International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1041

(05/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Network security

Security framework for voice-over-long-term-evolution (VoLTE) network operation

Recommendation ITU-T X.1041

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	X.1140–X.1149
Security protocols (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.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed legder technology security	X.1400–X.1429
Security protocols (2)	X.1450–X.1459
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
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

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

Recommendation ITU-T X.1041

Security framework for voice-over-long-term-evolution (VoLTE) network operation

Summary

Voice over LTE (VoLTE) is a voice communication service over IP multimedia subsystem (IMS) network, and its traffic is routed through long term evolution (LTE) wireless network, evolved packet core (EPC) core network and IMS core network. VoLTE adopts a full Internet protocol (IP) network framework based on session initiation protocol (SIP), which makes VoLTE more vulnerable to attacks than traditional voice service, which is based on circuit switch. Therefore, there is an urgent desire to establish the overall security framework for VoLTE network operation.

Recommendation ITU-T X.1041 analyses security threats encountered by the VoLTE network and recommends countermeasures for telecommunication operators to ensure the secure operation. It also provides a security reference framework for VoLTE network.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1041	2018-05-14	17	11.1002/1000/13603

Keywords

Countermeasures, security reference framework, threats, VoLTE.

[*] 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, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Recommendation ITU-T X.1041

Security framework for voice-over-long-term-evolution (VoLTE) network operation

1 Scope

This Recommendation analyses security threats encountered by VoLTE network and recommends countermeasures for telecommunication operators to ensure secure operation. It also provides a security reference framework for VoLTE network.

This Recommendation:

– Describes security threats to VoLTE network operation.

– Provides technical and management measures for countering security threats.

– Defines a security framework for VoLTE network operation.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 session border controller (SBC): A device deployed in VoLTE network to exert control over signalling and media streams involved in setting up, conducting, and tearing down telephone calls or other interactive media communications for the telecommunication operator. It provides functions such as security (e.g., Firewall, topology hiding), control-plane interworking between different protocols, network address translation, transcoding between different user-plane data types, load-balancing and routing, etc. [b-GSMA FCM.01].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AKA	Authentication and Key Agreement
AS	Application Server
CLR	Cancel Location Request
CSCF	Call Session Control Function

DB	Database
DDoS	Distributed Denial of Service
DoS	Denial of Service
ECGI	Evolved Universal Terrestrial Radio Access Network Cell Global Identifier
EPC	Evolved Packet Core
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
GUTI	Globally Unique Temporary UE Identity
HSS	Home Subscriber Server
I-CSCF	Interrogating Call Session Control Function
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet protocol
IPSec	IP Security Protocol
ISDN	Integrated Services Digital Network
LTE	Long Term Evolution
MME	Mobile Management Entity
MS	Mobile Station
MSISDN	Mobile Subscriber International ISDN Number
OM	Operation and Management
OS	Operating System
P-CSCF	Proxy-Call Session Control Function
PDN	Public Data Network
PGW	PDN Gateway
QoS	Quality of Service
RSZI	Regional Subscription Zone Identity
SBC	Session Border Controller
S-CSCF	Serving-Call Session Control Function
SGW	Serving Gateway
SIP	Session Initiation Protocol
SQL	Structured Query Language
TAI	Tracking Area Identity
TAS	Telephony Application Server
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
VoLTE	Voice over LTE
XSS	Cross-Site Scripting

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 Recommendation is to be claimed.

