ITU Workshop on “Security for 5G and beyond”
22 August 2022

Japan’s 5G security guidelines

Ayumu Kubota
KDDI Research Inc.

Background

- In 5G era, we expect significant changes in mobile network infrastructure and surrounding environment, and threat landscape will also changes
  - Virtualization
  - Use of open-source software
  - Exposures of network interfaces
  - Increased complexity of system and networks
  - Supply chain risks
- Although there are many security enhancements in 5G specifications, 5G operators need a comprehensive guidance in order to securely configure and operate 5G networks
- Supported by the Ministry of Internal Affairs and Communications (MIC), Japanese operators, a manufacturer and a research institute had been collaborated to develop a 5G security guideline document

Scope of Japan’s 5G security guidelines

■ This guideline document,

- **provides comprehensive guidance on securing the 5G System in practice**
- **focuses on 5G Standalone (SA)**
- **covers not only technology but also people and process aspects affecting the security of 5G services**
- **describes security threats and recommended controls at a high-level and provides references to established standards and best practices where relevant**
  - described security threats and recommended controls are the result of a threat modelling exercise as well as practical security tests performed in a 5G laboratory network

■ Intended audience

- **primarily intended to be used by telecommunication service providers deploying and operating a 5G System**
- **the document also contains recommendations for suppliers of 5G technology**

Usage of the guidelines

- The guidelines present security threats to the 5G system and relevant security controls in a structured manner.

- The purpose is to provide readers with practical advice on identifying and addressing common security challenges.

- Rather than specifying each security control in full detail, the document assumes that readers adapt control prioritization and implementation to their individual scenario and the associated security risk.

Threat analysis and security tests in 5G laboratory network

- **First, we identified threats to the 5G system and supporting technologies based on the STRIDE-LM model**

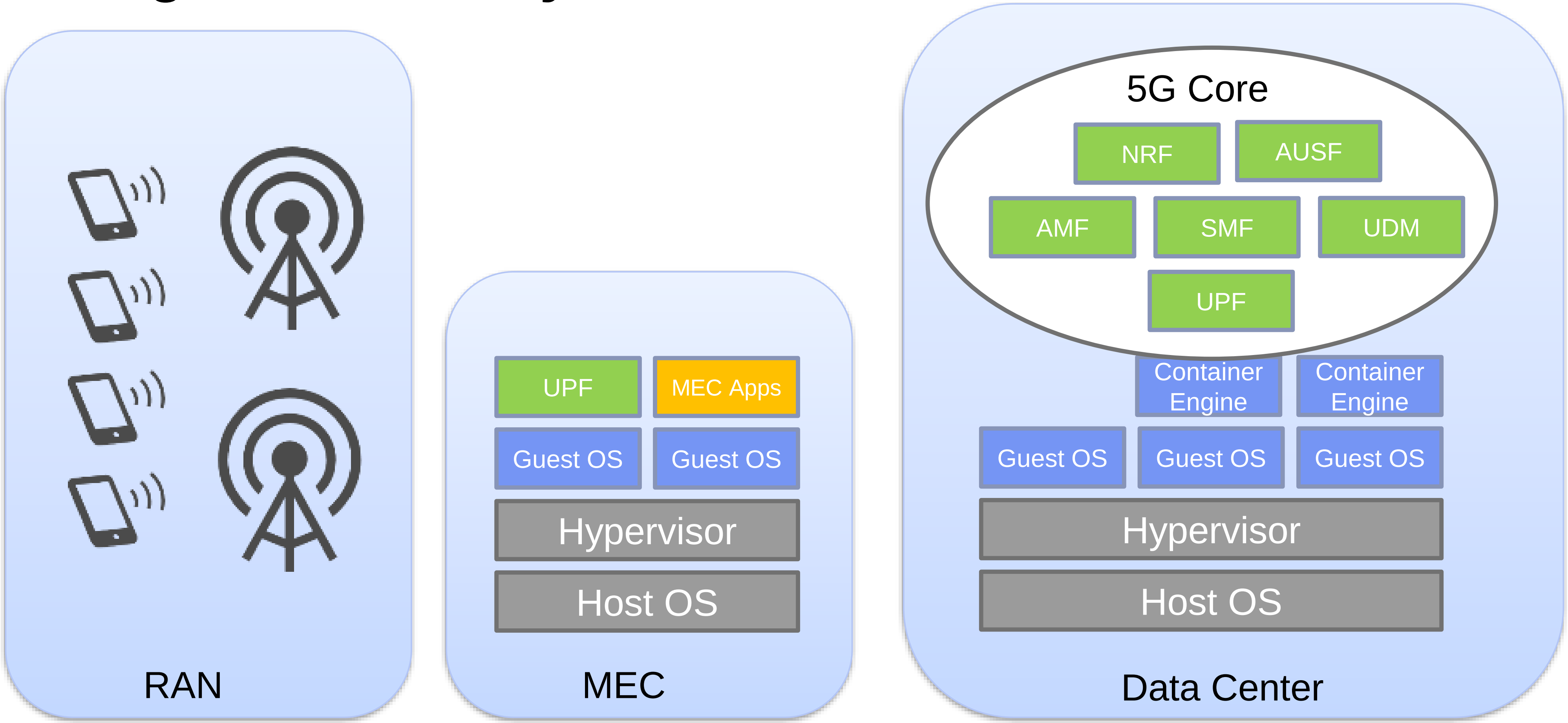
- **Results of security tests performed in a 5G laboratory network are also incorporated**

