ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1815 (03/2023)

SERIES X: Data networks, open system communications and security

IMT-2020 Security

Security guidelines and requirements for IMT-2020 edge computing services

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.1815

Security guidelines and requirements for IMT-2020 edge computing services

Summary

The IMT-2020 network will enable a variety of services, including enhanced mobile broadband (eMBB) services, massive machine type communications (mMTC) based services and ultra-reliable low latency communications (URLLC) based services, on an infrastructure of network and computing resources. In line with the key features and the requirements identified for the IMT-2020 network, it is required to be more efficient, personalized, intelligent, reliable and flexible.

To support the typical services in the IMT-2020 network, especially eMBB services and URLLC based services, edge computing is acknowledged to be one of the key technologies for meeting the demanding key performance indicators (KPIs) of the IMT-2020 network, especially as far as low latency and bandwidth efficiency are concerned.

Edge computing enables the operator and the third party service provider to deploy the services close to the user's access point, thus achieving high-efficiency service delivery through reduced end-to-end latency and load on the transport network.

In order to ensure the security of edge computing service deployment and application, the security threats and relevant security requirements specific to edge computing service need to be analysed and the overall security framework need to be established.

This draft Recommendation aims to analyses the deployment scheme and typical application scenarios of edge computing services, specifies the security threats and requirements specific to edge computing services in IMT-2020 and thus establishes security capabilities for the operator to safeguard its applications.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1815	2023-03-03	17	11.1002/1000/15113

Keywords

Edge computing services, IMT-2020 network, security guidelines.

* 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/.

Table of Contents

Recommendation ITU-T X.1815

Security guidelines and requirements for IMT-2020 edge computing services

1 Scope

This Recommendation provides a potential deployment scheme and typical application scenarios of edge computing services, specifies the security threats and requirements specific to edge computing services in IMT-2020 and thus provides security capabilities guidelines for the operator to safeguard its applications.

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

[3GPP TS 23.501] 3GPP TS 23.50 (2022), *5G; System architecture for the 5G System (5GS) (version 17.4.0 Release 17)*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 IMT-2020 [b-ITU-T Y.3100]: (Based on [b-ITU-R M.2083]) Systems, system components, and related technologies that provide far more enhanced capabilities than those described in [b-ITU-R M.1645].

3.1.2 Trojan horse [b-ITU-T E.800]: A piece of software which appears benign or even useful. This conceals the real purpose of the software which intends to disrupt the system or to steal information.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 IMT-2020 edge computing service: A service provided via the IMT-2020 system which enables a service to be hosted close to the user equipment's access point, so as to achieve an efficient service delivery through the reduced end-to-end latency and load on the transport network.

3.2.2 IMT-2020 system: 3GPP system consisting of the IMT-2020 access network (AN), IMT-2020 core network and user equipment (UE).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AF Application Function

AMF	Access and Mobility Management Function
AN	Access Network
CDN	Content Delivery Network
EASDF	Edge Application Server Discovery Function
DDoS	Distributed Denial of Service
DC	Data Centre
DN	Data Network
DNN	Data Network Name
DNS	Domain Name System
eMBB	enhanced Mobile Broadband
EHE	Edge Hosting Environment
GW-C	Gateway-Control Plane
GW-U	Gateway-User Plane
IMS	Internet protocol Multimedia Subsystem
IP	Internet Protocol
KPI	Key Performance Indicator
MEC	Mobile Edge Computing
mMTC	massive Machine Type Communications
NAT	Network Address Translation
NEF	Network Exposure Function
NB IoT	Narrow Band Internet of Things
NFVO	Network Functions Virtualization Orchestrator
NRF	Network Repository Function
VNFM	Virtualized Network Function Manager
OSS	Operation Support Systems
PDU	Protocol Data Unit
PSA	Protocol data unit Session Anchor
QoS	Quality of Service
RAN	Radio Access Network
SBA	Service Based Architecture
SIM	Subscriber Identification Module
SMF	Session Management Function
TLS	Transport Layer Security
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communications
V2X	Vehicle to Everything

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keyword "**should**" indicates a requirement which is recommended but which is not absolutely required. This requirement need not be present to claim conformance.

6 Overview of IMT-2020 edge computing

The IMT-2020 network will enable a variety of services, including enhanced mobile broadband (eMBB) services, massive machine type communications (mMTC) based services and ultrareliable low latency communications (URLLC) based services [ITU-T Y.3101], on an infrastructure of network and computing resources. In line with the key features and the requirements identified in IMT-2020 network, it is required to be a more efficient, personalized, intelligent, reliable and flexible network.

