NOKIA Bell Labs

NIST NCCoE 5G Security Workshop

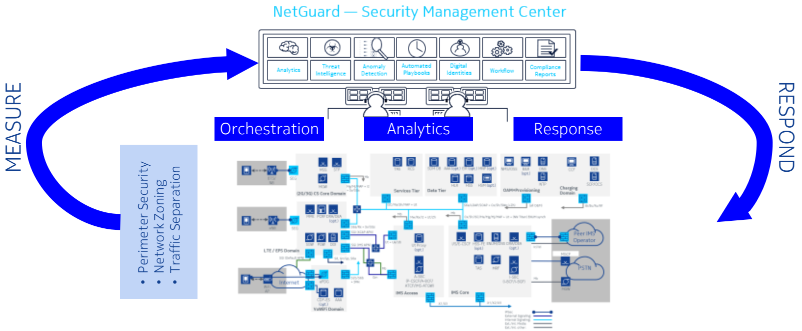
10/10/2019

© 2019 Nokia

Enabling a Secure 5G Networking Infrastructure

Dynamic Defense for known and unknown threats

SOAR



Designed-in security measures

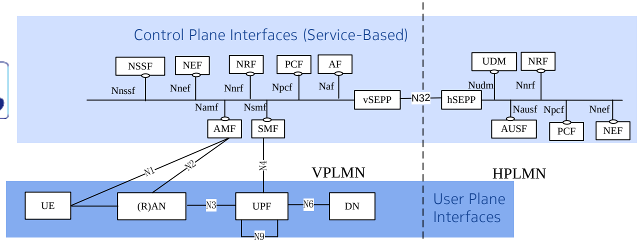
DFSec 2.0

- threat and risk analysis per network element
- network element security architecture
- secure coding
- hardening
- security testing
- security audit
- security vulnerability monitoring
- patching process

VNFs

Standards-compliant Security Architectures

Research & Standardization



From 3GPP TS 23.501

NIST 5G Security Workshop

Potential use cases for NIST 5G Security project

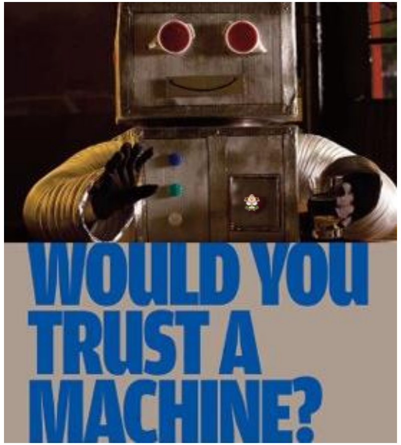
Potential initial use cases

- Trustworthy Computing and Remote Attestation for 5G Systems
- Dependable Geolocation Attributes for VNFs in 5G
- Honeypots in 5G Security Threat Analysis

Other potential use cases

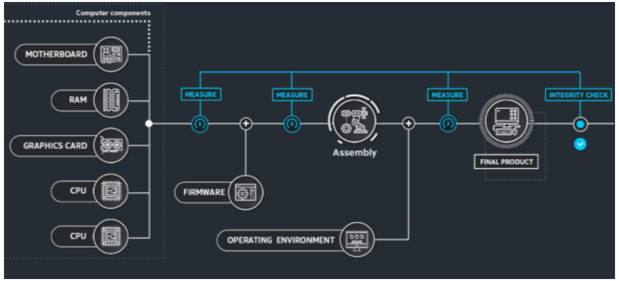
- End to End Network Slicing Security
- 5G networks virtualization security aspects
  - Secure Virtual RAN, Virtual CORE etc

Trustworthy Computing and Remote Attestation for 5G Systems - Introduction



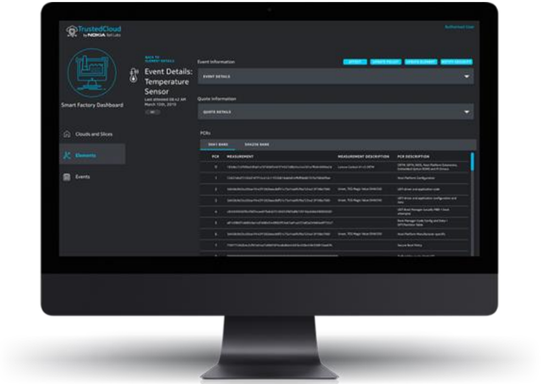
VERIFIABLE ATTESTATION ECOSYSTEM

Guarantee the integrity and provenance of the systems,services and data running across Core, Edge and IoT elements



