

Recommendation

ITU-T X.1818 (09/2024)

SERIES X: Data networks, open system communications
and security

International Mobile Telecommunications (IMT) security

Security controls for operation and maintenance of IMT-2020/5G network systems

ITU-T X-SERIES RECOMMENDATIONS

Data networks, open system communications and security

PUBLIC DATA NETWORKS	X.1-X.199
OPEN SYSTEMS INTERCONNECTION	X.200-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999
INFORMATION AND NETWORK SECURITY	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1839
METaverse AND DIGITAL TWIN SECURITY	X.2000-X.2199
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1818

Security controls for operation and maintenance of IMT-2020/5G network systems

Summary

Recommendation ITU-T X.1818 provides comprehensive guidance on securing the international mobile telecommunications (IMT-2020)/5G system during operation and maintenance phases in practice. The described security threats and recommended security controls are the result of a threat analysis.

The focus of this Recommendation is the IMT-2020/5G Standalone (5G SA) system as well as the virtual infrastructure and associated management systems that are expected to form the foundation for IMT-2020/5G deployments. Furthermore, consideration has been given not only to technology, but also people and process aspects affecting the security of IMT-2020/5G services. Recommended security controls are described at a high-level and reference established standards and best practices where relevant.

History*

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1818	2024-09-06	17	11.1002/1000/15663

Keywords

IMT-2020/5G system, multi-access edge computing (MEC), network function virtualization (NFV), network slicing, radio access network (RAN), security control, threats.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2024

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	2
5 Conventions	5
6 Overview	5
6.1 Specific terms for threat and control in this Recommendation	5
6.2 Structure of this Recommendation	7
6.3 How to use this Recommendation.....	7
7 Security threats for IMT-2020/5G systems	8
7.1 Generic security threats	8
7.2 Threats to NFV infrastructure and MANO	15
7.3 Threats to NFV workloads	17
7.4 Threats to radio access network	18
7.5 Threats to core network	20
7.6 Threats to network slicing	24
7.7 Threats to MEC	25
8 Security controls for IMT-2020/5G system.....	27
8.1 Organizational controls	27
8.2 People controls	31
8.3 Operational controls	32
8.4 Physical controls.....	39
8.5 Technical controls	40
Appendix I – Key technical concepts of IMT-2020/5G systems.....	62
I.1 The IMT-2020/5G system	62
I.2 Network function virtualization	63
I.3 Network slicing	64
I.4 Multi-access edge computing.....	65
I.5 Criticality of IMT-2020/5G system domains	66
Bibliography.....	69

Recommendation ITU-T X.1818

Security controls for operation and maintenance of IMT-2020/5G network systems

1 Scope

This Recommendation provides recommended security controls for international mobile telecommunications (IMT-2020)/5G network systems including network functions virtualization (NFV), radio access network (RAN), network slicing, and multi-access edge computing (MEC). This Recommendation covers:

- Security threats for IMT-2020/5G network systems, categorized in the high-level threats.
- Recommended security controls, categorized in the major control domains.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 This Recommendation uses the following terms from [ITU-T X.800]:

- access control;
- authentication;
- authorization;
- availability;
- confidentiality;
- denial of service;
- integrity;
- privacy;
- repudiation.

In addition, this Recommendation uses the following additional terms defined elsewhere:

3.1.2 distributed denial-of-service (DDoS) attack [b-ISO/IEC 27039]: Unauthorized access to a system resource or the delaying of system operations and functions in the way of compromising multiple systems to flood the bandwidth or resources of the targeted system, with resultant loss of availability to authorized users.

3.1.3 network function [b-ITU-T Y.3100]: In the context of IMT-2020 a processing function in a network.

NOTE 1 – Network functions include but are not limited to network node functionalities, e.g., session management, mobility management and transport functions, whose functional behaviour and interfaces are defined.

NOTE 2 – Network functions can be implemented on a dedicated hardware or as virtualized software functions.

NOTE 3 – Network functions are not regarded as resources, but rather any network functions can be instantiated using the resources.

3.1.4 network function virtualization [b-ISO/IEC TR 22417]: Technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collections of multiple virtual networks can simultaneously coexist over the shared networks.

3.1.5 network slice [b-ITU-T Y.3100]: A logical network that provides specific network capabilities and network characteristics.

NOTE 1 – Network slices enable the creation of customized networks to provide flexible solutions for different market scenarios which have diverse requirements, with respect to functionalities, performance and resource allocation.

NOTE 2 – A network slice may have the ability to expose its capabilities.

NOTE 3 – The behaviour of a network slice is realized via network slice instance(s).

3.1.6 orchestration [b-ITU-T Y.3100]: In the context of IMT-2020, the processes aiming at the automated arrangement, coordination, instantiation and use of network functions and resources for both physical and virtual infrastructures by optimization criteria.

3.1.7 risk assessment [b-ISO/IEC 27000]: Overall process of risk identification, risk analysis and risk evaluation.

