International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1364

(03/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Internet of things (IoT) security

---

Security requirements and framework for narrowband Internet of things

Recommendation ITU-T X.1364

ITU-T

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 ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
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
QUANTUM COMMUNICATION	X.1700–X.1729

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

Recommendation ITU-T X.1364

Security requirements and framework for narrowband Internet of things

Summary

Recommendation ITU-T X.1364 analyses potential deployment schemes and typical application scenarios for narrowband Internet of things (NB-IoT). It specifies security threats and requirements specific to the NB-IoT deployments and establishes a security framework for the operator to safeguard new NB-IoT technology applications.

Current developments in telecommunication technology in the mobile communication domain, are leading to changes in communication patterns from person-to-person to person-to-thing and thing-to-thing, making inevitable the evolution to the Internet of things.

Compared to short distance communication technologies such as Bluetooth, ZigBee and others, cellular mobile networks characterized by wide coverage, mobility and extensive connections that bring richer application scenarios will become the main interconnection technology of IoT.

NB-IoT is based on cellular mobile network technology, using a bandwidth of approximately only 180 KHz. It may be deployed on global system for mobile communication (GSM) networks, universal mobile telecommunications system (UMTS) networks or long-term evolution (LTE) networks directly to reduce costs and achieve a smooth upgrade.

Based on its low power dissipation, wide coverage, low cost and high capacity, NB-IoT is expected to be massively adopted by operators with wide application in multiple vertical industries.

As a new technology, NB-IoT has its own characteristics that may bring new security issues. In order to ensure security of NB-IoT deployments and applications, security threats and relevant security requirements specific to NB-IoT need to be analysed and an overall security framework for NB-IoT needs to be established.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1364	2020-03-26	17	11.1002/1000/14088

Keywords

Framework, Internet of things, narrowband, security requirements.

* 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/.

© ITU 2020

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

Recommendation ITU-T X.1364

Security requirements and framework for narrowband Internet of things

1 Scope

This Recommendation analyses potential deployment schemes and typical application scenarios for narrowband Internet of things (NB-IoT). It specifies security threats and requirements specific to NB-IoT deployments and establishes a security framework for operators to safeguard applications of this new NB-IoT technology.

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.

[ETSI TS 123 401] ETSI TS 123 401 V15.8.0 (2019-10), LTE; *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401 version 15.8.0 Release 15)*.

[ETSI TS 123 501] ETSI TS 123 501 V15.6.0 (2019-10), 5G; *System architecture for the 5G System (5GS) (3GPP TS 23.501 version 15.6.0 Release 15)*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-ITU-T X.1141]: The process of determining whether someone or something is, in fact, who or what it is declared to be within a degree of confidence.

3.1.2 capability [b-ITU-T X.1145]: An ability that a system or an equipment provides for offering a service.

3.1.3 cellular IoT [ETSI TS 123 401]: Cellular network supporting low complexity and low throughput devices for a network of Things. Cellular IoT supports both IP and Non-IP traffic.

3.1.4 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.5 encryption [b-ITU-T X.800]: The cryptographic transformation of data (see cryptography) to produce cipher text.

NOTE – Encipherment may be irreversible, in which case the corresponding decipherment process cannot feasibly be performed.

3.1.6 entity [b-ITU-T X.1252]: Something that has separate and distinct existence and that can be identified in context.

NOTE – An entity can be a physical person, an animal, a juridical person, an organization, an active or passive thing, a device, software application, service etc. or a group of these entities. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc.

3.1.7 evolved packet core [b-ITU-T Q.1743]: A framework for an evolution or migration of the 3GPP system to a higher-data-rate, lower-latency, packet-optimized system that supports, multiple RATs.

3.1.8 evolved packet system [b-ITU-T Q.1743]: An evolution of the 3G UMTS characterized by higher-data-rate, lower-latency, packet-optimized system that supports multiple RATs. The evolved packet system comprises the evolved packet core together with the evolved radio access network (E-UTRA and E-UTRAN).

