International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1814

(09/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

IMT-2020 Security

Security guidelines for IMT-2020 communication systems

Recommendation ITU-T X.1814

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	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	**X.1800–X.1819**

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

Recommendation ITU-T X.1814

Security guidelines for IMT-2020 communication systems

Summary

Connected Internet of things (IoT) devices and mobile applications require wireless network access that is resilient, secure and able to protect individuals' privacy. IMT-2020 communication systems should be designed to meet these high-level requirements. There is a need to define a security framework for IMT-2020 communication systems which could act as a foundation for developing further detailed technical Recommendations on IMT-2020 security topics.

Recommendation ITU-T X.1814 identifies all components related to the security of IMT-2020 communication systems and defines security guidelines for the IMT-2020 communication system. It describes a generic IMT-2020 architecture and its domains. It also identifies threats to and specifies requirements for security capabilities for each component, taking into account unique network features. This Recommendation is based on the 3GPP 5G security architecture.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1814	2022-09-02	17	11.1002/1000/14992

Keywords

Capability, IMT-2020 communication system, multiaccess edge computing, network slicing, network virtualization, security guidelines, threats.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, 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 2022

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

Recommendation ITU-T X.1814

Security guidelines for IMT-2020 communication systems

1 Scope

This Recommendation provides security guidelines for the development of IMT-2020 communication systems. It identifies all components related to the security of an IMT-2020 communication system, i.e., user equipment, access network and core network. It describes a generic IMT-2020 architecture and its domains. It also identifies threats to and specifies requirements on security capabilities for each component, taking into account unique network features such as multiaccess edge computing, software-defined networking, dynamic network function virtualization and network slicing. This Recommendation is based on the 3GPP 5G security architecture.

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*.

[ITU-T X.1038] Recommendation ITU-T X.1038 (2016), *Security requirements and reference architecture for software-defined networking*.

3 Definitions

3.1 Terms defined elsewhere

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

– access control;
– authentication;
– availability;
– confidentiality;
– data integrity;
– privacy;
– repudiation;
– security service.

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

3.1.2 **control** [b-ITU-T X.1408]: Measure that is modifying risk.

NOTE 1 – Controls include any process, policy, device, practice, or other actions which modify risk.

NOTE 2 – Controls may not always exert the intended or assumed modifying effect.

3.1.3 distributed denial-of-service (DDoS) attack [b-ITU-T Y.4807]: 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.

3.1.4 guideline [b-ITU-T X.1401]: Description that clarifies what should be done and how, to achieve the objectives set out in policies.

3.1.5 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.

3.1.6 network function virtualization [b-ITU-T X.1811]: 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.

3.1.7 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).

3.1.8 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.

3.1.9 security capability [b-ISO 81001-1]: Broad category of technical, administrative, or organizational controls to manage risks to confidentiality, integrity, availability and accountability of data and systems.

3.1.10 supplier [b-ISO 10393]: Organization or person that provides a product or service.

3.1.11 system [b-ISO/IEC 27000]: Applications, services, information technology assets, or other information handling components.

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

3.1.13 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 domain: A grouping of network entities according to physical or logical aspects that are relevant for an IMT-2020 network.

3.2.2 IMT-2020 communication system: A system of managing IMT-2020 communication processes for IMT-2020 services.

NOTE 1 – 5G is referred to as IMT-2020 in ITU-T context.

NOTE 2 – The IMT-2020 communication system is identical to IMT-2020 system in this Recommendation.

3.2.3 IMT-2020 ecosystem: A set of stakeholders which interact to form a stable functioning IMT-2020 system.

NOTE – This mainly relies on IMT-2020 communication technology, in which a community of living organisms contains producers, consumers and suppliers who contribute vast amounts of products, technology and expertise to make an IMT-2020 system work on different levels such as infrastructure, network, platform, service and application.

3.2.4 IMT-2020 service: A benefit provided by the IMT-2020 ecosystem.

3.2.5 flow table overflow attack: An attack that consumes flow tables that forward and process packets of flows, which results in no space left for other flows to install flow rules and thus incurs network denial-of-service (DoS).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

4G	Fourth Generation of Mobile Communication Technology
AMF	Access and Mobility management Function
API	Application Programming Interface
AUSF	Authentication Server Function
C-PDU	Control Protocol Data Unit
CU/DU	Central Unit/Distributed Unit
DCI	Data Centres Interconnect
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
eMBB	enhanced Mobile Broadband
FAT	File Allocation Table
IMSI	International Mobile Subscriber Identity
IMT-2020	International Mobile Telecommunications-2020
IoT	Internet of Things
LTE	Long-Term Evolution
MAC	Message Authentication Code
MEC	Multiaccess Edge Computing
MEHW	Mobile Equipment Hardware
mIoT	massive Internet of Things
mMTC	massive Machine-Type Communications
MNO	Mobile Network Operator
NAS	Non-Access Stratum

NF	Network Function
NFV	Network Function Virtualization
NFVI	Network Functions Virtualization Infrastructure
NRF	Network Function Repository Function
OAM	Operation, Administration and Management
O&M	Operations and Management
PII	Personally Identifiable Information
PSK	Pre-Shared Key
RA/CA	Registration Authority and Certification Authority
RRC	Radio Resource Control
SBA	Service-Based Architecture
SBI	Service-Based Interface
SDN	Software-Defined Networking
SMF	Session Management Function
SQL	Structured Query Language
SSL	Secure Sockets Layer
TA	Trust Anchor
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber's Identity
TPM	Trusted Platform Module
UDM	Unified Data Management
UE	User Equipment
UICC	Universal Integrated Circuit Card
URLLC	Ultra-Reliable and Low-Latency Communications
USIM	Universal Subscriber Identity Module
VM	Virtual Machine
VNF	Virtual Network Function
VoIP	Voice over Internet Protocol

5 Conventions

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

6 Overview of security for the IMT-2020 communication system

6.1 Simplified IMT-2020 architecture

This clause gives an overview of security for the IMT-2020 communication system. Connected mobile devices and mobile applications require wireless network access that is resilient, secure and

trustworthy. The IMT-2020 communication system should be designed to meet these high-level requirements.

An IMT-2020 communication system consists of devices connected to an IMT-2020 access network, which in turn is connected to the rest of the system, which is called an IMT-2020 core network.

Figure 1 shows a simplified 3GPP 5G system architecture. The IMT-2020 access network includes 3GPP radio base stations and/or a non-3GPP access network. The IMT-2020 core network architecture is significantly better than 4G in terms of being able to support cloud implementation and the Internet of things (IoT), with major improvements in network slicing and service-based architecture (SBA).

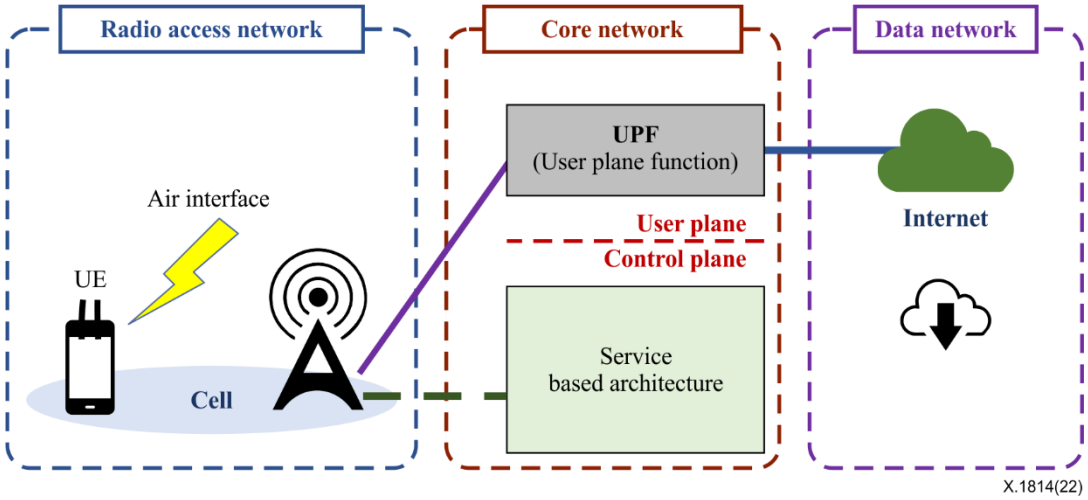

Figure 1 – Simplified IMT-2020 architecture

6.2 General architecture of IMT-2020 system

The IMT-2020 system aims at providing a wide range of services with different performance requirements. The services provided in IMT-2020 networks can be classified into three categories according to 3GPP specifications: (1) Enhanced mobile broadband (eMBB) supports higher data rates and higher user mobility than the fourth generation of mobile communication technology/long term evolution network (4G/LTE); (2) Massive Internet of Things (mIoT) provides massive machine type communications; (3) Ultra-reliable and low-latency communications (URLLC) support the mission critical services which require higher reliability and lower latency. The IMT-2020 system is to be a flexible platform enabling new business cases and integrating verticals such as automotive, manufacturing, energy, eHealth and entertainment. Moreover, the deployment and maintenance of the IMT-2020 system is to be easier compared with the previous generations of mobile networks. To address these challenging requirements, the IMT-2020 system has introduced a number of innovation technologies, such as network slicing, network function virtualization (NFV), software-defined networking (SDN), SBA and central unit/distributed unit (CU/DU) separation.

A general architecture of the IMT-2020 system [b-ITU-T X.1811] is illustrated in Figure 2, which includes the transport layer, network layer, service layer and management plane according to the required functionalities.

