S3-234011
(revision of S3-yyxxxx)

Smarter technology for all

Release 19
Study on enablers for Zero Trust Security (eZTS)

Lenovo

2020 Lenovo Internal. All rights reserved.

Motivation (1/2)

To Enable Zero Trust Security Adaptations for 5G Core Network

- Service Access and Interactions in 5G system are built on certain security principles:
  - Authentication and/or Authorization
  - Secured connection establishment
- Heterogenity and varied NF deployment options (could be distributed across cloud infrastructure/locations):
  - May run into errors due to configuration issues
  - May get exposure to insider threats
  - May get compromise due to cyber attack
- Trust over a NF or AF can‘t be assumed static and intact throughout its lifetime despite all security pre-configurations
- If any NF gets compromised in its life-time:
  - Impacts set of UEs service
  - May impact other network services e.g., connected NFs (i.e., by lateral movement of the attack)

Lenovo 2020 Lenovo Internal. All rights reserved.

Motivation (2/2)

Zero Trust Security

- The core principle of Zero Trust includes:
  - Continuous security evaluation/monitoring, trust validation and minimizing impacts if any security breach occurs due to external (example., end-users) or by an insider (example., compromised or malicious NF)
  - Adaptation of Zero Trust approach can prevent the lateral movement and further compromises limiting the threats and associated risks.

In the scope of 5G Core:
Existing 5GS core network features assume NFs, set with initial access Configurations as trusted (i.e., reliable) throughout its life-time.

- Adaptation of Zero Trust approach in 5G Core can benefit largely to:
  - prevents the threat lateral movement and further compromises (limiting the threats & associated risks).
  - realize full potential benefits for vertical service customers, and business.
  - ensures service reliability among network functions and for the end users.

Lenovo 2020 Lenovo Internal. All rights reserved.

Related ZTS effort made in Release – 18

TR 33.894 - Study on applicability of the Zero Trust Security principles in mobile networks

- Study Outcome resulted in the following recommendations/observations:
  - **Key Issue(s):**
    - Key Issue #1: Need for continuous security monitoring
    - Potential security requirements: ‘The 5GS is required to support mechanisms to collect necessary data to enable security monitoring’.
  - **Zero Trust Tenet evaluation (Tenets 1 to 7):**
    - Some of the NIST ZT tenets were evaluated in TR 33.894 and identified that tenets (T1, T2, T3) related to authentication, communication security and authorization were already supported by the 5G system core network.
    - Tenet 5 evaluation was complete:
      - Evaluation says, ‘It is worth investigating whether there is any additional information that could be exposed by the 5G Core NFs for monitoring purposes’, ‘’this information needs to be well defined and explicitly specified to allow for interoperability and secure operation of installed base.
    - Tenet 6 and 7 were partially evaluated and the following aspects were not addressed.
      - For T6, as per evaluation ‘how the data from security monitoring is considered in access decisions is not addressed’.
      - For T7 even though the evaluation recommends to facilitate data collection, processing of data and using of insights to improve policy creation and enforcement, there is an EN on further evaluation.
    - Tenet 4 has not been evaluated.

Lenovo 2020 Lenovo Internal. All rights reserved.

