International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1470

(11/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Web security (2)

Security guidelines of web-based online customer service

Recommendation ITU-T X.1470

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.1470

Security guidelines of web-based online customer service

Summary

Web-based online customer service is an important service for a service provider. It contains the user's important data and provides critical operational functions of the user's services. It is the service provider's responsibility to provide security for web-based online customer service.

Recommendation ITU-T X.1470 analyses the security threats of web-based online customer service in three aspects: network security, system security and service security. It specifies security guidelines of web-based online customer service and corresponding security measures. It also proposes test procedures to verify that the specified security requirements are satisfied by corresponding security measures.

This Recommendation can help service providers to ensure their web-based online customer services' security and protect benefits of their users.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X.1470	2021-11-13	17	11.1002/1000/14803

Keywords

Security guidelines, security test, web-based online customer service.

[*] 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.1470

Security guidelines of web-based online customer service

1 Scope

This Recommendation analyses security threats of web-based online customer service, specifies security guidelines and measures, and proposes testing methods to verify the security requirements are satisfied by corresponding security measures.

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/IEEE 15288] ISO/IEC/IEEE 15288: 2015(E), *Systems and Software Engineering – System Life Cycle processes*.

[NIST SP 800-160] NIST SP 800-160 Vol. 1: 2018, *Systems Security Engineering – Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 web-based online customer service: A web-based interface provided by a service provider for supporting self-services.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CSRF	Cross Site Request Forgery
HTTPS	Hyper Text Transfer Protocol Secure
ID	Identifier
SDLC	System Development Life Cycle
SIM	Subscriber Identity Module
SMS	Short Message Service
SQL	Structured Query Language

SSH	Secure Shell
XSS	Cross Site Scripting

5 Conventions

None.

6 Overview

Web-based online customer service is becoming an essential service offered by service providers. A web-based online customer service contains important data of the user (such as the user's call records, etc.) and provides critical inputs to operational functions of the user's services (e.g., recharges, payments, etc.). It is the responsibility for the provider to provide secure web-based online customer service.

6.1 System life cycle

The life cycle of a typical service (system) can be summarized as a series of stages and processes. As shown in Figure 1, [ISO/IEC/IEEE 15288] describes the system life cycle stages as concept, development, production, utilization, support, and retirement. The system development life cycle (SDLC) model is helpful in order to visualize the mapping of the security requirements, control measures and testing methods and where each of these should be applied to the entire web-based online customer service development life cycle.