ATTESTATION AT ALL TIMES

Hardware and Software can be verified, traced and trusted at all stages of the supply chain



WORKING SYSTEM

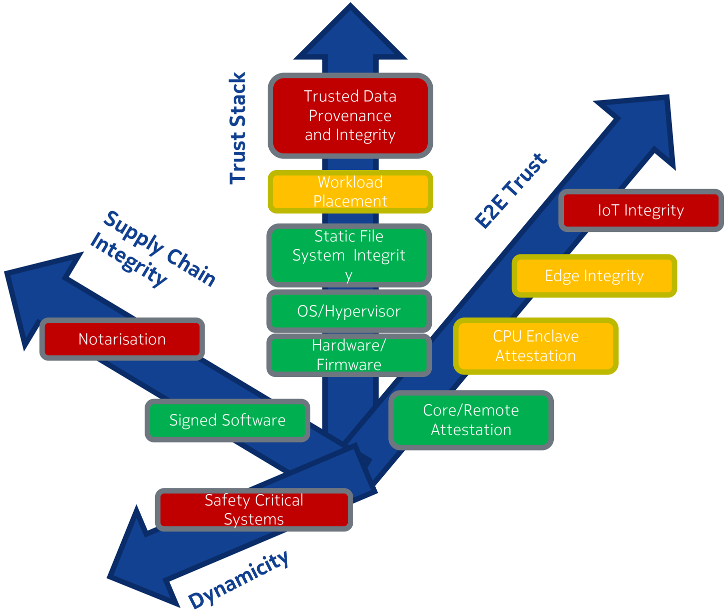
The Working, LIVE, core attestation system. Extensible to data provenance E2E and Supply Chain

VERIFIABLE PRODUCT AND SOFTWARE SUPPLY CHAIN ATTESTATION WITH TRUSTWORTHY COMPUTING

Trustworthy Computing and Remote Attestation for 5G Systems – Technical details

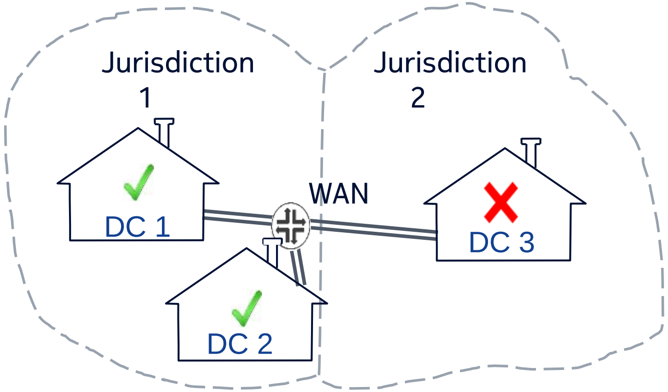
- **Three fundamental questions:**
  - **Can I trust my platform?**
  - **Can I trust my configuration?**
  - **Can I trust my services?**
- **Firmware attacks: hard to detect, devastating in consequences**
- **Leverage the use of Root-of-Trust Technologies (TPM2.0, Remote Attestation etc) a verifiable ecosystem of trust for devices, services and data.**
- **Create an attestation platform that verifies the identity and integrity of our devices and virtual workload against cryptographic measurements**
- **Establish E2E trust by splitting the devices into security attributed slices according to their needed level of trust (e.g. high trust for critical systems)**
- **Introduce a framework for detecting and analyzing trust failures**

Dimensions of Trusted Computing Research



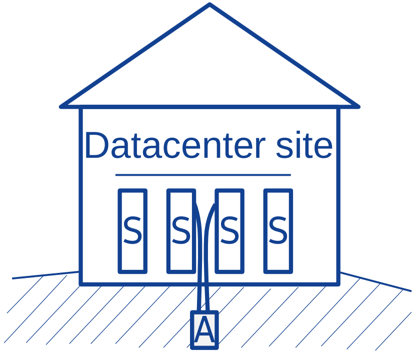
VERIFIABLE 5G PRODUCTS AND SOFTWARE SUPPLY CHAIN ATTESTATION WITH TRUSTWORTHY COMPUTING