3.1.8 security control [b-NIST SP800-53]: The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

3.1.9 spoofing [b-ITU-T X.1279]: A process of detecting and preventing spoofing of a biometric system through illegitimate actions.

3.1.10 threat [b-ITU-T X.1406]: Potential cause of an unwanted incident, which can result in harm to a system or organization.

3.1.11 virtualized network function [b-ITU-T Y.3150]: A network function whose functional software is decoupled from hardware and runs on virtual machine(s).

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 lateral movement: Techniques that cyber attackers use to move deeper into a network after gaining initial access.

3.2.2 tampering: An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behaviour, or data.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

5G NR	5G New Radio
5G SA	5G Standalone
AI	Artificial intelligence

AF	Application Function
AMF	Access and Mobility management Function
API	Application Programming Interface
AUSF	Authentication Server Function
BCP	Business Continuity Planning
CP	Control Plane
CU	Centralized Unit
(D)DoS	(Distributed) Denial of Service
DLP	Data Loss Prevention
DN	Data Networks
DNS	Domain Name Server
DTLS	Datagram Transport Layer Security
DU	Distributed Unit
EASDF	Edge Application Server Discovery Function
FQDN	Fully Qualified Domain Name
gNB	gNodeB
GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
HBRT	Hardware-based Root of Trust
ICMP	Internet Control Management Protocol
IDS	Intrusion Detection System
IMT	International Mobile Telecommunications
IPUPS	Inter PLMN UP Security
IR	Incident Response
JOSE	JavaScript Object Signing and Encryption
JWS	JSON Web Signature
LADN	Local Area Data Network
MAC	Medium Access Control
MANO	Management and Network Orchestration
ME	Mobile Equipment
MEC	Multi-access Edge Computing
MitM	Man-in-the-Middle
ML	Machine Learning
MME	Mobility Management Entity
MNO	Mobile Network Operator
N3IWF	Non-3GPP Interworking Function
NAS	Non-Access Stratum protocol

NDA	Non-disclosure agreement
NDS	Network Domain Security
NEF	Network Exposure Function
NF	Network Function
NFV	Network Functions Virtualization
NFVI	Network Functions Virtualization Infrastructure
NFVO	NFV Orchestrator
NG-RAN	Next Generation-Radio Access Network
NRF	Network Repository Function
NSACF	Network Slice Admission Control Function
NSSAAF	Network Slice-specific and SNPN Authentication and Authorization Function
NSSF	Network Slice Selection Function
OS	Operating System
PCF	Policy Control Function
PDCP	Packet Data Convergence Protocol
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PRINS	Protocol for N32 Interconnect Security
RAN	Radio Access Network
RRC	Radio Resource Control
(R)RU	(Remote) Radio Unit
R.U.D.Y.	R-U-Dead-Yet
SCP	Service Communication Proxy
SDN	Software Defined Networking
SEPP	Security Edge Protection Proxy
SLA	Service Level Agreement
SMF	Session Management Function
SNMP	Simple Network Management Protocol
SR-IOV	Single-root input/output virtualization
SSH	Secure Shell Protocol
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TARA	Threat and Risk Assessment
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscription Identifier
TNGF	Trusted Non-3GPP Gateway Function

UDM	Unified Data Management
UDP	User Datagram Protocol
UE	User Equipment
UP	User Plane
UPF	User Plane Function
USIM	Universal Subscriber Identity Module
VNF	Virtual Network Function
VNFI	Virtual Network Function Image
VNFM	VNF Manager

5 Conventions

In this Recommendation, the keyword "should" or "recommended" indicates a specification which is recommended but which is not absolutely required. Thus, this specification need not be present to claim conformance.

Additionally, this Recommendation uses the following reference points, as defined in [b-3GPP TS 33.501]:

F1: Reference point between gNB-CU and gNB-DU;

N2: Reference point between the (R)AN and the AMF;

N3: Reference point between the (R)AN and the UPF;

N6: Reference point between the UPF and a data network;

N9: Reference point between two UPFs;

N26: Reference point between MEE and AMF;

N32: Reference point between SEPP in the visited network and the SEPP in the home network;

N33: Reference point between NEF and AF;

Xn: Reference point between two NG-RAN nodes.

6 Overview

6.1 Specific terms for threat and control in this Recommendation

6.1.1 Threat description

Threats are categorized according to common threat models, such as STRIDE-LM [b-STRIDE LM], and the threat category at a high level (high-level threat) is summarized with the mapping to the related security property in Table 1.

Table 1 – High-Level Threats and Related Security Properties

High-Level Threat	Related Security Property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization
Lateral Movement	Network Segregation

Given the complexity and increased exposure of the IMT-2020/5G system towards multiple external entities, network segregation and policy enforcement on security boundaries is crucial for ensuring security.