3.1.9 key management [b-ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

3.1.10 narrowband-IoT [ETSI TS 123 401]: A 3GPP Radio Access Technology that forms part of Cellular IoT. It allows access to network services via E-UTRA with a channel bandwidth limited to 180 kHz (corresponding to one PRB). Unless otherwise indicated in a clause, Narrowband-IoT is a subset of E-UTRAN.

3.1.11 threat [b-ITU-T X.800]: A potential violation of security.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 CIoT serving gateway node (C-SGN): The cellular Internet of things (CIoT) serving gateway node (C-SGN) is a combined node evolved packet core (EPC) implementation option that minimizes the number of physical entities by collocating evolved packet system (EPS) entities in the control and user planes paths (e.g., mobility management entity (MME), serving gateway (S-GW) and packet data network gateway (P-GW), which may be preferred in CIoT deployments.

NOTE – The functions listed in this definition refer to [ETSI TS 123 401].

3.2.2 evolved node b (eNodeB): A wireless access node that hosts functions for radio resource management, uplink data decompression and encryption of user data stream, routing of user plane data etc.

NOTE – The functions listed in this definition refer to [ETSI TS 123 401].

3.2.3 evolved universal terrestrial radio access network (E-UTRAN): A radio access network, its functions include header compression and user plane ciphering, MME selection, uplink and downlink bearer level rate enforcement, bearer level admission control, congestion control etc.

NOTE – The functions listed in this definition refer to [ETSI TS 123 401].

3.2.4 home subscriber server (HSS): A mobile core network element with the functions of user's subscription information storage and management.

NOTE – The functions listed in this definition refer to [ETSI TS 123 401].

3.2.5 mobility management entity (MME): A mobile core network element with the functions of tracking area list management, user equipment (UE) location mapping, serving gateway (S-WG) and packet data network gateway (P-WG) selection, handover selection, authentication, authorization, bearer management etc.

NOTE – The functions listed in this definition refer to [ETSI TS 123 401].

3.2.6 packet data network gateway (P-WG): A mobile core network element with the functions of per-user based packet filtering, user equipment (UE) Internet Protocol (IP) address allocation, transport level packet marking, service level charging etc.

NOTE – The functions listed in this definition refer to [ETSI TS 123 401].

3.2.7 service capability exposure function (SCEF): A mobile core network element with the functions of authentication and authorization, exposed service capabilities discover, policy management, network parameter configuration etc.

NOTE – The functions listed in this definition refer to [ETSI TS 123 401].

3.2.8 serving gateway (S-WG): A mobile core network element with the functions of the local mobility anchor point for inter-eNodeB handover, mobility anchoring for inter-3GPP mobility, packet routing and forwarding, transport level packet marking, accounting for inter-operator charging etc.

NOTE – The functions listed in this definition refer to [ETSI TS 123 401].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3G	3rd Generation
3GPP	3rd Generation Partnership Project
CDMA	Code Division Multiple Access
CIoT	Cellular Internet of Things
C-SGN	CIoT Serving Gateway Node
DDoS	Distributed Denial of Service
EPC	Evolved Packet Core
eNodeB	Evolved Node B
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Access Network
GSM	Global System for Mobile Communication
HSS	Home Subscriber Server
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
LTE	Long Term Evolution
MME	Mobility Management Entity
NB-IoT	Narrowband Internet of Things
P-GW	Packet Data Network Gateway
RAT	Radio Access Technology
SCEF	Service Capability Exposure Function
S-GW	Serving Gateway
SMS	Short Message Service
SIM	Subscriber Identification Module
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UTRA	Universal Terrestrial Radio Access

5 Conventions

None.

6 Overview of NB-IoT

Current developments in telecommunication technology in mobile communication domain are leading to changes in communication patterns from person-to-person to person-to-thing and thing-to-thing, making inevitable the evolution to the Internet of things (IoT).

Compared to short distance communication technologies such as Bluetooth, Zigbee and others, cellular mobile networks characterized by wide coverage, mobility and extensive connections that bring richer application scenarios will become the main interconnection technology of IoT.

NB-IoT is based on cellular mobile network that uses a bandwidth of approximately only 180 KHz. It could be deployed on global system for mobile communication (GSM) networks, universal mobile telecommunications system (UMTS) networks or long-term evolution (LTE) networks directly to reduce costs and achieve a smooth upgrade.