A Short Summary

Tenet evaluation status in TR 33.894

Tenets	NIST	TR 33.894	Status
1	All data sources and computing services are considered resources.	Tenet #1: Resources	# Any Network Functions and their services in the 5G Core are to be considered as a resource in the context of a ZT deployment plan. # Evaluation completed. No additional work needed.
2	All communication is secured regardless of network location.	Tenet #2: All communication is secured regardless of network location	# The 5G Core standards provide the necessary means (i.e., on network layer, there is NDS/IP applicable to all interface in 5GC they are IP based; on transport layer there is TLS applicable to service-based ones as they are HTTP based) to secure the communication with and within the 5GC. # Evaluation completed. No further work needed.
3	Access to individual enterprise resources is granted on a per-session basis.	Tenet #3: Access granularity	# NF consumers and producers required to mutually authenticate during the TLS session establishment via certificates. Then the NF consumer may be required to present an OAuth2.0 authorization token to the producer in the service request within the TLS tunnel. These two mechanisms provide the necessary tools for an operator to control authorization at almost a service invocation level. # Evaluation completed. No further actions identified.
4	Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.	Not evaluated so far. So it does not exist in the TR	# Evaluation not done (no consensus reached yet!)
5	The enterprise monitors and measures the integrity and security posture of all owned and associated assets.	Tenet #5: Security posture	# Evaluation Completed. (Action needed!) Copied evaluation summary below: # A security monitoring function can be outside the SBA and the security monitoring function itself would be mostly proprietary. # <u>It is worth investigating whether there is any additional information that could be exposed by the 5G Core NFs for monitoring purposes</u>. # In the event of that this study determines that strengthening of the external to 3GPP security monitoring is needed, with not yet specified data collection, <u>this information needs to be well defined and explicitly specified</u> to allow for interoperability and secure operation of installed base.
6	All resource authentication and authorization are dynamic and strictly enforced before access is allowed.	Tenet #6: Access security	# Incomplete evaluation Editor's Note: How the data from security monitoring is considered in access decisions is FFS. Editor's Note: further evaluation is FFS
7	The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.	Tenet #7: Data collection to improve security posture	# Almost complete (But there is an EN, which makes the evaluation incomplete) Editor's Note: The rest of the evaluation is FFS.

Lenovo 2020 Lenovo Internal. All rights reserved.

Background on how ZT related Tenets (1 to 7) can be applicable to 5GS

(An example overview)

Already Supported

2-3

UE to Network Security

UE and Network mutual authentication with EAP-AKA'/5G AKA or using any optional EAP methods.
NAS, AS and RRC protection using keys resulting from mutual authentication.
Subscription based service access control

Already Supported

2-3

Core Network - Service Based Interfaces Security:

- Mutual Authentication
  # All NFs supports mutual authentication with TLS and HTTPS.
  # TLS - Transport layer protection (or)
  # NDS/IP - Network layer protection
- Authorization
  - # Static Authorization – local authorization policy
  - # Token based Authorization (e.g., Oauth 2.0 access token)

Already Supported

2-3

5G Core and Access Network Non-Service Based Interfaces Security:

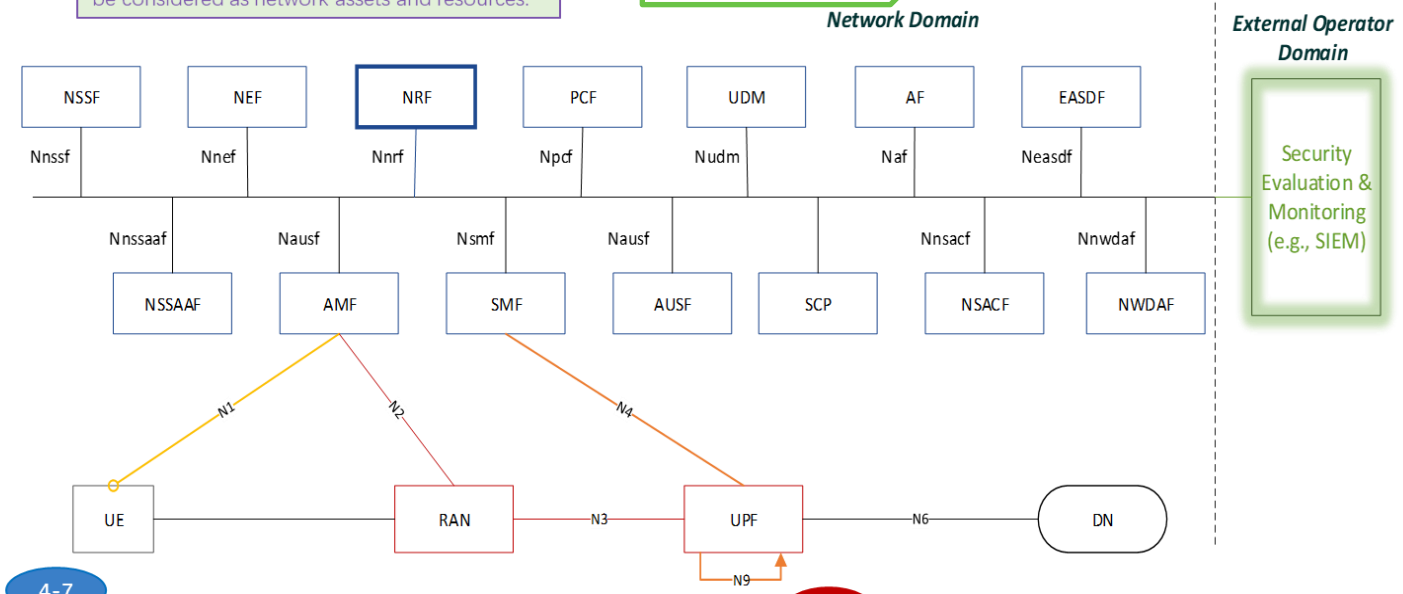
- IP based interfaces
  # NDS/IP - Network layer protection
  - Implements IPsec ESP and IKEv2 certificates-based authentication
  # In addition DTLS (Transport layer security) is supported for mutual authentication
  # Non-SBA Interfaces internal to Core: N4 and N9.
  # Other Non-SBA Interfaces: N2, N3, Xn