Dependable Geolocation Attributes for VNFs in 5G - Introduction



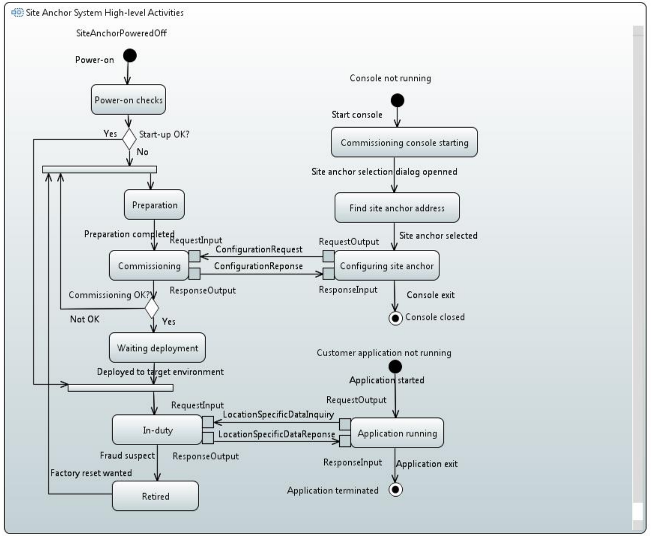
Verifying Location of Data

To protect cloudified data from being stored to hostile jurisdictions, there must be trustful means to detect geolocation of the allocated host.



Trusted Location Anchor

A special certified device for dependably storing datacenter site specific attributes, thus providing root of geographical trust.



Raising Problem Awareness

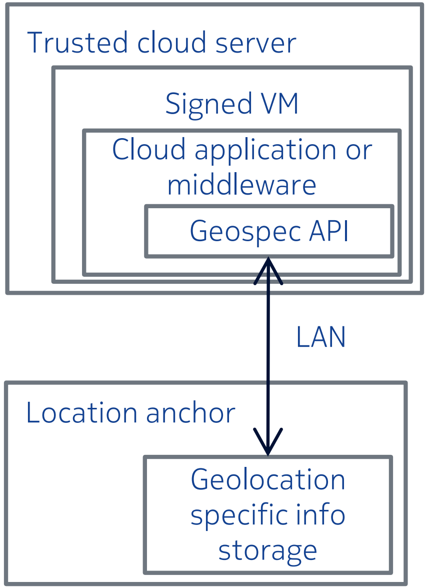
Problem domain dissemination (journal and conference papers, meetings). Proof-of-concept implementation development ongoing.

Supporting dependably geolocation specific attributes for datacenters.

Dependable Geolocation Attributes for VNFs in 5G – Technical details

- **Datacenter (DC) specific info needed, not just global coordinates.**
  - **E.g., jurisdiction code, country code, site name, …**
- **A trustable storage device needed for the above DC attributes.**
  - **Trustable location anchor device (LAD).**
- **Geographical trust is based on:**
  1. **Dependable DC attributes stored into LAD using commissioning terminal.**
  2. **Trusted auditor supervises the data in LAD.**
  3. **LAD initialized once, used forever. LAD contents unrevocable.**
  4. **Trusted software stack in cloud servers – Geospec API and trusted boot.**

Trusted site specific data software stack


Trusted cloud server
Signed VM
Cloud application or middleware
Geospec API
LAN
Location anchor
Geolocation specific info storage

Datacenters with certified geolocation attributes.

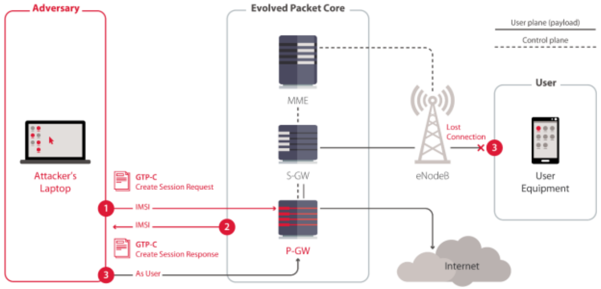
Honeypots in 5G Security Threat Analysis - Introduction