Typical characteristics of NB-IoT include:

– low power dissipation: NB-IoT devices could be used for five to ten years;

– wide coverage: in the same band, the NB-IoT has 15 to 20 dB gain compared to the current network, and a coverage area up to 100 times greater;

– high capacity: a single NB-IoT sector could support about 100,000 devices;

– low cost: the price of one NB-IoT device is about 5 US dollars.

Based on its low power dissipation, widely coverage, low cost and high capacity, it is expected that NB-IoT will be massively adopted by operators with wide applications in the multiple vertical industries.

7 Deployment scheme and typical application scenarios

7.1 Deployment scheme

7.1.1 Deployment using existing mobile core network

In this deployment scenario, operators deploy NB-IoT using existing deployed 2/3/4G mobile core networks.

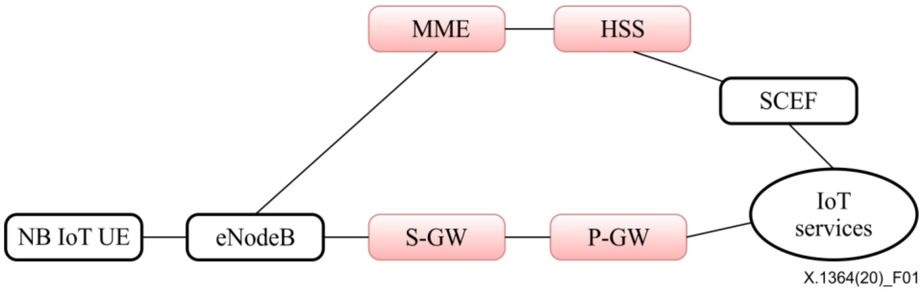
Elements of existing mobile core network including mobility management entity (MME), serving gateway (S-GW) and packet data network gateway (P-GW) need to be optimized for NB-IoT to support the following characteristics [ETSI TS 123 401]:

– ultra low user equipment (UE) power consumption;

– large number of devices per cell;

– narrowband spectrum radio access technologies (RATs), for instance evolved universal terrestrial radio access network (E-UTRA), universal terrestrial radio access (UTRA), GSM, CDMA2000; and

– Enhanced coverage level.



NOTE – Existing mobile core network elements are in pink colour.

Figure 1 – Deploy by using existing mobile core network

In addition to these optimized network elements, other network elements in Figure 1, as identified in [ETSI TS 123 401], are as follows:

– evolved node b (eNodeB): this wireless access node hosts functions for radio resource management, uplink data decompression and encryption of user data stream, routing of user plane data, etc.;

– home subscriber server (HSS): stores user's subscription information, e.g., authentication parameter, location information, etc.;

– service capability exposure function (SCEF): securely expose services and capabilities which are provided by 3GPP network interfaces.

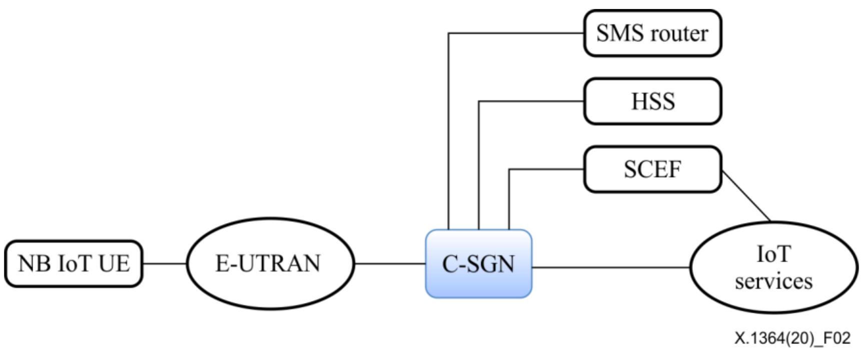
These network elements, along with their functions, support the NB-IoT services through mobile telecommunication network.

7.1.2 Deployment using a newly built dedicated mobile core network

In this deployment scenario, operators create a dedicated mobile core network newly built for NB-IoT services.

The cellular Internet of things (CIoT) serving gateway node (C-SGN) is defined by [ETSI TS 123 401].

A C-SGN supports sub-set and necessary functionalities of the existing evolved packet system (EPS) core network elements. It is a combined node of evolved packet cores (EPCs). It implements the option of minimized number of physical EPS entities; It collocates EPS entities functions both in the control plane and user plane paths. A C-SGN combines MME, P-GW and S-GW functions to provide a highly optimized CIoT solution. A C-SGN implementation supports options of its external interfaces. These interfaces correspond to the interfaces of respective EPC entities such as MME, S-GW and P-GW.



NOTE – Newly built mobile core network elements are in blue colour.

Figure 2 – Deployment using a newly built dedicated mobile core network

In addition to these newly built network elements, other network elements in Figure 2 are as follows [ETSI TS 123 401]:

– E-UTRAN: hosts functions such as header compression and user plane ciphering, MME selection, bearer level rate enforcement, congestion control, and transport level packet marking in the uplink, etc.;

– HSS: stores and manages user's subscription information, e.g., authentication parameter, location information, etc.;

– SCEF: provides securely expose services and capabilities which provided by 3GPP network interfaces;

– short message service (SMS) router: supports to transfer attach request without combined EPS attach (request for EPS services and non-EPS services). This feature is only available to UEs that only support NB-IoT.

These network elements, along with their functions, support the NB-IoT services through mobile telecommunication network.

7.2 Typical applications

7.2.1 Remote meter reading

In this application scenario, an NB-IoT device is used to receive meter readings indicating utility consumption, e.g., water, gas, etc., and to send these results through the wireless network to utility service providers.

Using NB-IoT technology makes meter reading more convenient, more accurate and more efficient compared to the traditional manual meter reading techniques.

7.2.2 Smart parking

In this application scenario, a parking lots deploy NB-IoT devices as sensors to detect whether a parking lot has spaces available or not. This allows drivers using a smart parking application to obtain a recommended parking choice, as well as to utilize online payment for parking fees.

Using NB-IoT technology may help solve the difficulties in finding open parking lots and spaces, as well as related payment issues.

7.2.3 Smart agriculture

In this application scenario, NB-IoT devices are used as sensors to record agriculture parameters such as salinity, moisture, temperature etc. Based on these records, a farmer can obtain recommendations on watering or fertilization solutions.

Using NB-IoT technology facilitates smarter agriculture through its use of real time information analysis instead of farmer experiments in traditional agriculture practices.

8 Threats for NB-IoT

The security threat analysis of NB-IoT has two vantage points: the characteristics of NB-IoT and the functional framework view of NB-IoT layers, as described in clauses 8.1 and 8.2.

8.1 Characteristics of NB-IoT

Typical characteristics of NB-IoT include low power dissipation, high capacity, low cost and wide coverage.

8.1.1 Low power dissipation

1) Characteristics description

The features of NB-IoT devices include, low power consumption, durability and therefore less frequent need for recharging, low calculation capability, etc. The embedded systems are also lightweight and simpler.

Generally, systems that operate on traditional IoT terminal equipment have features such as strong calculation capabilities. They utilize complex network transmission protocols and strict security reinforcement solutions. Due to high power consumption, they need to be frequently recharged.

2) Threats to NB-IoT

Denial of service threats could be realized by simply consuming the resources of an NB-IoT device. Costs against software and hardware are relatively low for such attacks.

Considering the NB-IoT device features of lightweight, low power consumption and low calculation capability, data encryption during transmission for security cannot be ensured. Sometimes data may be transmitted in plain text. Therefore, there might be high security threats in authentication and data validation. For example, attackers may use unauthorized devices to communicate with base station to send forged data.

8.1.2 High capacity

1) Characteristics description

The capacity of NB-IoT is much larger than traditional IoT. For example, one NB-IoT sector could support about 100 000 devices.

2) Threats to NB-IoT

With large numbers of devices, even a slight vulnerability could cause critical influences to network security. For example, a trojan virus may infect other terminal equipments and cause network unavailability.

Considering a deployment scenario with NB-IoT devices which may use the existing mobile core network, the terminal equipment might be capable of infecting mobile core network elements such as the mobility management entity, the home subscriber server and other devices in order to influence mobile communication users. In such a case, users' access to the network may be refused, or subscribers' information may be modified to avoid telephone call, short message or data traffic fees for example.

8.1.3 Low cost

1) Characteristics description

The cost of NB-IoT devices is usually very low.

2) Threats to NB-IoT

Low device costs are enabled by using, among other things, simplified protocols. Therefore attackers could make use of vulnerabilities of these simplified protocols to implement attacks to the devices and the network.

8.1.4 Wide coverage

1) Characteristics description

The coverage of NB-IoT is much wider in reach than traditional IoT. For example, in the same band as compared to current networks, NB-IoT has 15-20 dB gain, providing an extensive coverage area of up to 100 times.

2) Threats to NB-IoT

Devices deployed at a remote location may be easily captured and exploited by attackers.

8.2 NB-IoT layer

8.2.1 Device layer

Attackers may implement attacks by duplicating subscriber identification module (SIM) cards for illegal purposes such as free network access.

Security vulnerabilities may exist in protocol stacks of newly developed lightweight terminal modules.

Existing IoT terminal equipment manufacturers may use hardware that supports Wi-Fi, Bluetooth, ZigBee and other protocols when they release new equipment that support NB-IoT. Because they may simply be adding support for NB-IoT to this equipment, it is possible that security vulnerabilities and threats may result during the progress of development. Examples could include aras such as ports for debug may not be protected properly, weak encryption algorithms may be used, failure to apply hardware update and lack of timely integrity check when needed.

8.2.2 Network layer

Network data communication hijacking tools could monitor sessions between terminal equipment and base stations to capture data packets exchanged between these components. Consequently, the communication is hijacked resulting in attackers being able to analyse security vulnerabilities through data extracted from the hijacked communication messages.

With large numbers of devices and shared mobile telecommunication networks with mobile telecommunication subscribers, the tampered-with NB-IoT devices may result in a signalling storm.

There may be risk of data disclosure due to multiple data collections by NB-IoT services, transferred on-network and processed by many network elements.

The signalling of NB-IoT core network may be forged, tampered or replay attacked due to lack of an authentication mechanism among network elements.

Multiple attacks from the Internet may harm the interface between mobile core network and the Internet. For example, in a 5G system, the interface between the mobile core network and the Internet is known as the N6 interface [ETSI TS 123 501]; this N6 interface connects the user plane function and the Internet.

8.2.3 Application layer

NB-IoT is suitable for business scenarios with static business, low sensitivity to latency, discontinuous movement and real-time data transmission.

Omissions or false alarms may occur in automatic abnormality reporting businesses (such as in a smoke alarm detector) and periodic reporting business (such as in an environmental status monitoring system). For example, if an attacker captures the smart electric meter reading a of a user, the numbers may be modified or forged, thus compromising benefits of the user.

Besides, malicious instruction could also be a risk of remote instruction business (such as smart home equipment that could be remotely turn on or off by the users).

Businesses of NB-IoT are deeply integrated with various industries and as such, are exposed to vulnerabilities such as those inherent to complicated business logics and multiple application protocols.

Services of NB-IoT may be abused, for example, by set-card separation when inserting a subscribed NB-IoT card into other device rather than NB-IoT device, or when sending spam short message by the subscribed NB-IoT card, etc.

9 Security requirements

9.1 Security requirements of terminal device

9.1.1 Physical security

Physical protection of interfaces and chips is offered by the NB-IoT terminal device, which ensures that an attacker cannot access data even if the hardware is captured.

For different interfaces, the NB-IoT terminal device supports authentication and authorization functions.

9.1.2 Update security

The system, software, hardware etc. of the NB-IoT device are required to have the capability of updating to ensure system and application security.

Protection of confidentiality and integrity for updating files is required to avoid tampering.

9.1.3 Privacy protection

Flexible privacy protection mechanisms in the NB-IoT terminal device are needed to support privacy protection based on NB-IoT service requirements.

9.2 Security requirements of networks

9.2.1 Authentication

Authentication is required to confirm identities of the NB-IoT entity using an NB-IoT service. Authentication ensures validity of claimed identities of the entity and provides assurance that the entity is not attempting to masquerade as an authorized entity.