Threat actors are individuals or groups of people who, intentionally or unintentionally, can materialize threats against the IMT-2020/5G system. Depending on their role and level of access, they are expected to have access to certain attack vectors and be able to mount different types of attacks. This Recommendation classifies threat actors into the following categories:

- Internal actors:
 - Negligent insiders (Ⓐ)
 - Malicious insiders (Ⓜ)
- External actors:
 - Suppliers and service providers (Ⓕ)
 - Enterprise and end customers (Ⓒ)
 - Other external parties (Ⓓ), incl. hackers, organized crime, etc.

This Recommendation does not consider different capability levels of threat actors (e.g., script kiddie, skilled individuals, nation state actors), but instead limits itself to outlining which type of controls are needed to ensure basic protection against the threats identified. Readers are encouraged to perform an in-depth risk assessment customized for their specific environment and augment the recommended controls as appropriate.

6.1.2 Control description

Control domains are used to group security controls based on the nature of the security challenges they are supposed to mitigate. This includes not just technology, but also people and process considerations. Control domains used throughout this Recommendation include:

- Organizational controls
- People controls
- Operational controls
- Physical controls
- Technical controls

Control types describe when a given control is performed with regards to the occurrence of an information security incident. This includes the following types:

- **Preventive:** Controls performed prior to a security incident in order to prevent its occurrence.
- **Detective:** Controls performed continuously throughout a system's operation in order to identify security incidents as they occur.

- **Corrective:** Controls performed during and after a security incident in order to, for example, minimize its impact and recover from adverse situations.

Security concepts describe how a given control addresses a certain security threat. This Recommendation uses the terminology as defined in [b-ISO/IEC 27110], which defines the following concepts:

- **Identify:** Develop an organizational understanding to manage cybersecurity risk concerning people, operation, capabilities, physical and software assets. The identify function enables organizations to focus and prioritize the risks.
- **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical business services. The protect function enables organizations to limit or contain the impact of a potential cybersecurity event.
- **Detect:** Develop and implement capabilities to identify the occurrence of a cybersecurity event. The detect function enables organizations to discover security incidents in a timely manner.
- **Respond:** Develop and implement capabilities to take action in the event of a cybersecurity incident. The respond function enables organizations to limit or contain the impact of an incident.
- **Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to cybersecurity incident. The recover function enables organizations to recover to normal operations timely to reduce the impact from a cybersecurity incident.

NOTE – The term "security concepts" may be used interchangeably with "security functions", which is the terminology employed by the NIST cybersecurity framework [b-NIST CSF].

6.2 Structure of this Recommendation

The remainder of this Recommendation is structured into two main clauses.

Clause 7 summarizes the threats identified during the preparation of this Recommendation, categorized in the high-level threats. Each threat is assigned a unique threat identifier and linked to the threat actor(s) who may act on it.

Clause 8 describes recommended security controls, categorized in the major control domains outlined in clause 6.1.2. Each control is assigned a responsible party expected to implement and/or enforce it. Controls reference the threat(s) they address. Furthermore, they contain a high-level prioritization based on the impact assessment of the IMT-2020/5G system described in clause I.5.

6.3 How to use this Recommendation

This Recommendation ought to be a starting point in securing IMT-2020/5G deployments. By presenting security threats to the IMT-2020/5G system and relevant security controls in a structured manner, it aims to provide readers with practical advice on identifying and addressing common security challenges. Rather than specifying each security control in full detail, the Recommendation assumes that readers adapt control prioritization and implementation to their individual scenario and the associated security risk. An exemplary approach for using the Recommendation as part of an organization's continuous risk management activities is outlined below.

Step 1. Identify: Start with assessing the security risk landscape of your individual IMT-2020/5G system deployment by performing a threat and risk assessment (TARA). Rather than aiming for full detail, start with a high-level assessment and improve iteratively. Key considerations to be taken into account during this initial step include:

- Who are the users of the IMT-2020/5G network (e.g., public or private deployment)?

- Which entities need access to the network infrastructure and services (e.g., internal staff, system integrators, third-party service integrations)?
- What use cases and associated data are carried over the IMT-2020/5G system (e.g., machine-to-machine communication, mobile broadband, voice)?
- Where are different IMT-2020/5G system components deployed (e.g., private, hybrid, or shared infrastructure)?

Step 2. Prioritize: Based on the findings in step 1, select relevant security controls described in this Recommendation. Utilize the provided criticality as a starting point and refine the prioritization of controls according to your individual risk profile. This process should be informed by different considerations, such as:

- What are high-impact, high-likelihood risks on the IMT-2020/5G system in question?
- Which security controls already exist in some form?
- How mature are the existing controls?

NOTE – Depending on the exact scenario, certain controls may be either not covered by this Recommendation or not relevant as described. The aim of this Recommendation is to provide a sensible baseline, not an exhaustive list of threats and controls.