- **5G Laboratory Network**
  - **Uses 3 different 5G implementations**
    - R&D purpose implementations including open sources
  - **NFV Infrastructure (OpenStack, Kubernetes)**

- **Security Tests**
  - **Fuzzing**
  - **DoS attack**
  - **Security conformance tests**
  - **Penetration tests**

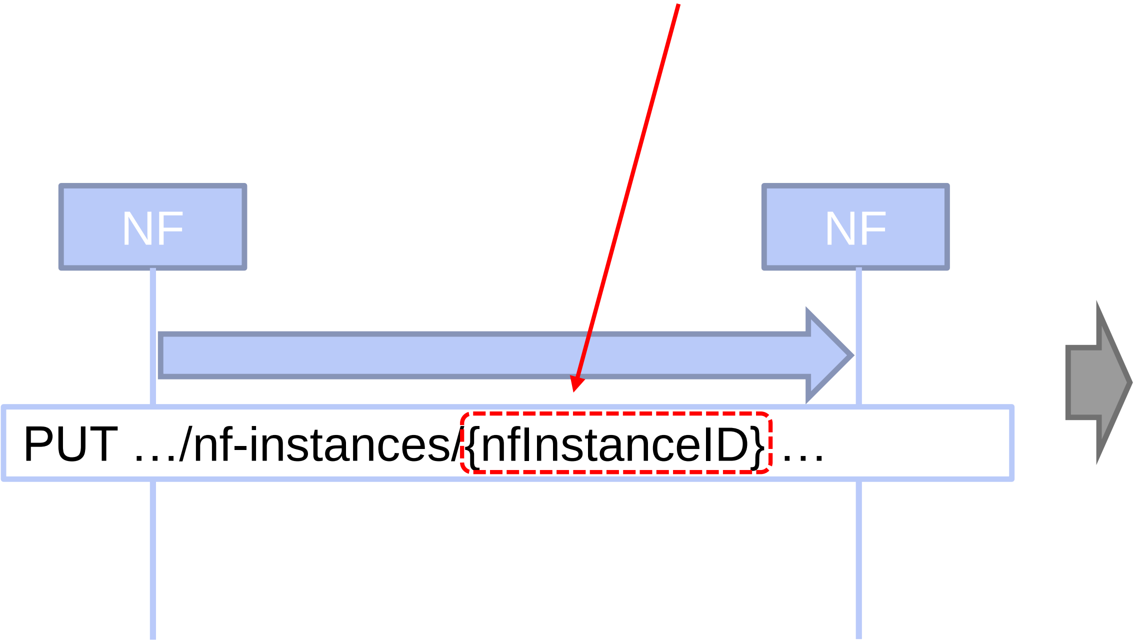
5G Laboratory Network

- Entire 5G system (Core, RAN, MEC, Virtualization infrastructure) is the target for security tests



Examples of security tests - Fuzzing

- **Fuzzing test against interfaces of NFs (Network Function)**
  - **e.g. Sending malformed requests**
    - Increase the size of nfInstanceID in the request, in this example



Verify the result and NF’s status after handling the request

Examples of security tests – conformance tests

Test cases:

- Validating the protection of initial NAS messages
- Validating the freshness of the Subscription Concealed Identifier
- Validating the protection of network capabilities
- Validating NF De-registration Requests
- Validating TLS enforcement in NF-NF communication

.