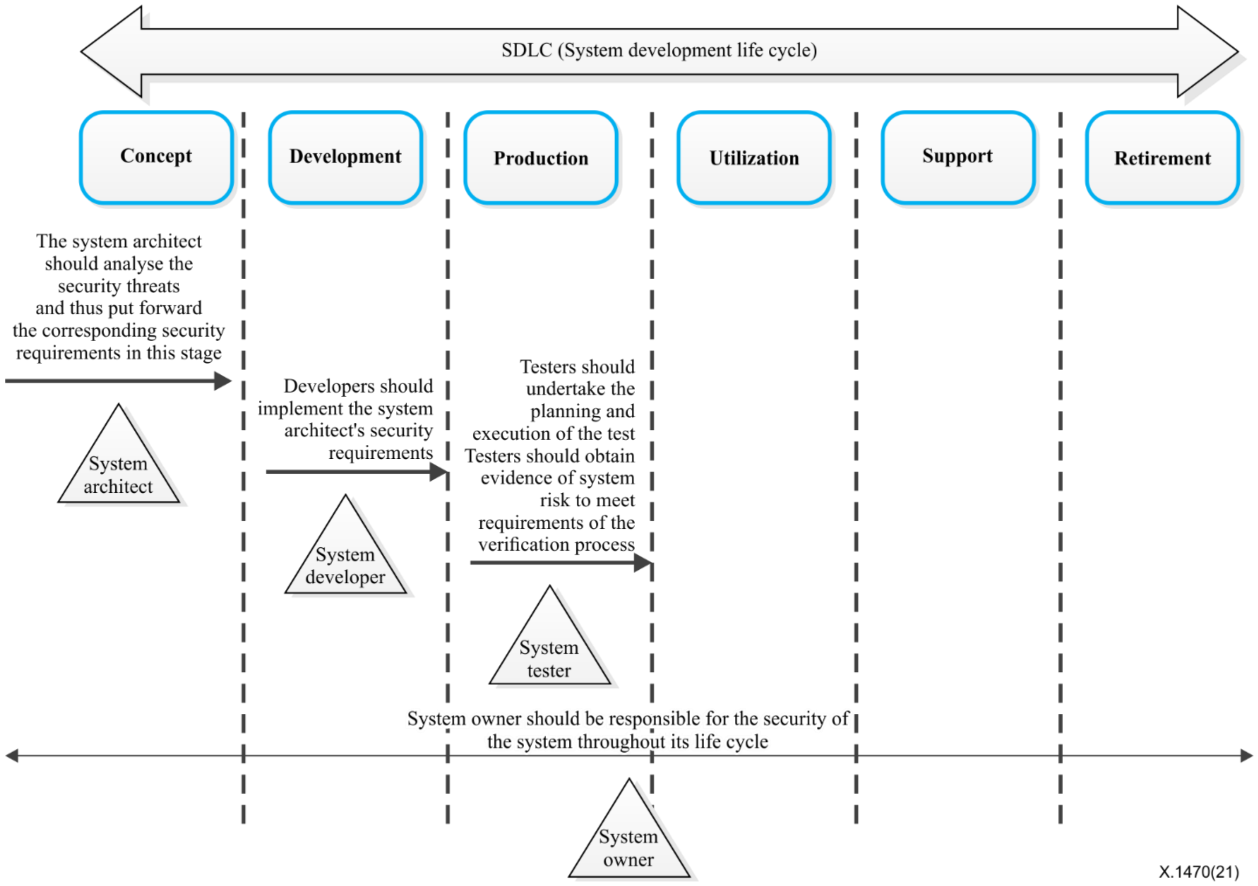

SDLC (System development life cycle)
Concept
Development
Production
Utilization
Support
Retirement
The system architect should analyse the security threats and thus put forward the corresponding security requirements in this stage
System architect
Developers should implement the system architect's security requirements
System developer
Testers should undertake the planning and execution of the test Testers should obtain evidence of system risk to meet requirements of the verification process
System tester
System owner should be responsible for the security of the system throughout its life cycle
System owner
X.1470(21)

Figure 1 – System development life cycle

The stages included in the SDLC model are:

– **Concept**: This stage is an initial exploration, fact-finding, and planning period. It develops preliminary system requirements and a feasible architecture and design solution.

– **Development**: This stage begins with sufficiently detailed technical refinements of the system requirements, system architecture, and the security solution and transforms these into one or more feasible products that enable one or more services during the utilization stage.

– **Production**: This stage begins with the approval to produce the system-of-interest. This stage is executed to produce or manufacture the system-of-interest, test it and produce related enabling systems as needed.

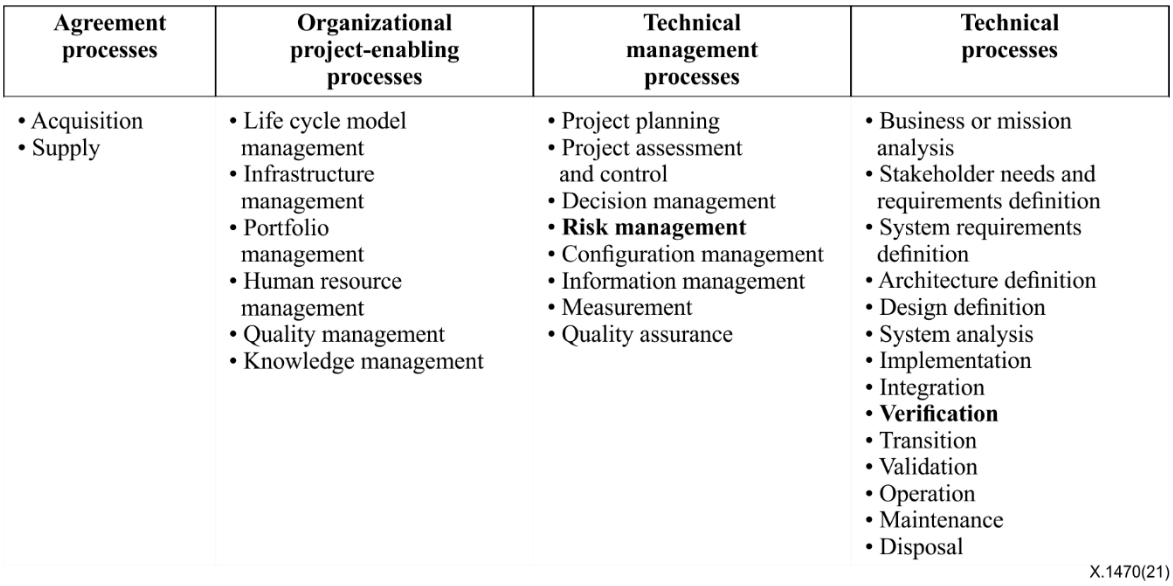
– **Utilization**: This stage includes those processes related to the use of the system to provide services, as well as monitoring performance and identifying, classifying, and reporting anomalies, deficiencies, and failures.