In order to support the typical services in the IMT-2020 network, especially eMBB services and URLLC based services, edge computing is acknowledged to be one of the key technologies for meeting the demanding key performance indicators (KPIs) of the IMT-2020 network, especially as far as low latency and bandwidth efficiency are concerned.

IMT-2020 edge computing enables the operator and the third party service provider to deploy the services close to the user's access point via IMT-2020 system, thus achieves high-efficiency service delivery through reduced end-to-end latency and load on the transport network.

6.1 Deployment scheme

The IMT-2020 system architecture specified by 3GPP in the IMT-2020 system has two available options, one with the traditional reference point and interface approach and the other where the core network functions interact with each other using a service based architecture (SBA).

Figure 6-1 describes an IMT-2020 System architecture which based on [3GPP TS 23.501].

From the operator's perspective, the deployment scheme of IMT-2020 edge computing services with SBA may include the following IMT-2020 network functions:

– UPF (user plane function): The UPF is one of the network functions (NFs) of the IMT-2020 core network. It is responsible for packet routing and forwarding, packet inspection, quality of service (QoS) handling, and external protocol data unit (PDU) session for interconnecting data network (DN), in the IMT-2020 architecture.

– AMF (access and mobility management function): The AMF receives all connection and session related information from the user equipment (UE) through N1 and the (radio) access Network ((R)AN) through the N2 interface (see Figure 1) but is responsible only for handling connection and mobility management tasks.

– SMF (session management function): The SMF is a fundamental element of the IMT-2020 SBA. It is primarily responsible for interacting with the decoupled data plane, creating, updating and removing PDU sessions and managing session context with the UPF.

– EASDF (edge application server discovery function): The EASDF includes one or more of the following functionalities: registering to the network repository function (NRF) for EASDF discovery and selection and handling the DNS messages according to the instruction from the SMF. The EASDF has direct user plane connectivity (i.e., without any network address translation (NAT)) with the PDU session anchor (PSA) UPF over N6 interface for the transmission of domain name system (DNS) signalling exchanged with the UE.

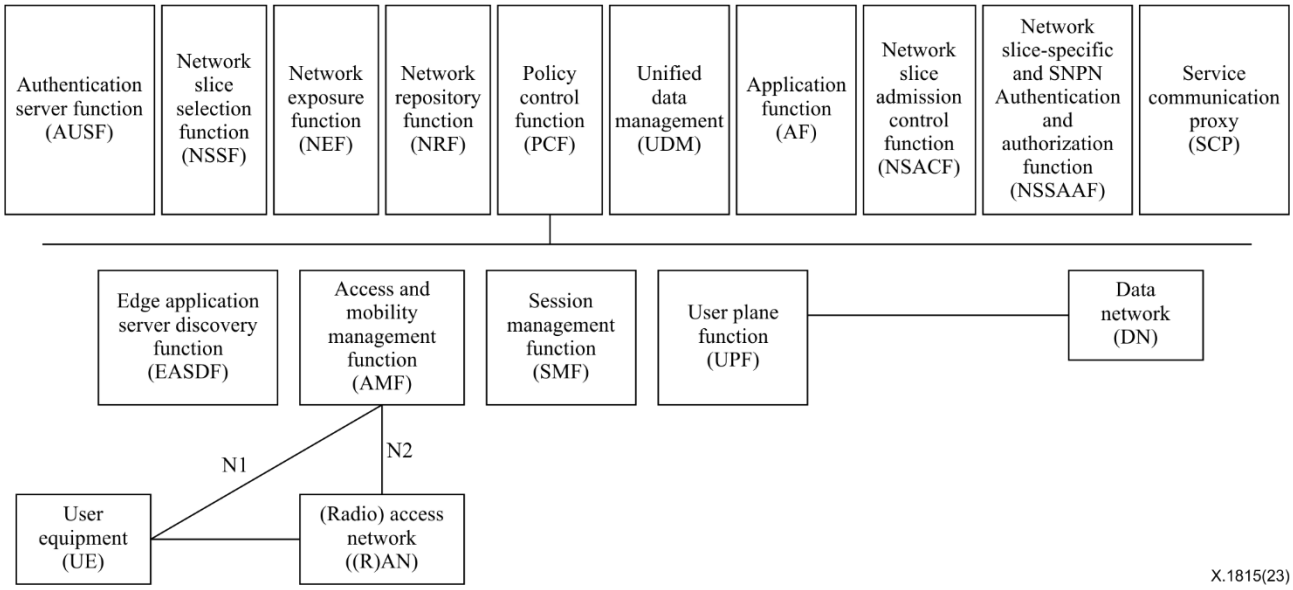

Figure 6-1 – The IMT-2020 system architecture

Figure 6-2 describes a deployment scheme of IMT-2020 edge computing services.