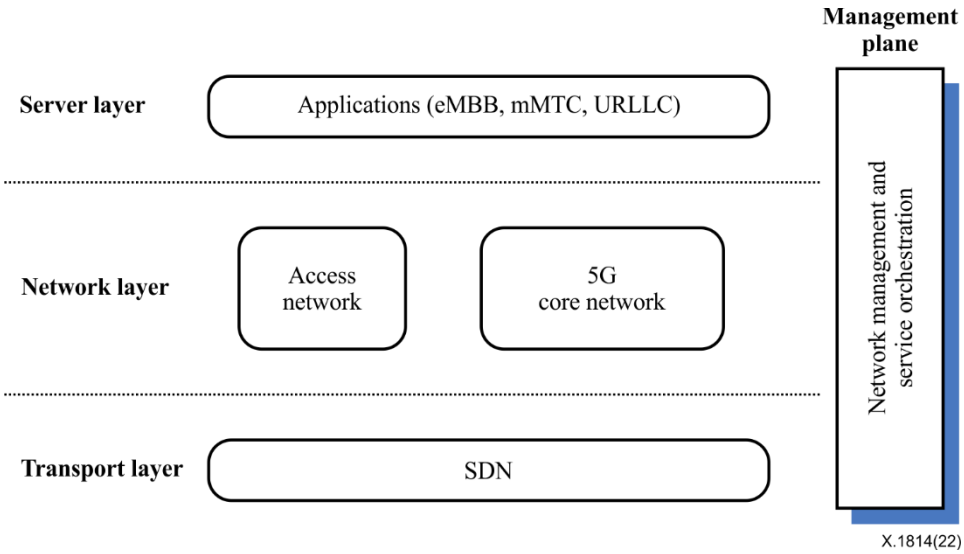

Figure 2 – General architecture of IMT-2020 system [b-ITU-T X.1811], [b-TS 33.501]

- Transport layer: This is used to transport packets between the source and the destination. Besides legacy transport technologies (e.g., Multiprotocol label switching), the IMT-2020 system has introduced SDN technology for higher transport speeds and easier adoption of service requirements.
- Network layer: This is composed of the access network and the core network. The former allows UE access to the IMT-2020 network. The latter is designed with a SBA to allow for extensibility and simplicity. It is made up of a number of network functions to support data connectivity and service deployment. Examples of network functions include the authentication server function (AUSF), access and mobility management function (AMF), and session management function (SMF).
- Service layer: This consists of the applications running on the top of the IMT-2020 system, which may be eMBB, mMTC or URLLC applications.
- Management plane: This is responsible for the network management and service orchestration.

6.3 Domains of IMT-2020 system

IMT-2020 security should be defined according to domains, layers, security requirements and security capabilities.

A domain is a grouping of network entities according to physical or logical aspects that are relevant for an IMT-2020 network. The concept of a slice domain is used to capture network slicing aspects. It can represent different functionalities, services and actors in IMT-2020 networks. Figure 3 represents the typical IMT-2020 domain.

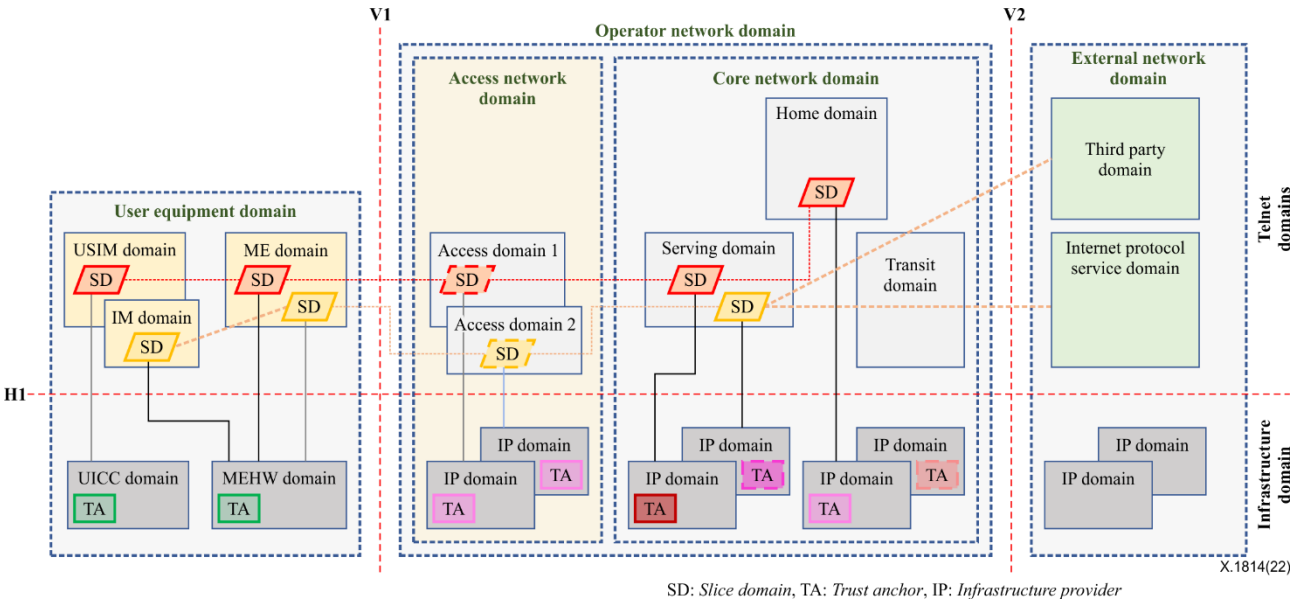

Figure 3 – Typical IMT-2020 domains

The network elements positioned above line H1 in Figure 3 represent aspects of the logical network, which are called tenant domains, and those positioned below line H1 represent aspects of the physical network, which are called infrastructure domains. The line V1 separates the user equipment (UE) domain from the access network domain, and the line V2 further separates the core network domain from the external network domain, e.g., Internet protocol services used by the operator network.

The infrastructure domains contain network elements implemented by hardware and software, and act as the infrastructure provider. This includes hypervisors (software that creates and runs virtual machines) as well as trust anchors (authoritative entity for which trust is assumed and not derived) [b-ITU-T X.509].

On the UE side below line H1, UE domains consist of the universal integrated circuit card (UICC), offering a tamper-resistant module, and mobile equipment hardware (MEHW) domain, offering hardware support including a trusted execution environment.

On the network side below line H1, there is an infrastructure provider (IP) domain, which consists of access (radio) specific hardware as well as hardware for the compute, storage and networking required for core functionality.

The trust anchors (TAs) are used to provide trust for virtualized systems. This includes ensuring the integrity of the tenant domain and that the tenant domain executes on designated and trusted infrastructure. The TAs can also be used to verify an infrastructure domain's integrity and to bind tenant domains with infrastructure domains.

The tenant domains contain several logical domains that use infrastructure domains, e.g., to execute their functions. On the UE side, they consist of mobile equipment, a universal subscriber identity module (USIM), one of several software applications that reside in the hardware part, called the UICC, storing subscriber-related information and implementing the security functions pertaining to authentication and ciphering on the user side and identity management domain. The tenant domains on the network side consists of access (A), serving (S), home (H), transit (T), 3rd party (3P), Internet protocol service and management (M) domains.

6.4 General security requirements and capabilities

This clause summaries the general security dimensions (requirements) described in [b-ITU-T X.805]. The objective of this clause is to provide the basis for the security capability for the IMT-2020 system. The Appendix I provides the generic network security architecture for providing end-to-end network security.

A security layer refers to a hierarchy of network equipment and facility groupings [b-ITU-T X.805]. A security layer comprises of a grouping of protocols, data and functions related to one aspect of the services provided by one or several domains. The layer of the IMT-2020 security architecture provides a high-level view of protocols, data and functions that are related in the sense that they are exposed to a common threat environment and exhibit similar security requirements. They include radio jamming, false base station attacks, user plane data injection over-the-air and spoofed radio resource-control (RRC) messages and are common threats to communication between UE and a radio access network. On the other hand, tracking of subscription identifiers, spoofing of control plane messages and tampering with security capabilities and so on are common threats to communication between UE and the core network. Some examples of common threats to management services in IMT-2020 networks include unauthorized configuration changes, compromise of network keys and certificates, and on-the-fly addition of malicious network functions. The management layer consists of aspects related to conventional network management (configuration, software upgrades, system-user account management, log collection/analysis, etc.) and, in particular, security management aspects (security monitoring audit, key and certificate management, etc.). Furthermore, aspects related to the management of virtualization and service creation/composition (orchestration, network slice management, isolation and virtual machine (VM) management, etc.) belong to this stratum.

A security area extends the security domains and is subject to the security requirements of one or more layers or domains.

A security capability is in general defined as a broad category of technical, administrative or organizational controls to manage risks to confidentiality, integrity, availability and accountability of data and systems [b-ISO 81001-1]. It refers to a collection of security functions and mechanisms (including safeguards and countermeasures) for one security aspect, e.g., integrity. It contains security functions and mechanisms to avoid, detect, deter, counteract and minimize security risks to IMT-2020 networks, in particular, risks to a network's physical and logical infrastructure, its services, UE, signalling and data. Table 1 provides security requirements for security domains.

Table 1 – Security requirements for each security area

Security area	Security requirement
Access network	Security requirements related to access layer and domain are identified to address the threats related to this domain. An example of these requirements includes the confidentiality and integrity protection of user plane and control plane data as well as secure mobility.
Application or service	Security requirements for the application layer providing end-user application and service (e.g., VoIP, VoLTE) are identified to address the threats related to this domain. Examples of these requirements include the authentication and authorization of the user for using an application and secure service discovery.
Management	Security requirements for the management layer and management domain are identified to address the threats related to this domain, including security management (e.g., secure upgrades, secure orchestration) and management of security (i.e., monitoring, key and access management).

Table 1 – Security requirements for each security area

Security area	Security requirement
UE	Security requirements related to UE domain including access control of the device are identified to address the threats related to this domain. Examples of these requirements include mutual authentication with the network and the secure storage of security context.
Network	Security requirements related to the core network and communications between the operator network and external networks are identified, including aspects related to securely exchanging signalling and end-user data between nodes in the operator and external network domains. Examples are network security, subscriber privacy and subscriber authentication.
Infrastructure and virtualization	Security requirements of the IP domain are identified, for example, for attestation, secure slicing/isolation, and trust issues between tenant domains, and between tenant domains and infrastructure domains.