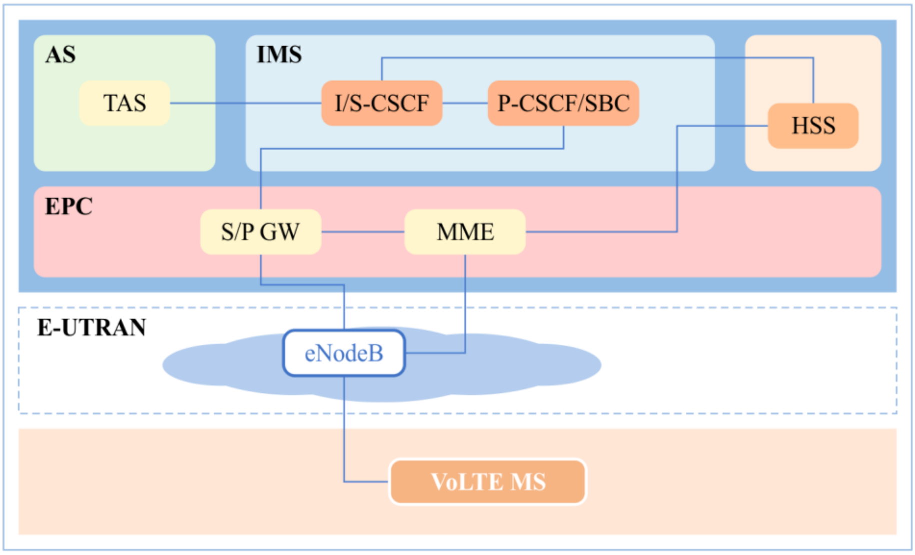
The keywords "is recommended" indicate a requirement which is recommended but not absolutely required, if conformance to this Recommendation is to be claimed.

6 Introduction

6.1 Background

VoLTE is a GSMA profile of the standards defined for the delivery of services (mainly voice) over the packet switched only network of long term evolution (LTE), leveraging the IP multimedia subsystem (IMS) core network [b-GSMA FCM.01]. VoLTE is deemed as a standardized system for providing voice service for 4G mobile users.

A VoLTE architecture is depicted in Figure 6-1. It is composed of a VoLTE mobile station (MS), evolved universal terrestrial radio access network (E-UTRAN), evolved packet core (EPC), IMS, home subscriber server (HSS) and various application servers (AS).



X.1041(18)_F6-1

Figure 6-1 – VoLTE architecture

VoLTE MS is the mobile terminal which is authorized to access the network and use VoLTE service. It may be a smartphone or tablet or another kind of communication device.

E-UTRAN consists of eNodeBs which are in charge of wireless transceiver and base station control. The eNodeBs connect to the mobile management entity (MME) for signalling transmission, while data transmission is directly routed to the serving gateway (S-GW) and public data network (PDN) gateway (P-GW).

EPC is the 4th generation of the 3GPP core network. The EPC basically contains MME and S/P-GW. MME is the most important control point in the core network and it is responsible for most of the control plane functions. S-GW is responsible for the quality of service (QoS). P-GW allocates IP addresses to user equipments (UEs), selects routes and provides interfaces towards Internet and IMS.

IMS is a standalone system that connects to the LTE network via P-GW. VoLTE service is provided through the call session control function (CSCF) that controls the phone calls in the IMS network.

The CSCF manages VoLTE registration information, connects calls and relays voice call transmission and reception. According to its dedicated function, the CSCF is classified into proxy CSCF (P-CSCF), interrogating CSCF (I-CSCF) and serving CSCF (S-CSCF). The main function of P-CSCF is to forward all SIP messages between the UE and the IMS. The I-CSCF finds the corresponding S-CSCF by querying HSS. The S-CSCF provides session management such as session set up, session deletion and session control.

The main AS is called telephony application server (TAS) and it is responsible for both signalling and media manipulation for many services such as local number portability, free-call routing resolution, unified messaging and conference bridge services.

The HSS contains all the information related to the subscribers and provides details of the subscribers to other network entities. The authentication center is part of HSS, which is responsible for generating authentication vectors for each subscriber.

6.2 Threats analysis

VoLTE network is subject to various security threats and vulnerabilities. This Recommendation categorizes these threats into four groups:

1) Threats to data: The threats to the sensitive data for VoLTE network operation.
2) Threats to applications: The threats to session initiation protocol (SIP) signalling, voice media and other application services.
3) Threats to networks, all the common threats to E-UTRAN, EPC and IMS network.
4) Threats to infrastructure: The threats to the software and hardware of the VoLTE network elements.

6.3 Countermeasures

This Recommendation describes security measures in five dimensions according to different types of threats in the VoLTE network.

1) Countermeasures for data security.
2) Countermeasures for application security.
3) Countermeasures for network security.
4) Countermeasures for infrastructure security.
5) Security management.

6.4 Security reference architecture

This Recommendation provides a security framework to address security challenges of the VoLTE network operation. The security framework is designed based on the analysis of threats and countermeasures.

