International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1146

(10/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (1) – Web security

Secure protection guidelines for value-added services provided by telecommunication operators

Recommendation ITU-T X.1146

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	**X.1140–X.1149**
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed legder technology security	X.1400–X.1429
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1146

Secure protection guidelines for value-added services provided by telecommunication operators

Summary

With the rapid development of network and user-terminal capability, more and more telecom operators provide various services based on their network resources to the users. These services are called value-added services as they add additional value to basic telecommunication services such as voice call, short message service (SMS), multimedia messaging service (MMS) and data access. Typical value-added services include mobile office automation, e-reading, e-commerce, etc. In many cases, the value-added services will involve sensitive operations or critical data, which will be the target of malicious attackers. Malicious users may utilize the service vulnerabilities to get benefits or do harm to the service and other users.

Recommendation ITU-T X.1146 provides secure protection guidelines for value-added services provided by telecommunication operators. In addition to analysing typical service scenarios, security threats and attack methods, Recommendation ITU-T X.1146 provides technical measures to counter threats and attacks. This will help the operators to assure the security of the value-added service and will also protect the users' benefits.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1146	2017-10-14	17	11.1002/1000/13368

Keywords

Protection guidelines, security.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1146

Secure protection guidelines for value-added services provided by telecommunication operators

1 Scope

This Recommendation provides secure protection guidelines for value-added services provided by telecommunication operators. In addition to analysing typical service scenarios, security threats and attack methods, this Recommendation provides technical measures to counter threats and attacks.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 value-added service: A service that is offered in addition to or in conjunction with basic telecommunication services such as voice call, short message service (SMS), multimedia messaging service (MMS) and data access. These value-added services allow operators to drive up their average revenue per user (ARPU). The scope of value-added services in this Recommendation is limited to those provided by telecommunication operators and the servers hosting such services reside in operators' networks. Typical value-added services include mobile office automation, e-reading and e-commerce.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2G second Generation

3G third Generation

4G fourth Generation

API Application Programming Interface

ARPU Average Revenue Per User

ID Identification

IP Internet Protocol

LAN Local Area Network

MMS Multimedia Messaging Service

SMS Short Message Service

SQL Structured Query Language

URL Uniform Resource Locator

WLAN Wireless Local Area Network

5 Conventions

None.

6 Introduction

With the rapid development of network and user terminal capability, more and more telecom operators are providing various services based on their network resources to users. These services are described as value-added services because they add additional value to basic telecommunication services (e.g., voice call, SMS, MMS and data access).

The structure of value-added services is shown in Figure 6-1.

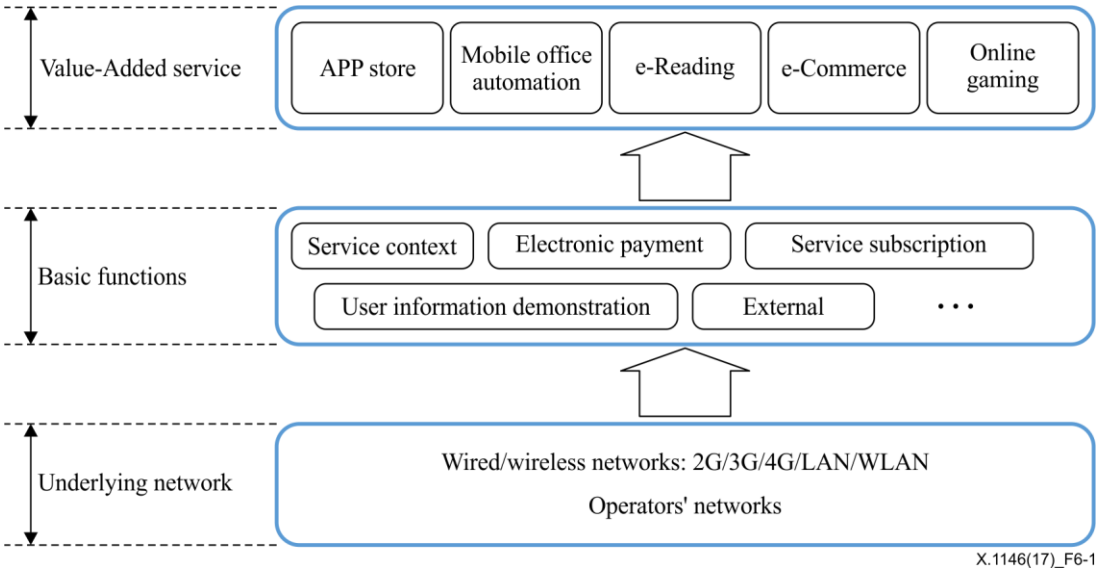

Figure 6-1 – Structure of value-added services

In many cases, value-added services involve sensitive operations or critical data that are targets of malicious attackers. Some typical scenarios are:

– Subscription, alteration and unsubscription of service.