Table 2 describes the security capability of each security dimension [b-ITU-T X.805]. Seven of them, namely, identity and access management, authentication, non-repudiation, confidentiality, integrity, availability and privacy were adopted from [b-ITU-T X.805]. The other three, namely, audit [b-ITU-T X.800], trust and assurance, and compliance, are security dimensions in the IMT-2020 security architecture.

Table 2 – Security capabilities

Security dimensions	Security capability
Identity and access management	The security capability refers to a collection of security functions and mechanisms (including safeguards and countermeasures) for access control and management of credentials and roles.
Authentication	The security capability refers to a collection of security functions and mechanisms (including safeguards and countermeasures) for authentication that serves to verify the validity of a user's authentication attributes, e.g., claimed identity.
Non-repudiation	The security capability refers to a collection of security functions and mechanisms (including safeguards and countermeasures) for a non-repudiation service that protects against false denial of involvement in a particular action.
Confidentiality	The security capability refers to a collection of security functions and mechanisms (including safeguards and countermeasures) for a confidential service that protects data against unauthorized disclosure.
Integrity	The security capability refers to a collection of security functions and mechanisms (including safeguards and countermeasures) for an integrity service that protects data against creation or modification.
Availability	The security capability refers to a collection of security functions and mechanisms (including safeguards and countermeasures) for availability of resources, even in the presence of attacks. Disaster recovery mechanisms are included in the classification.
Privacy	The security capability refers to a collection of security functions and mechanisms (including safeguards and countermeasures) for a privacy service that serves to provide the right of entities to determine the degree to which it will interact and share its personally identifiable information.

Table 2 – Security capabilities

Security dimensions	Security capability
Audit	The security capability refers to a collection of security functions and mechanisms (including safeguards and countermeasures) for an audit service that provides review and examination of a system's records and activities to determine the adequacy of the system capability and detect breaches in system security and capability. An audit to collect data is also included.
Trust and assurance	The security capability refers to a collection of security functions and mechanisms (including safeguards and countermeasures) for a trust and assurance service that serves to convey information about the trustworthiness of a system.
Compliance	The security capability refers to a collection of security functions and mechanisms (including safeguards and countermeasures) for a compliance service that allows an entity or system to meet contractual or legal obligations.

7 Components and trustworthiness of the IMT-2020 communication system

7.1 IMT-2020 components

Connected IoT devices and mobile applications require a wireless network access that is resilient, secure and able to protect individuals' privacy. The IMT-2020 communication system should be designed to meet the requirements described in clauses 7.8 and 7.9 of [b-ITU-T Y.3101]. An IMT-2020 network consists of four components: UE, radio access network, transport network and core network, which are shown in Figure 4.

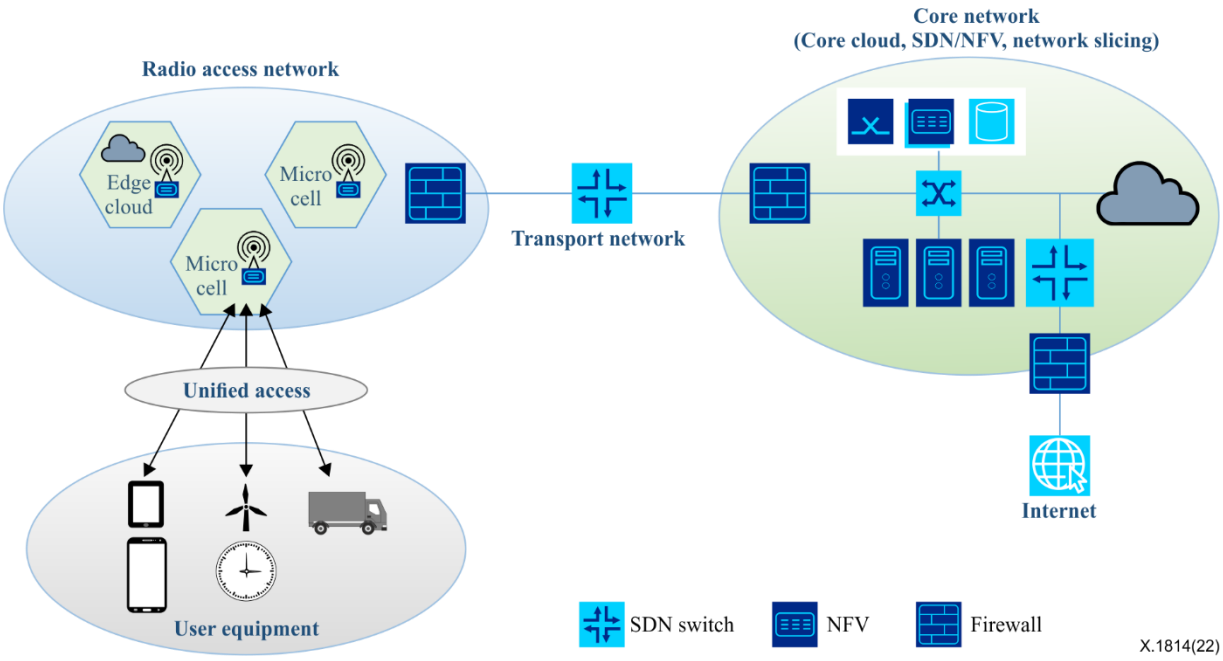

Figure 4 – IMT-2020 communication network (adapted from [b-ITU workshop])

The IMT-2020 system will be built on mobile clouds, SDN, NFV and network slicing to meet the challenges of massive connectivity, flexibility and cost minimization. Therefore, there is a need to define securities for NFV, network slicing and edge cloud computing.

NFV separates network functions from proprietary hardware appliances and runs them as software in VMs.

A virtual network function (VNF) is a logical outcome of NFV, which is a network function whose functional software is decoupled from hardware and runs on VM(s) [b-ITU-T Y.3100]. VNFs perform specific network functions such as firewalls, switching, intrusion detection systems and intrusion protection systems.

Network slicing is a form of virtual network architecture which uses the principles behind SDN and NFV in fixed networks. IMT-2020 networks are subdivided into virtual networks, each optimized for one business case, known as a network slice. They can span multiple network domains, including access, core and transport, and be deployed across multiple operators as shown in Figure 5.

SDN is an architecture that aims to make networks agile and flexible. The goal of SDN is to improve network control by enabling companies and network service providers to respond quickly to changing business requirements.

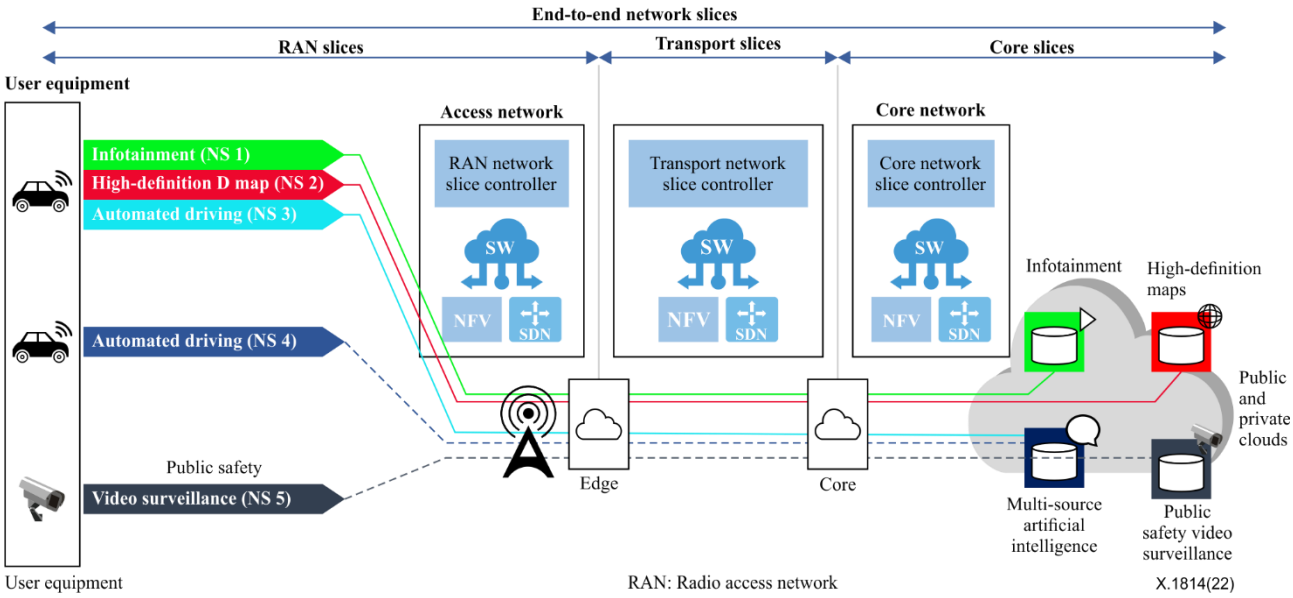

Figure 5 – IMT-2020 network slices

An IMT-2020 transport network is an IP transport infrastructure that delivers mobile IMT-2020.

Edge computing brings the capabilities of cloud computing to the edge of the IMT-2020 network. Edge computing is a distributed computing paradigm in which computation is largely or completely performed on distributed device nodes known as smart devices or edge devices, as opposed to primarily taking place in a centralized cloud environment. Edge computing brings the processing and storage of data closer to the equipment. This enables IoT devices to provide their service with low latencies.

