**SA WG3 Meeting #115-Ad-Hoc-eS3-241105**

**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: Man-in-the-Middle (MitM) attacks**

**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.y Use case #y: Man-in-the-Middle (MitM) attacks

#### 5.1.y.1 Description

Man-in-the-Middle (MitM) attacks can be prevalent in SBA networks due to their fully interconnected nature. MitM attacks in SBA exploit the communication between functions as well asintercept and potentially alter data.One of the prevalent attack is replay attacks wh TLS is compromised, such as using self-signed certificate, weaker signature algorithm, expired certificate etc. These attacks can incur unauthorized network configurations, compromise the confidentiality and integrity of sensitive information, leading to unauthorized access and fraud, compromised network services and potential data breaches. Examples include during a network slice creation process, an attacker could intercept the API calls between the Network Slice Management Function (NSMF) and the Network Slice Subnet Management Function (NSSMF), manipulating the data or commands being exchanged.

#### 5.1.y.2 Relevant data

The data to be exposed includes:

- Data source: Communication between NFs

- Attributes of data source:

- Time

- Relevant activities and events

- Application layer: authentication latency metrics, authentication, data traffic patterns (e.g., changes in packets payload size)

- Security related information: authentication logs (e.g., to detect the downgrade attacks), changes in digital certificate and validation, duplicated session IDs/sequences #, changes in encryption protocols.

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

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