Lightweight authentication is needed taking into consideration the characteristics of NB-IoT.

9.2.2 DDoS attack prevention

This is required to pre-deploy security mechanisms to prevent and deal with a distributed denial of service (DDoS) attack in a timely manner.

9.2.3 Network entity security

Core network entities of NB-IoT are required to support security capabilities in order to resist forgery, tampering and reply attacks.

9.3 Security requirements of applications

9.3.1 Service usage/operation compliance monitoring

Service usage/operation compliance monitoring is required to monitor peak values, total number of flows to discover abnormal service usage/operation according to requirements of NB-IoT services.

9.3.2 Service abuse prevention

Service abuse prevention through set-card separation is required by monitoring characteristics of an international mobile equipment identity (IMEI) change.

9.3.3 Identification, analyses and disposal capabilities of security threats

It is required to identify, analyse and dispose of security threats based on big data analysis of behaviour of the NB-IoT terminal device.

10 Security capabilities for NB-IoT

10.1 Security capabilities of terminal device

NB-IoT terminal device should include the following security capabilities:

– SC_terminal device 1: key management capability;
– SC_terminal device 2: cryptographic algorithm negotiation capability;
– SC_terminal device 3: data encryption capability;
– SC_terminal device 4: data integrity capability;
– SC_terminal device 5: capability of secure update, including system, software, hardware etc;
– SC_terminal device 6: capability to implement secure protocols based on lightweight cryptography.

10.2 Security capabilities of network

NB-IoT network should include the following security capabilities:

– SC_network 1: key management capability;
– SC_network 2: cryptographic algorithm negotiation capability;
– SC_network 3: data encryption capability;
– SC_network 4: data integrity capability;
– SC_network 5: access control capability to ensure that only authorized entity is allowed access to NB-IoT network elements, stored information, information flows, services and applications;
– SC_network 6: tamper detection and/or tamper prevention capability;
– SC_network 7: capability against DDoS attack;
– SC_network 8: capability to perform secure configurations;
– SC_network 9: capability of set-card separation detection.

10.3 Security capabilities of applications

Applications should include the following security capabilities:

– SC_applications 1: capability to protect against malware infection through the use of malware protection software;
– SC_applications 2: capability for service usage/operation compliance through network key indicator (e.g., peak value, total number of the flows) monitoring;
– SC_applications 3: capability for application level security to prevent security threats based on the big data analysis of the behaviour of NB-IoT terminal device.

10.4 Relationship between security capabilities and security requirements

The security capabilities listed and described in clause 10 are used to satisfy some of the security requirements specified in clause 9. The mapping of security capabilities to security requirements is shown in Table 1.

In Table 1, the symbol "√" in a cell indicates that the security requirement is related to a particular security capability. More precisely, the marked security requirement should be supported by implementation of the marked capability.

Table 1 – Illustration of relationship between security requirements and security capabilities

Requirements / Capabilities	Physical security	Update security	Privacy protection	Authentication	DDoS attack prevention	Service usage/operation compliance monitoring	Service abuse prevention	Identify analysis and disposal capabilities of security threats
SC_terminal device 1	√			√				
SC_terminal device 2	√							
SC_terminal device 3			√					
SC_terminal device 4		√						
SC_terminal device 5	√	√						
SC_terminal device 6			√	√				
SC_network 1				√				
SC_network 2		√	√					
SC_network 3		√	√					
SC_network 4		√						
SC_network 5			√	√				
SC_network 6						√		
SC_network 7					√			
SC_network 8		√						
SC_network 9							√	
SC_applications 1		√						
SC_applications 2					√	√	√	
SC_applications 3			√					√

Bibliography

[b-ITU-T Q.1743] Recommendation ITU-T Q.1743 (2016), *IMT-Advanced references to Release 11 of LTE-Advanced evolved packet core network*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for open systems interconnection for CCITT applications*.

[b-ITU-T X.1141] Recommendation ITU-T X.1141 (2006), *Security Assertion Markup Language (SAML 2.0)*.

[b-ITU-T X.1145] Recommendation ITU-T X.1145 (2017), *Security framework and requirements for open capabilities of telecommunication services*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

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, 2020