The IMT-2020 system supports the edge hosting environment (EHE) deployed in the DN beyond the PSA UPF. An EHE may be under the control of either the operator or third parties [b-3GPP TS 23.548]. The local part of the DN in which the EHE is deployed may have user plane connectivity with both a centrally deployed PSA and a locally deployed PSA of the same DNN.

From the operator's view, the deployment scheme of IMT-2020 edge computing services is as shown in Figure 6-2.

– Edge DC: Provides mobile edge computing (MEC) functionality which enables IMT-2020 edge computing services and gateway-user plane (GW-U) and UPF functionalities.

– Local DC: Provides GW-U, content delivery network (CDN) and UPF functionalities.

– Area DC: Provides gateway-control plane (GW-C), AMF/SMF, NB IoT and IMS etc. functionalities.

– Manage domain: Includes cloud manage platform, network functions virtualization orchestrator (NFVO) and virtualized network function manager (VNFM).

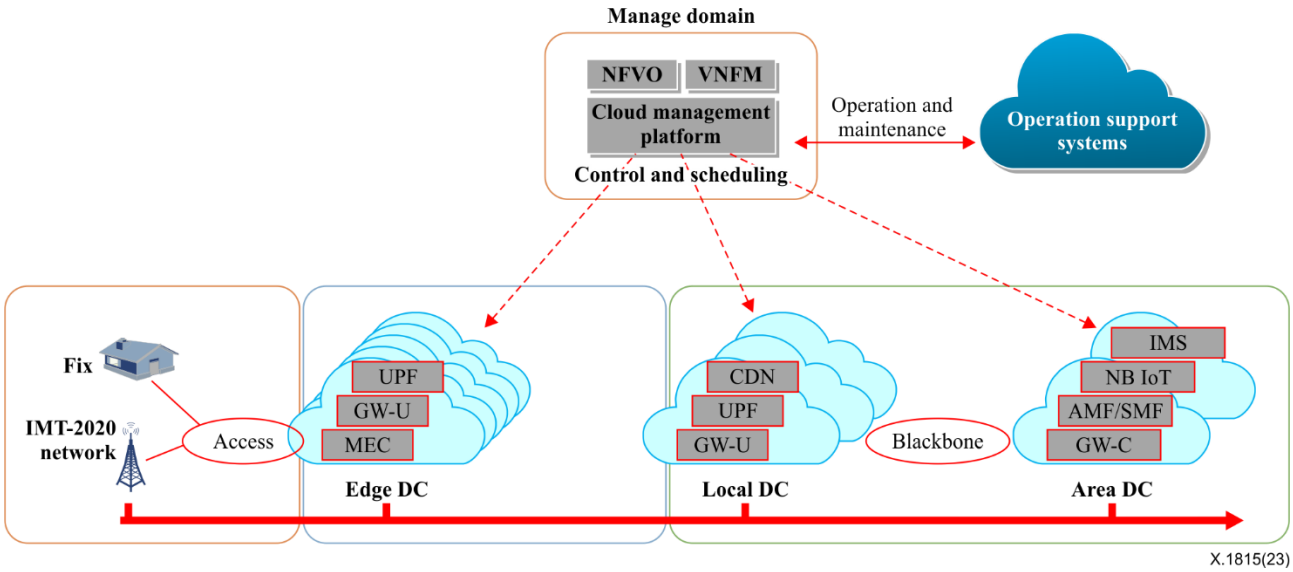

Figure 6-2 – The deployment scheme of IMT-2020 edge computing services

6.2 Typical application scenario

6.2.1 Vehicle to everything (V2X)

In the scenario of V2X, the volume of connected devices with multiple applications brings increasing data transfer requirements to the network side. The network is required to offer enhanced broadband and computation capabilities for data usage and storage.

