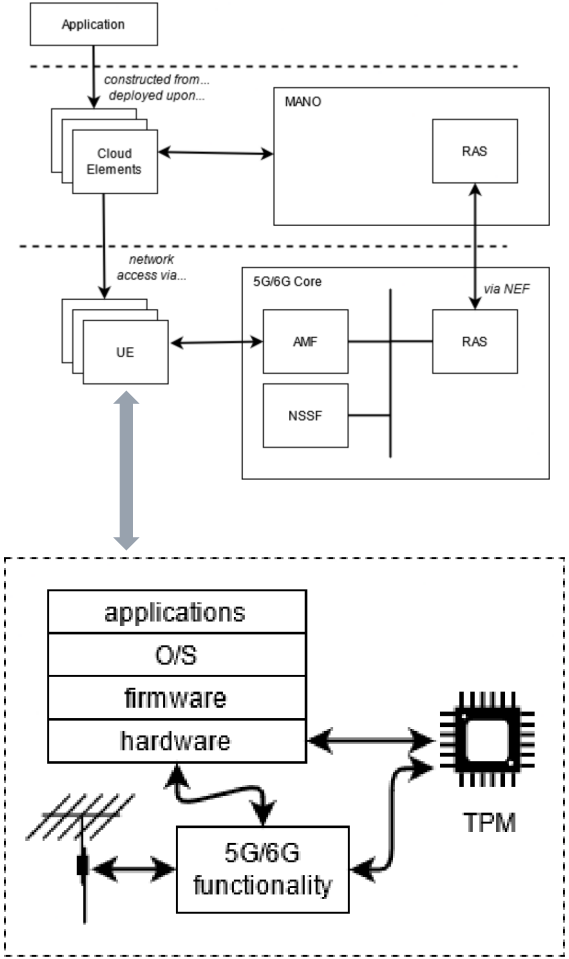
Trusted Computing



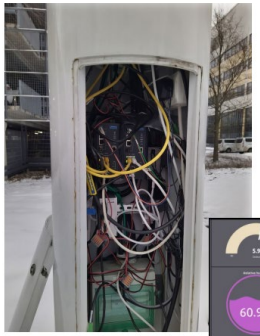
- Root-of-trust (TPM, DICE etc)
  - Proof of Identity
  - Proof of Integrity
  - Attestation
- Boot-time Integrity (SRTM)
  - Secure Boot
  - Measured Boot
  - DRTM (Intel TXT)
- Run-time Integrity Measurements
- TPM & TEE / Enclaving
  - ARM TrustZone, Intel SGX
- Software/VM/Container Integrity

Extended Map & 5G/6G Example

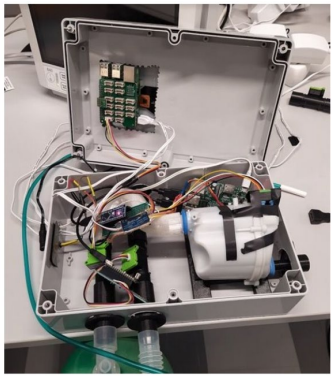




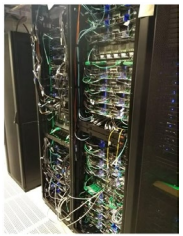
Verticals

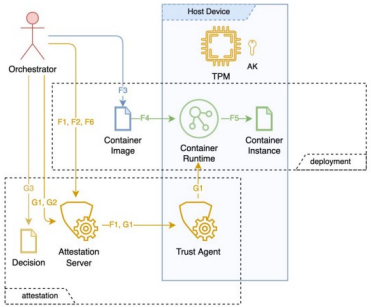


Industry 4.0

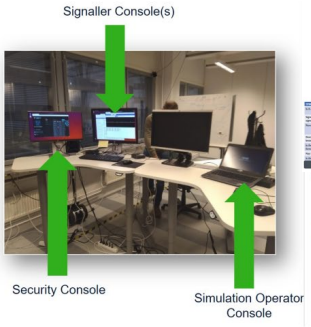


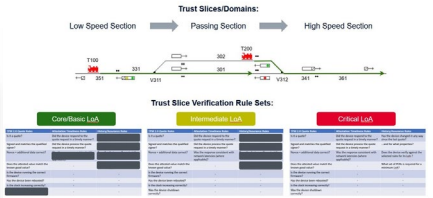
Medical





Edge + Container Trust





Trusted Railway Signalling POC

- Trust in Low Latency Environments
- Trusted Hardware
- Trusted Control Plane
- Dynamic Environment
- Secure App Design Learnings
- FMEA and RCA for Trust
- Security & Trust Processes

Railways

Ronny Bäckmann (2020). Simulating Rail Traffic Management with Trusted Computing. BSc Thesis, XAMK.