7.2 Trustworthiness of the IMT-2020 communication system

The trustworthiness of the IMT-2020 communication system is the result of five properties, namely: resilience, communication security, identity management, privacy, and security assurance:

- Resilience: the capability of an organization to resist being affected by disruptions. A variety of complementary and partially overlapping features in IMT-2020 can help achieve the IMT-2020 communication system's resilience to cyberattacks and non-malicious incidents.
- Communication security: this is applied to data communication in IMT-2020. Secure communication for devices and for its own infrastructure is vital in an IMT-2020 communication system.

- Identity management: the processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in identities known in an IMT-2020 domain. A secure IM for identifying and authenticating subscribers, roaming or not, ensuring that only genuine subscribers can access network services, should be provided. It should build on strong cryptographic primitives and security characteristics.
- Privacy: Data privacy is defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information in [b-ISO/TS 21719-2]. Privacy is to protect personally identifiable information (PII) that can be used by unauthorized parties to identify subscribers.
- Security assurance: Security assurance is grounds for justified confidence that a claim about meeting security objectives has been or will be achieved. Security assurance is a means to ensure that network equipment meets security requirements and is implemented following secure development and product lifecycle processes.

8 Threats to components and functions

Figure 6 shows examples of threats to IMT-2020 systems. They are classified into three categories: well-known threats from software vulnerabilities, configuration mistakes and flooding attacks; threats from infrastructure sharing; and threats from the network level, such as threats related to SDN, NFV, network slicing and cloud computing.

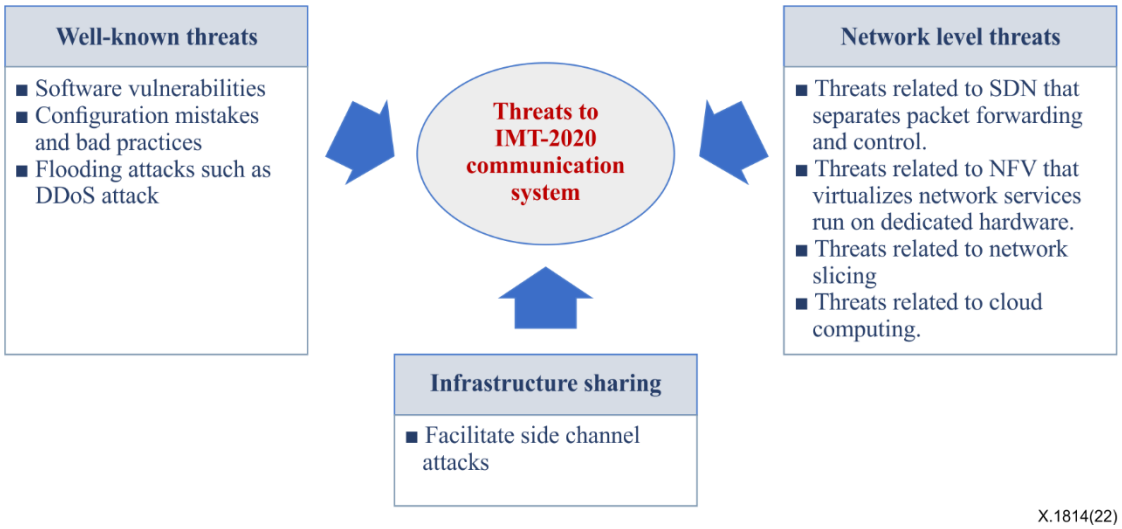

Figure 6 – Exemplar threats in IMT-2020 [b-ITU workshop]

8.1 Generic threats

The following generic threats are identified in [b-ENISA]:

- **Denial-of-service (DoS)** [b-ENISA]: This attack seeks to make a network resource unavailable to its intended users by temporarily or indefinitely interfering with or disrupting the network service by flooding it with a massive number of requests. Multiple types of these threats such as flooding, amplification, signalling storm and saturation attacks, may lead to a DoS. Popular DoS attacks include: (1) Buffer overflow attacks – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks. (2) ICMP flood – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death. (3) SYN flood – sends a request to connect to a server, but never completes the handshake.

Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

- **Distributed-denial-of-service (DDoS)** [b-ENISA]: A DDoS attack is where multiple systems target a single system with a DoS attack, orchestrating a synchronized DoS attack to a single target. The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once.
- **Data breach, leak, theft, destruction and manipulation of information** [b-ENISA]: This includes the theft of PII through unauthorized access to the systems and/or network, unauthorized access to and possible publication of personal data/biometric/medical data, organization confidential information or government/state-related information. The theft, breach or leak of other types of data such as user credentials, encryption keys, network security logs, software configuration and so on may also help attackers conducting different types of attacks.
- **Eavesdropping** [b-ENISA]: Eavesdropping is a term used to describe the unauthorized interception of information. It is a threat in which the intruder seeks to tamper with the application and communication layers of the various IMT-2020 network elements (SDN controller, network function, edge node, virtualization orchestrator). It includes eavesdropping on subscribers' data, confidential information, system time, subscriber location, electronic messages and the signal of data relayed over the network. The threat actor monitors, spies and/or eavesdrops on organizations to track locations or access sensitive information.
- **Exploitation of software and hardware vulnerabilities** [b-ENISA]: This type of threat enables a malicious attacker to take advantage of unknown (to the vendor and user) software or hardware flaws or known but unpatched flaws to perform an attack. Examples include the exploitation of known hardware and software flaws such as meltdown and buffer overflow. It also includes the exploitation of other known vulnerabilities related to previous generations of mobile telecommunications.
- **Malicious code or software** [b-ENISA]: Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. The threat includes the installation and distribution of malicious software or the implant of specific code or software inside a product or updates. Examples of malicious software include malware, ransomware, virus, worms, trojans, SQL (structured query language) injections [b-SQL], rogue security software, rogueware and careware. An example of malicious software in the IMT-2020 context considers the use of an unauthorized VNF that could abusively install and register itself into the core network to expose malicious APIs.
- **Compromised supply chain, vendor and service providers** [b-ENISA]: If supply chain, vendor and service providers are compromised, this enables the vendors to insert into the product concealed hardware, malicious software and software flaws. It also enables them to implement uncontrolled software updates, manipulate functionalities and include functions to bypass audit mechanisms and backdoors.

  If untrustworthy personnel from third parties are involved during product testing, maintenance, configuration and operation, they will be able to access the network management facilities (both locally and via remote interface) in order to perform maintenance activities and provide technical support. This privileged access to the operation, administration, and management (OAM) of the network provides an opportunity to such personnel to access various type of data such as subscriber, system and network configuration data and telemetry data.

- **Targeted threats** [b-ENISA]: Targeted threats come from malware destined for one specific organization or industry. A type of crimeware, these threats are of concern because they are designed to capture sensitive information. Highly sophisticated attacks or advanced persistence threats may target sensitive information, or the availability of sensitive and critical services.
- **Exploiting flaws in security, management and operational procedures** [b-ENISA]: Although it is not directly related to IMT-2020, this threat will become relevant when dealing with the complexity of the technology and the need to introduce operational procedures to the management of the network. This threat includes, but is not limited to, the exploitation of flaws in the operational and security management of the network, configuration, update and patch management of the software. The errors from the lack or poor design of operational and security procedures may have consequences for the integrity and availability of the network.
- **Abuse of authentication** [b-ENISA]: This threat may affect multiple network entry points such as UE (mobile devices and IoT), operation and management interfaces, roaming and vertical services. This threat relates to the theft of user credentials, brute force of user accounts, password cracking, masking user identity and impairing IoT grouping authentication as techniques used by threat actors to abuse the IMT-2020 authentication systems.
- **Identity theft or spoofing** [b-ENISA]: Identity theft is the intentional use of another entity's identity. This may be a threat when a malicious attacker successfully determines the identity of a legitimate entity and then masquerades as it to launch further attacks. Identity spoofing refers to the action of taking on the identity of some other entity and then using that identity to accomplish a goal. Identity spoofing is a threat that can affect any software component or human agent. In this attack, an attacker spoofs the identity of a legitimate controller and interacts with the network functions controlled by the legitimate controller (i.e., elements of the data plane) to trigger several other types of attack (instigate network flows, divert traffic, etc.). Social engineering and brute force user account/password cracking may also be used as a technique to spoof or steal user credentials. For example, international mobile subscriber identity (IMSI) catching attacks can be used to reveal the identity of a subscriber by catching the IMSI of the subscriber's UE. Such attacks can also be conducted by setting up a fake base station that is considered the preferred base station by UE that has lost access to a temporary mobile subscriber's identity (TMSI). The subscriber will respond with their IMSI. Moreover, IMT-2020 networks have different actors such as virtual mobile network operators (VMNOs), communication service providers (CSPs) and network infrastructure providers.

8.2 Threats to user equipment

The following security threats to UE have been identified:

- **Malicious software infection** [b-ENISA]: If malicious software is installed on UE, an attacker may leverage the infected UE to launch some kind of attack such as stealing personal data inside the UE, launching a DDoS or trying to infect other UE. Examples of malicious software include malware, ransomware, viruses, worms, trojans and rogue security software. Once malicious software infects UE, the mobile endpoint is included as a botnet.
- **Threat from botnets** [b-Khan]: Botnets are a type of malware that can control a set of Internet-connected devices. Mobile botnets can target many mobile endpoints to automatically launch a variety of attacks (e.g., DoS) on IMT-2020 systems. As IMT-2020 interconnects mobile phones with high computing power, these threats are increasing. In addition, the connection of IoT devices opens up new threat types. As a result, IoT devices are vulnerable to IoT botnet attacks. An example is the Mirai botnet, which affected millions of IP cameras in 2016.

- **Threats from mobile malware** [b-Khan]: Mobile malware can allow attackers to steal PII data stored on mobile devices or even initiate attacks (such as DoS attacks) against other entities such as other UE, mobile access networks and mobile operator core networks.
- **Unauthorized access to and destruction, disclosure or modification of user and signalling data**: An attacker can obtain unauthorized access to or carry out the destruction, disclosure or modification of user and signalling data communicated between UE and next generation node B.
- **Tampering with subscription credentials**: An attacker can tamper with a subscription credential which is used for authentication and confidentiality.