TELCO ATTACK VISIBILITY

DISCOVER THE REAL ATTACKS AGAINST MOBILE CORE NETWORK

TELCO CORE HONEYPOT

DECEIVE ATTACKERS TO REVEAL PRESENCE AND TECHNIQUES



CREATE AND DEPLOY

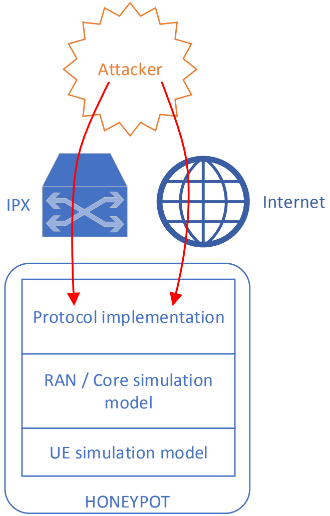
AUTOMATE DECEPTION, DETECTION AND PROCESSING

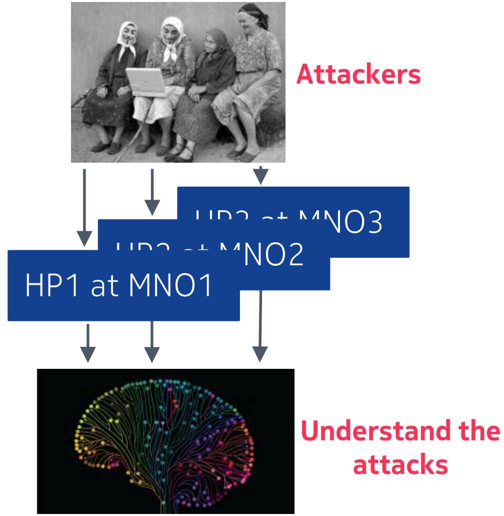
AUTOMATED AND EXTENSIVE INTELLIGENCE ON 5G NETWORK INFRASTRUCTURE THREATS

Honeypots in 5G Security Threat Analysis – Technical details

- Accidental exposure and abuse of telco core nodes is known to take place but little knowledge exists of attacks targeting the nodes
- There is a need to gain threat intelligence
  - Implement core network specific protocol behavior on a self-standing simulation backend
  - Expose protocol port(s) to attackers
  - Record & analyze traffic to protocol port
- Place honeypot into carriers networks as an independent malicious activity sensor
- Collate data from multiple sensors for malicious traffic clustering and follow-up mitigation creation / deployment
  - Multiple honeypots enable cross-correlation between attack traffic and possibly attacker profiling
  - Step towards attack attribution

Telco honeypot architecture





Connectivity and backend simulation system layers, deployment strategy

AUTOMATED AND EXTENSIVE INTELLIGENCE ON 5G NETWORK INFRASTRUCTURE THREATS

NIST 5G Security Workshop

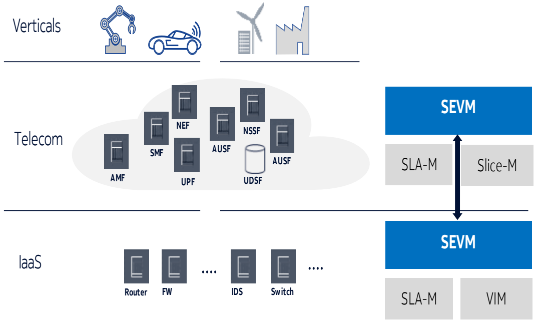
Secure slicing use cases

- End-to-end security solutions for 5G and mission critical networks must enable end-to-end network slicing security.
- We need “**slicing-native security solutions**” that will ensure security and trustworthiness of the end-to-end network slices –
- These security solutions are based on 5 key areas that can be explored further in the NIST project:
  - **"Accountable Security"** that provides failproof distributed self-managed identification of industrial IoT devices in mobile and dynamic environments e.g. by utilizing Blockchain technology
  - **"Physical and Virtual entity Integrity Protection"** that provides scalable integrity attestation (hardware, firmware, OS, and applications) across the supply chain including the patching process.
  - **Artificial Intelligence enabled** "Threat Detection and Mitigation for Network Slices" like detecting malicious third party and open-source 5G services based on an anomaly detection.
  - **"Fine-grained Security Policy Management"** which dynamically tailors network slice elements to meet specified security requirements
  - **Automated "Dynamic data protection"** which addresses the issue of data **isolation** across mobile devices, applications and slices

Automated Security Management for 5G Network Slicing

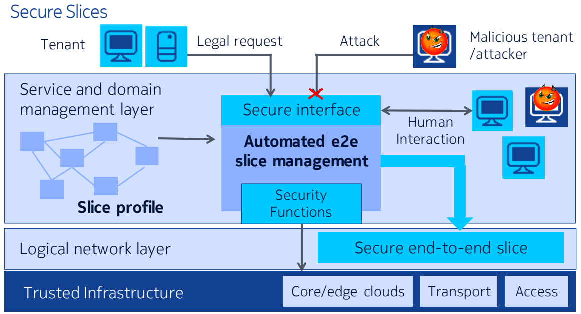
5G: How to secure diverse sensitive services over a huge attack surface

Sliced 5G networks are expected to support highly sensitive services, but will have a huge attack surface. A plethora of protection measures are required and need to be managed in a highly dynamic way.