.

.

.

.

- Prohibiting illegal AS algorithm values

Pre-conditions:

- Test environment with a UE in a non-registered state
- Network public key provisioned to the UE
- SUPI concealment enabled in USIM

Execution steps

1. UE performs primary authentication with a SUCI
2. Tester records the SUCI value provided
3. UE disconnects from the network
4. UE invalidates previous security context
5. UE initiates another primary authentication with SUCI (not 5G GUTI)

Expected result

- SUCI value used in both authentication runs is different

Some finding from security tests

■ Implementation problems

- ● **Susceptible to DoS**
  - Excessive Registration Requests caused instability of 5G core
- ● **Problem in API implementation**
  - Fuzzing test against caused reboot of a certain NF
- ● **Failures to security conformance tests**
  - SUCI freshness, Validation of NF De-registration requests, OAuth implementation etc.

→ 5G operators should consider building their own security test catalog and automated test pipeline that each 5G component has to pass before being deployed in production

■ Virtualization increases number of attack surfaces

- ● **Especially when multiple virtualization technologies (virtual machines and containers) co-exist**

→ Appropriate isolation of workloads/networks is critical

Structure of guideline

1. Scope

2. Introduction

2.1 Terminology used
2.2 Structure of this guideline
2.3 How to use this guideline

3. Key Technical Concepts

3.1 5G System
3.2 Network Function Virtualization
3.3 Network Slicing
3.4 Multi-Access Edge Computing
3.5 Criticality of 5G System Domains

4. Security Threats

4.1 Generic Security Threats
4.2 Threats to NFV Infrastructure and MANO
4.3 Threats to NFV Workloads
4.4 Threats to Radio Access Network
4.5 Threats to Core Network
4.6 Threats to Network Slicing
4.7 Threats to MEC