Step 3. Adapt and expand: Once the control prioritization is determined, develop a concrete implementation plan. The guidance provided in the controls clause should be understood as an outline of fundamental best practices. Use the external resources referenced in order to confirm the completeness of existing controls and supplement them based on your individual risk profile.

Step 4. Review and improve: The risk landscape of the IMT-2020/5G system is constantly evolving, either due to emerging vulnerabilities or changes in how the system is used and by whom. For this reason, it is needed to regularly review the risk assessment of the IMT-2020/5G system and reassess the adequacy of security controls.

7 Security threats for IMT-2020/5G systems

As described in Appendix I, IMT-2020/5G network is composed of the IMT-2020/5G system and related functional components, such as network functional virtualization (NFV), network slicing, multi-access edge computing (MEC). This clause outlines the identified threats to the IMT-2020/5G system and supporting technologies. Clause 7.1 describes common security threats that are generally applicable to all areas of the IMT-2020/5G system. Clause 7.2 and beyond describe specific threats to individual system domains.

7.1 Generic security threats

7.1.1 Spoofing

7.1.1.1 Network spoofing

Threat ID	#TC_S_01
Related threat actors	ⓂⓈⒸⓄ

Spoofing attacks targeting network protocols can occur on multiple layers of the IMT-2020/5G system, whenever authentication between communication parties is not strictly enforced. Well-known examples include, for example:

- MAC spoofing: an attack that changes or impersonates the real MAC address of a targeted device to bypass access blocks at the network identifier level;
- IP spoofing: an attack that replaces a packet header's source IP address with a fake, or spoofed IP address;

- DNS spoofing: an attack that corrupts DNS data (such as domain name and IP address) to redirect traffic to a fraudulent site.

7.1.1.2 Spoofing of software packages

Threat ID	#TC_S_02
Related threat actors	MSCC

Malicious actors may attempt to spoof third-party software components or software updates in order to infiltrate an organization's IT infrastructure. Unless the original source of software can be reliably verified, this supply chain attack vector can be used to mount follow-up attacks.

7.1.1.3 Phishing

Threat ID	#TC_S_03
Related Threat Actors	MSCC

Spoofing attacks are not always targeted against technology but can attempt to deceive people as well. These so-called phishing attacks may utilize methods, such as website spoofing, email spoofing, and voice phishing (vishing) over the phone. As such, phishing attacks can be considered a specific form of social engineering. The impact of a successful phishing attack can be severe, depending on the victim's privileges, such as access to sensitive information or restricted services. The potential impact of such attacks may include:

- Breach of sensitive information, e.g., entered into a spoofed website;
- Loss of control, e.g., over an account taken over with a phished password; and
- Financial loss, e.g., following a CEO fraud vishing attack.

7.1.2 Tampering

7.1.2.1 Tampering with data in transit

Threat ID	#TC_T_01
Related threat actors	MSCC

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. Such conditions may occur, for example, due to:

- Flawed implementation or configuration of network protocols;
- Use of insecure cryptographic algorithms; or
- Breach of cryptographic keys.

Ensuring the integrity of network data in transit is particularly important for management traffic, including administrative access, configuration, and log data.

7.1.2.2 Tampering with the physical platform

Threat ID	#TC_T_02
Related threat actors	MSO

Tampering may also be targeted at the computing platform itself, with adversaries trying to compromise fundamental system components such as security coprocessors or internal communication channels. These attacks may be enabled by insufficient physical protection of the overall system or exposure of unnecessary hardware interfaces (e.g., debugging ports).

7.1.2.3 Tampering with software packages

Threat ID	#TC_T_03
Related threat actors	MSO

Software packages, including source code, binaries, container images, and virtual machine images, can be tampered with at multiple stages of their lifecycle. Such modification may occur from initial development to procurement, storage, deployment, and eventually operation. They can be unintentional, for example, caused by:

- Network transmission errors; or
- Data degradation.

Alternatively, they can also be intentional, involving malicious acts, such as:

- Tampering with the source code itself or its external dependencies;
- Tampering with software development or build environments; or
- Tampering with the final software product, e.g., by reverse engineering.

In the worst case, an attacker manages to modify software products to introduce malicious code or vulnerabilities as a "backdoor" allowing follow-up attacks further down in the supply chain. A backdoor refers to a covert entrance to a computer system that can be used to bypass security controls. A backdoor could be created by the system developer intentionally or unintentionally through flaws in the implementation. If not discovered during security testing, backdoors can threaten the IMT-2020/5G network and its users by allowing malicious actors to take control over the systems. Examples of technology backdoors include, among others, redundant or hidden interfaces, libraries, features, or user accounts; hidden system parameters and intentional vulnerabilities allowing third parties to circumvent legitimate authentication and authorization.

7.1.2.4 Tampering with stored data

Threat ID	#TC_T_04
Related threat actors	ⓃⓂⓈⓄ

Similar to binary software packages, other forms of data stored on a computer system may also be subject to tampering. This could be caused by, for example:

- Unintentional data modification by negligent insiders;
- Intentional tampering by insiders with control over system components, including IMT-2020/5G network functions and underlying cloud infrastructure; or
- Intentional tampering by malicious intruders.