Key: slice-aware, adaptive security orchestration

Slice-aware and adaptive security management and orchestration is the key enabler for protecting 5G networks and fulfilling per-slice security service level agreements.



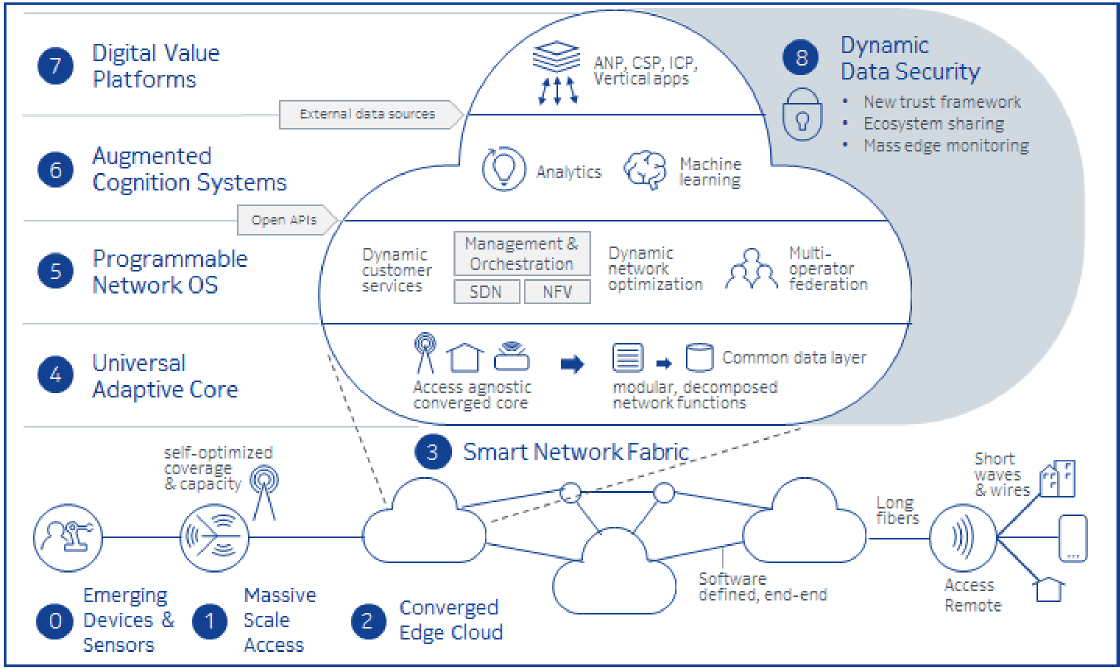
Automated security for the lifecycle of slices

Security management tasks during deployment and operation of 5G network slices are automated. Security management supports different use cases and business models.

Automate and optimize security management for end-to-end slices

© 2018 Nokia

What is the Nokia Future X Labs?


7 Digital Value Platforms
External data sources
6 Augmented Cognition Systems
Open APIs
5 Programmable Network OS
4 Universal Adaptive Core
ANP, CSP, ICP, Vertical apps
8 Dynamic Data Security
New trust framework
Ecosystem sharing
Mass edge monitoring
Analytics
Machine learning
Dynamic customer services
Management & Orchestration
SDN
NFV
Dynamic network optimization
Multi-operator federation
Access agnostic converged core
modular, decomposed network functions
Common data layer
3 Smart Network Fabric
self-optimized coverage & capacity
Long fibers
Short waves & wires
Software defined, end-end
Access Remote
0 Emerging Devices & Sensors
1 Massive Scale Access
2 Converged Edge Cloud

Future X Labs

- Located in Murray Hill, New Jersey
- Several 5G Security use cases.
- 5G Security is a co-operative effort among network equipment vendors, operators, governments, academia and even users,

© 2018 Nokia