7 Threats analysis

VoLTE suffers from various security threats, such as the leakage of data, eavesdropping, flood attack and so on. These threats can be categorized into four groups: threats to data, threats to application, threats to network and threats to infrastructure.

7.1 Threats to data

The network elements in VoLTE store important and sensitive data. It is essential to provide confidentiality, integrity and availability of these data.

Sensitive data mainly includes the following:

- Users' personal data: International mobile subscriber identity (IMSI), mobile station international subscriber directory number (MSISDN), international mobile equipment identity (IMEI), temporary mobile subscriber identity (TMSI), globally unique temporary user equipment identity (GUTI), etc.
- Location data: Regional subscription zone identity (RSZI), tracking area identity (TAI), evolved universal terrestrial radio access network cell global identifier (ECGI), latitude and longitude of eNodeBs, etc.
- Network authentication data: Root key, authentication parameters, encryption key, integrity key, etc.
- Users' service data: Access time, online time, call time, credit rating, arrears, billing, etc.

Sensitive data are subject to information disclosure in the process of data storage, as well as data transmission, data usage, and data destruction. The disorganized management of staff, computer rooms and equipment, can result in serious security risks. Moreover, some malicious attacks can also lead to sensitive data leakage. For example, an attacker may eavesdrop on data transmitted over the air interface and use a stolen key to decrypt user data or signalling. Attackers can also utilize the diameter protocol to launch inter-network location queries, and illegally obtain user location.

7.2 Threats to applications

The application layer of the VoLTE system refers to the services above IP layer, including the SIP signalling, the voice media, and the supplementary web services.

7.2.1 Threats to SIP signalling

VoLTE uses the SIP protocol to carry the signalling messages. Attackers can exploit the vulnerabilities of SIP to launch SIP malformed packet attack, and DoS attack.

SIP malformed packets do not conform to SIP protocol specifications such as [b-IETF RFC 3261] and [b-IETF RFC 3455]. It is easy to maliciously customize SIP malformed packets to detect the vulnerabilities of SIP protocol stack. The imperfections of an abnormal SIP signalling processing mechanism can lead to system exceptions, or even server crash.

The attackers may attempt to inject a large amount of SIP messages to abuse the crucial resources of the core network, such as bandwidth, session and processing capability, and to degrade the network performance or to make the network unable to provide services.

7.2.2 Threats to VoLTE voice media

Threats to VoLTE voice media include caller ID spoofing, session hijack, etc. Attackers may also construct non-compliant media packets to launch DoS attack on session border controller (SBC) or remote media servers.

7.2.3 Threats to web services

As indicated in Figure 6-1, there is a main AS called TAS responsible for many services in VoLTE. Besides voice services, TAS also contains a web server to provide supplementary services, such as call forwarding, which can be configured and managed by subscribers via the Internet. The web server may suffer from common web threats such as structured query language (SQL) injection or cross-site scripting (XSS).

7.3 Threats to network

In the VoLTE system, threats to the network come from two sources: attacks from the Internet, and attacks from other networks.

The VoLTE network connects with the Internet through the SGi interface, and this interface is the source of remote attacks on the core network from the Internet.

The interchanging of protocol between different networks, such as Diameter, may cause a substantial security risk if not protected properly. For example, attackers can forge a Diameter cancel location request (CLR) signalling message to intercept any user's VoLTE service, or send other kinds of Diameter messages to initiate attacks on MME, HSS or other VoLTE network elements.

7.4 Threats to infrastructure

Threats to infrastructure include but are not limited to:

– Operating system (OS)/database (DB) vulnerability exploitation: OS and DB vulnerabilities are usually due to improper programming or other functional self-defects introduced during the system design or development process. OS and DB vendors continuously publish patches for known vulnerabilities. If VoLTE equipment's do not apply these patches in a timely manner, attackers may exploit these vulnerabilities and cause damages.

– Improper security configuration: Improper security configuration can lead to the misuse of files and directories. If there is no mechanism to ensure that the passwords are strong enough, updated periodically and stored in encrypted storage, attackers can log onto the device illegally and control it maliciously by the means of brute force attacks. If P-GW is not properly configured, illegal direct IP connections may be established between the VoLTE MSs and cause DoS billing issues for VoLTE users.