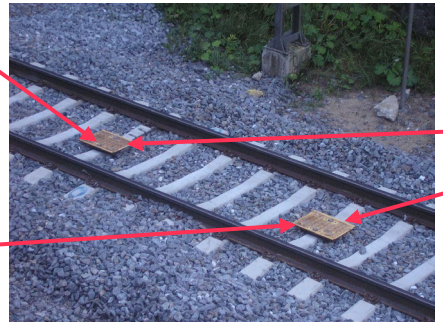
Example - Balise

Is this who it says it is?

Data Integrity?

Software?

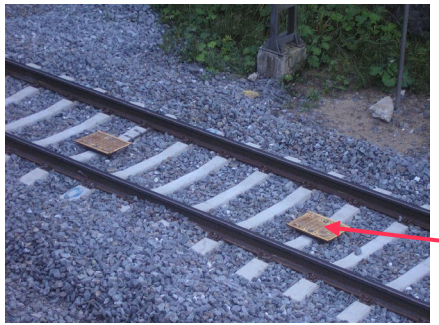
Firmware?



Do they trust each other?

Antti Leppänen - Own work Balises on Orivesi-Jyväskylä railway in Muurame, Finland. CC BY-SA 3.0 File:Balises in Finland.jpg Created: 2009-07′ (3 August 2009, according to Exif data). https://en.wikipedia.org/wiki/Eurobalise#/media/File:Balises_in_Finland.jpg

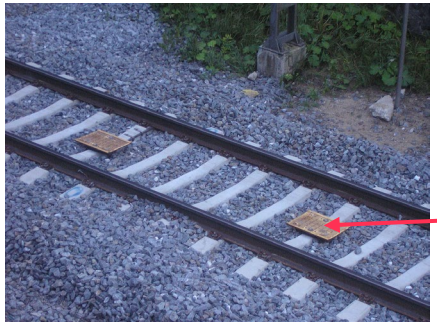
Example – Train-Balis Attestation



How does the train attest the balise?

What does it attest?

Example

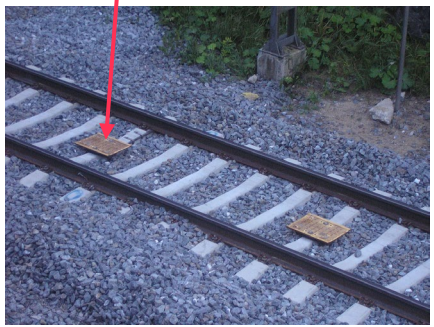


How does the train attest the balise?

Example – Supply-Chain

From where do these components originate?

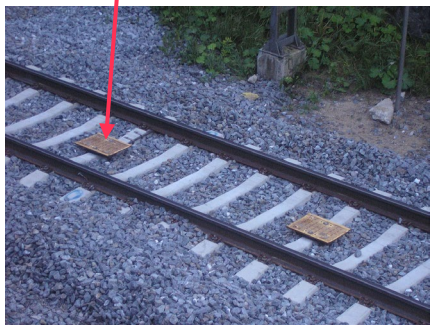
Attestation authority?



Example – Run-Time

Failure Handling
RCA/Safety characteristics

Forensics



Good & Bad(?)

- Supply-Chain
  - Device identity
  - Device integrity measurements
- Run-Time
  - Customer validation
  - Remote Attestation
  - Zero-Trust
- Network Capabilities
  - Trusted 5G Slicing
  - Trusted UE/gNB/ORAN/Core

- x86 UEFI – Standardised
  - PowerPC has DRTM capabilties
- ARM/RISC-V/others
  - TPM available
  - No/limited secure boot/measured boot
  - Some SoCs have build-in TPM (this is good!)
- Lack of Infrastructure
- Legacy Systems
- Latency
- Models of Infrastructure Trust
  - Failure handling

NOKIA