By applying IMT-2020 edge computing technology in V2X, it becomes possible to deploy the applications in the edge node, thus reducing the end-to-end time delay and increasing reliability in line with the specific requirements of the different V2X services (i.e., Safe driving service needs stringent requirements of both latency and reliability) benefitting from the shorter transmission route, and offer more powerful computation and storage resources.

The services in IMT-2020 edge computing technology based V2X include but are not limited to:

– Information service: The edge computing service offers functions of map load and update, audio and video entertainment, and remote detection for the vehicle. These functions require an edge computing service offering an enhanced mobile broadband capability, e.g., at least 25 Mbps for 4K high-definition video service.

– Safe driving service: The edge computing service assists the driver to make vehicle control decisions (e.g., by giving a collision warning) through vehicle information, pedestrian information and roadside unit information acquisition. It is required that the edge computing service offer low latency and high reliability capabilities (generally, the delay is less than 20 ms and the telecommunication reliability is at least 99%).

– Enhanced driving efficiency service: The edge computing service optimizes the efficiency of traffic facilities based on the IMT-2020 V2X and big data analysis technologies, e.g., traffic light control, speed of vehicle guide.

6.2.2 Internet of Things (IoT)

By applying IMT-2020 edge computing technology in the IoT, it becomes possible to deploy applications in the edge node, thus reducing the end-to-end time delay benefitting from the shorter transmission route, and offer more efficient service via local data computation.

The service scenarios in IMT-2020 edge computing technology based IoT include but are not limited to:

– The smart city;

– The smart building;

– The smart home.

6.2.3 Industrial Internet

IMT-2020 edge computing technology supports the industrial internet services (especially for the case of real-time IoT applications, where data processing usually takes place far away from a centralized data centre and low latency is a mandatory requirement), by coordinating the IMT-2020 network with the edge controller, edge gateway and edge cloud.

The edge controller is in charge of task orchestration, application deployment and life cycle management from the edge gateway, and controls industrial devices, etc.

The edge gateway implements task orchestration, industrial device registration, application deployment and life cycle management from the edge cloud, and analyses edge data, etc.

The edge cloud is in charge of task orchestration, industrial device registration, application deployment and life cycle management from the edge gateway, and coordinates the edge servers and analyses edge data, etc.

7 Security threats

From the layered point of view, offering an IMT-2020 edge computing service, involves an infrastructure layer, a network layer and an application layer, and therefore security threats must be considered from all these perspectives. It is important to note that, though MEC has the characteristic of security and privacy protection because data transmission takes place directly to MEC servers rather than through central servers, thus reducing the risk of data leakage in the process of data transmission in the network, the exploitation of a large number of mobile devices and the deployment of edge cloud servers leads to new security challenges. Specifically, traditional cloud computing security solutions could be not suitable for MEC as the environments of IoT devices at the edge encounter a number of new threats that are quite different from those in the traditional management of cloud. In practice, it is impossible to apply current data security methods on edge devices because most edge devices are resource constrained and the network becomes vulnerable due to the highly dynamic environment of MEC. An exhaustive vulnerabilities evaluation on MEC was performed by the ENISA (European Union Agency for Cybersecurity) [b-ENISA] that considers the 5G specifications according to 3GPP Release 16. Hence, to develop a MEC environment for future 5G applications while ensuring security still remains an issue to be further investigated in the near future.

7.1 The infrastructure layer

7.1.1 Cloud management platform

The deployment of an IMT-2020 edge computing service may need a cloud management platform. Besides the general security threats to such a platform, an attacker may use the interface between the cloud management platform and the IMT-2020 network to launch a further attack on the IMT-2020 network.

7.1.2 Virtualized infrastructure

Virtualized infrastructure may be unavailable if the physical resources are attacked or broken. This potential system vulnerability may be used by an attacker to gain unauthorized administration access to the virtual resource management system and modify configuration information.

7.1.3 Malicious hardware/software injections

Unauthorized software and hardware components known as Trojan horses can be injected into infrastructure to degrade the efficacy of existing edge servers and devices and even allow for exploitation of service provider [b-Daniel]. This may allow those entities providing software and

hardware solutions for edge computing service to execute unwittingly malicious activities on an attacker's behalf.

7.1.4 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 potential attackers. An attacker may destroy edge nodes, and in turn, compromise the efficacy of the entire network.

7.2 The network layer

7.2.1 Analyse the network flow

An attacker may monitor and/or steal link data and analyse flow characteristics to obtain information on services, and thereby proceed to further attack the network.