– Unauthorized physical access: If unauthorized devices physically access the VoLTE network, attackers can use them to steal sensitive data, or even destroy the continuity of VoLTE network operation.

– Malicious software: Malicious software, such as zombies, trojans and worms, which are installed illegally, may cause severe consequences, such as, rendering the system unstable, turning the equipment into maliciously controlled devices, data theft, or interruption of VoLTE network services.

8 Countermeasures

To protect the security of VoLTE network, schemes combining technology and management measures are needed. This Recommendation describes the countermeasures in five dimensions: data security, application security, network security, infrastructure security and security management.

8.1 Countermeasures for data security

8.1.1 The security of data storage

When data are stored in the VoLTE network, certain measures should be taken to ensure the security of data storage such as the following:

– Data should be managed in accordance with data sensitivity and stored based on its security levels.

– The storage of sensitive data should be securely protected. Related measures include, but are not limited to, the following: establishing the authentication and access control mechanism, and conducting regular risk assessments.

– Data backup and recovery mechanism should be enforced. Data disaster emergency plans must be prepared in advance. Once data are lost or destroyed, they must be detected and recovered in a timely manner.

8.1.2 The security of data transmission

When data packets are transported across various networks or systems, certain measures should be taken to prevent data disclosure during transmission.

– Prior to transmitting sensitive data to other systems, it is required that the system be reliable.

– Transmitted data should be encrypted using secure encryption algorithms.

8.1.3 The security of data destruction

When a service system containing sensitive data is removed from service, or when sensitive data are expected to expire, reliable technical measures are required to ensure that sensitive data are destroyed and cannot be restored. Regarding data destruction, the following should be ensured:

– The data destruction process should be established, and action taken when users withdraw from the service, or data are beyond the retention period.

– The data destruction process should be recorded for follow-up security audits.

– Once sensitive data has been destroyed, reliable technical measures should be used to ensure that the data cannot be restored.

8.2 Countermeasures for application security

8.2.1 SIP signalling reinforcement

The main countermeasures for malformed SIP packets include protocol conformance checking and protocol robustness verification using the multi-level filtering mechanism. It is recommended that the following malformed SIP packets should be filtered:

– Overlength segment packets: When the length of the SIP packet exceeds a specified threshold.

– Multi-header-fields SIP packet: When the number of fields, such as via, contact or route, in a SIP packet exceeds the specified threshold.

– SIP packets with incorrect IP address: When the IP address in the via header is different from the source IP of the transport layer.

– Self-loop SIP packets: When the IP addresses of sender and receiver are identical.

8.2.2 SIP signalling flood prevention

Some restriction schemes, as listed below, should be applied according to the features of the SIP signalling to prevent DoS attacks.

– Limiting the rate of requests per single user in an SBC: Limit the number of register requests during a period by single user for the SBC to eliminate register signalling attacks.

– Limit total SIP signalling rates for all users in core network to prevent DoS attacks.

– SIP signalling should be analyzed by classification and statistics to determine whether the behavior is aggressive. If the user is identified as having an aggressive behavior, the packet rate should be limited or the packets should be dropped.

8.2.3 Voice media security

IMS-AKA should be deployed and enforced to authenticate the MS and IMS network to prevent caller ID spoofing attack and session hijack attack. The network should have the capability to filter illegal media packets.

The SBC should be examined for the legitimacy of received media packets. This can prevent attackers from initiating media packet attacks that can affect the normal operations of legitimate users.

8.2.4 Web service security

Measures should be taken to ensure the security of the websites, such as format legitimacy, checking of user input and regular security inspection on the website.

8.3 Countermeasures for network security

8.3.1 Security deployment

Security deployment is achieved by isolating the various security domains. Systems with the same security attributes and similar security levels should be deployed into the same security domain. Appropriate security policies should be configured to control inter-domain access between different security domains. It is necessary to divide VoLTE network into security domains, such as: wireless access security domain, core network security domain, operation and management (O&M) network security domain, billing security domain, etc.

8.3.2 Inter-networking security

It is necessary to ensure the security of the connection between the VoLTE network and a 2G/3G core network, as well as the connection between different VoLTE network operators. Hence the security protection measures of boundaries between different networks should be taken to ensure interconnection security. Networks must be segregated and boundary protection equipment such as SBC or firewalls should be deployed.