Data subject to tampering could include user data, application binaries, log files, or others. It is especially critical when targeted at system or service configuration files, since alteration of these can easily promote subsequent security threats.

7.1.2.5 Data poisoning

Threat ID	#TC_T_05
Related threat actors	ⓂⓈⓄ

An increasing number of software applications, incl. security-related applications, utilize artificial intelligence or machine learning (AI/ML). The functionality of this class of algorithms depends significantly on the data set that is used to train the AI/ML model. If a malicious actor is able to influence these training data, it can have negative effects on the performance of the overall application, depending on the type of algorithm and application, such as:

- False classification, e.g., incorrectly identifying spam emails; or
- Flawed anomaly detection, e.g., causing weaker intrusion detection capabilities.

This threat not only applies to models under an organization's own control, but also those of external suppliers.

7.1.3 Repudiation

7.1.3.1 Modification of log data

Threat ID	#TC_R_01
Related threat actors	ⓂⓈⓄ

Reliable system log data is at the core of running effective security operations. As such, this information needs to be protected from tampering at rest and in transit. Common threats to the integrity of log files are the use of local storage at the data origin, the transfer of log files over insecure protocols, or insufficient protection of central logging servers.

7.1.3.2 Account takeover

Threat ID	#TC_R_02
Related threat actors	ⓂⓄ

Accounts of legitimate users could be abused to facilitate an attack when taken over by a malicious actor. Well-known examples for such attacks are business email compromise and abuse of remote access systems. Such account takeovers may be facilitated by use weak credentials, leaked secrets, or lack of multi-factor authentication.

7.1.4 Information disclosure

7.1.4.1 Cryptographic attacks

Threat ID	#TC_I_01
Related threat actors	ⓂⓄ

Cryptography is vital for ensuring confidentiality of data transferred over the network. However, if they are not implemented and configured properly, cryptographic controls could fail to provide the expected protection against targeted attacks and potentially even give a false sense of security. Common attacks against cryptographic controls include:

- Collision attacks: an attack on a cryptographic hash function that attempts to find two inputs resulting in the same hash value, i.e., a hash collision;
- Oracle attacks: an attack on a system that abuses a weakness as an "oracle"¹ revealing information about the system or processed data to the attacker;
- Brute-force attacks: an attack that utilizes trial-and-error against authentication challenges, cryptographic control, and others, to obtain sensitive information.

7.1.4.2 Side channel attacks

Threat ID	#TC_I_02
Related threat actors	ⓈⓈⓄ

Adversaries may use covert channels to bypass security controls and obtain additional information on a system, either resulting in a security incident directly or providing the attacker with additional information that in turn can be used to mount a consecutive attack. Possible side channels are:

- System power usage;
- Emitted electromagnetic waves;
- Emitted sound.

It should be noted that side channel attacks are not only relevant to physical systems, but also virtualized workloads and communication infrastructure, such as network slices. A lack of isolation

¹ Oracles are hints that a system under attack provides to the attacker.

between workloads running on the same hardware can enable neighbouring workloads to obtain information about each other based on changes in resource utilization or response behaviour.

7.1.4.3 System fingerprinting

Threat ID	#TC_I_03
Related threat actors	ⓂⓄ

Systems can also reveal information more overtly than via covert channels. If not properly hardened, attackers may analyse a system's exposed components and functions, debug messages, or the general response behaviour to deduce security-relevant information. This is particularly relevant to operating system services and applications with network connectivity, for example, network protocol implementations (transport layer security (TLS), secure shell protocol (SSH), simple network management protocol (SNMP), etc.), web servers, and application servers.

7.1.4.4 Malicious software

Threat ID	#TC_I_04
Related threat actors	ⓃⓂⓈⓈⓄⓈ

Malicious software, also known as malware, takes many different forms and can violate different security properties, including confidentiality. In the context of the IMT-2020/5G system, it can target network products or supporting business systems, such as e-mail servers. Common examples for malicious software include rootkits, worms, trojan viruses, and ransomware. The latter is described in further detail in the clause on denial-of-service threats.

Attackers can also attempt to deploy malicious software to technology vendors in order to attack victims further down in the supply chain, such as government organizations or corporations. As a result, the IMT-2020/5G network under attack may not provide the confidentiality, integrity, or availability that is expected of it. Depending on the use cases and applications it supports, this can impact purely digital assets or even people's physical safety.

7.1.4.5 Social engineering

Threat ID	#TC_I_05
Related threat actors	ⓃⓄ

Social engineering describes the act of deceiving others into revealing confidential information. A more generic term than phishing, it can comprise various forms of information gathering, pretexting, and eventually engaging with the victim to perform the attack. Using these techniques, attackers can, for example, try to compromise user accounts of IMT-2020/5G operator's personnel and abuse their privileges to attack the network and its services.

7.1.4.6 Intentional data breaches

Threat ID	#TC_I_06
Related threat actors	ⓂⓈ

Privileged insiders can be the cause of information disclosures intentionally if they breach confidential data themselves or aid third parties in obtaining unauthorized access. Note, that this includes, current staff, former employees who no longer work for the organization but may still have access to information, and also service providers who need a certain level of access to provide their services.

7.1.5 Denial of service

7.1.5.1 Volumetric attacks

Threat ID	#TC_D_01
Related threat actors	Ⓒ

Volumetric attacks attempt to use the target system's network bandwidth in order to induce a denial-of-service situation for other legitimate communication peers. In order to achieve sufficiently high bandwidths, these attacks are usually performed in a distributed manner that is, using a large number of clients sending traffic towards the target system. Common types of volumetric attacks include:

- ICMP flood: a form of denial of service (DoS) attack in which an attacker sends a large number of ICMP packets to a targeted system in a short time.
- UDP flood: a form of DoS attack in which an attacker sends a large number of UDP packets to a targeted system in a short time.
- Reflection/amplification attack: a form of distributed denial-of-service (DDoS) attack in which an attacker attempts to overload a targeted system by sending small requests to a large number of publicly available systems and tricking them into sending their relatively large-responses to the system under attack.

7.1.5.2 Protocol attacks

Threat ID	#TC_D_02
Related threat actors	Ⓒ

Protocol level denial of service attacks try to induce a negative impact on service quality by taking up resources at the target system itself, such as example main memory or computing capacity. To achieve this, they commonly utilize weaknesses in network protocols or their implementations. Examples for protocol DoS attacks include:

- SYN flood: a form of DoS attack in which an attacker opens large number of transmission control protocol (TCP) connections with the target system by sending SYN packets (TCP packets for initial connection setup) without finalizing connection establishment.
- IP fragmentation attack: a form of DoS attack in which an attacker attempts to use all of the network bandwidth by exploiting the IP fragmentation mechanism.
- Ping of death: a form of DoS attack in which an attacker sends non-standard, malicious ping messages, normally used to check connectivity to a system.

7.1.5.3 Application layer attacks

Threat ID	#TC_D_03
Related threat actors	Ⓒ

Application layer attacks target the victim at higher system layers and attempt to create a denial-of-service situation by crashing the receiving application. Hence, this type of attack is usually enabled or facilitated by an implementation vulnerability that can be exploited. Possible entry points for application layer DoS attacks include application servers, web server, and other applications communicating over the network. Possible DoS attacks on application layer include:

- Slowloris attack: a form of DoS attack in which an attacker attempts to bind all resources of a targeted system and causes a service outage by keeping many HTTP connections to the web server open without disconnecting them.
- R.U.D.Y. attack: a form of DoS attack in which an attacker abuses HTTP Post messages by informing the receiving system of the amount of data to be expected, but then transmitting that data intentionally very slow.

7.1.5.4 Physical sabotage

Threat ID	#TC_D_04
Related threat actors	ⓂⓄⓈ

Denial of service (DoS) can also be induced by physical harm against the compute platform itself or the network infrastructure connecting it. This is especially relevant to deployments on the network edge (i.e., RAN and MEC components) that may be subject to less physical protection than traditionally more centralized network functions. With the introduction of distributed RAN in IMT-2020/5G, the attack surface for this type of attack may potentially increase, depending on the exact deployment scenario. Furthermore, it is not just the network elements itself that may be subject to sabotage or vandalism, but also supporting systems and utilities, such as power supplies.

7.1.5.5 Ransomware and other extortion schemes

Threat ID	#TC_D_05
Related threat actors	ⓃⓄ

Ransomware is a specific type of malicious software that encrypts a system's data and restricts user access to it unless a ransom is paid to unlock it. Once a system is infected, ransomware usually spreads to other hosts in the same network. Ransomware may be embedded in email attachments, or hidden behind an ad or a link, in order to trick employees into unknowingly downloading ransomware onto their system. It may also spread via other channels from external suppliers to their customers, such as technology management channels. Hence, an initial infection in the IT domain can potentially spread into the IMT-2020/5G network domain as well, negatively impacting the availability of network services.

In addition to malicious software, attackers also employ other extortion schemes to pressure victims into making a ransom payment. This could include, for example, targeted network DoS attacks, account takeover, or threatening to release sensitive information. Moreover, different techniques can be combined into double- or even triple-extortion schemes.

7.1.5.6 Breach of legislation

Threat ID	#TC_D_06
Related threat actors	ⓃⓄ

A fundamental prerequisite for operating public mobile networks is compliance to local laws and regulation. Unless basic security requirements prescribed in the legislation are effectively enforced, providing mobile network services is not allowed.

