Security Conference

ETSI NFV & NFV Security State of the Nation

Presented by: Leslie Willis

19/10/2023

Introductions

Bio: Leslie Willis

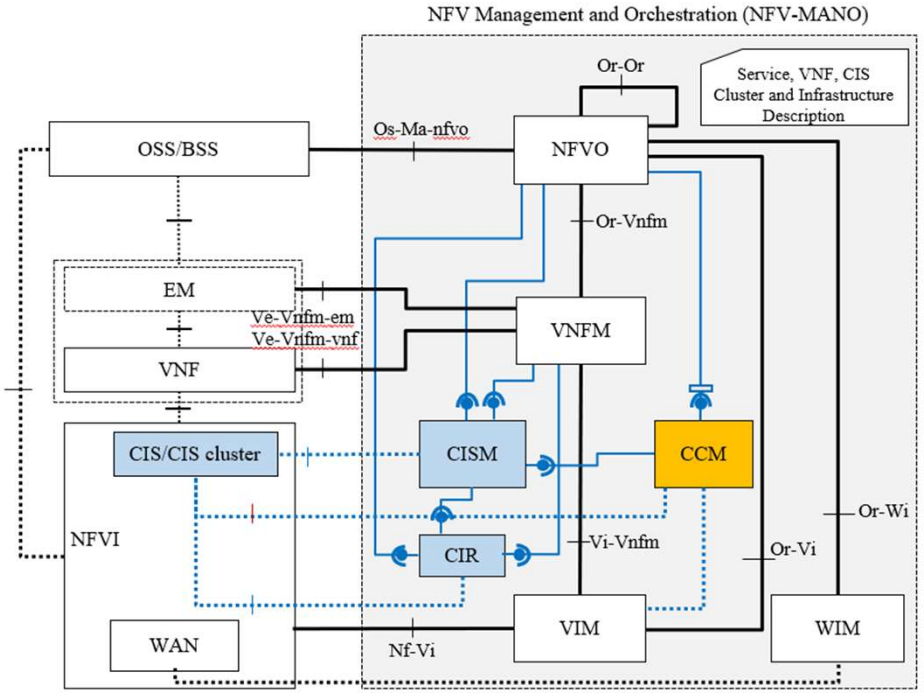
- ETSI ISG NFV SEC Working Group Chair
- Principal Security Authority and Distinguished Engineer at BT plc
- Working in cyber security for the last 18 years and working at BT since 1996

ETSI NFV Release 4

Focus: orchestration, cloudification and simplification of network deployment and operations.

Interfaces, modelling, etc. to support new features such as (not exhaustive list):

- Container-based deployments
- Further 5G support
- Autonomous management and automation
- Generic OAM functions, …



ETSI NFV Release 5

Work on release 5 has already started.

Focus: consolidation and ecosystem.

Interfaces, modelling, etc. to extend current and new features such as (not exhaustive list):

- VNF configuration
- Green NFV
- NFV for vRAN
- Flexible VNF deployments
- Service-based architecture concepts
- Cloud-native VNF reliability, etc

ETSI NFV SECurity, Past to Present

NFV-SEC 001 published 2014

- Set out potential areas of concern

NFV-SEC 003 published 2014 and updated in 2016

- Describes security and trust guidance that is unique to NFV development, architecture and operation

23 ETSI NFV SEC work items (WIs) over several releases (Rel-2, Rel-3, Rel-4)

- Reports (GRs) and Specifications (GSs)
- 6 active non-published WIs with 2 more being published imminently

Several IFA and SOL relevant specifications

- IFA026, IFA033, SOL004, SOL013, etc.