8.3.3 Multiple protection mechanism

Deploy dedicated security protective devices in a VoLTE network to realize network security-in-depth defences, such as firewalls, anti distributed denial of service (DDoS) systems and IPS equipment, ensure that abnormal traffic or malicious behaviour can be detected and blocked in a timely manner.

8.3.4 IP transmission encryption

It is required to deploy IP security protocol (IPSec) to ensure the confidentiality of IP transmission. An IPSec tunnel should be established between the MS and P-CSCF to protect confidentiality of SIP signalling [b-3GPP TS 24.229].

8.4 Countermeasures for infrastructure security

8.4.1 Security baseline for net equipment configuration

It is necessary to set up a standardized security baseline for the configuration of a VoLTE infrastructure.

The security baseline includes the authentication and authorization requirement, security logging and audit.

The VoLTE infrastructure should be configured according to the security baseline.

The network elements that need to be securely configured include: OS, DB, router, firewall, server, LTE/EPC, IMS, etc.

Some common baseline requirements for the network elements are:

– Unnecessary and unsafe network ports or services should be closed.

– Access to the file systems should be granted with least-privilege.

– Strong password should be enforced for each account, and unnecessary accounts should be deleted.

In particular, P-GW should be configured to prohibit the direct IP communication between different MSs. It is recommended that P-GW should be configured to only allow communication between MS and the CSCF for SIP signalling and communication between the MS and the internal DNS server.

8.4.2 Physical access security

The hosting environment of the communication infrastructure should be regulated to prevent unauthorized access.

8.4.3 Software integrity protection

Software integrity protection should be designed to prevent system and application software from being illegally tampered with. Software component integrity should be verified by using an integrity protection algorithm.

8.5 Security management

The security management for VoLTE network addresses the risks before, during and after the event.

8.5.1 Security evaluation

It is required to establish an internal security evaluation process and recommended to pass the third-party authorities' security certification, such as EAL3 of CC [b-ISO/IEC CC].

8.5.2 Security operation and maintenance

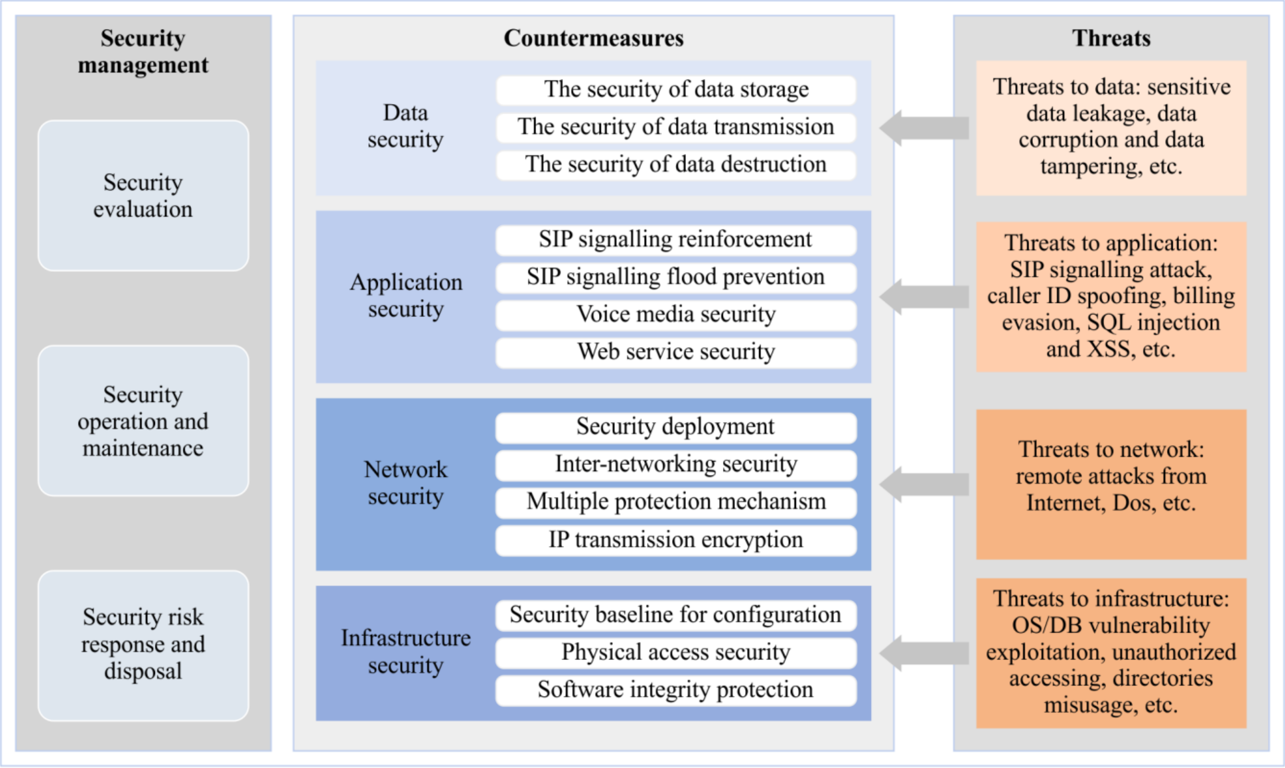
Some measures should be taken to ensure the security of daily operation and maintenance, such as periodical network/service vulnerability scanning, regular software robustness testing, centralized log management, etc.