8.3 Threats to access networks

The following security threats to access networks have been identified:

- **Malicious or accidental high traffic** [b-NGMN]: As network capacity and the number of items of UE increase, there is a high risk of large changes in accidental or malicious network traffic patterns due to large events. At this scale, the intention of network surges cannot be discerned, so preventing malicious events is the main goal, but includes both scenarios.
- **Key leakage between operator links** [b-NGMN]: The air interface encryption (and sometimes integrity) key is calculated from the home core network and then sent to the visited wireless network via a signal link such as SS7 (Signalling System No. 7) [b-ITU-T Q.700] or Diameter [b-RFC 3588]. This is an obvious point of exposure and shows how the key is leaking.
- **Compromise of user plane integrity** [b-NGMN]: There is a threat that the entire session will be intercepted and used to insert bad data into the mobile connection (or that the data is wasted by passing the data to the service endpoint, which is wasted).
- **Optional security implementation** [b-Khan], [b-NGMN]: This threat comes from optional security implementation. There are many security provisions that do not affect interoperability (mostly interoperability with UE) and historically these options have been treated as deployment options. Such a choice can lead to risks in which the operator is inevitably affected by the actions of other operators without being at fault. It also compromises system-level security assumptions. Without this authentication step, the key tier cannot achieve one of its design goals, that is, to protect customers from faulty base stations.
- **Threat based on false buffer status reports** [b-Khan]: Attackers can exploit the buffer status reports of access network components such as base stations to obtain information such as packet scheduling, load balancing and admission control algorithms to achieve their malicious intents. An attacker can then send false buffer status reports by pretending to be legitimate UE to jeopardize the operations.
- **Message insertion threats** [b-Khan]: Message injection can launch DoS attacks on IMT-2020 networks. For example, an SDN device with an incorrect flow table update can be overloaded. An attacker can also inject control protocol data units (C-PDUs) into the system during wake-up time to perform DoS attacks on newly arriving UE.
- **Threats from micro cell** [b-Khan]: The physical size of base stations has been sharply reduced and they have been placed in indoor locations such as shopping malls, public places, stadiums and hospitals. In addition, the use of new frequencies such as the mmWave frequency will also facilitate the use of these micro base stations. However, they are not as physically secure as the macro base stations used in pre-IMT-2020 networks. Moreover, the increase in the number of base stations will increase the potential vulnerabilities in IMT-2020 networks.

- **Session hijacking** [b-ENISA]: Session hijacking, which relates to air interface, is an attack where a user session has been taken over by an attacker. If a legitimate authenticated session is taken over, an attacker controls the whole session of specific traffic to conduct another type of attack.
- **Threats from fake access network** [b-ENISA]: If a base station is compromised, the attacker can impersonate a legitimate base station and conduct a man-in-the-middle attack or modify the network traffic. This threat results in tampering with the communication between the mobile UE and the network to launch the other action.
- **Manipulation of access network configuration data** [b-ENISA]: If an access network element such as a base station is compromised, an attacker can forge configuration data and launch other attacks (e.g., DoS).
- **Threats from identity (IMSI) catching** [b-ENISA]: If cellular paging protocols are exploited, an attacker can associate a victim's soft identity with the paging occasion. A malicious attacker can verify a victim's location information, inject fabricated paging messages and launch denial-of-service attacks.
- **Service disruption from manipulated RRC connection request**: If an attacker manipulates the RRC connection request message transmitted in plaintext, then the victim's temporary identification information can be used to block the victim's onward network connection. The detailed attack scenario is described in Appendix II.

8.4 Threats to software-defined networking

The threats to SDN are described in [ITU-T X.1038].

8.5 Threats to core network

Following security threats to core network are identified:

- **DDoS** [b-Khan]: DDoS attacks can be initiated in the form of signalling amplification and AUSF & UDM saturation by using botnets controlling multiple infected UE.
- **Threats related to transport layer security (TLS)/secure sockets layer (SSL)** [b-Khan]: The TLS/SSL based communications used in SDN-based core networks are vulnerable to attacks such as TCP/SYN (synchronized) DDoS, RC4 biases in TLS, browser exploit against SSL/TLS (BEAST) attack, compression ratio info-leak made easy (CRIME) attack, LUCKY 13 attack [b-Goodin]_and padding oracle on downgraded legacy encryption (POODLE) attack [b-Möller].
- **SDN scanner** [b-Khan]: An attacker can analyse SDN traffic and manually collect network information such as the Infrastructure Protocol and key network elements of the SDN controller. The collected information can be used to perform various attacks such as DoS, TCP reset, replay and spoofing attacks.
- **Malicious diversion of traffic** [b-ENISA]: Compromising a network element allows attackers to divert traffic flows and eavesdrop on network traffic. Traffic diversion is a threat relating to network elements of the data plane. The typical example of traffic diversion in virtualized networks is trespassing the network slice. This threat may occur when the isolation between slices is compromised in any active node or when the enforcement of access to a slice in the edge equipment is either bypassed or misconfigured.
- **Misuse of audit tools** [b-ENISA]: Audit tools are used by network operators to monitor the activity of the network and obtain information that can be used for multiple purposes such as optimization, security or commercial purposes. This type of software tool may allow malicious attackers to perform reconnaissance activities for an attack. A malicious attacker typically uses insiders to the mobile network operator (MNO) with privileged access to these tools to extract sensitive information.

- **Leak of long-term key for user authentication/authorization data** [b-ENISA]: This threat relates to the disclosure of long-term keys for authentication and security controls conducted by an insider or hostile or untrustworthy personnel operating in the core network.
- **Exploitation of misconfigured or poorly configured systems/networks** [b-ENISA]: If systems and networks are poorly configured or misconfigured, attackers can access critical assets. The exploitation of a system that is unintentionally misconfigured creates an opportunity for an attacker to reach critical assets in the network. Configuration mistakes may happen at various stages of the solution implementation lifecycle, such as during product installation and maintenance.
- **Traffic sniffing** [b-ENISA]: A sniffer used by attackers a tool to intercept, log and analyse network traffic and data that is either a software or hardware tool. With sniffing, an attacker is also able to eavesdrop data from network elements or to link and steal sensitive information. Sniffing can happen anywhere where there is constant traffic.
- **Registration of malicious network functions** [b-ENISA]: This threat is when malicious network functions are deployed in IMT-2020 networks. An unauthorized network function or function embedding a trojan, which is introduced to the network by an insider (to the MNO) or a vendor/service provider, could be abusively installed in the SBA and registered in the core network via a network function repository function (NRF), in order to expose other malicious APIs. By having an unauthorized network function (NF) installed or activated, an attacker may have access to sensitive assets in the network to perform other types of attacks such as DoS, distribution of malicious software or stealing sensitive information.
- **Insecure NFs exposure to third party application functions** [b-Ta-Hao Ting]: Network function exposure between internal and external networks provides a dynamic and flexible deployment of IMT-2020. If a message is spoofed or tampered with, it will cause harm to the whole core network.
- **Insecure service-based interface** [b-TS 33.501]: A message between network elements through a service-based interface (SBI) is spoofed or tampered with and could be modified and disclosed.

8.6 Threats to network slicing

The following threats to network slicing have been identified:

- **Threats to internetwork slice communication** [b-Khan]: An attacker can disrupt the communication between slices to prevent the proper lifecycle management of slices.
- **Impersonation attack** [b-Khan]: An attacker can impersonate a physical host platform to allocate unavailable resources. Moreover, an attacker can impersonate a network slice manager to steal a network slice creation parameter.
- **Security policy mismatch** [b-Khan]: Variance of security policies and security protocols for different slices allows attackers to access the network slicing system and control entities via a less secure slice.
- **DoS** [b-Khan]: An attacker performs a DoS attack either on a virtualized network or on physical resources to exhaust the available network resources for other slices.
- **Side channel** [b-Khan]: An attacker gains access to one slice and attacks a set of slices which share the same primary hardware.
- **Privacy leakage** [b-Khan]: Infrastructure providers or VNF suppliers steal cross-slice user information.
- **Threats related to hypervisor** [b-Khan]: Attacks against the hypervisor to jeopardize the virtualization of resources. These attacks include software errors in the hypervisor, backdoor entry via the hosting operating system, DoS attacks and hardware resource attacks.

8.7 Threats to multiaccess edge computing

The following threats to edge computing have been identified:

- **False or rogue MEC gateway** [b-ENISA]: The open nature of edge gateways can create an attack scenario where attackers can deploy their own gateway devices. This threat results in the same effect as the man-in-the-middle attack.
- **Edge node overload** [b-ENISA]: If specific mobile applications or IoT devices initiate flooding of the edge node with requests or traffic directed to this component, overload of the edge node may occur on a local or service level. This attack comes from edge networks consisting of IoT devices disrupting the neighbour nodes of the affected network.
- **Abuse of edge open APIs** [b-ENISA]: If vulnerabilities in the MEC type of applications are exploited, open APIs in MEC nodes can be abused. The need for open APIs in MEC is mainly to provide support for federated services and interactions with different providers and content creators. This threat can be associated with DoS, man-in-the-middle, privacy leakages and VM manipulation.
- **Physical tampering with devices**: Physical tampering with devices is more likely to be possible as computational resources in the edge computing architecture are located closer to attackers. The attacker may destroy edge nodes, and in turn, compromise the efficacy of the entire network.