7.2.2 Sniff the network topology

An attacker may compromise the service node which may be deployed in open environments to launch an attack that sniffs the network topology.

7.2.3 DDoS attack

An attacker may compromise subscribed users and/or service nodes which may be deployed in open environments to launch a DDoS attack. When DDoS attacks are happening, an existing network resource is overwhelmed with traffic from other compromised resources within the network, which is another edge computing security risk.

7.2.4 Eavesdrop or manipulate the communication data

The services that use IMT-2020 edge computing are based on the open wireless network. An attacker may eavesdrop or manipulate communication data; in some scenarios, e.g., industry and manufacture, smart city, communication data may include extremely important information such as user identifiers and credentials, business information and public safety information.

7.2.5 Cross-domain attack

Since the edge computing service in IMT-2020 network needs to coordinate the functionalities among the access network, core network and cloud management platform, the single point of compromise may incur a cross-domain attack which leads to the network and service being unavailable.

7.2.6 Unauthorized access

In order to enable the UE to connect to the best edge computing service, signalling interactions between the UE and IMT-2020 core network are necessary. If signalling is tampered with by an attacker, it may make unauthorized access to the edge computing service and even a DDoS attack possible.

7.2.7 Network exposure to edge application

The IMT-2020 network could expose network information to the local application function (AF) with possible scenarios such as local PSA UPF exposing network information to the local AF via the local network exposure function (NEF) or directly.

7.2.8 Routing information attacks

A routing information attack, or simply a routing attack, occurs at the network layer of an edge network. Routing attacks interfere with the way that traffic is transferred within a network, which can affect throughput, latency and data paths.

7.2.9 Session hijacking

The hacker intercepts and hijacks a user session to obtain access to user data and services.

7.3 The application layer

7.3.1 Vulnerability of the technical framework

In IMT-2020 edge computing services, since a huge amount of the nodes use the same technical framework among different scenarios and vertical industries, if one node is compromised this will affect others.

7.3.2 Unauthorized usage

The threat of unauthorized usage occurs when an illegal or unsubscribed user gains access to IMT-2020 edge computing services by masquerading as an authorized entity.

7.3.3 Trojan horses and viruses

Attacks using Trojan horses and viruses occur when a malicious IMT-2020 edge computing service or attacker impersonates a legal service provider and injects Trojan horses or viruses into an application which may be harmful to user devices and data, and even launch a further attack on the mobile telecommunication network.

7.3.4 Data disclosure

Data disclosure occurs when attackers impersonate a legal entity to elicit data during the application data migration, transmission, storage, sharing and destruction processes of an edge computing service.

8 Security requirements

8.1 The infrastructure layer

The security requirements of a cloud management platform should include:

a) That the cloud management platform support authentication and authorization for the data plane gateway, edge computing platform management and edge computing application.

b) That it protects sensitive data in order to resist unauthorized access and data tampering (for example, in industrial scenarios sensitive production data need to be protected to perform industrial processes correctly and avoid any outage due to network attacks).

c) That the cloud management platform be securely isolated with IMT-2020 core network elements (e.g., NEF, UPF).

d) That side-channel analyses be conducted to detect hardware trojans using timing, power and spatial temperature analyses. Basically, this method detects malicious firmware or software installed on edge nodes by identifying unusual system behaviours, such as increases in execution time and power consumption.

e) That Trojan hardware detection methods which compare Trojan-afflicted hardware with non-Trojan-afflicted hardware be used to detect malicious attacks.

f) That the physical security of any edge nodes that are not placed in highly secure edge data centres be enforced, such as by employing additional physical protection techniques during manufacture or implementing locking mechanisms and other physical safeguards in the field.

g) That independently of the above, parts of the edge system dealing with cryptographic material is required to be protected against side-channel attacks using e.g., hardened, resistant SIM cards.

The security requirements of virtualized infrastructure should include:

a) That if the infrastructure of IMT-2020 edge computing service is deployed by virtual machine, the vCPU, memory, and I/O of the virtual machine need to be securely isolated.

b) That the virtualized infrastructure supports secure isolation among the containers.

c) That the virtualized infrastructure supports the mirroring of repositories and signature.

d) That segmentation with network slicing separates traffic and isolates compute resources [b-ENISA].