8.5.3 Security risk response and disposal

It is required to take worldwide security events into account. Threat intelligence and globally exposed vulnerabilities should be collected in a timely manner and risk analysis should be updated accordingly. A security operation workflow to guide the risk analysis and system reinforcement should be set up with high efficiency. Once the threat intelligence that may affect the operation of VoLTE network is disclosed, the workflow should be activated in time to make sure that the threats and risks are properly disposed.

9 Security reference architecture for VoLTE network

Based on the above analysis of threats and countermeasures, the recommended security reference framework for VoLTE network is shown in Figure 9-1:


Security management
Security evaluation
Security operation and maintenance
Security risk response and disposal
Countermeasures
Data security
The security of data storage
The security of data transmission
The security of data destruction
Application security
SIP signalling reinforcement
SIP signalling flood prevention
Voice media security
Web service security
Network security
Security deployment
Inter-networking security
Multiple protection mechanism
IP transmission encryption
Infrastructure security
Security baseline for configuration
Physical access security
Software integrity protection
Threats
Threats to data: sensitive data leakage, data corruption and data tampering, etc.
Threats to application: SIP signalling attack, caller ID spoofing, billing evasion, SQL injection and XSS, etc.
Threats to network: remote attacks from Internet, Dos, etc.
Threats to infrastructure: OS/DB vulnerability exploitation, unauthorized accessing, directories misusage, etc.

X.1041(18)_F9-1

Figure 9-1 – Security reference framework for VoLTE network operation

The framework is designed to address the security challenges of VoLTE network operation. It classifies the security threats into four groups (Data, Application, Network, and Infrastruture), provides technical countermeasures for each group, and contains management countermeasures for all the four groups.

This Recommendation lists the most common and representative security threats and corresponding countermeasures for VoLTE network operation, and organize them into the above security reference framework. It should be understood that due to the complexity of the VoLTE network deployment, all the security threats and countermeasures cannot be exhausted in a single document. At the same time, the threats in VoLTE network evolve continually and countermeasures need to be reinforced constantly.

The security reference framework in this Recommendation is designed to help operators and vendors better understand threats and to efficiently counter the attacks encountered or those that are imminent in the years to come. It is recommended that VoLTE network operators and vendors use this security reference framework to identify and organize any future threats and/or countermeasures, and improve their capabilities to cope with the security challenges of VoLTE network operation.

Bibliography

[b-IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[b-IETF RFC 3455] IETF RFC 3455 (2003), *Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP).*

[b-3GPP TS 23.228] 3GPP TS 23.228:2014, *IP Multimedia Subsystem (IMS).*

[b-3GPP TS 24.229] 3GPP TS 24.229:2017, *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).*

[b-ISO/IEC CC] ISO/IEC 15408-1:2009, *Information technology – Security techniques – Evaluation criteria for IT Security – Part 1: Introduction and general model.*

[b-GSMA FCM.01] GSMA FCM.01:2014, *VoLTE Service Description and Implementation Guidelines Version 2.0.*

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, 2018