  These operations usually contain sensitive data (e.g., type and amount of service or service order). Attacks on these data harm client benefits and lead to user complaints.

– Electronic payment of service.

  Electronic payment is very common in e-commerce. Cash and purchase data can attract attackers.

– Display of user information

  Such a scenario typically occurs during service queries. User information is displayed as the result of a query. Some user information is extremely valuable and must be strictly protected.

– Application interface to the external platform.

  The application programming interface (API) expresses an application component in terms of its operations, inputs, outputs, etc. An API makes it feasible to develop a program by external developers. It also provides an entry point for external attacks.

Malicious users can exploit service vulnerabilities to divert benefits or do harm to the service and other users. The negative effects of malicious attacks can include:

– service subscription without user permission;

– service use without payment;

– access to valuable user information without user authorization.

In order to protect user rights and operator benefits, telecommunication organizations are responsible for providing sufficient security protection for their value-added services.

To guarantee the security of value-added services, five different areas should be considered.

1) **Network topology security**: servers that provide value-added services should be deployed in well-designed network security domains and appropriate security measures should be taken.

2) **Equipment or operating system security**: network equipment should be securely configured and protected, while the operating system of the servers should be carefully configured.

3) **Platform or software security**: the vulnerabilities of software platforms and third-party components, generally used in the development of value-added services, directly affect service security.

4) **Service process security**: a series of operation sequences designed to implement the service function. The security mechanisms of all operation sequences should be sufficient to ensure service security.

5) **Terminal security**: Users need to access services using different terminals, such as personal computers, tablet computers and mobile phones, whose security protections are also essential to service security.

The security of the first three levels 1) to 3) and 5) is related to common hardware and software security, for which many security guidelines can be followed. As for 4), comprehensive guidelines are absent at the time of publication. Consequently, this Recommendation focuses on security protection of the service process.

7 Typical scenarios for value-added services

7.1 User identity authentication

User identity authentication is a method of confirming the user's identity. According to the verification result, the value-added service reacts appropriately. Generally speaking, there are mainly three ways of verifying a user's identity, based on:

– what the user knows, e.g., a password (static);

– what the user has possession of, for example, a smart card, a SMS password, a universal serial bus key or a dynamic password;

– who the user is, based on unique physical characteristics, e.g., fingerprints, handwriting, DNA, retinal imaging and body biometrics.

The general process of user authentication is shown in Figure 7-1.

– Authentication information

The user identity and authentication information are sent to the service server from the client-side.

– Authenticate

The service system authenticates the information from the user-side.

– Authentication result

The service server sends the user authentication result to the user-side. If the authentication fails, reject information is returned; if the authentication succeeds, the return is a user authentication credential.

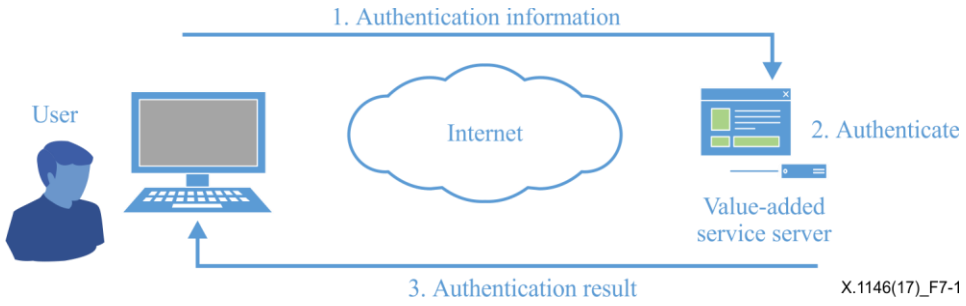

Figure 7-1 – User authentication process

7.2 Subscription service

Value-added services generally provide different kinds of service or service packages to meet the various needs of users. Users can change their choices through a subscription service, including service subscription and service unsubscription.