8.8 Threats to network function virtualization

The following threats to NFV have been identified:

- **Abuse of the data centres interconnect (DCI) protocol** [b-ENISA]: If vulnerabilities of DCI protocols are exploited, an attacker could create spoofed traffic. If virtualized systems are deployed within data centres, this may generate security threats to data centres that need to be considered.
- **Abuse of cloud computational resources** [b-ENISA]: If an attacker uses a simple registration process in a cloud computing service provider, powerful computing infrastructure, including both software and hardware components, can be abused. The attackers take advantage of the prevailing computing power of cloud networks and can initiate attacks in a very short time. For example, an attacker can launch brute force attacks and DoS attacks by abusing the power of cloud computing.
- **Network virtualization bypassing** [b-ENISA]: Issues related to bad network slicing implementation and configuration, or improper isolation can cause loss of data confidentiality/privacy (data/traffic intercepted by entities of other slices). A network used by different tenants needs to ensure that only legitimate traffic enters or leaves a network slice, but also that any switching element checks and enforces the traffic isolation by installing legitimate flow rules preventing slice trespassing. At the core network level, a hostile attacker would exploit hypervisor vulnerabilities and flow rule configuration to trespass on slice isolation and disclose data belonging to other tenants.
- **Abuse of virtualized host** [b-ENISA]: If applications run on virtualized hosts, this may cause the abuse of shared resources from a virtualized environment. In virtual environments, where physical resources are shared between tenants, there may be a set of behaviours that result in the disclosure of sensitive information. For instance, exposure via scavenging in virtualized environments is even more serious than in physical systems. While interception is a common threat in physical systems (e.g., networking environments), its effect is further exacerbated in virtual environments because it permits the cross-inspection of various tenants' data flow, as well as topology inference that could serve to set up a DoS attack.
- **Infrastructure integrity threat** [b-Alwakeel]: An attacker impersonates a service provider to appear part of the real services of NFV to gain access to user data.

- **Misuse of resources** [b-Alwakeel]: An attacker frees up some resources and uses them for his or her own benefit.
- **Change in NFV function definition** [b-Alwakeel]: An attacker modifies some of the operations in NFV functionality, definition or even produces DoS. This is usually done by injection.
- **Privilege modification** [b-Alwakeel]: An attacker changes the privileges of users in a non-control data attack, by upgrading or degrading their access to system entities in an unauthorized manner.
- **Confidentiality attack based on shared resources** [b-Alwakeel]: Using a side-channel attack, attackers can pull some private information about other users using a shared service in an unauthorized manner.
- **Malicious insider** [b-Alwakeel]: Trusted members from inside an organization use their authority to access the private data of users in an unauthorized manner.

8.9 Threats to management

The following threats to management have been identified:

- **Insecure management interface** [b-TR 33.811]: This is a threat when the interface is not secured. It enables attackers to gain access to capabilities for network management without authorization and to create network slice instances requiring significant network resources or a large number of network slice instances.
- **Disclosure of supervision and reporting data related to the management function** [b-TR 33.811]: This is a threat when supervision and reporting data is not protected in an appropriate manner. This will result in an attacker tampering with the results of supervision/reporting and eavesdropping on the transmission of supervision and reporting data and extracting sensitive information that can be used to execute attacks of running network slice instances.
- **Unauthorized access to the management exposure interface** [b-Ta-Hao Ting]: If the interface is compromised by unauthorized access, the network functions such as SDN, NFV and network slice can be subject to inappropriate malfunctions such as unauthorized changes of network functions, creation of inappropriate network configurations and network function modification**.**

9 Requirements for security capabilities related to components and functions

9.1 Security capabilities related to user equipment

The following security capabilities of UE should be supported:

- **Anti-malware capability to secure UE**: Anti-malware is a type of software program designed to prevent, detect and remove malicious software (malware) on UE. Three methods, signature-based malware detection, behaviour-based malware detection and sandboxing, are used to protect UE from being infected by malicious software.
- **IMSI security capability to secure the subscriber identity (IMSI) through encryption**: The IMSI should be encrypted by the ephemeral encryption key using a symmetric cryptographic algorithm. The precondition is that the UE has its own IMSI and the home network's public asymmetric key and each mobile operator (called the 'home network' here) has a public/private pair of asymmetric keys. It is assumed that the home network's private asymmetric key is kept secret by the home network, while the home network's public asymmetric key is pre-provisioned in mobile devices along with subscriber-specific IMSIs.
- **Identity verification capability**: verifies user identity for roaming and cloud services.

- **Key management capability**: supports the verification of user identity and mutual authentication between the UE and network element.
- **Location security capability**: ensures the security of the user location.
- **Authentication of the serving network**: The UE should authenticate the serving network identifier through implicit key authentication, i.e., that authentication is provided through the successful use of keys resulting from authentication and key agreement in subsequent procedures.
- **Confidentiality and integrity of user data and signalling data** [b-ITU-T X.1811]: UE has a capability to support the confidentiality of data through cipher algorithms for encryption and to support integrity protection and replay protection of user data between UE and the network nodes.
- **Secure storage and processing capability of subscription credentials** [b-Craven]: UE has a capability to provide integrity protection for credentials and their long-term keys through tamper-resistant hardware. The long-term keys should not be available unencrypted outside the tamper-resistant hardware. The program should be run in the tamper-resistant hardware using an authentication algorithm and subscription credentials.

9.2 Security capabilities related to access network

The following security capabilities of access network should be supported:

- **Link security capability**: provides confidentiality and integrity for communications for control channels and user traffic channels with UE.
- **UE authentication capability**: The serving network should authenticate the subscription permanent identifier in the process of authentication and key agreement between UE and the network.
- **UE authorization capability** [b-Craven]: The serving network should authorize the UE by using the subscription profile obtained from the home network.
- **Serving network authorization capability of the home network** [b-Craven]: It should be ensured that the UE is connected to a serving network authorized by the home network.
- **Access network authorization capability** [b-Craven]: An access network should be authorized by the serving network to provide services to UE.
- **Confidentiality capability of user and signalling data** [b-Craven]: The access network should support the encryption of user data in transit and for RRC signalling.
- **Integrity capability of user and signalling data** [b-Craven]: The nodes, like the UE, should support the integrity protection and replay protection of user data going between the UE and the next node B.
- **Setup and configuration capability** [b-Craven]: When operations and management (O&M) systems setup and configure, the next node B should be authenticated and authorized by a registration authority and a certification authority (RA/CA) so attackers will not be able to modify the next node B settings and software configurations.
- **Capability for key management inside the next node B** [b-Craven]: There is a need to protect the different elements of encryption keys provided by the IMT-2020 network core to the next node B.
- **Handling user plane and control plane data capability** [b-Craven]: The capability for key management is similar to that for handling user plane and control plane data for the next node B.
- **Capability for a secure environment** [b-Craven]: The secure environment that all of this unencrypted data is running is also subject to requirements. It should support secure storage through, for example, long-term cryptographic secrets and vital configuration data.

- **Capability to address threats of service disruption from RRC connection requests**: To prevent a manipulated RRC connection request threat, the base station needs to maintain the RRC connection with the existing user for a longer period of time. This results in the base station maintaining a connection longer than the waiting timer for the existing RRC connection. In addition, "Limit Time" and "Limit Count" parameters at the base station should be used and a monitoring process checking whether this attack is taking place should be added. The detailed attack scenario is described in Appendix II.

9.3 Security capabilities related to software-defined networking

The following security capabilities to SDN should be supported [ITU-T X.1038]:

- **Authentication capability** of the SDN application to authenticate the SDN controller/the user/the administrator;
- **Authorization capability** of the SDN application to authorize the user/administrator to access system information;
- **Data confidentiality capability** of the SDN application to provide confidentiality protection for system information stored in the application platform and to perform confidentiality protection for data transportation over the application-control interface;
- **Key/certificate management capability** of the SDN application, to support key/certificate management;
- **Security management capability** of the SDN application to support log and audit;
- **Application protection capability** of the SDN application to support defence against application vulnerabilities;
- **Data integrity capability** of the SDN application to support the performance of integrity protection for data transportation over the application-control interface;
- **Authentication capability** of the SDN controller to authenticate administrators/the SDN application/the SDN switch;
- **Authorization capability** of the SDN controller to authorize administrators/the SDN application to manage the SDN controller;
- **Authentication and security management capability** of the SDN controller to support anti-DoS protection;
- **Data integrity capability of the SDN controller** to perform integrity protection for configuration data stored in the SDN controller, to perform integrity protection for user data stored in the SDN controller, to perform integrity protection for data transportation over the application-control interface and to perform integrity protection for data transportation over the resource-control interface;
- **Key/certificate management capability** of the SDN controller to perform key/certificate management;
- **Data confidentiality capability of the SDN controller** to perform confidentiality protection for configuration data stored in the SDN controller, to perform confidentiality protection for user data stored in the SDN controller, to perform confidentiality protection for data transportation over the application-control interface and to perform confidentiality protection for data transportation over the resource-control interface;
- **Operating system hardening capability of the SDN controller** to support the operating system's hardening functionality;
- **Authentication capability of the SDN resource layer** to authenticate administrators/the SDN controller;

- **Authorization capability of the SDN resource layer** to authorize administrators to manage SDN switches;
- **Security management capability of the SDN resource layer** to support log and audit;
- **Data integrity capability of the SDN resource layer** to perform integrity protection for configuration data stored in the SDN switch, and to perform integrity protection for data transportation between SDN switches/to perform integrity protection for data transportation over the resource-control interface;
- **Key/certificate management capability of the SDN resource layer** to perform key/certificate management;
- **Data confidentiality capability of the SDN resource layer** to perform confidentiality protection for configuration data stored in the SDN switch, to perform confidentiality protection for data transportation between SDN switches and to perform confidentiality protection for data transportation over the resource-control interface;
- **Flow table overflow prevention capability of the SDN resource layer**. The SDN controller needs to dynamically maintain the flow table by inserting and deleting flow entries.

9.4 Security capabilities related to core network

The following security capabilities should be supported:

- **DoS and DDoS detection and protection capability** to protect the centralized control point in SDN;
- **Configuration verification capability** to verify flow rules in the SDN network element;
- **Access control capability** to limit access to SDN and core network elements.