– **Support**: This stage provides logistics, maintenance, and support services. It also includes those processes related to providing services that support the utilization of the system-of-interest.

– **Retirement**: This stage begins whenever a system-of-interest reaches its end-of-service life. In this stage a system-of-interest and related operational and support services, and the retirement system itself are removed.

According to [NIST SP 800-160] and [ISO/IEC/IEEE 15288], system development life cycle processes, as shown in Figure 2, were proposed as a complement along with the SDLC model. These processes and the six stages of the model do not have a one-to-one mapping relationship. Instead, engineers or managers can use the necessary processes based on the actual needs of a system during any stage.

Among processes defined in [ISO/IEC/IEEE15288], *risk management* and *verification*, shown in bold in Figure 2, are related to system security. It is recommended to use them throughout the system development life cycle.



Agreement processes	**Organizational project-enabling processes**	**Technical management processes**	**Technical processes**
• Acquisition • Supply	• Life cycle model management • Infrastructure management • Portfolio management • Human resource management • Quality management • Knowledge management	• Project planning • Project assessment and control • Decision management • **Risk management** • Configuration management • Information management • Measurement • Quality assurance	• Business or mission analysis • Stakeholder needs and requirements definition • System requirements definition • Architecture definition • Design definition • System analysis • Implementation • Integration • **Verification** • Transition • Validation • Operation • Maintenance • Disposal

X.1470(21)

Figure 2 – System development life cycle processes [ISO/IEC/IEEE15288]

- **Risk management**: This process identifies and analyses security risks so that appropriate security risk treatment is implemented. Monitoring measures should be continued to ensure the effectiveness of the assessment of security risk management.
- **Verification process**: This process produces evidence to demonstrate that the system satisfies its security requirements and security characteristics with the level of assurance that applies to the system. The vulnerability should be obtained through demonstration, inspection, evaluation, and testing.

Security requirements refer to the analysis result of the security risks faced by a web-based online customer service and thus put forward corresponding security requirements. These security requirements should be implemented throughout the entire system development life cycle. At the same time, tests should be strictly completed during the production stage of the system development life cycle to reduce the security risks as much as possible before it is released.

6.2 System components

Web-based online customer service consists of two parts: service scenarios and fundamental components, as shown in Figure 3.

- Service scenarios: A series of operational sequences designed to implement the service function.
- Fundamental components: General software used in system development, including web frameworks, third-party components, databases, operating systems, etc.

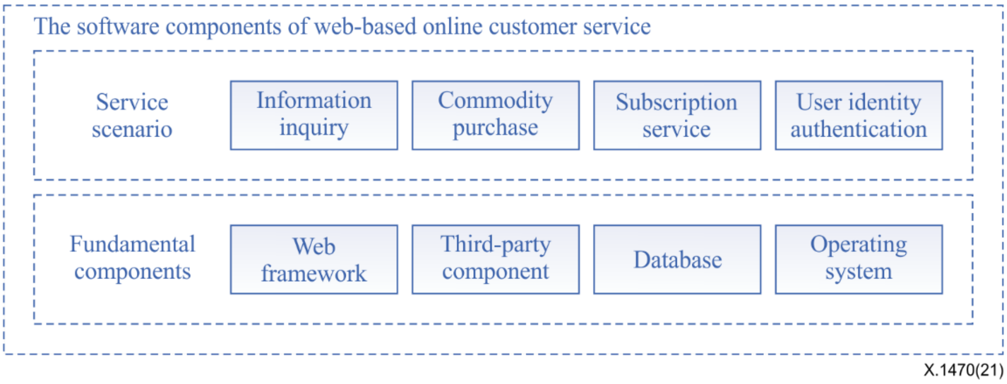


Figure 3 – System components of web-based online customer service

6.3 Security risks

Web-based online customer service is the most common service offered by service providers. Users can use it for information inquiry, service subscription, payment, etc. Service providers can also exchange data and information with external platforms. However, many security risks exist in these service scenarios, such as user information leakage, user identity fraud, transaction information tampering, unauthorized subscription, application programming interface (API) abuse, services vulnerabilities exploitation, and so on. For these reasons, systems or services might be attacked. Clause 7 addresses these risks in detail.

6.4 Security requirements

To address the security risks mentioned in clause 6.3, security requirements must be considered, including encryption of data, user identity authentication and authorization, access control, checking input data, subscription confirmation, periodical updating against vulnerabilities of web services, and so on. Clause 8 proposes security requirements and measures based on analysis of security threats in some specific service scenarios.

6.5 Security tests

To ensure a security measure is in place, is implemented as planned, and behaves as expected, tests should be implemented before the service is released. 3GPP TS 33.117 *Technical Specification Group Services and System Aspects; Catalogue of general security assurance requirements* [b-3GPP TS 33.117] describes what a test process should be as follows:

Test plan

A test plan should be prepared to provide an overview of the security requirements for the system, a system boundary description and the system identification. The test plan can also contain, as supporting appendices or as references, other key security-related documents such as a risk assessment report, contingency plan, security configurations, incident response plan and so on.

Test pre-condition

Functional documents, network topology, management documents, system-related data, user information and so on.

Test execution steps

Tester prepares a security test. It provides the main content of security test and detailed steps.

Test expected results

System output if security requirements are met and evidence of this should be kept.

7 Security risks analysis

7.1 Security risks

Clause 6 lists concisely different scenarios and potential risks which could lead the system to be attacked and damaged as the following:

Fundamental component vulnerabilities

Proper operation of a service provided depends on the integrity of the fundamental components of the service system which are usually composed of the web frameworks, third-party components, databases, operating systems, etc. The service system could be damaged due to fundamental component vulnerabilities exploitation and viruses.

User information leakage

User information leakage could occur anywhere in the process of information transmission, storage and inquiry. There are two methods to acquire information: One method is using tools to intercept the packets in the transmission network and the other method is directly attacking the system to obtain the data in storage from the provider's database.

User identity fraud

In the scenarios of system login and service subscription, etc., the attacker could disguise himself as a normal user during interaction with provider's service system and then use the service as a legal customer.

Transaction information tampering

The transaction information might be tampered with by an attacker to obtain extra benefits. For example, an attacker could maliciously tamper with the service price and service type in the process of a payment service, which would result in economic losses for both users and operators.

Unauthorized subscription

The risk could lead to infringement of customers' rights. For example, the attacker could intrude on the subscription database or disguise it as a normal subscription process to produce a false subscription record without authorization by the user.

API abuse

This risk could lead system resources to be occupied massively, the normal operation of the service could be affected, and customers could be harassed. For example, the abuse of a short message service (SMS) verification code interface might cause SMS bomb events, and a frequently calling interface would lead system resources to be exhausted quickly and normal customers could be prevented from using services.

Unauthorized access

Attackers could obtain access to the system through the password, a system vulnerability and by other means such as a brute-force attack from attackers.

Message replay

Attackers can capture data packets (e.g., authentication data packets or other interactive data packets) sent to the service system and then replay them abnormally. If the service system handles the replayed packets as normal, then the attackers can be authenticated by the service system, or SMS bomber attacks can take place.

Denial of service

The attacker slows down or slams the service system so that the system does not serve the user properly.

7.2 Relationship between security risks and system components

Security risks appear in particular places of the software components of a web-based online customer service. The relationship of security risks to service scenarios is shown in Table 1.a while the relationship between security risks and system components is shown in Table 1.b.

In Table 1.a and Table 1.b, the letter "Y" (Yes) in each cell indicates that the entity is related to a particular security risk.

Table 1.a – Relationship of security risks to service scenario

Entities / Threats	Service scenario			
	Information inquiry	**Commodity purchase**	**Subscription service**	**User identity authentication**
User information leakage	Y	Y	Y	Y
User identity fraud		Y	Y	Y
Transaction information tampering	Y			Y
Unauthorized subscription			Y	

Table 1.a – Relationship of security risks to service scenario

Entities / Threats	Service scenario			
	Information inquiry	**Commodity purchase**	**Subscription service**	**User identity authentication**
API abuse		Y		
Unauthorized access	Y	Y	Y	
Message replay	Y	Y	Y	Y
Denial of service	Y	Y	Y	Y

Table 1.b – Relationship between security risks and fundamental components

Entities / Vulnerabilities	Fundamental component			
	Web framework	**Third-party component**	**Database**	**Operating system**
SQL injection	Y	Y	Y	
XSS	Y	Y		
CSRF	Y	Y		
File upload	Y	Y		Y
Weak password	Y	Y	Y	Y

8 Security requirements and measures

This clause will analyse security risks identified in clause 7 through the description of various scenarios, specify corresponding safety requirements, and corresponding test cases are provided in clause 9 to verify whether security requirements are satisfied by security measures.

8.1 Fundamental component security

8.1.1 Issue description

Proper operation of services provided depends on the integrity of fundamental components which are usually composed of the network, operating system middleware, database, etc.

8.1.2 Security risk analysis

Vulnerabilities of fundamental components could lead to network attacks on the service system and failures/unavailability of service.