An ordinary process of order service is:

– User chooses service

User chooses a certain service on the webpage or sends an SMS code to the service subscription number.

– System accepts the service subscription

The service system accepts the user's choice. If the service needs to be paid, refer to the payment scenarios in clause 7.3.

– System initiates service

Service system informs the user that the service subscription is successful. According to the service agreement, the service is provided on schedule.

7.3 Payment for service

Users generally need to pay for the services. The payment methods are mainly of two types: pre-payments and post- payments.

7.3.1 Pre-payments

Users pay for the service before using it, usually through third parties' online electronic payment, e.g., credit cards.

Users can pay for just one service at a time; a single payment for a number of services is also acceptable.

7.3.2 Post-payments

For some services, users need not pay immediately. The fee for services is included in the user's phone bill and payment is made according to the billing cycle. Settlement methods include the purchase of prepaid cards, as well as electronic and cash payments.

7.4 User information demonstration

User information includes personal information recorded by the service system, as well as service operations and ordering information. User information includes:

– user ID;
– associated phone number, email address, etc.;
– address information;
– identification card number;
– order number;
– receipt number;
– operational information.

A user information demonstration indicates the scenario in which the user information needs to be displayed on system interfaces (especially graphical user interfaces).

7.5 Application interface to the external platform

In order to provide more extensive services, value-added service systems need to interact with other systems via external interfaces. According to the direction of information flow, external interfaces can be divided into two types: external data application and data release.

For external data applications, the value-added service system initiates data acquisition.

For data release, the external system initiates data acquisition.

The basic process of applications interfacing with external platforms is shown in Figure 7-2.

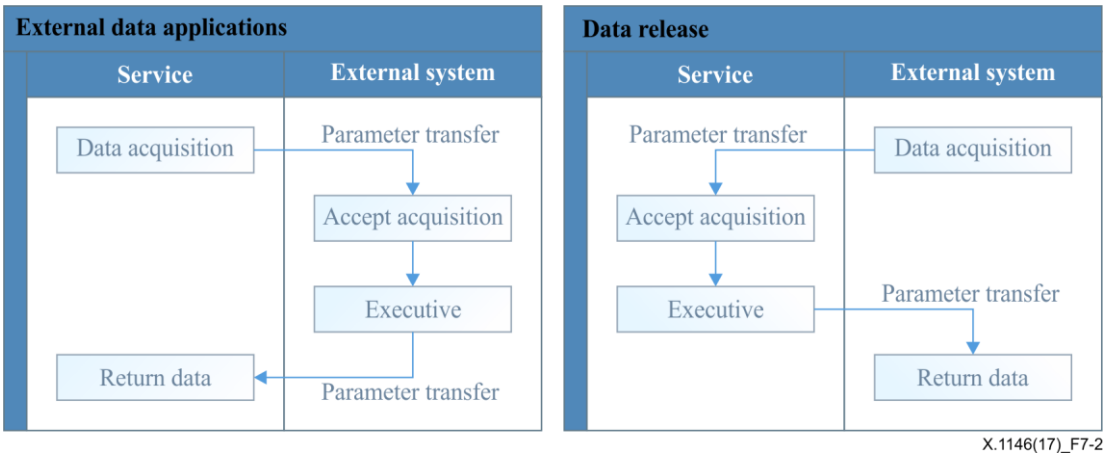

Figure 7-2 – Process of applications interfacing with external platforms

7.6 Password retrieval

The service system usually provides a retrieval function in case users forget their passwords. Typical password retrieval procedures are depicted in Figure 7-3.

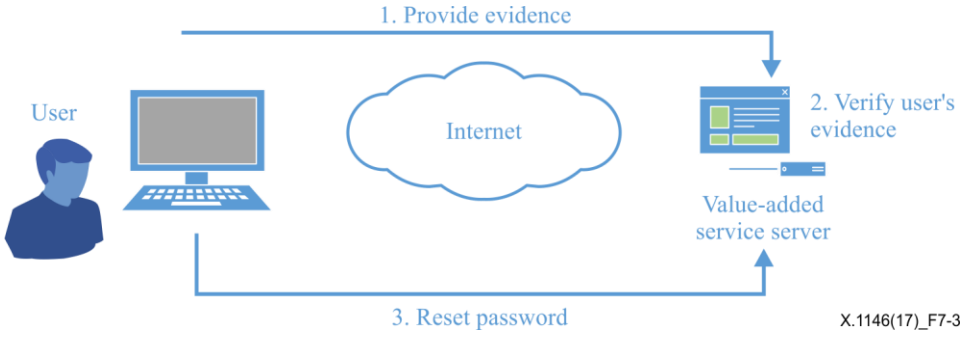

Figure 7-3 – Process of password retrieval

– User provides evidence

In order to retrieve the password, the user needs to provide some evidence to prove ownership of the account. Optional evidence is as follows:

- phone number

  The service system sends an SMS verification code to the user's phone number. If the phone number is valid, the user usually can input the verification code into a dialogue box on the web page.

- e-mail box

  The service system sends a password reset link to the user's email address. If the mailbox is valid, the user can log in and access the password reset link.

- Important information about the user

  Some important information about the user, e.g., identification numbers, registered address, as well as registered question and answer.

- Service use information

  Recent service use information, e.g., recent orders and current service types.

– System verifies user evidence

The service system verifies the evidence provided by the user. If the verification is successful, the service system provides the address of the password reset web page. If not, the password retrieval request is refused.

– Reset password

The user resets the password and the service system is updated accordingly.

8 Threats to value-added services

8.1 Threats to user identity authentication

8.1.1 Fake identity

By disguising themselves as normal users logging in to the service system, attackers can use value-added services apparently as a legal user.

There are two methods by which attackers can log into the service system using a fake identity (see clauses 8.1.1.1 and 8.1.1.2).

8.1.1.1 Password exhaustion

For a service system that supports static passwords, attackers can try to disguise themselves as normal users by guessing passwords for specific user accounts using various combinations of characters. For example, for a four digit password that is composed of digits only, there is a total of 10 000 kinds of digital combination. After a maximum of 9999 real attempts, the attacker can find the real password and log into the service system using the normal user's identity.

8.1.1.2 Account exhaustion

Value-added services offered by telecom operators usually use users' phone numbers as log-in IDs. This means that users' log-in accounts can be guessed. This reduces the difficulty for attackers to obtain the correct information about user account and password pairs. Attackers can use a small number of commonly used weak passwords (such as "123456") and continually change user account names (i.e., the phone numbers) and try to log into the service system. By this means, attackers can quickly obtain a large number of user account and password pairs. Based on these accounts, they can log into the service system using normal user identities.

8.1.2 False authentication

Usually, the user authentication module of the service system compares the log-in information submitted by the user with the information stored in the system database. If they are consistent, user authentication succeeds. In some cases, if there are implementation defects in the authentication module, attackers can carefully construct the log-in information and cheat the authentication module into producing false authentication results.

Structured query language (SQL) injection attack is a common method of doing this. Attackers insert an SQL command into the user's authentication credentials, to cheat the authentication module into executing it and producing false authentication results.

For example, "--" is a comment symbol in SQL. According to SQL semantics, statements after "--" are neglected. On the log-in interface, attackers can enter the user ID "admin--" and password "123". When the log-in information is submitted to the service system and the authentication module executes the authentication by comparing it to the SQL statement in the database (such as "SELECT COUNT(*) FROM Login WHERE UserName='admin'--' AND Password='123'"), the password comparing statement after the "'admin'" is neglected. Subsequently, user authentication will always succeed for the account "admin".

8.1.3 Authentication result tampering

After a user has submitted log-in information and the authentication module has authenticated it, the result needs to be returned to the client-side. The service client accepts or rejects the user request, based on the authentication result. In some cases, an attacker can intercept and modify the authentication result and return an authentication result that has been tampered with to the client. The attacker can bypass identity authentication by this means.

8.1.4 Session attack

In order to maintain a user's state, the client-side must send a unique identification (session ID) to the server-side. For the server-side, the unique ID is used to authenticate the user. The session ID is therefore a piece of information at risk for a web-based service.

In session-based attacks, the attacker first captures a legitimate user session and then impersonates that user to access the system. Therefore the attacker must first obtain a valid session ID of a normal user. There are several ways for attackers to do this, including:

– Brute force crack: Attackers try a variety of session IDs, until the correct session ID is found.

– Prediction analysis: If the session ID is produced in a non-random way, it is possible to be calculated and predicted.

– Sniffer: Use a network sniffer to steal the session ID information.

– Cheat: The attacker lures a normal user to use a specified session ID through different ways such as a hyper link in an email or a SMS, XSS attacks, etc.

After obtaining a user's session ID, attackers can logon to the user's account and use the valid session of the user.

8.2 Threats to service subscription

8.2.1 Subscription information tampering

When a user subscribes to a service, the subscription information (including the service type and subscription user) needs to be sent from the client-side to the server-side. Subscription information is at risk of tampering by attackers.

There are different ways in which an attacker can tamper with subscription information:

– User information tampering: the attacker modifies subscription user data, ordering the service for another user without the legitimate user's knowledge.

– Service type tampering: the attacker modifies the service type, ordering another service for the user without the user's knowledge.

8.2.2 Subscription repudiation

After subscribing to a service, a malicious user may deny having taken out the service subscription.

8.3 Threats to service payment

8.3.1 Payment amount tampering

In the payment process, an attacker can try to tamper with payment information in order to obtain more services at lower cost. Different ways of tampering with payment information include:

– Service price: Modification of the service price, to access the service with a lower amount to pay.

– Freight: Some services include shipping charges (total payment consists of service price plus freight cost). If the attacker can modify the freight cost, the total payment amount can be lowered. In particular, if the freight cost can be modified to a negative number, the amount to be paid can be reduced to zero.

– Service type: The attacker may first choose a service of a lower price and then modify the submitted service type to another service at a higher price. Then the attacker has access to higher value services at lower prices.

8.3.2 Payment bypass

In many cases, after a user's payment process is completed, the client-side sends a payment success message to the server-side. When the service system receives the payment success message, the payment process is flagged as successful in the system. If an attacker can forge a payment success message and send it to the server-side, the payment process can be bypassed.

The attacker usually bypasses the payment process in the following way.

The attacker first completes a normal payment process and intercepts the payment success message sent from the client-side to the server-side. During the next payment process, the attacker does not pay, but sends the payment success message of the preceding payment process to the server-side. If the server-side is not well implemented, the attacker completes the payment process without any cash transfer. The attacker can also modify the parameters of the payment success message to adapt to different situations.

8.4 Current examples of threats to user information

8.4.1 Revelation on a terminal

There are two circumstances under which user information can be revealed on a terminal:

– when user information is displayed on a user's terminal, it is seen by others;

– when an employee of an operator handles a user's service demand (e.g., service subscription or service inquiries), user information may be displayed on the employee's terminal and be seen by the employee or another person nearby.

8.4.2 Transmission interception

User information can be obtained by attackers during transmission between the service system server and the terminal. If the information is not encrypted or if the encryption can be cracked easily, user information can be intercepted without authorization.

8.4.3 Information acquisition without authorization

Usually, user information is not stored on the terminal-side. When the user queries the information, the terminal sends a request message to the system server. There is usually a parameter in the request message that specifies the user ID. If the user ID sent to the server is figured out, attackers can forge the request message of the user and try to obtain the user's information. User information includes:

– user ID parameter;
– phone number;
– email address;
– predictable user session ID.

SQL injection can also be used to obtain user information without authorization.

8.5 Threats to an application interface with an external platform

8.5.1 Illegal input

Attackers can construct special API input data (e.g., overlong parameters, special SQL statements, special scripts) that can result in system crash, data leakage or privilege escalation.

8.5.2 Replay attacks

Attackers can capture the normal message packet sent by an external system to a service system via the API and then replay it to the service system. If the service system handles the replayed message as normal, there may be the following consequences:

– if the packet is the authentication data sent by the external system, attackers can be authenticated by the service system and interact as a normal external system via the API;
– if the packet is used to send a message (e.g., an SMS or e-mail) to users, then it is possible to cause an SMS bomb or e-mail spam.