The following security capabilities of the network exposure function and service-based interface should be supported:

- **Secure network functions exposure capabilities** [b-TS 33.501]: Mutual authentication based on client and server certificates should be performed between the network exposure function and the application function of third party application functions outside the IMT-2020 operator domain, which is provided by a secure tunnel such as TLS. The traffic between the Network Exposure Function (NEF) and the application function should be used to provide integrity protection, replay protection and confidentiality protection.
- **Confidentiality, integrity of data and authentication of network elements through a service-based interface** [b-TS 33.501]: The traffic between the network elements through the SBI should provide integrity protection, replay protection and confidentiality protection of data and authentication of network elements through a secure tunnel such as TLS.

9.5 Security capabilities related to network slicing

The following security capabilities related to the slice lifecycle should be supported [b-Olimid]:

- **Slice lifecycle security capability**: Security should be enforced in all four phases because a vulnerability in one phase can introduce vulnerabilities in other phases.
- **Appropriate logging and auditing capability**: Different levels of logging should be implemented in distinct network slices, depending on various factors such as regulations, the targeted security level for the consuming services, the dedicated type of customer devices (e.g., human vs machine usage). The results of the logs and reports should be protected, as their exposure would leak sensitive information.
- **Network slice template security capability**: This should be confidentiality and integrity protected in transmission and storage, and the template source should be authenticated.

- **Security orchestration capability**: Customized security services should be orchestrated and deployed according to the security requirements of different vertical industries [b-ITU-T X.1047].
- **Slice isolation capability**: Isolation should be secured at slice creation, monitored and, if needed, updated, during the run-time [b-ITU-T X.1047].
- **API security capability**: APIs should be secure in terms of access and operational rights and should not expose traffic data; APIs should only allow capabilities and data access as agreed between the parties by legal means.
- **Decommissioning capability**: At decommissioning, sensitive data should be destroyed (or by case, securely stored), and resources and network functions should be freed.

The following security capabilities related to intra-slice security should be supported:

- **End-to-end security capability**: Slices are end-to-end logical networks, so end-to-end security should be considered [b-ITU-T X.1047].
- **Adequate usage capability of security mechanisms**: All communication (e.g., between the slice and the resource layer, the slice and the slice manager, the sub-slices of a slice, the customer device and the access point in the network) should use adequate mechanisms to assure the target security level; minimal requirements should include confidentiality, integrity, authenticity of the data and mutual authentication between peers.
- **UE authentication capability**: IMT-2020 customer devices should be strongly authenticated by primary and preferable secondary authentication.
- **Secure resource functionality consuming capability**: All resources and network functions consumed by a slice should be secured.
- **Tenant security capability**: New facilities introduced by tenants (e.g., network functions, configurations, services) and their integration should be adequately secured to prevent weaknesses that can be further exploited.
- **Identity security capability**: Sensitive identifiers should be protected and no correlation between identifiers should be leaked.
- **Lawful interception**: This should be accessible at both the slice and service layers.
- **Tenants access, rights and configuration capabilities**: This should conform with the legal agreements between the parties.

The following security capabilities related to inter-slice communication should be supported:

- A minimal security level should be granted for every slice.
- **Slice isolation capability**: Isolation between the slices should be strong enough to prevent attacks via the less secured slices [b-ITU-T X.1047].
- **Minimum communication security capability**: Communication between slices should be reduced to a minimum, defined by strict rules and implemented via secured channels.
- **Key management capability**: Cryptographic keys (and other sensitive parameters) should not be shared between slices.
- **Minimum resource allocation capability**: Allocation of resources should guarantee a minimum level of availability for each slice; in particular, security mechanisms should be able to run regardless of the resource consumption.
- Slices with a significant difference in security levels should not share resources or network functions; in particular, slices in test mode should never be run together with slices in run-time phase.
- **Independent security capability**: Distinct authentication, authorization and access control mechanisms should be independent for each slice.

9.6 Security capabilities related to multiaccess edge computing

The following security capabilities should be supported:

- **DDoS mitigation capability** to protect cloud web services;
- **Access control capability** to limit access multiaccess edge computing network elements;
- **Integrity verification capability** to secure data and the storage system in cloud computing;
- **Service access control capability** to limit the service-based cloud computing element;
- **A physical security capability**: The physical security of any edge nodes that are not placed in highly secure edge data centres, such as those employing additional physical protection techniques during manufacture or implementing locking mechanisms and other physical safeguards in the field should be provided for.

9.7 Security capabilities related to network function virtualization

The following security capabilities should be supported:

- **Traffic isolation capability**: This is to ensure virtual slices and virtual network functions.
- **DoS attack prevention capability** [b-Alwakeel]: Network elements, for instance, firewalls and load balancers, should be used to mitigate DoS/DDoS attacks.
- **Infrastructure integrity capability** [b-Alwakeel]: A chain of trust and a trusted platform module (TPM) should be used to ensure the security of different providers of VNF services.
- **Resource misuse mitigation capability** [b-Alwakeel]: An advanced hypervisor scheduler that provides fair share allocation among the processes, limiting the maximum amount allowed for each virtual service, should be provided.
- **NFV function definition change protection capability** [b-Alwakeel]: A copy of the user virtual services should be kept on separate storage to prevent malware-injection attacks. A file allocation table (FAT) is utilized that contains information about the services and the software that the user is executing.
- **Privilege modification prevention capability** [b-Alwakeel]: Protecting the virtualization entity from unauthorized access by adding restrictive policies to access the resources should be provided.
- **Shared resources mitigation capability** [b-Alwakeel]: A capability mitigating side-channel attacks should be used to limit access to the VM images and network functions virtualization infrastructure (NFVI) components and control the usage of the resources. This can be achieved by using a virtual firewall to prevent unauthorized access to the system.
- **Malicious insider mitigation capability** [b-Alwakeel]: Insider attacks can be mitigated using several capabilities, one of which is logging accesses within the NFV environment which can then be used for internal audits to detect suspicious activity. Another mechanism is to set up strict policies for authentication and authorization for users with access.

9.8 Security capabilities related to management function

The following security capabilities [b-TR 33.811] should be supported:

- **Mutual authentication capability** between the management service consumer and the management service producer using a secure tunnel such as TLS, based on either 1) the client and server certificates or 2) pre-shared keys (PSK) with TLS-PSK;
- **Integrity protection, replay protection and confidentiality protection capability** for the interface between the management service producer and the management service consumer residing outside the 3GPP operator's trust domain TLS;

- **PI security capability to management interface**: APIs should be secure in terms of access and operational rights and should not expose traffic data; APIs to the management interface should only allow capabilities and data access as agreed between the parties by legal means.

Annex A

Security architecture for IMT-2020 communication system

(This annex forms an integral part of this Recommendation.)

Figure 4-1 in [b-TS 33.501] gives an overview of security architecture for the IMT-2020 communication system.

Figure 4-1 in [b-TS 33.501] illustrates the following security domains:

– Network access security (I): the set of security features that enable UE to authenticate and access services via the network securely, including via the 3GPP access network and non-3GPP access network, and in particular, to protect against attacks on the (radio) interfaces. In addition, this includes the security context delivery from the serving network (SN) to access network (AN) for access security.

– Network domain security (II): the set of security features that enables network nodes to securely exchange signalling data and user plane data.

– User domain security (III): the set of security features that secures user access to mobile equipment.

– Application domain security (IV): the set of security features that enables applications in the user domain and in the provider domain to exchange messages securely. Application domain security is out of scope of the present Recommendation.

– SBA domain security (V): the set of security features that enables NFs of the SBA architecture to securely communicate within the SN domain and with other network domains. Such features include network function registration, discovery and authorization security aspects, as well as protection for service-based interfaces. SBA domain security is a new security feature compared with [b-TS 33.401].

– Visibility and configurability of security (VI): the set of features that enables the user to be informed whether a security feature is in operation or not.

Appendix I

Generic network security architecture for providing end-to-end network security

(This appendix does not form an integral part of this Recommendation.)

This appendix describes a generic network security architecture for providing end-to-end network security, which is described in [b-ITU-T X.805], a basis for this Recommendation.

In [b-ITU-T X.805] a network security architecture for providing end-to-end network security is defined. This architecture can be applied to various kinds of network where end-to-end security is a concern and functions independently of the network's underlying technology. Recommendation [b-ITU-T X.805] defines the general security-related architectural elements that are necessary for providing end-to-end security. The objective of [b-ITU-T X.805] is to serve as a foundation for developing detailed recommendations for end-to-end network security.

Recommendation [b-ITU-T X.805] defines eight security dimensions:

1) Access control;
2) Authentication;
3) Non-repudiation;
4) Data confidentiality;
5) Communication security;
6) Data integrity;
7) Availability; and
8) Privacy.

Recommendation [b-ITU-T X.805] also defines three security layers which build on one another to provide network-based solutions:

1) The infrastructure security layer;
2) The services security layer; and
3) The applications security layer.

In addition, [b-ITU-T X.805] defines three security planes:

1) The management plane;
2) The control plane; and
3) The end-user plane.

Appendix II

Threat of service disruption from a manipulated radio resource control (RRC) connection request and its capability

(This appendix does not form an integral part of this Recommendation.)

II.1 Overview

An RRC connection request is a message transmitted when UE accesses a network and is sent in plaintext. It includes a globally unique temporary identity (GUTI) or S-TMSI, that is, a temporary identification information of the UE. There are several ways to find out the temporary identification information of a specific user. If an attacker captures this RRC connection request and modifies the message transmitted in plaintext in the previous step, then the victim's temporary identification information can be used to continuously block the victim's network connection.