8.2 The network layer

The security requirements of network telecommunication should include:

a) That it supports confidentiality and integrity protection for data transmission.

b) That it uses a security protocol (e.g., TLS v1.2) to set up a secure channel among the network elements.

c) Use of encryption of data traffic between the parties by using a secure end-to-end transport protocol, use of a long random number or string as the session key, and regenerating the session id after each successful login.

d) That it supports DDoS protection capability by carefully filtering traffic so that non-legitimate requests are not allowed through, while legitimate ones pass through without significant delays.

The security requirements of network management should include:

a) That the operation supports systems (OSS) support authentication and authorization for interaction with the cloud management platform.

b) That the functions between edge computing service management and the OSS be securely isolated.

c) That it be continuously monitored whether the network is slow or faulty, and alarms of network attacks and issues be given in time.

d) That reliable routing protocols be established.

8.3 The application layer

The security requirements of the edge application should include:

a) That it implements security assessment which includes a security compliance check, assets management, virus scan, etc.

b) That the edge application support authentication and authorization for interactions among the cloud management platform and other edge applications.

c) That it protects sensitive data in order to resist unauthorized access and data tampering.

d) That it supports integration verification for the edge application.

e) That it verifies the administrator's identity and authority during edge application loading and instancing.

f) That it supports the confidentiality and integration protection for data migration, transmission, storage, sharing and destruction processes.

g) That it supports an automatic identification and security hardening function based on program language security extension and static program analysis.

h) That it supports real-time monitoring, analysis and alarm functions for application performance, traffic, source channel and the client environment.

i) That it supports application audit, regularly collect the security logs of edge devices and applications, store and analyse them, and then alarm and trace back violations, ultra vires and abnormal application behaviours.

9 Security capabilities guidelines for the edge computing service

9.1 The infrastructure layer

To achieve the security requirements for the infrastructure layer, the necessary security capabilities that should be provided are as follows:

a) Data security risk monitoring and early warning to prevent data tampering and leakage.

b) Data security storage, including the capabilities of encrypted storage and encapsulation of the sensitive data.

c) Security protection capabilities for the virtualization platform, through system security reinforcement, security isolation, security control, data encryption and other capabilities to ensure data security in the virtualization network.

d) Security functions to ensure the security of virtualization NFs, including:

- Authentication controls;
- Access controls;
- Remote verification for system security;
- Communications security;
- Attestation;
- Mirror;
- Signature;
- Security isolation;
- Hardware-mediated execution enclaves;
- Hardware-based root of trust;
- Hardware encryption;
- Trusted execution environment;
- Self-encrypting storage;
- Direct access to memory;
- Hardware security modules;
- Software integrity protection and verification.

9.2 The network layer

Security capabilities for the network layer that should be provided include, but are not limited to:

a) Capabilities for protecting the confidentiality and integrity of data transmission, such as time stamp, serial number, link encryption and other mechanisms.

b) Support for the capabilities to prevent session hijacking, such as encrypting the data traffic between the parties, using a long random number or string as the session key, and regenerating the session id after a successful login.

c) Data security control for the edge nodes, including identity authentication, security isolation, continuous monitoring and early warning, data encryption, data desensitization and backup.

d) Reliable routing protocols.

9.3 The application layer

Security capabilities for the application layer that should be provided include, but are not limited to:

a) Controlling the application permissions of different users and scenarios, in order to ensure the confidentiality, integrity and availability of application layer data and services.

b) Protecting against virus attacks and timely updating of the virus database to prevent data leakage or theft.

c) Identifying and evaluating sensitive data, including desensitization authorization, encrypted storage, monitoring and tracking, abnormal alarm, audit management, destruction and other capabilities.

d) Identity authentication, continuous monitoring and early warning.

Bibliography

[b-ITU-T E.800] Recommendation ITU-T E.800 (2008), *Definitions of terms related to quality of service*.

[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-R M.1645] Recommendation ITU-R M.1645 (2006), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000*.

[b-ITU-R M.2083] Recommendation ITU-R M.2083 (2015), *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*.

[b-3GPP TS 23.548] 3GPP 23.548 (2021), 5*G system enhancements for edge computing (version 17.2.0 release 17).*

[b-Daniel] B. Daniel, *Is edge computing secure? Here are 4 security risks to be aware of* 9 December 2020. https://www.trentonsystems.com/blog/is-edge-computing-secure.

[b-ENISA] ENISA (European Union Agency for Cybersecurity), *ENISA Threat Landscape For 5G Networks*, December 2020. Available to: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

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, 2023