Security considerations clause in GRs

ETSI NFV SECurity Current Work

NFV-SEC 020 Identity Management and Security Specification

NFV-SEC 022 Access Token Specification for API Access

NFV-SEC 023 Container Security Specification

NFV-SEC 024 Security Management Specification

NFV-SEC 025 Secure End-to-End VNF and NS management specification

NFV-SEC 026 Isolation and trust domain specification

NWI Security Assurance Specification (SCAS) for (VIM, VNFM & NFVO)

Remote Attestation and Trusted Compute

Working definition:

- A platform that uses roots of trust to provide reliable reporting of the characteristics that determine its trustworthiness.

Initially explored in NFV-SEC 003 Security and Trust Guidance.

Attestation technologies and practices covered in NFV-SEC 007 (2017) and attestation architecture further covered in NFV-SEC 018 (2019).

Further work is ongoing within

- NFV-SEC 023 Container Security Specification
- NFV-SEC 025 Secure End-to-End VNF and NS management specification
- NFV-SEC 026 Isolation and trust domain specification

Challenges and Benefits

Challenges

- Complexity of Technology – HMEE's (Intel SGX, AMD SEV, etc) and TPMs
- Interoperability
- Root of Trust – Protection of the root key and ground truth database
- Legacy debt
- Support from Chip to Kernel and beyond

Benefits

- Establishes a secure root of trust, ensuring the integrity of the system from the moment it boots up
- Secure boot processes that prevent the execution of unauthorized or tampered code during system startup
- Provides the capability to remotely attest to the integrity of a system or application, ensuring its trustworthiness to external parties
- Helps meet regulatory and compliance requirements by providing robust security measures and audit capabilities

Security Considerations

ETSI NFV-SEC 001, 003, etc are still very relevant.

Secure Boot: Leaking of UEFI signing keys & software bugs an issue

- CVE-2022-21894 - The BlackLotus campaign

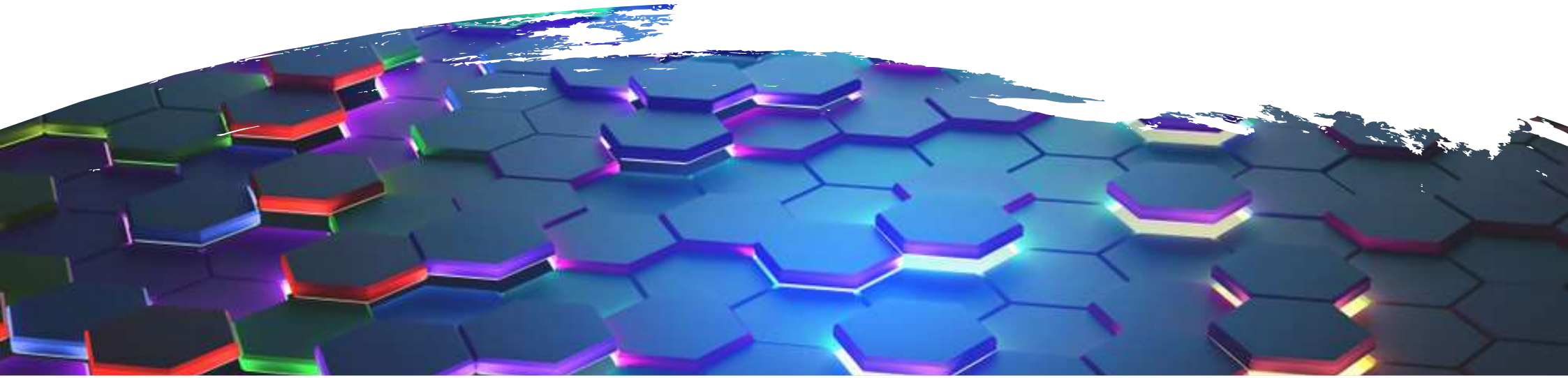
Remote Attestation:

- Need to integrate into OpenStack (Trusted Compute Pool) and Kubernetes
- Fully supported Telco ready Remote Attestation Service
- Monitoring the Verification Function and Relying Party
- Supply Chain Attack Mitigations

Any further questions?

Contact me:

Leslie.willis@bt.com



Thank you for your attention

Follow us on: