International Telecommunication Union

ITU-T X.1369

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(01/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

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

Security requirements for IoT service platform

Recommendation ITU-T X.1369

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.1369

Security requirements for IoT service platform

Summary

Recommendation ITU-T X.1369 specifies security requirements for the IoT service platform. It assesses security threats and challenges to the IoT business service platform and describes security measures that could mitigate security threats and challenges.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1369	2022-01-07	17	11.1002/1000/14799

Keywords

IoT, service platform, security requirements, security risks.

* 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.1369

Security requirements for IoT service platform

1 Scope

This Recommendation specifies the security requirements for the IoT service platform. It assesses security threats and challenges to the IoT service platform and describes security measures that could mitigate security threats and challenges.

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.

[ISO/IEC 30141] ISO/IEC 30141 (2018), *Internet of things reference architecture*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 Internet of things (IoT) [b-ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 IoT service platform: A system platform to which IoT devices are connected and where IoT applications are executed.

From a functional perspective, the IoT service platform provides capabilities of device management, connection management, application enablement and business analysis, and so on. From a data management perspective, the IoT service platform collects, stores and processes data (including users' personal data and confidential information) for IoT applications and for advanced analysis.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CSRF	Cross-Site Request Forgery
DDoS	Distributed Denial of Service
DoS	Denial of Service
IMEI	International Mobile Equipment Identity
PVLAN	Private VLAN

SIM	Subscriber Identity Module
SQL	Structured Query Language
SSRF	Server Side Request Forgery
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMM	Virtual Machine Monitor
XSS	Cross-Site Script

5 Conventions

In this Recommendation the keyword "should" indicates a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

6 Overview

[ISO/IEC 30141] defines an entity-based IoT reference model, as shown in Figure 1. The IoT service platform is a key component of the *Application and Service sub-system* shown in this figure, which provides capabilities such as device management, connection management, application enablement and service analysis. The IoT service platform also implements data collection, storage and analysis for IoT applications.

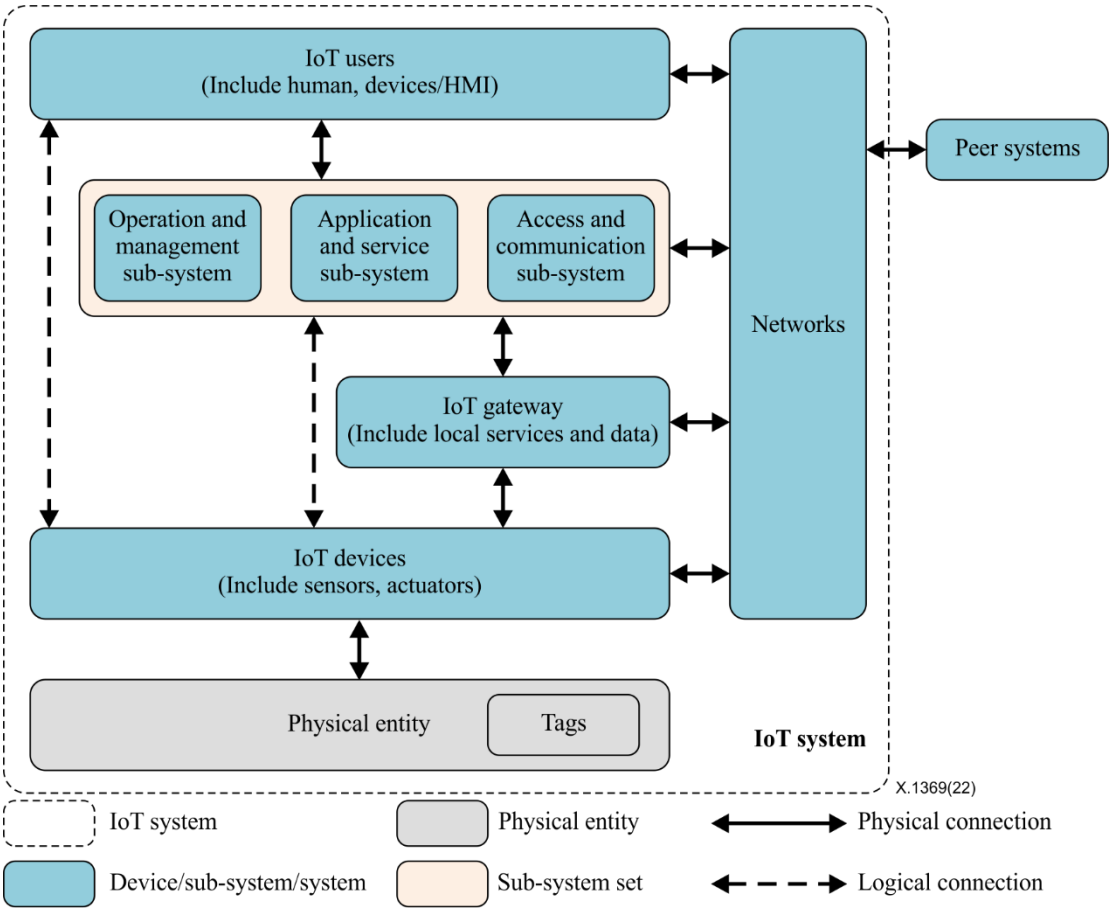

Figure 1 – Entity-based IoT Reference Model [ISO/IEC 30141]

Generally, the IoT service platform can be divided into four parts, which are the device management system, connectivity management system, application enablement system and business analytics system.

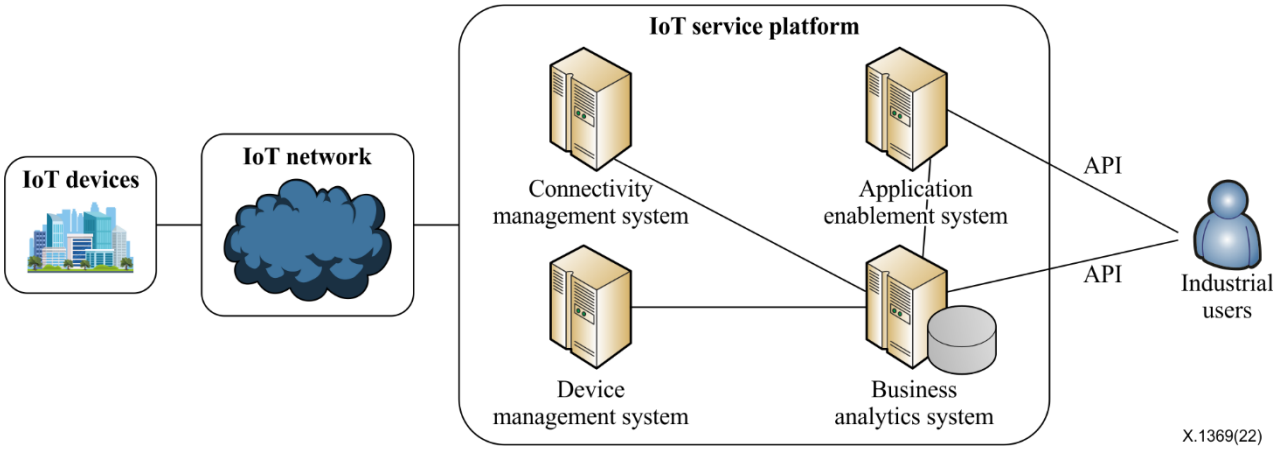

Figure 2 – Overview of the IoT service platform

- Device management system

This is the management system of IoT devices. It provides remote monitoring, re-configuration, software upgrade, system upgrade, troubleshooting, life cycle management and other functions.

- Connectivity management system

This is the centralized management system of the subscriber identity module (SIM) card. It focuses on cellular network applications and enables user self-service, such as querying data usage and connection status, recharging a SIM card and traffic management.

- Application enablement system

This is a platform-as-a-service platform that provides different function application programming interfaces (APIs) to support the implementation of different service systems. With the system, telecommunication operators open their primary telecom capabilities (data, SMS, telephone, authentication, billing, etc.) to different service systems, such as intelligent transportation, smart city, smart home, etc.

- Business analytics system

This collects various data from the device management system, connectivity management system and application enablement system to analyse and generate visual analysis results for the operators and consumers.

The security of IoT service platform plays an important role in the whole IoT environment. Any weakness of or attack on the platform would affect the security of the related devices, networks and data. The IoT service platform is vulnerable to threats including denial of service (Dos), privilege elevation, unauthorized access, brute force and arbitrary code execution, which may lead to malicious invasion, sensitive information leakage, malicious instruction to devices and other serious consequences.

In this Recommendation, the security risks of the IoT service platform are analysed. A security framework methodology and security measures are proposed.

The security of the IoT service platform covers infrastructure security, system security, data security, and application security from the bottom level to the upper level. API security and operational security involves the four levels. In clauses 7 to 9, security risks, security framework and security requirements are detailed, respectively, based on those six aspects.

7 Security threats to the IoT service platform

7.1 Application security threats

Application security threats include web attacks, unauthorized access, elevation of privileges and service vulnerabilities.

7.1.1 Web attacks

The IoT service platform uses traditional web technologies as well as communication technology, big data, cloud computing and so on. As a result, it inherits the main security risks for all of these technologies, such as distributed denial of service (DDoS) attacks, brute force attacks, structured query language (SQL) injections, cross-site script (XSS) vulnerabilities, cross-site request forgery (CSRF) vulnerabilities, server side request forgery (SSRF) vulnerabilities, etc.

7.1.2 Unauthorized access and elevation of privileges

A large number of IoT applications are deployed on the centralized platform. This makes it difficult for efficient security isolation and access control among different applications, which may lead to unauthorized access, operation and elevation of privileges. Besides, it is prone to unauthorized access and elevation of privileges among different users and devices.

7.1.3 Service vulnerabilities

IoT applications have complex service logic and a large number of application protocols, which may introduce flaws during the design and realization processes, leading to service vulnerabilities and abuse. In some application scenarios of IoT, terminals can be controlled through the platform. A compromised platform will result in the compromise of a large number of terminals, and further impact industrial manufacture and the social life of users.

7.1.4 Capability exposure

As an application enablement platform, the IoT platform can provide different function APIs to support the implementation of different service systems. It brings convenience to different services, but the opening of capability may also bring risks to the platform. The capability may be accessed by unauthorized developers or abused by different services. What is more, the opening of primary telecom capabilities (data, SMS, telephone, authentication, billing, etc.) may invite attacks on the telecom core network if it is not properly protected.

7.2 Data security risks

The confidentiality, integrity and availability of data form the baseline of data security. However, during the process of data collection, transmission, migration, storing, processing and destruction, there are many risks.

7.2.1 Data leakage

IoT application data are usually collected by IoT terminals and transmitted to the platform, and the data of these applications are usually stored on the platform. Therefore, an adversary can fetch the data if they are not protected properly by the way of SQL injection attacks, buffer overflow attack, privilege promotion, etc.

7.2.2 Data tampering

Data may be tampered with, replayed or modified during transmission. During the transmission and storage process of the application data, an adversary is able to tamper with data if they are not protected properly. For example, an adversary can replay used information or forge fake information and send the information to the IoT platform if data integrity is not considered during transmission.

7.3 System security risks

7.3.1 Account compromise

If the accounts of administrators for the IoT service platform's operating system are not complicated enough, or if an unnecessary port for the system is open, accounts may be compromised by brute force, monitoring and so on. Improper access control threatens the system's security.

7.3.2 Privilege abuse

IoT services provided by the platform run on the operating system and middleware. If the operating system or middleware is not updated in time, there are risks that an old-version system or middleware has vulnerabilities which could be exploited by hackers, leading to elevation of privileges.

7.4 Infrastructure security risks

The infrastructure is vulnerable to physical security, network security, virtualized security and equipment security threats.

7.4.1 Physical threats

The physical environment of the IoT platform also affects security. For example, it is vulnerable to natural threats such as earthquakes, floods, storms and tornadoes. In addition, facilities such as power and cooling systems, and even security systems themselves, can be a threat to an IoT platform. What is more, human factors should also be considered, which may include deliberate destruction, theft and explosion.

7.4.2 Network threat

Attackers may scan the Internet to find access points for IoT service platforms. Lack of network isolation for service platforms may lead to data access across different services.

7.4.3 Virtualized risks

Server virtualization technology has greatly improved the construction efficiency, operational flexibility, and economic benefits of the IoT platform, but it has also brought new risks. For example, the design flaws of the virtual machine monitor (VMM) make it possible for attackers to intrude omtp virtual host and sharing a network card with the virtual machine of the same host makes it easy for security problems to spread. There are also other kind of risks such as virtual machine (VM) hopping, DoS attacks and remote management platform vulnerabilities.

7.5 Interface security risks

The interface of the IoT service platform includes the web interface, third-party API and vendor backend API, which faces the risk of information leakage, cross-site scripting, weak authentication and weak access control.

7.6 Operational security risks

During operation and maintenance, service may be interrupted due to the incorrect operational actions of operation and maintenance personnel. For example, personnel may use a USB flash disk infected by malware or may delete data accidentally. Abnormal connection, default passwords, malicious attacks and audit mechanisms should also be taken into consideration.

8 The security architecture of the IoT service platform

The security architecture of the IoT service platform focuses on six aspects of security protection requirements: application security, interface security, data security, system security, infrastructure security and operational security.

The overall security architecture is shown in Figure 3.

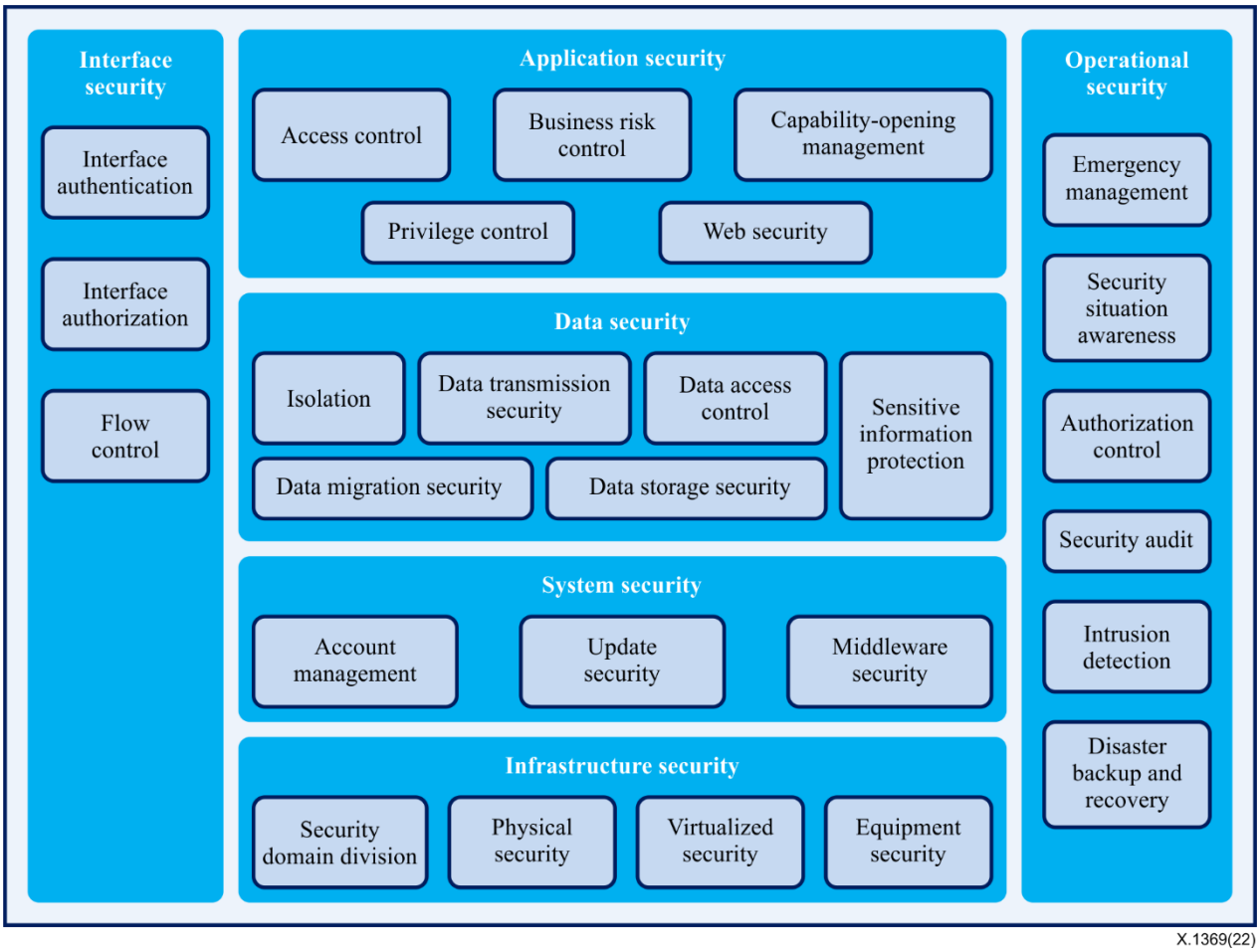

Figure 3 – Security architecture of the IoT service platform

8.1 Application security

Application security includes access control, privilege control, business risk control, web security and capability exposure management, which would be conducive to solving the problems of privileges elevation, unauthorized access, etc.

8.2 Data security

Data security includes isolation, data transmission security, access control and data storage security, which would be conducive to solving privacy leakage problems and other data security problems.

8.3 System security

System security includes account management, software update security and middleware security, which would be conducive to solving the problems of the malicious use of known vulnerabilities.

8.4 Infrastructure security

Infrastructure security includes security domain division, physical security, visualized security and equipment security, which would be conducive to solving problems of the malicious use of known vulnerabilities.

8.5 Interface security

Interface security includes interface authentication, interface authorization and flow control, which would be conducive to solving the problems of breaches of personally identifiable information, SQL injection, etc.

8.6 Operational security

Operational security includes emergency management, security situation awareness, authorization control, security audit, intrusion detection, disaster backup and recovery, which would be conducive to solving operational security related problems.

9 Security requirements for the IoT service platform

9.1 Application security

The service platform should be able to prevent attacks from Internet on the boundary, especially attacks on big data, cloud computing, web applications and other technologies. The ability to prevent DDoS, tampering, intrusion and viruses should be provided to ensure the secure and stable operation of the service platform.

9.1.1 Access control

9.1.1.1 User access control

1. A user identification system should be constructed to assign a unique identity label for each user, which should remain the same even if the user changes the mobile phone number, mailbox or other information.
2. Periodic detection for weak passwords should be deployed. In addition, the password should be encrypted during the transmission process. For high-security services, the mandatory periodic password replacement mechanism should be considered.
3. The use of dynamic short messages should be strictly handled. Security measures such as background verification, immediate invalidation after use, limiting the number of false logins, avoid local authentication, etc., should be adopted.
4. A graphic authentication code mechanism should be used in the login scenario. Background scrambling measures such as background noise, non-binarization, anti-segmentation, through-line, font rotation distortion, etc. should be considered to prevent rapid machine recognition.
5. The platform should have capabilities for risk control and anti-collision. It should have the ability to identify legitimate access. For example, violent cracking should be prevented by a numerical limitation of failed logins, IP address, device ID, lock-in time, unlock mode and simultaneously online.
6. During the process of password reset and recovery, identity should be verified strictly to prevent authentication bypass and identity counterfeiting.

9.1.1.2 Application access control

1. Construct application identification system and assign unique ID to each application.
2. The validity of an application which accesses the platform should be authenticated. Only an authenticated application should be allowed to access the service platform to carry out subsequent service invocations.
3. It is forbidden to transfer keys in plaintext or apply weak algorithm (such as MD5) transformation for keys during the process of application authentication.

4. Different keys should be assigned to different applications, and key management functions for the generation, distribution, storage and update of keys should be supported.
5. The invocation of interfaces should be authenticated to limit the scope of resources and operational authority that can be operated.

9.1.1.3 Device access control

1. A device identification system should be constructed. Assign each IoT device a unique ID and bind the ID to the corresponding equipment information, such as device manufacturer, device type, mould, etc.
2. Assign a unique device key to each device through a key pre-distribution scheme or key exchange scheme, etc. The device key and device ID should be bounded together and key management functions for the generation, distribution, storage and update of keys should be supported.
3. Apply identity authentication when the device accesses the platform. Only an authenticated device should be allowed to access the service platform for subsequent service operations.
4. It is forbidden to transfer keys in plaintext or apply weak algorithm (such as MD5) transformation for keys during the process of application authentication.

9.1.2 Privilege control

1. User classification and grouping management should be supported. Different privileges should be granted according to different user classifications and groupings. Only authorized users should be allowed to access the specified data and perform corresponding operations.
2. Different privileges should be granted according to different application classifications. Only authorized applications should be allowed to invoke specified service capabilities and perform corresponding operations.
3. Different privileges should be granted according to different device types or classifications. Only authorized devices should be allowed to access specified data and information and execute corresponding operations.

9.1.3 Business risk control

9.1.3.1 IoT card security management and control

The communication functions of IoT cards should be strictly limited for different types of services based on the principle of "minimum, necessary, and controllable". For example, the function of voice, short message should be unidirectional in some scenarios, and the function of data should be restricted when the data flow is abnormal.

9.1.3.2 Service security management and control

This should have the ability to limit the total amount and frequency of data flow, short message, voice, etc., and shut down the service when the amount exceeds the threshold.

9.1.3.3 User behaviour control

The total flow amount, frequency, and time that users access the platform should be limited. When users behave abnormally, access should be stopped immediately.

9.1.3.4 Device anomaly monitoring

Device behaviour should be monitored. When abnormal device behaviour (for example, unconventional time, unconventional visits, abnormal location area) is detected, an alarm and processing mechanism should be provided.

9.1.3.5 Service risk monitoring

The data of IoT terminals should be analysed multidimensionally, such as by total amount and peak flow, so as to detect service operation abnormity in time. During service operation, the service abuse should also be monitored. For example, a split of device and card could be detected by monitoring the international mobile equipment identity (IMEI) numbers of devices. At the same time, by using the big data collected from the terminal operation, the ability to detect, analyse and eliminate security risks could be enhanced from a global point of view.

9.1.4 Web security

1. A strong anti-DDoS-attack ability should be provided, and anti-DDoS strategies (for example, traffic traction, network traffic cleaning and so on) for the application layer and network layer should be customized.
2. The platform should have web vulnerability scanning capability, which can detect and prevent security issues such as file upload, SQL injection, XSS vulnerabilities, CSRF vulnerabilities and SSRF vulnerabilities.
3. The platform should have the ability to scan for host vulnerabilities and find vulnerabilities in the information system, including security vulnerabilities, security configuration problems, application system security vulnerabilities and weak passwords.
4. The platform should have the ability to limit the time of the database connection and network access in web applications to avoid unnecessary resource consumption.
5. The platform should have the ability of intrusion detection, recording the source IP, attack type, attack purpose and attack time of an intrusion, and providing an alarm when serious intrusion occurs.

9.1.5 Capability exposure management

9.1.5.1 Identity authentication

The application enablement system should support identity authentication. When the developer asks for and applies some API functions, the legality of the developers and the applications should be authenticated, and the identity of legitimate developers and applications should not be counterfeited.

9.1.5.2 Application reinforcement and protection

The application enablement system should have a function to support the reinforcement and protection to applications which invoke the API functions, to prevent an application from being tampered with and decompiled.

9.1.5.3 Data security protection

The application enablement system should ensure the confidentiality and integrity of sensitive information related to accounts, credentials of users and applications, to prevent the information from being stolen or tampered with during storage, transmission and use. For example, sensitive information transmitted between the IoT application and the platform should be encrypted, and integrity protection should be considered, ensuring that sensitive information is not exposed to unauthorized entities and processes, nor modified, corrupted or replayed by them, etc.

9.1.5.4 Capability invocation authentication

The application enablement system should support capability invocation authentication and authorization. When the application invokes the capability, the frequency, total amount and type of the capability that the developer and application can invoke should be authenticated. The capability should only be invoked after authorization.

9.1.5.5 Capability invocation monitoring

The application enablement system should support the monitoring of the frequency, time and total amount of the capability invocation. When the limit is exceeded or the behaviour is abnormal, the function should be stopped immediately and an alarm given at the same time.

9.2 Data security

The platform should protect the data through the whole lifecycle, including storage, transmission and usage, etc. The critical service data should be backed up periodically, and a recovery mechanism should be configured, to ensure data confidentiality, integrity and availability.

9.2.1 Data isolation

Different data should be executed and saved in isolating environments. The platform should be able to isolate sensitive information logically and control the interactions between different fields strictly.

9.2.2 Data transmission security

1. The sensitive information transmitted between the service platform and IoT devices and other service platforms (including background administrator password, operating system login password, network device login password, and the password protection answers associated with these passwords) should be protected confidentially.
2. The integrity of sensitive information between service platforms, IoT devices and other service platforms should be protected.

9.2.3 Access control

The platform should support the function of access control, for example, different access policies for the database of different virtualization systems should be set to ensure that users can only operate within the authorization of the database for the corresponding service system and cannot access the data of other unauthorized service systems.

9.2.4 Data storage security

1. Data should be classified according to their significance, and different mechanisms should be adopted according to the classification level of the data. For example, less important data can be stored in plaintext, while the confidentiality of important data should be guaranteed.
2. The platform should provide a secure key storage mechanism. For example, store the keys inside the encryption machine or a specific proxy to ensure that the keys are not leaked.
3. The integrity of the data should be protected and an integrity detection mechanism should be provided for extremely sensitive data, so that the damage and loss of those data can be detected in time. Extremely sensitive data include username, account number, etc.
4. The platform should provide a complete data backup and recovery mechanism. If data are lost or destroyed, the backup mechanism should be used to restore data to ensure that they will not be lost after an accident has occurred.
5. The platform should have the ability of archiving all kinds of data and files and the function of cleaning temporary data and files automatically and periodically.
6. The storage space of files, directories and databases in the system should be released or redistributed, which should be able to be completely cleared and irrecoverable.

9.3 System security

The system used by the platform should take account management, software update security and middleware security into consideration, which would be conducive to solving the problems of the malicious use of known vulnerabilities.

9.3.1 Account management

1. The system of the platform should automatically record system logs, such as user login information, operational information, etc.
2. For systems that are remotely maintained by HTTP protocol, the system should support encryption protocols such as HTTPS.
3. A system with a character interface should support timing account automatic exit.
4. The system should take host resource access control into consideration, for example, to establish a role model and set a proper security policy to control different role users' access to host resources.

9.3.2 Software update security

1. The operating system's version/security patches should be updated in time.
2. Only required components and applications should be allowed to be installed.
3. The system should only open necessary ports and close unnecessary ones.

9.3.3 Middleware security

1. Version/security patches of the middleware should be updated in time.
2. Unnecessary interfaces of the middleware should be disabled to prevent system information leakage.
3. The middleware flag (software name/version number banner) should be protected to prevent system information leakage.

9.4 Infrastructure security

Infrastructure security should consider security domain division, physical security, visualized security and equipment security, which would be conducive to solving the problems of the malicious use of known vulnerabilities.

9.4.1 Network security domain division

1. Security domains should be divided between service platforms and the Internet, between service platforms and internal support systems and between the different services' systems hosted within the platform. Security domain boundaries should be divided between other domains and the access domain, between the access domain and core domain and within the core domain.
2. Different service systems in the service platform should be divided into different virtual local area networks (VLAN), and different security domains should use different VLAN segments. Different service systems in each security domain should use different VLANs, and all VLANs are isolated by default. In the same VLAN, VM isolation at different security levels of the same service system should be supported, such as dividing a sub-VLAN by private VLAN (PVLAN) technology.
3. A policy of mutual access should be set. For example, conduct the strategic configuration for mutual access of different security domains within the service system, and mutual access between different service systems.
4. The function of security domain isolation should be supported. For example, the platform network can be divided into the management domain, service domain, interface domain, etc. Devices of different functions should be distributed to different security domains. Intrusion detection and access control should be implemented at the borders of security domains.

9.4.2 Physical security

1. The physical environment should meet the safety protection requirements of location, power supply, fire, waterproofing, anti-static and temperature and humidity control.

9.4.3 Virtual security

1. The platform should support hypervisor protection, VM isolation, cloud host system reinforcement, VM security monitoring, malware protection, application control and other functions to avoid common virtualization security issues.

9.4.4 Equipment security

1. Physical facilities should meet the safety protection baseline configuration requirements and testing requirements. Trusted computing should be introduced to enhance facility security.

9.5 Interface security

Interface security includes interface authentication, interface authorization and flow control, which would be conducive to solving the problems of personally identifiable information breaches, SQL injection, etc.

9.5.1 Interface authentication

1. The platform should have the ability to verify the legitimacy between service systems, so as to prevent the unauthorized use of and access to the platform.
2. The service platform should have the function of recording the complete operation log of the resources invoked.

9.5.2 Interface authorization

1. The service platform should have the function of authorizing according to the source IP address range. In addition to providing a static password, the invoked service platform also needs to authorize the IP address range.
2. For interfaces that require user access rights, am access mechanism of a deny/allow list should exist to intercept illegal user access.

9.5.3 Flow control

1. The platform should have the ability to control the flow rate by setting the flow control policy, and the configuration value in the policy can be modified according to the performance adjustment of the API server at the back end. When the number of concurrent requests exceeds the limit, exceeded requests are rejected and an error response is returned.

9.6 Operational security

Operational security includes emergency management, security situation awareness, authorization control, security audit, intrusion detection, disaster backup and recovery, which would be conducive to solving the operational security related problems.

9.6.1 Emergency management

1. The platform should establish the mechanism for responding to emergency incidents, such as cybersecurity incidents, workplace safety incidents, etc.
2. Arrange regular emergency drills and establish a system for regular drills of emergency plans.

9.6.2 Security situation awareness

1. It is recommended to build a security situation awareness system to realize the monitoring, evaluation, early warning, visualization, and centralized response of the platform's security situation, so as to effectively improve the network security threat monitoring, situation awareness, emergency response, tracing and other capabilities, and improve the security operation and maintenance efficiency.

9.6.3 Authorization control

1. The platform should make necessary authentication and authorization for different operations to the platform. For high-level privileges, only trusted system personnel can perform high-level privilege operations.
2. The platform should establish role models, and control user access to host resources according to the security policies.

9.6.4 Security audit

1. All operations of administrators should be recorded and formed to a log.
2. When the storage space is almost exhausted, the audit log should be guaranteed not to be lost.
3. The audit logs should be backed up.
4. The audit logs should be protected from unauthorized access, modification and destruction.
5. The audit logs should be exported and deleted.
6. Logs should be accessed in a secure way to ensure the confidentiality and integrity of the transmission process.
7. The platform should have the functions of real-time monitoring and periodic auditing of abnormal behaviours such as abnormal connection, abnormal access and abnormal application based on traffic analysis, log auditing, sandbox and so on, and timely warning and disposal should be provided according to the found abnormal behaviour.

9.6.5 Intrusion detection

1. The platform should deploy intrusion detection equipment to detect any intrusion in a timely fashion.

9.6.6 Disaster backup and recovery

1. In case of fire, earthquake and other disasters, the platform should be able to switch to the remote redundant backup system in time to continue its service.
2. The platform should support the disaster recovery of sensitive data (such as service data, billing data, system configuration data, administrator operation and maintenance records, user information, etc.) to ensure that when critical data are deleted maliciously, the system can recover in time.

Bibliography

[b-ITU-T X.1361] Recommendation ITU-T X.1361 (2018), *Security framework for the Internet of things based on the gateway model*.

[b-ITU-T X.1362] Recommendation ITU-T X.1362 (2017), *Simple encryption procedure for Internet of things (IoT) environments*.

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things.*

[b-ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2022