1

All Network functions, devices and services can be considered as network assets and resources.

Already applicable Analogy

Outside 3GPP domain



4-7

Based on TS 23.288 - Limited effort exist for UE related usecases:
Example: NWDAF detects following risk:

- Suspicion of DDoS attack
  - PCF may request SMF to release the PDU session.
- Too frequent Service Access
  - AF may release the AF session; PCF may request SMF to release the PDU session

Limited Support available

4-7

No security mechanism exist for Network related usecases:
Initiated 3GPP Rel.18 SA3 TR 33.894 - Study on applicability of the Zero Trust Security principles in mobile networks. So far, there is no related support exist in any SA3 specs,

Not yet Supported

Take away for core network (SBA security):

- T1-T3 are supported.
- T5 needs additional effort as identified in TR 33.894
- T4, T6,T7 evaluation need to be completed to check if an additional effort is required.

Lenovo 2020 Lenovo Internal. All rights reserved.

What can we potentially analyse during the course of the study:

- For any NF that is compromised/exhibits abnormal behaviour, what impacts will it have?
  - Do we have methods to identify the NF that has been compromised/behaving abnormally?
  - Simply terminating a compromised/misbehaving NF would impact all ongoing services.
  - As required analyse and identify suitable mechanisms to prevent threat lateral movement and to ensure service availability in this case.
  - Identify and correct the means of compromise to ensure the replacement NF will not be compromised in the same manner.
- Complete evaluations of Tenet 4, 6 and 7.

Lenovo 2020 Lenovo Internal. All rights reserved.

Scope

- The Objective of the study includes:
  - *Based on TR 33.894 KI#1 security requirement and Tenet 5 evaluation, analyze and identify the data to be collected in the 5G core network and enable the external security evaluation and monitoring (if not completed in Rel.18).*
    - *NOTE: The external security evaluation and monitoring is up to operator's implementation i.e., outside the 3GPP domain.*
  - *Analyse the impacts and threats related to compromised NF(s) and abnormal NF behaviors.*
  - *For NFs that have been identified as compromised/misbehaving, analyze suitable security mechanism to prevent lateral movement and minimize impact to service availability.*
  - *Study how logical aspects of Policy Decision Point (PDP)/Policy Enforcement Point (PEP) can be integrated into the existing network function(s).*
  - *Provide Recommendations for network based Zero trust security adaptation, where the recommendations may include but are not limited to requirements, technical enhancements, and procedural fixes.*
  - *Complete evaluations of Zero Tenet 4, 6, and 7.*

Lenovo 2020 Lenovo Internal. All rights reserved.

thanks.

Smarter technology for all

Lenovo