7.1.6 Elevation of privilege

7.1.6.1 Vertical privilege escalation

Threat ID	#TC_E_01
Related threat actors	ⓂⓄⓈ

Vertical privilege escalation (privilege elevation) is aimed at obtaining a higher layer of permissions than intended. This assumes the attacker to have some limited access to the target system in the first place. By breaching or bypassing security controls, the attacker is able to obtain additional privileges.

7.1.6.2 Horizontal privilege escalation

Threat ID	#TC_E_02
Related threat actors	ⓂⓄⓈ

Horizontal privilege escalation is aimed at obtaining access to resources or services restricted to other parties. This is a type of impersonation attack in which the application performs the correct actions

in communication with the user, only in the wrong security context. A successful account takeover (see clause 7.1.3.2) is an example for a horizontal privilege escalation, where the system in question may provide the appropriate services to the compromised account, albeit in the wrong security context, i.e., to the wrong user.

7.1.7 Lateral movement

7.1.7.1 Network lateral movement

Threat ID	#TC_L_01
Related threat actors	ⓂⓈⒸⓄ

Malicious actors usually attempt to expand their reach in the network following an initial breach. The act of moving through the IT infrastructure while trying to avoid detection is referred to as network lateral movement. This also includes attacks spreading across organizational boundaries, for example, affecting connected customers environments, following an initial breach at some point in the supply chain.

Similar to malicious actors, so can malicious software spread further inside an organization's IT infrastructure. In order to do so, it does not always rely on direct network connectivity, but instead propagates through alternative channels, for example, removable storage media or shared storage.

7.2 Threats to NFV infrastructure and MANO

7.2.1 Spoofing

7.2.1.1 Spoofing of NFV workloads

Threat ID	#TM_S_01
Related threat actors	ⓂⓈ

If the network functions virtualization infrastructure (NFVI) fails to verify the provenance of software at the time of deployment, a malicious actor with control over management and network orchestration (MANO) components can attempt to provision harmful NFV workloads. Such an incident can occur intentionally, for example, through an insider or third-party system integrator, or unintentionally if the virtual network function (VNF) image has been tampered with. For the second scenario, please refer to "Tampering of VNF Images (VNFI)".

7.2.2 Tampering

7.2.2.1 Tampering of VNF images

Threat ID	#TM_T_01
Related threat actors	ⓂⓈⒸⓄ

Software tampering can lead to the introduction of malicious code or vulnerabilities to VNF images. This can occur at various points in the supplier's IT environment, during provisioning from suppliers to customers, or while the software is stored in customers' VNF image library. If an attacker manages to tamper with a VNF image at any of these stages, the changes will affect every VNF instance created from it.

7.2.2.2 Tampering information in transit between mano components

Threat ID	#TM_T_02
Related threat actors	ⓂⒸ

A lack of integrity protection between MANO components can lead to security incidents affecting large parts of the network, if malicious actors are able to modify the information exchanged. Such information may include network (security) policies, management and orchestration commands, or monitoring data. This threat affects the entire MANO domain but is particularly crucial in scenarios

in which MANO entities are controlled by separate entities and traffic is exchanged between security domains (e.g., high-level network orchestration by the IMT-2020/5G operator and NFVI orchestration by an external infrastructure provider).

7.2.3 Information disclosure

7.2.3.1 Untrusted NFV workloads

Threat ID	#TM_I_01
Related threat actors	ⓂⓈ

The virtualization layer implements crucial security functions by isolating host operating system and physical platform from NFV workloads. However, enabling certain functionalities within a VNF may need to expose parts of the platform to virtual workloads directly, without indirection through the virtualization layer. Care should be taken when deciding which workloads are granted this level of access, as such functionality increases the risk of untrusted software abusing the increased access to the host system. Examples include:

- Single-root input/output virtualization (SR-IOV) which allows virtualized software direct access to physical networking hardware.
- Shared folders between host and guest operating system.
- Direct access to host sockets (e.g., the Docker daemon socket).

7.2.3.2 VNF sprawl

Threat ID	#TM_I_02
Related threat actors	ⓈⓃ

Virtualized deployments make it easier for developers and operational staff to provision additional resources if needed. However, the unrestricted creation new workloads can make it difficult to enforce a consistent security baseline across the entire deployment and complicate operational security tasks, such as incident detection and response. Due to the increased attack surface and the lack of visibility, it increases the risk to the overall technology ecosystem.

7.2.4 Denial of service

7.2.4.1 Resource depletion through NFV workloads

Threat ID	#TM_D_01
Related threat actors	ⓃⓂⓈ

Insufficient enforcement of usage quotas on virtualized workloads through the NFVI, can lead to a depletion of resources and thus, adverse effects on overall service quality. This may not only be caused by malicious workloads intentionally trying to cause a denial of service, but also legitimate ones consuming more resources based on their current utilization. Failure to enforce such resource limits can be caused by, for example, software vulnerabilities in the virtualization layer or simply improper configuration by the IMT-2020/5G operator.