II.2 Attack scenario

An attacker can intercept the RRC connection request message transmitted in plaintext and identify the GUTI or S-TMSI, which provide temporary identification information. When sending a forged RRC connection request message, the attacker misuses the temporary identification information, and their message is mistaken as being sent from the victim's UE. Although the attacker's RRC connection is released due to a MAC (message authentication code) authentication failure during non-access stratum (NAS) signalling, the attacker can continuously block the victim's radio connection by sending the same forged message again. In addition, temporary identification information is newly created at regular time intervals according to specific rules based on IMSI. If the S-TMSI is changed, then the attacker can detect the change and send an attack message again. To block victim UE from radio access, the attacker needs to send a forged RRC connection request message. There are two prerequisites for this attack: (1) The attacker needs to place his or her mobile device in the same cell as that of the victim's UE to capture radio traffic; (2) The attacker has UE that can send a forged message.

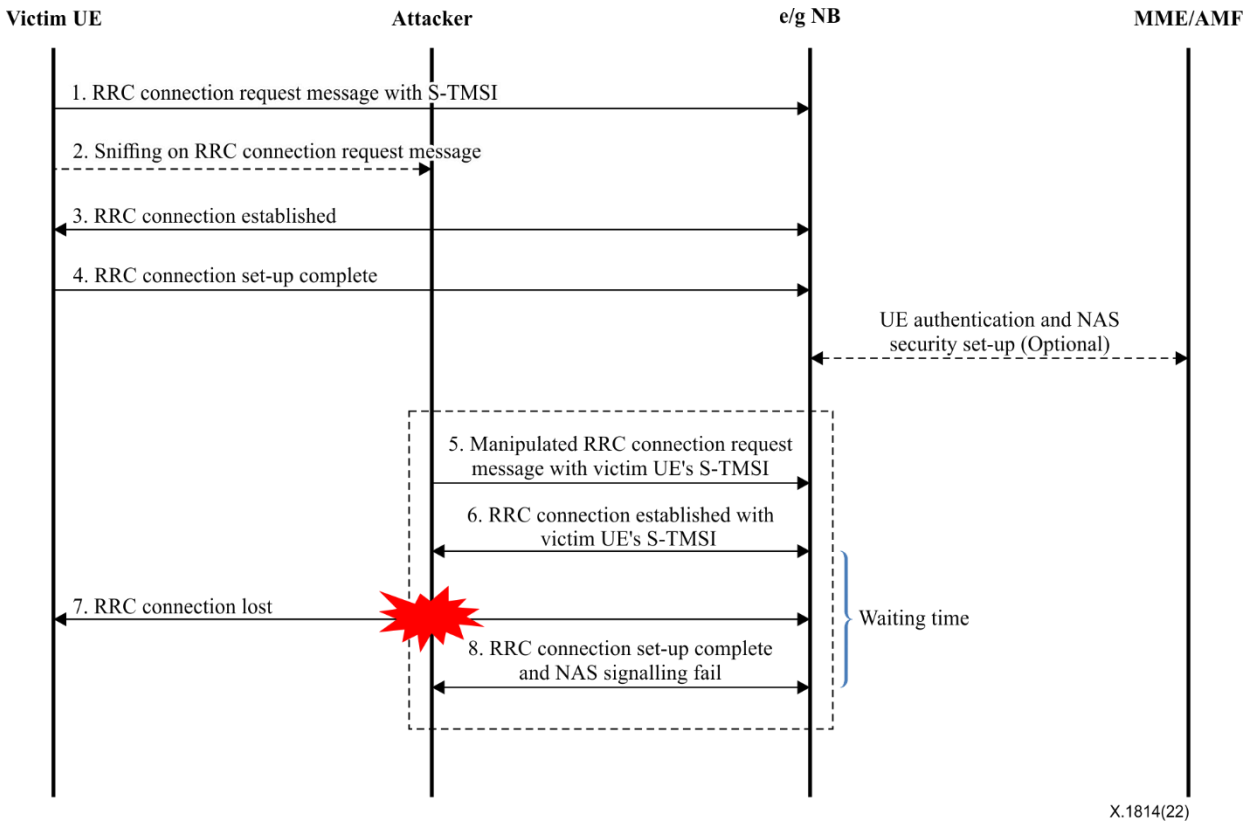

Figure II.1 – Manipulated RRC connection request attack scenario

II.3 Consequence

Due to this vulnerability, where there is no check to determine whether the message has been tampered with, the radio network equipment (e/gNodeB) disconnects the existing connection with the victim's UE according to the message sent by the attacker and connects to the attacker's UE. The victim's UE may remain in a state where it cannot access the network normally.

II.4 Countermeasures

The simplest and most effective countermeasure is that the base station maintains the RRC connection with the existing user for a certain period of time. After the attacker establishes the RRC connection using the stolen ID of the victim, the connection will be released when the NAS signalling process fails. Therefore, if the victim's existing connection is maintained until the attacker's RRC connection is released, the radio connection can be maintained. Usually, the time from when an attacker attempts RRC connection until RRC release due to a failure in the NAS signalling process corresponds to the duration for which the base station transmits RRC connection setup and waits for RRC connection setup complete. Therefore, the "waiting timer"[1] is implemented in the e/gNodeB to count the time from when it sends RRC connection setup to the UE until it receives RRC connection setup complete. A process should be added so that the base station maintains a connection longer than the waiting timer for the existing RRC connection, which now sends a request with a duplicate ID and maintains the existing connection when a new connection is released within the corresponding time. The maintenance time is to be minimized in consideration of its influence on communication service and equipment performance.

1 For example, T352 as defined in 3GPP TS 25.331.

In addition, an attacker can repeatedly send RRC connection requests to the base station to sustain the service disruption status to a victim. To mitigate this situation, a "limit time" and "limit count" at an e/gNodeB should be set, if RRC connection and release are repeatedly performed within the time limit and over a number of the count limit, adding a process so that the base station alerts the network operator to monitor attacks.

Bibliography

[b-ITU-T Q.700] Recommendation ITU-T Q.700 (1993), *Introduction to CCITT Signalling System No. 7*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open systems interconnection – The directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[b-ITU-T X.1047] Recommendation ITU-T X.1047 (2021), *Security requirements and architecture for network slice management and orchestration*.

[b-ITU-T X.1401] Recommendation ITU-T X.1401 (2019), *Security threats of distributed ledger technology*.

[b-ITU-T X.1406] Recommendation ITU-T X.1406 (2021), *Security threats to online voting systems using distributed ledger technology*.

[b-ITU-T X.1408] Recommendation ITU-T X.1408 (2021), *Security threats and requirements for data access and sharing based on the distributed ledger technology*.

[b-ITU-T X.1811] Recommendation ITU-T X.1811 (2021), *Security guidelines for applying quantum-safe algorithms in IMT-2020 systems*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-ITU-T Y.3101] Recommendation ITU-T Y.3101 (2018), *Requirements of the IMT-2020 network*.

[b-ITU-T Y.3150] Recommendation ITU-T Y.3150 (2020) *High-level technical characteristics of network softwarization for IMT-2020*.

[b-ITU-T Y.4807] Recommendation ITU-T Y.4807 (2020) *Agility by design for telecommunication/ICT systems security used in the Internet of things*.

[b-ITU workshop] Third annual ITU IMT-2020/5G Workshop and Demo Day (July 18, 2018), *5G security activities and future plan in ITU-T SG17*.

[b-ISO 10393] ISO 10393:2013, *Consumer product recall – Guidelines for suppliers*.

[b-ISO 81001-1] ISO 81001-1:2021, *Health software and health IT systems safety, effectiveness and security – Part 1: Principles and concepts.*

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/TS 21719-2] ISO/TS 21719-2: 2018, *Electronic fee collection – Personalization of on-board equipment (OBE) – Part 2: Using dedicated short-range communication*.

[b-RFC 3588] IETF RFC 3588 (2003), *Diameter base protocol*.

[b-TR 33.811] 3GPP TR 33.811 (2018), *Study on security aspects of 5G network slicing management*.

[b-TS 33.401] 3GPP TS 33.401 (2021), *3GPP System Architecture Evolution (SAE); Security architecture*.

[b-TS 33.501] 3GPP TS 33.501 (2022), *Security architecture and procedures for 5G System*.

[b-Alwakeel] Alwakeel, A.M., Alnaim, A., and Fernández, E.B., *A Survey of Network Function Virtualization Security*, IEEE Southeast Conf. 2018. https://www.researchgate.net/publication/328146655_A_Survey_of_Network_Function_Virtualization_Security

[b-Craven] Craven, C., *5G Security Standards: What Are They?* 10 June 2020. https://www.sdxcentral.com/5g/definitions/5g-security-standards/

[b-ENISA] European Union Agency for Cybersecurity (ENISA) (2019), *ENISA Threat Landscape for 5G Networks*.

[b-Goodin] Goodin, D. (2013), *Lucky Thirteen attack snarfs cookies protected by SSL encryption* Ars Technica. https://arstechnica.com/security/2013/02/lucky-thirteen-attack-snarfs-cookies-protected-by-ssl-encryption/

[b-Khan] Khan, R., Kumar, P., Jayakody, D.N.K, and Liyanage, M. (2019), *A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions*, IEEE Communications Surveys and Tutorials, Vol. 22, No. 1, July, pp. 196-248.

[b-Möller] Möller, B, Duong, T, and Kotowicz, K. (2014), *This POODLE Bites: Exploiting The SSL 3.0 Fallback*. https://www.openssl.org/~bodo/ssl-poodle.pdf

[b-NGMN] The Next Generation Mobile Networks Alliance (NGMN Alliance) (2016), *5G security recommendations package*.

[b-Olimid] Olimid, R., and Nencioni, G. (2020) *5G Network Slicing: A Security Overview*, IEEE Access, Vol. 8, June, 99999-100009.

[b-SQL] OWASP, *SQL injection.* https://owasp.org/www-community/attacks/SQL_Injection

[b-Ta-Hao Ting] Ta-Hao Ting, Tsung-Nan Lin, Shan-Hsiang Shen, and Yu-Wei Chang (2019), *Guidelines for 5G end to end architecture and security issues*. https://arxiv.org/abs/1912.10318

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022