8.1.3 Security requirements and measures

The following measures should be taken and verified by the corresponding test case in clause 9:

- Install anti-virus software and periodically install updates for operating systems, middleware, and databases to ensure that there are no undiscovered web vulnerabilities. Test case number T-1-1.
- Check the list of operating system services. Turn off unnecessary services, processes and unnecessary remote access to the operating system. Test case number T-1-2.
- Enable logging of the database and operating system and periodically audit logs. Test case number T-1-3.
- Configure the operating rights of the system account according to the principle of least privilege. Test case number T-1-4.
- Configure the firewall to prevent network attacks:
  - Set the access control list correctly;
  - prohibit unnecessary network services.

  Test case number T-1-5.
- Divide the internal network of the system into isolated security domains, according to actual needs. Test case number T-1-6.
- Adopt cryptographically network protocols without known vulnerabilities for information exchange between the user-side and server-side. Test case number T-1-7.

8.2 Information inquiry scenario

8.2.1 Description of service function

Users check their account balance, payment records, call records, etc. through a web-based online customer service by themselves.

8.2.2 Security risk analysis

If the user information is not properly protected, this will risk user information leakage, denial of service, user identity fraud and message replay attacks.

8.2.3 Security requirements and measures

The following measures should be taken and verified by the corresponding test case in clause 9:

- Data packets between user-side and service-side should be labelled in some way, such as checksum. Packets that do not comply with the rule will be discarded. Test case number T-2-1.
- Second user authentication should be used via SMS, service password (different from the login password) or some other verification method setup in advance during querying the call records. Test case number T-2-2.
- If the authentication failure reaches a certain amount (e.g., 3 times), the account should be locked. Test case number T-2-3.
- The use of tamper-proof measures is especially valuable for the protection of key data, including:
  - username or ID;
  - payment amount;
  - call records;
  - business types;
  - user information and
  - authentication result.

  Test case number T-2-4.

8.3 Commodity purchase scenario

8.3.1 Description of service function

Users purchase commodities through the service system, including recharge cards, subscriber identity module (SIM) cards and material goods (such as mobile phones, electronic devices, etc.), using different payment methods, including third-party payment (such as Visa Card, MasterCard, Union pay, Alipay, etc.) and store credits.

8.3.2 Security risk analysis

If there are vulnerabilities in the payment process, there is a risk that the payment information would be tampered with thus leading to user identity fraud or transaction information tampering. For example, the attacker can tamper with the payment information to subscribe to the service at a lower price. Other risks such as for example API abuse could exist.

8.3.3 Security requirements and protection measures

Protection measures including the following should be made and verified by corresponding test cases in clause 9:

– In the process of purchase, the transaction information (including the user ID, commodities type and commodities amount) should be encrypted by industry-accepted algorithms. Test case number T-3-1.

– Technical measures are required to monitor abnormal behaviours of the purchase, including:

  - Suddenly massive subscriptions;
  - Repeated payment requests and cancellations;
  - A large number of orders without payment; etc.

  Test case number T-3-2.

– Two-step verification of the service is required when abnormalities occur. Additional authentication methods (e.g., based on an SMS) should be used to confirm the order is the user's own operation. Test case number T-3-3.

– When payment is completed, a notification message should be sent to the user, by SMS, voice call or e-mail. Test case number T-3-4.

– The total amount of payment should be recalculated on the server-side. Test case numbers T-3-5 and T-3-6.

– The accomplishment of the payment should be confirmed between the server-side and the external financial system. Test case number T-3-6.

8.4 Subscription service scenario

8.4.1 Description of service function

Users change their subscriptions through a subscription service, e.g., service subscription and service un-subscription.

8.4.2 Security risk analysis

When a user subscribes to a service through the service portal, the subscription information (including service type and user information) will be sent to the server. The subscription information could be tampered with or forged by an attacker, resulting in security risks such as unauthorized subscription.

8.4.3 Security requirements and measures

The following measures should be taken and verified by the corresponding test case in clause 9:

– When a user changes a subscription through the system, the system should confirm the identity of the user, usually by SMS verification code, or service password (when the user opens the phone number the first time, a service password should be set, etc.). Test case number T-4-1.

– After successful service subscription, the system should remind users of the subscription service information (including the service content, service fee, effective time, expiration time, etc.) by SMS, voice call or email. Test case number T-4-2.

– The system should monitor the abnormal behaviours of service subscriptions, such as:

  - The number of subscriptions of a certain user increases suddenly;
  - The subscription volume of a certain service changes abnormally;
  - Repeated service subscriptions and cancellations, etc.

  Test case number T-4-3.

8.5 User identity authentication scenario

8.5.1 Description of service function

Web-based online customer service needs to verify the user's identity before providing services. For example, users are required to enter a password to sign in or to provide proof of identity in order to buy a SIM card.

8.5.2 Security risk analysis

If there is a security vulnerability in the user identity verification process, an attacker can bypass the verification process to complete the authentication, which could cause a security risk for user identity fraud or unauthorized access.

8.5.3 Security requirements and measures

The following measures should be taken and verified by the corresponding test case in clause 9:

– When user authentication errors occur on the server-side, the system should confuse the error message and avoid displaying software-level error prompts to the user. Test case number T-5-1.

– Additional measures for user authentication should be set up, including:

  - The maximum number of failed validations (e.g., 3 times) should be set. If the number of logins exceeds the number of online logins, the account should be locked. After the account is locked, the system no longer accepts user login requests. Test case number T-5-2.
  - User account lockout time should be set. Users cannot login to the system during the lockout time. Test case number T-5-2.
  - The user should be prohibited from logging in repeatedly. If the user logs in multiple times, the last user login session will be invalid. Test case number T-5-3.

– If the system uses a static password for user authentication, the user should be required to set a static password according to the password complexity requirements (mix letters, numbers and even symbols in the passwords.). Test case number T-5-4.

– The first time the user logs in, the system should verify the identity of the user and then force the user to change the password. User authentication methods include:

  - The information provided by the user when purchasing a calling card such as contacts, email, bankcard information, etc.

- Dynamic verification code, via SMS or voice call, etc.

  Test case number T-5-5.

– The system should be able to recognize the automatic login of the machine, including:

  - Setting a graphic recognition verification code;
  - Puzzle verification, etc.

  Test case number T-5-6.

9 Security tests

In this clause, test cases are defined based on the security requirements and protective measures specified in clause 8, to make sure they are properly implemented before the utilization stage. Testers should prepare materials and test environments in accordance with the test pre-condition, test the system in accordance with the exercise step and check whether the test results meet expectations.

9.1 Fundamental component security

Test number: T-1-1
Test proposal: Fundamental component security – vulnerabilities and anti-virus
Test pre-condition: 1. The documentation about the security configuration used by the service system 2. The network where the client is located can access the service to be tested
Execution steps: 1. The tester scans the system for vulnerabilities to check whether there are known web vulnerabilities in the host. 2. The tester reviews the configuration document to check whether the system regularly updates with anti-virus software, operating systems, middleware, and databases.
Expected results: The system has no known web vulnerabilities.

Test number: T-1-2
Test proposal: Fundamental component security – unnecessary services
Test pre-condition: 1. The documentation about the security configuration used by the service system 2. The network where the client is located can access the sever to be tested
Execution steps: 1. The tester logs into the service system, views the list of operating system services to check whether there are unnecessary services and processes and remote access to the operating system.
Expected results: 1. The system has shut down unnecessary services and processes. 2. The system has shut down unnecessary remote access.

Test number: T-1-3
Test proposal: Fundamental component security – log audit
Test pre-condition: 1. The documentation about the security configuration used by the service system 2. The network where the client is located can access the sever to be tested
Execution steps: 1. The tester checks whether the system has started the database and operating system log function. 2. The tester reviews the security configuration document to check whether audit logs are required periodically.
Expected results: 1. The system enables logging of the database and operating system. 2. The requirement of log audit would be implemented periodically.

Test number: T-1-4
Test proposal: Fundamental component security – least privilege
Test pre-condition: 1. The documentation about the security configuration used by the service system 2. The network where the client is located can access the sever to be tested
Execution steps: 1. The tester views the permission list of system accounts to check whether the system configure the operating rights of the system account according to the principle of least privilege
Expected results: The system reasonably configures account permissions.

Test number: T-1-5
Test proposal: Fundamental component security – firewall
Test pre-condition: 1. The documentation about the security configuration used by the service system 2. The network where the client is located can access the sever to be tested
Execution steps: 1. The tester reviews the firewall configuration and checks that the firewall is correctly configured with the access control list. 2. The tester reviews the firewall configuration and check whether the firewall prohibits unnecessary network service access.
Expected results: 1. The firewall sets access control list correctly. 2. The firewall prohibits unnecessary network service access.

Test number: T-1-6
Test proposal: Fundamental component security – security domains
Test pre-condition: 1. The documentation about the security configuration used by the service system 2. The network where the client is located can access the sever to be tested
Execution steps: 1. The tester checks the network topology diagrams and router/firewall configurations to detect whether the system has been divided into security domains, and the security domain has been isolated.
Expected results: 1. The system has been divided into security domains. 2. The security domain has been isolated

Test number: T-1-7
Test Proposal: Fundamental Component Security – security protocols
Test pre-condition: 1. The documentation about the security configuration used by the service system 2. The network where the client is located can access the sever to be tested
Execution steps: 1. The tester captures the communication data between the client and the server, and detects whether the encrypted network protocols are used in the communication data.
Expected results: The encrypted network protocols have been implemented with hyper text transfer protocol secure (HTTPS).

9.2 Information inquiry

Test number: T-2-1
Test proposal: Security of authentication during information query – data packet tamper-proof
Test pre-condition: 1. The documentation about the security configuration used by the service system 2. The network where the client is located can access the sever to be tested
Execution steps: 1. The tester tries to simulate normal user to query information 2. The tester intercepts the communication data packet between the client and the server in the process and modifies it arbitrarily 3. The tester checks whether the server discards the modified packet
Expected results: The system discards the modified packet.

Test number: T-2-2
Test proposal: Security of authentication during information query – second authentication
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester tries to simulate a normal user to query information. 2. The tester checks whether he can receive the message about secondary authentication (such as SMS verification code or service password).
Expected results: The system will perform secondary authentication before the user querying the call record.

Test number: T-2-3
Test proposal: Security of authentication during information query – account locked
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester attempts to input incorrect identity information (such as incorrect username or passport) repeatedly (such as more than 5 times) for secondary authentication. 2. The tester detects if the service system has locked the account (e.g., login failures more than three times).
Expected results: 1. The system has locked the account when authentication failures more than three times.

Test number: T-2-4
Test proposal: Security of authentication during information query – key data tamper-proof
Test pre-condition: 1. The documentation about the security configuration used by the service system 2. The network where the client is located can access the sever to be tested
Execution steps: 1. The tester checks the security document to see if there are measures to prevent tampering of key information. 2. The tester intercepts the data packets between the server and the client and modifies them, then replays them. 3. The tester checks whether the data packets have been verified on the server-side and client-side
Expected results: The data packets have been verified.

9.3 Commodity purchase

Test number: T-3-1
Test proposal: Security of commodity purchase – transaction information encrypted
Test pre-Condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester tries to simulate the process of normal commodity purchase. 2. The tester captures the communication data packet between the client and the server in the process. 3. The tester checks whether the key information (including the user ID, commodities type and commodities amount) in the communication data protection is encrypted by an industry-accepted algorithm.
Expected results: The key transaction information in the data packet has been encrypted.

Test number: T-3-2
Test proposal: Security of commodity purchase – abnormal behaviours monitor
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester tries to simulate the normal process of commodity purchase. 2. The tester intercepts, modifies, forward and replays data packets between server and client sides to simulate the abnormal process, including suddenly massive payments, repeated payment requests and cancellations, a large number of orders without pay and so on. 3. The tester checks whether the system verifies the transaction process again.
Expected results: The system uses different methods to verify user identity in the transaction process.

Test number: T-3-3
Test proposal: Security of commodity purchase – two-step verification
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester tries to simulate the normal process of commodity purchase. 2. The tester checks whether the confirmation message is received, including SMS, voice call or e-mail, after the payment is completed.
Expected results: The confirmation message is received.

Test number: T-3-4
Test proposal: Security of commodity purchase – notification message
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester tries to simulate the normal process of users buying goods. 2. The tester checks whether receive a notification message (such as SMS, voice call or e-mail) from the system when the process is finished.
Expected results: The notification message is received.

Test number: T-3-5
Test proposal: Security of commodity purchase – total amount recalculated
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester tries to simulate the normal process of commodity purchase. 2. The tester intercepts and modifies the total amount of payment before the client side send to the sever, then, replays the modified data pockets. 3. The tester checks whether the system recalculates the total amount.
Expected results: The system recalculates the total amount of payment.

Test number: T-3-6
Test proposal: Security of commodity purchase – total amount recalculated
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester tries to simulate the normal process of commodity purchase. 2. The tester intercepts and modifies the total amount of payment in the data packets between server and client sides, then, replays the modified data pockets. 3. The tester checks whether the system recalculates the total amount.
Expected results: The system recalculates the total amount of payment.

Test number: T-3-7
Test proposal: Security of commodity purchase – external financial system confirmed
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester intercepts the communication data between the server and the external financial system. 2. The tester checks whether the accomplishment of payment is confirmed between them.
Expected results: The accomplishment of payment has been confirmed between the server and the external financial system

9.4 Subscription service

Test number: T-4-1
Test proposal: Security of subscription service – identity confirmation
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester simulates users to change a subscription through the system. 2. The tester detects whether the system authenticates the user who modifies the subscription service.
Expected results: The system confirms the user's identity, by SMS verification code, or service password.

Test number: T-4-2
Test proposal: Security of subscription service – subscription service information
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester completes the entire normal subscription service process. 2. The tester detects whether the system sends subscription service information to remind the users.
Expected results The system sends subscription service information (including the service content, service fee, effective time, expiration time, etc.).

Test number: T-4-3
Test proposal: Security of subscription service – abnormal user behaviours
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester tries to simulate the normal process of the subscription service. 2. The tester intercepts, modifies, forward and replays data packets between server and client sides to simulate the abnormal process in order to simulate abnormal user subscription behaviours including suddenly massive increased or decreased subscriptions, repeated service subscriptions and cancellations, etc. 3. The tester detects whether the system prompts abnormal subscription behaviour.
Expected results: The system monitors abnormal subscription behaviours.

9.5 User identity authentication

Test number: T-5-1
Test proposal: Security of user identity authentication – error message display
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester logged into the system with the wrong user identity or special characters. 2. The tester checks whether the system confuses the error message. 3. The tester checks whether the login error message given by the system contains software-level information.
Expected results: The error message does not contain software-level information.

Test number: T-5-2
Test proposal: Security of user identity authentication – user authentication measures
Test pre-condition: 1. The documentation about the security configuration used by the service system repeatedly. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester logged into the system with the wrong user identity. 2. The tester checks whether the system locks the account after multiple login failures (e.g., more than 3 times). 3. The tester tried to log in to the system again after the system locked the account. 4. The tester records the time that the system can log in again after the account is locked.

Expected results: 1. The system locks the account and prohibits the account from trying to log in again. 2. The duration that the system locks the account should be long enough (for example, no less than 5 minutes).

Test number: T-5-3
Test proposal: Security of user identity authentication – multi-login
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester completes the normal login process. 2. The tester tries to log in to the system again with the same account through another client. 3. The tester checks whether the last login session is still valid.
Expected results: The original login session is no longer valid.

Test number: T-5-4
Test proposal: Security of user identity authentication – static password
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester tried to set a static password. 2. The tester checks whether a static password is required according to the password complexity requirements.
Expected results: The static password meets the password complexity requirements.

Test number: T-5-5
Test proposal: Security of user identity authentication – password change
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester creates a new account and uses this account to log in to the system. 2. The tester detects whether the system authenticates the user who logs in for the first time. 3. The tester detects whether the system forces the user to change the password.
Expected results: 1. The system authenticates the user who logs in for the first time. 2. The system forces the user to change the password.

Test number: T-5-6
Test proposal: Security of user identity authentication – automatic login
Test pre-condition: 1. The documentation about the security configuration used by the service system. 2. The network where the client is located can access the sever to be tested.
Execution steps: 1. The tester visits the authentication page of the system. 2. The tester checks whether there is a graphic verification code or other mechanisms to i man-machine identification on the page.
Expected results: There is a graphic verification code or other mechanisms for man-machine identification on the page.

Bibliography

[b-3GPP TS 33.117] 3GPP TS 33.117 Release 16: 2021(E), *Technical Specification Group Services and System Aspects; Catalogue of General Security Assurance Requirements*.

[b-IEEE 12207] ISO/IEC/IEEE 12207: 2017(E), *Systems and Software Engineering – Software Life Cycle Processes*.

[b-IEEE 15289] ISO/IEC/IEEE 15289: 2019(E), *Systems and Software Engineering – Content of Life-Cycle Information Items (documentation).*

[b-IEEE 15939] ISO/IEC/IEEE 15939: 2017(E), *Systems and Software Engineering – Measurement Process*.

[b-IEEE 16326] ISO/IEC/IEEE 16326: 2009(E), *Systems and Software Engineering – Life Cycle Processes – Project Management*.

[b-IEEE 24748-1] ISO/IEC/IEEE 24748-1: 2018(E), *Systems and Software Engineering – Life Cycle Management – Part1: Guidelines for Life Cycle Management*.

[b-IEEE 24748-2] ISO/IEC/IEEE 24748-2: 2018(E), *Systems and Software Engineering – Life Cycle Management – Part 2: Guide to the Application of ISO/IEC 15288 (System Life Cycle Processes).*

[b-IEEE 24765] ISO/IEC/IEEE 24765: 2017(E), *Systems and Software Engineering – Vocabulary*.

[b-IEEE 26515] ISO/IEC/IEEE 26515: 2018(E), *Systems and Software Engineering – Developing User Documentation in an Agile Environment*.

[b-IEEE 29148] ISO/IEC/IEEE 29148: 2018(E), *Systems and Software Engineering – Life Cycle Processes – Requirements Engineering*.

[b-IEEE 42010] ISO/IEC/IEEE 42010: 2011(E), *Systems and Software Engineering – Architecture Description*.

[b-ISO/IEC 15408-1] ISO/IEC 15408-1: 2009, *Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and General Model*.

[b-ISO/IEC 16085] ISO/IEC 16085: 2006, *Systems and Software Engineering – Life Cycle Processes – Risk Management*.

[b-ISO/IEC 27000] ISO/IEC 27000: 2018, *Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary*.

[b-NIST SP 800-160] NIST SP 800-160 Vol. 1: 2018, *Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*.

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, 2021