7.2.4.2 Unavailability of service providers

Threat ID	#TM_D_02
Related threat actors	Ⓢ

In scenarios in which the NFV infrastructure is provided by an external infrastructure provider, mobile network services are critically dependent on the availability of a third party. Therefore, any breach of service level agreements (SLAs) by these external parties, for example through unavailability, poses a threat to the mobile network.

7.2.5 Elevation of privilege

7.2.5.1 Guest-to-host escape

Threat ID	#TM_E_01
Related threat actors	©©

A hypervisor or container engine is the software layer isolating virtual workloads from the host system and mediating between the two. If this isolation can be broken or circumvented by the virtualized workload at any point, it opens the door for malicious software compromising the NFVI. Such a hypervisor breakout may be enabled by various vulnerabilities in the host machine's software stack. Past examples include flaws in the hardware emulation layer, hypervisor management tools, and even graphics drivers.

7.2.6 Lateral movement

7.2.6.1 Lateral movement within NFVI / MANO

Threat ID	#TM_L_01
Related threat actors	©©©

Similar to how a malicious actor can compromise individual systems to spread the reach of its attack, so can the compromise of central virtualization infrastructure facilitate network lateral movement. In particular, this applies to the following NFV system components:

- Virtualization layer, which may allow attackers to easily spread their attack to different virtual workloads deployed on a given virtualization technology.
- MANO, which provides control over large parts of the network if not segmented properly. Especially critical are shared MANO domains for deployments of different trust levels (e.g., between MEC and 5G Core).

7.3 Threats to NFV workloads

7.3.1 Spoofing

7.3.1.1 Spoofed host platform

Threat ID	#TW_S_01
Related threat actors	©©

Not only can spoofed software be the source of security incidents, but a similar threat also exists when legitimate software is executed on an untrusted hardware platform. Unless the NFV environment can assert the host's trust level, there is a possibility for sensitive network components to be deployed in a security domain with a lower trust level. In the context of the IMT-2020/5G System this could mean, for example, that resources for a high-security network slice are processed and/or stored on lower-security infrastructure (e.g., an edge cloud). Such a situation could, for example, cause regulatory compliance issues if personal identifiable data is processed in a non-compliant environment.

7.3.1.2 Spoofed MANO communication

Threat ID	#TW_S_02
Related threat actors	©©

The interface between a VNF and its VNF manager (VNFM) is the key communication interface between a VNF instance and the NFV environment. Authentication on this logical channel is a critical prerequisite for secure communication between the VNF and the MANO domain, needed for various management tasks, incl. migration, scaling, and deprovisioning. If security for these tasks cannot be guaranteed, an attacker can interfere in VNF lifecycle management.

7.3.2 Tampering

7.3.2.1 Active VNF introspection

Threat ID	#TW_T_01
Related threat actors	ⓂⓈ

VNF introspection provides a powerful tool to monitor and even modify information within virtual workloads through the virtualization layer. However, if access to this functionality is not sufficiently controlled and monitored, it can be abused by a malicious actor to tamper with the VNF or the data processed. Depending on the deployment scenario, such malicious actor could be internal operational staff, or personnel of the cloud provider.

7.3.3 Information disclosure

7.3.3.1 Passive VNF introspection

Threat ID	#TW_I_01
Related threat actors	ⓂⓈ

Similar to the risk of tampering due to misuse of VNF introspection, so can this functionality be abused to mount passive attacks, extracting sensitive information about the virtual workload or the data processed.

7.3.3.2 Communication between NFV workloads

Threat ID	#TW_I_02
Related threat actors	ⓂⓈ

In addition to isolation between virtualized workloads and the host system, the virtualization layer also needs to ensure isolation between the individual NFV workloads themselves. If the system fails to ensure this isolation, information in shared system memory, caches, or permanent storage may be accessible to peer VNF instances on the same system. The most prominent example of a breach of this kind is the meltdown attack [b-Meltdown].

7.4 Threats to radio access network

7.4.1 Spoofing

7.4.1.1 Rogue base stations

Threat ID	#TR_S_01
Related threat actors	Ⓒ

Attackers can impersonate legitimate radio transmission infrastructure in an attempt to mount a man-in-the-middle (MitM) attack between user equipment and gNodeB (gNB). The nature of these attacks limits them to a very narrow location, as they need the malicious transceiver to deliver greater signal strength to the victim device than other legitimate base stations. If the mobile handset is successfully deceived into attaching to the serving network via such a fake base station, the entire traffic is exposed to the malicious actor, exposing non-encrypted traffic and enabling message tampering.

7.4.2 Tampering

7.4.2.1 Bid-down of user equipment or network capabilities

Threat ID	#TR_T_01
Related threat actors	Ⓒ

Bid-down attacks try to abuse backwards compatibility of communication peers with the goal to negotiate potentially less secure configuration parameters of a given protocol. In the context of 3GPP