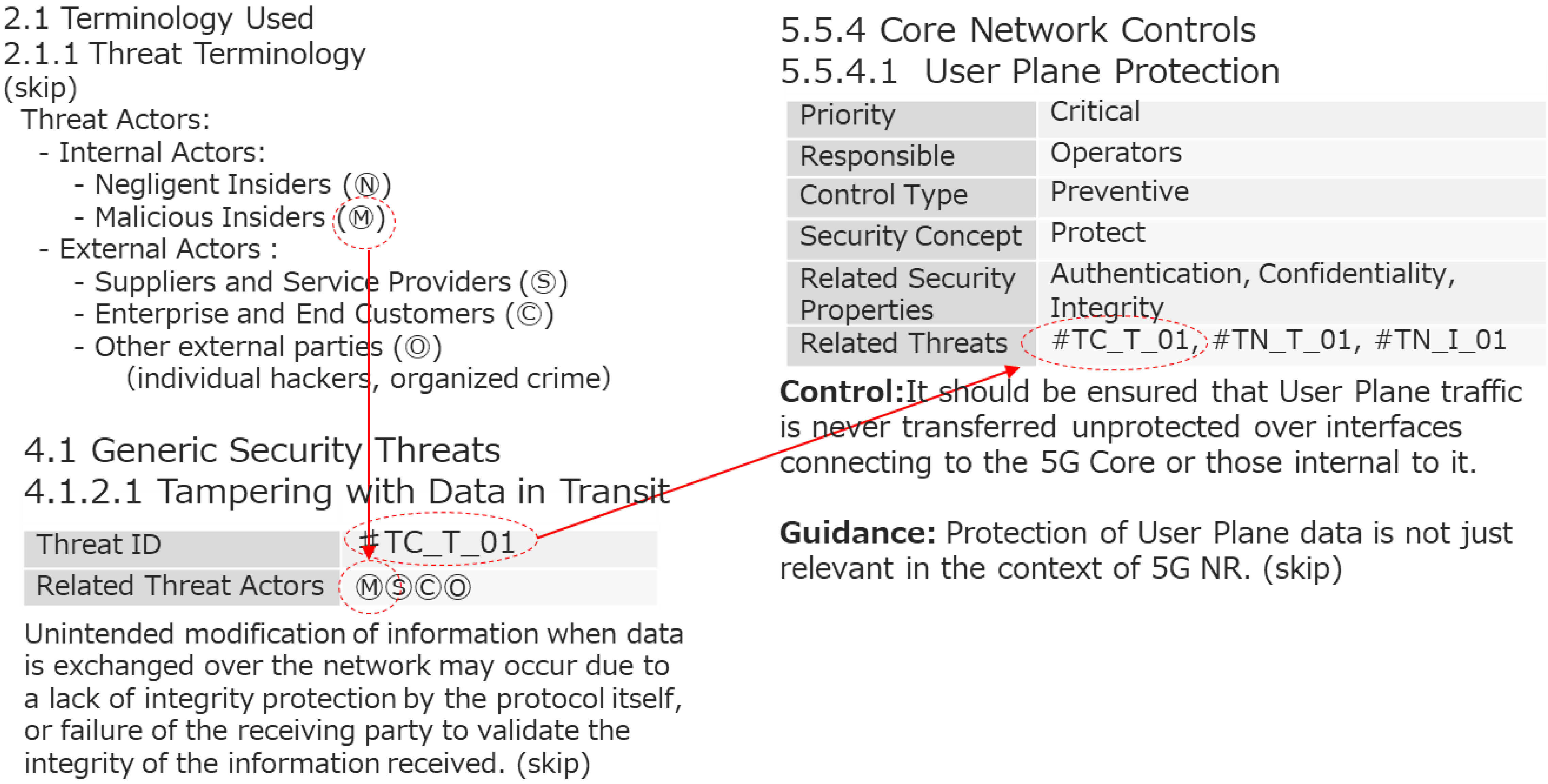
5. Security Controls

5.1 Organizational Controls
5.2 People Controls
5.3 Operational Controls
5.4 Physical Controls
5.5 Technical Controls
5.5.1 Generic Technical Controls
5.5.2 Virtualization Controls
5.5.3 Radio Access Network Controls
5.5.4 Core Network Controls
5.5.5 Network Slice Controls
5.5.6 MEC Controls

Appendix A

A.1 Open RAN Security Consideration

Structure of guideline



2.1 Terminology Used
2.1.1 Threat Terminology
(skip)

Threat Actors:

- Internal Actors:
  - Negligent Insiders (Ⓝ)
  - Malicious Insiders (Ⓜ)
- External Actors :
  - Suppliers and Service Providers (Ⓢ)
  - Enterprise and End Customers (Ⓒ)
  - Other external parties (Ⓞ)
    (individual hackers, organized crime)

4.1 Generic Security Threats
4.1.2.1 Tampering with Data in Transit

Threat ID	#TC_T_01
Related Threat Actors	ⓂⓈⒸⓄ

Unintended modification of information when data is exchanged over the network may occur due to a lack of integrity protection by the protocol itself, or failure of the receiving party to validate the integrity of the information received. (skip)

5.5.4 Core Network Controls
5.5.4.1 User Plane Protection

Priority	Critical
Responsible	Operators
Control Type	Preventive
Security Concept	Protect
Related Security Properties	Authentication, Confidentiality, Integrity
Related Threats	#TC_T_01, #TN_T_01, #TN_I_01

Control: It should be ensured that User Plane traffic is never transferred unprotected over interfaces connecting to the 5G Core or those internal to it.

Guidance: Protection of User Plane data is not just relevant in the context of 5G NR. (skip)

Current status

- The first version of the guideline document is released in April 2022
  - https://www.soumu.go.jp/main_content/000812253.pdf (in Japanese)

- Using our guidelines as a baseline document, we are to propose a new work item “Security controls for 5G network systems” in ITU-T SG17 this week

KDDI

KDDI Research