8.6 Threats to password retrieval

8.6.1 Evidence cracking

During the password retrieval process, a user needs to provide evidence and prove ownership of the account. Attackers can reset the user's password by cracking the evidence and pretending to be the user. The following situation can result in evidence cracking:

– the user address is too simple, e.g., it only includes the city, without any detailed street information;
– the answer to a secret question is easy to guess, e.g., "Who is your favourite National Basketball Association star?";
– the answer to an evidence question has multiple options whose range is not wide enough, meaning attackers can guess or brute force the answer.
– the SMS verification code, generally a 4–6 bit digital code, can be brute forced and is thus at risk of being cracked in a short time.

8.6.2 Evidence forgery

To retrieve a password via e-mail, the user receives a uniform resource locator (URL) link. The password is reset by clicking on the link. There is usually a parameter in the link that specifies the user ID. If the parameter is not encrypted, attackers can forge the password reset link and reset any user's password.

For example, the password reset link may be "http://www.xx.com/resetpwd/qid=123456", in which the value of "qid" is the user ID number in the service system. The attacker can reset another user's password by modifying the link to "http://www.xx.com/resetpwd/qid=123567".

8.6.3 Authentication on the user-side

In order to authenticate the user correctly, the verification operation should be executed on the server-side. If the authentication is wrongly designed to be carried on the user-side, the attacker can reset the password of any other user by forging the verification result and sending it to the server-side.

9 Protection measures

To prevent the security threats described in clause 8, the protection measures described in clauses 9.1 and 9.2 should be adopted in the process of supplying value-added services.

9.1 Basic protection measures

In order to ensure the security of value-added services, some basic protection measures can be used. These basic protection measures can be used in different service scenarios.

9.1.1 Confirm measures

Critical operations in the service process should be confirmed for a second time by users to prevent unauthorized operation. For the second confirmation, a different authentication method is needed. For example, if the user is authenticated by user name and password, an SMS verification code can be used for the second confirmation when an order is placed.

Critical operations refer to modification or viewing of information sensitive to the user, including service subscriptions, service types, services to unsubscribe from, payment information and changes of password.

The second confirmation method could be as follows:

– an SMS verification code;
– an e-mail verification code and hyperlink;
– a voice verification code via call-back;
– intelligent questions.

The user second confirmation process should be recorded in detail in the system log for later retrieval if needed.

9.1.2 Tamper-proof measures

For information exchange between the user- and server-sides, at least one of the following security measures should be adopted.

– Usage of cryptographically protected network protocols that incorporate sufficient security measures and whose versions contain no known vulnerabilities.
– Encryption by industry-accepted algorithms.

The use of tamper-proof measures is especially valuable for protection of key data, including:

– user password;
– payment amount;
– business type;
– user information;
– authentication result;

– etc.

9.1.3 Information check measures

All data input from the outside can be forged by the attacker. Therefore, it is necessary to validate, filter and encode input data before it is used by the service system.

External data include:

– URL;

– user input data;

– the user selection, including packages and prices; e.g., the price of a user's subscription should be checked against service choice and quantity;

– API input data.

9.1.4 System analysis measures

Analysis measures should be taken to identify service abuses that the protection measures described in clauses 9.1.1 to 9.1.3 cannot prevent.

Analysis measures focus on the abnormal business operations, including:

– a high number of failed log-ins using the same account or using different accounts from the same Internet protocol (IP) address;

– frequent business operations within a short period of time, e.g., changing the service many times a day;

– a sudden surge in activity, such as an atypical increase in number of orders for a certain service;

– a large number of business operations from the same IP address or area;

– a periodical audit of the use of the service, e.g., by comparing the total number of service subscriptions to payments received, is recommended.

9.1.5 Session security measures

To protect user sessions, the service system shall support the following session ID and session cookie requirements:

– the session ID shall uniquely identify the user and distinguish the session from all other active sessions;

– the session ID shall be unpredictable and regenerated for each new session (e.g., each time a user logs in);

– the session ID shall not contain user information and authentication information in clear text and shall be terminated automatically after a configurable maximum lifetime;

– other security requirements for the particular session configuration (e.g., the attribute "HttpOnly" shall be set to "true" and only accept server generated session IDs).

9.1.6 User information protection measures

In the process of displaying, using and storing user information, the following protection measures should be taken to prevent user information leakage:

– replacement of characters in user information by special characters when such information is sent to the terminal, if possible; e.g., the social security number "123456789" could be sent as "123***789";

– encryption of user information stored in database;

– detailed logging and periodic audit of any view, exportation or modification of user information.

9.1.7 User-side application restriction measures

Due to security uncertainties concerning the user-side, its capabilities should be restricted. In particular, user information authentication and API-based interaction should not be executed on the user-side.

– User information authentication: information for verification of the user should be sent to the server-side for authentication.

– API-based interaction: the server-side should be responsible for API-based interaction. For example, payment confirmation should be made by the server-side and the external financial system.

9.1.8 Interaction protection measures

To prevent replay attacks, message transmissions between the user-side and server-side should adopt at least one of the following security measures.

– Time-stamp

  A time-stamp is added to each message and the receiver accepts only packages stamped with a predetermined time.

– Sequence number

  A serial number is added to each message and an algorithm dedicated to building increments is negotiated in advance. The freshness of the message is the criterion whether to accept it in the interaction. Messages not complying with the incremental algorithm are discarded.

– Other protection measures that can identify replay messages.

9.2 Protection measures for typical scenarios

9.2.1 User identity authentication

Protection measures for this scenario focus on authenticating valid users of the service system:

– transmission of authentication information exchanged between the user-side and the server-side by using cryptographically protected network protocols or encryption by industry-accepted algorithms;

– information input by the user and the URL should be checked to prevent malicious input;

– each character in the password should be displayed as "*" on the terminal;

– after authentication, generation of a new session ID for the user complying with session security requirements;

– implementation of interaction protection measures to avoid replay attacks.

9.2.2 Subscription to service

Protection measures for this scenario focus on ensuring that service operation results from the user's own volition. Such measures also aim to impede malicious service operations of particular users. Protection measures include:

– an "authentication code" requirement for service ordering, which can ensure that the operation originates from human beings, not machines;

– a second confirmation method requirement to confirm service operation;

– transmission of user subscription information by using cryptographically protected network protocols or encryption by industry-accepted algorithms;

– limitation of the number of daily business orders from the same phone number.

9.2.3 Payment of service

Protection measures for this scenario focus on abuse of the billing point. Protection measures include:

– If the user places an order by the wireless application protocol or worldwide web, a two-step verification of the service order is required. A different authentication method (e.g., based on an SMS) should be used for the confirmation.

– Technical means are required to monitor abnormalities in service fee in a timely manner.

– When the type of service is changed, the user should receive an alert.

– A check of the cost of a user's subscription, based on, for example, the content and quantity ordered by the user, is required.

– Payment requires confirmation by interaction of the server-side and the external financial system.

9.2.4 User information demonstration

Protection measures for this scenario focus on the transmission and demonstration of users' personal information. Protection measures include:

– transmission of users' personal information by using cryptographically protected network protocols or encryption by industry-accepted algorithms;

– replacement of sensitive textual information by special characters when displayed on a terminal;

– auditing the query and modification operations of customer information;

9.2.5 Application interface to an external platform

Protection measures for this scenario focus on the information input via the API. Protection measures include:

– checking the source of the data input into the API – a black/white list can be used to assist in the judgement;

– discarding abnormal parameter input to the API, which is beyond the design scope and sending a uniform message to ensure that sensitive internal information is not disclosed.

– ensuring that interactions with external platforms are performed on the server-side.

9.2.6 Password retrieval

The control measures for this scenario focus on the evidence provided by the user. Protection measures include:

– transmission of retrieval information exchanged between the user-side and the server-side by using cryptographically protected network protocols or encryption by industry-accepted algorithms;

– checking of information input by the user and the URL to prevent malicious input;

– when a user sets a simple password retrieval answer, alert the user to change it;

– strict verification of all evidence provided by the user;

– generation of a new session ID complying with session security requirements after user evidence verification;

– implementation of interaction protection measures to avoid replay attacks.

Bibliography

[b-ITU-T X.1154] Recommendation ITU-T X.1154 (2013), *General framework of combined authentication on multiple identity service provider environments*.

[b-ITU-T X.1158] Recommendation ITU-T X.1158 (2014), *Multi-factor authentication mechanisms using a mobile device*.

[b-ITU-R M.1224-1] Recommendation ITU-R M.1224-1 (2012), *Vocabulary of terms for International Mobile Telecommunications (IMT).*

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2018