**SA WG3 Meeting #115-Ad-Hoc-eS3-241103**

**April 15th – 19th, 2024**

**Source: Dell Technologies, Defense Information Systems Agency EM, The MITRE Corporation, US National Security Agency, US Department of Homeland Security**

**Title: New use case for security evaluation and monitoring: NFV vulnerabilities**

**Document for: Approval**

**Agenda Item: 5.1**

**Work Item / Release: FS\_eZTS / Rel-19**

# 1 Decision/action requested

***This pCR proposes new use case for TR 33.794: Study on enablers for Zero Trust Security.***

# 2 References

[1] 3GPP TR 33.894, “Study on applicability of the Zero Trust Security principles in mobile networks”, Release 18.

[2] 3GPP SP-231784, New SID on enablers for Zero Trust Security, Release 19

[3] 3GPP TR 33.794 V0.1.0, “Study on enablers for Zero Trust Security”, Release 19

[4] 3GPP TS 23.288, “Architecture enhancements for 5G System (5GS) to support network data analytics services”, Release 18.

[5] 3GPP TS 29.520, “5G System; Network Data Analytics Services; Stage 3”.

[6] NIST Special Publication 800-207: "Zero Trust Architecture".

# 3 Rationale

The 5G Service Based Architecture (SBA) is characterized by a diverse set of Network Functions (NFs) that interact through defined application programming interfaces (APIs). However, the existing security mechanisms, which rely on Authentication and Authorization for access control, need to overlay with Zero Trust principles to counter the rapidly evolving threat landscape. An effective Zero Trust model demands continuous verification of all entities within the network, emphasizing on the need for identity and context-aware security measures that adapt in real-time to the threats. Implementing Zero Trust in 5G SBA involves deploying advanced security technologies that can dynamically adjust access controls and policies based on real-time assessment of user behaviour, device security posture, and context based factors for access control. Moreover, it shifts the focus on the NFs individually and ensures that security decision is informed by comprehensive data, including anomaly detection and threat intelligence.

The solution addressing this use case must evolve towards incorporating real-time threat detection and response mechanisms. These mechanisms could leverage advanced analytics and machine learning to adaptively assess and respond to threats, ensuring that access controls are dynamically adjusted in accordance with the risk profile of Zero Trust tenets [6].

To address the Zero Trust Security requirements in SBA, we need to analyse vulnerabilities associated with various aspects of components, interfaces, and their capabilities of the network architecture. From the vulnerabilities, the next step would be to analyse how network function virtualization (NFV) elements can be secured against exploitation, ensuring API interactions are robust against unauthorized access, and implementing advanced encryption to mitigate the risk of Man-in-the-Middle attacks. Additionally, it is important to develop effective identity verification process to prevent identity spoofing and implement comprehensive defence strategies against potential attacks. These areas should be considered to enhance SBA to be more resilient and secure aligned with Zero Trust principles. To support detection of vulnerabilities, enough data needs to be exposed. For detection of the attacks, the information contained in the data exposed includes:

- Data source: identity (including unique identifier which can identify the system, device, components, or the virtual functions that generate the logs)

- Attributes of data source

- Time

- Relevant activities and events

- Application layer

- Operation, e.g., for VNF

- Network access (physical and virtual)

- Security related information including authentication, authorization, privilege level and security protection configuration.

# Detailed Proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 5.1.w Use case #w: NFV vulnerabilities

#### 5.1.w.1 Description

The VNF in a SBA network could expose 5G networks to security risks. For example, vulnerabilities in virtualization layer can lead to failure in isolating VNFs and data breaches. If there are insufficient security controls within the VNFs, an attacker might gain unauthorized access to these functions. This could lead to a scenario where the attacker is able to manipulate network traffic, disrupt services, or even extract sensitive data being processed by these virtualized functions.

There are two modes of data collection, periodically or at the request based on the predefined events or triggers (as an example, they normally can be configured in the configuration file).

#### 5.1.w.2 Relevant data

The data to be exposed includes:

- Data source: VNFs with IDs (e.g., NF ID/NF instance ID)

- Attributes of data source:

- Time

- Relevant activities and events

- Application layer: performance metrics (e.g., latency and jitters), data traffic (e.g., http(s), FTP, and SNMP)

- Operation: VNF image installation logs

- Security related information: configuration change logs, access and authentication logs, system integrity checks

#### 5.1.w.3 Evaluation of the identified data

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*