International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 17

(09/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1143 – Supplement on threats and security objectives for enhanced web-based telecommunication services

ITU-T X-series Recommendations – Supplement 17

ITU-T
International Telecommunication Union

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	
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	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	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
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

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

Supplement 17 to ITU-T X-series Recommendations

ITU-T X.1143 – Supplement on threats and security objectives for enhanced web-based telecommunication services

Summary

Supplement 17 to the ITU-T X-series Recommendations describes threats to, and security objectives for, enhanced web-based telecommunication services using technologies such as Web 2.0 and mashups. Threats to enhanced web-based applications are identified, as are threats to traditional web-based applications. Moreover, security objectives for enhanced web-based application services are provided.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X Suppl. 17	2012-09-07	17

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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

Supplement 17 to ITU-T X-series Recommendations

ITU-T X.1143 – Supplement on threats and security objectives for enhanced web-based telecommunication services

1 Scope

This supplement describes threats to, and security objectives for, enhanced web-based telecommunication services using technologies such as Web 2.0 and mashups. There are many web service standards and web service security standards. These are partially developed by vendors and service providers, and not organized. This supplement provides an overview of the threats to, and security objectives for, enhanced web-based telecommunication services and is a baseline document for designers or implementers to analyse the vulnerabilities of web application services and to consider and improve the security aspects of web applications. The threats identified for enhanced web-based applications are not the only ones being investigated, but also those of traditional web applications, as these are still potential threats to enhanced applications. Moreover, the security objectives provided cope with the threats and would be applied to wired/wireless web-based application services.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This supplement uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.3 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.4 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

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

3.1.6 data origin authentication [b-ITU-T X.800]: The corroboration that the source of data received is as claimed.

3.1.7 hypertext markup language (HTML) [b-ITU-T M.3030]: A system of coding information from a wide range of domains (e.g., text, graphics, database query results) for display by World Wide Web browsers. Certain special codes, called tags, are embedded in the document so that the browser can be told how to render the information.

3.1.8 privacy [b-ITU-T X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

3.1.9 repudiation [b-ITU-T X.800]: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.2 Terms defined in this supplement

This supplement defines the following terms:

3.2.1 authentication: A process used to achieve sufficient confidence in the binding between the entity and the presented identity.

NOTE – Use of the term authentication in a web-based service context is taken to mean entity authentication.

3.2.2 JavaScript Object Notation (JSON): A lightweight, text-based, language-independent data interchange format.

3.2.3 mashup: A web application that combines content (data and code) or services from multiple origins to create a new service.

3.2.4 Web 2.0: Web technology and applications that facilitate participatory information sharing, interoperability, user-centred design and collaboration on the World Wide Web (WWW).

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

API	Application Programming Interface
CSRF	Cross-Site Request Forgery
DOM	Document Object Model
DoS	Denial of Service
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Security
JSON	Javascript Object Notation
MitB	Man-in-the-Browser
MitM	Man-in-the-Middle
OOP	Object-Oriented Programming
PKI	Public Key Infrastructure
REST	Representational State Transfer
RSS	Really Simple Syndication
SDU	Service Data Unit
SNS	Social Networking Service
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
URL	Uniform Resource Locator
WS	Web Service
WWW	World Wide Web
XML	eXtensible Markup Language
XSS	Cross-Site Scripting

5 Conventions

None.

6 Introduction

The benefits of web services have an important effect on human societies and become a part of human lives. Enhanced web-based technologies, such as Web 2.0 and mashups, are trends in the use of WWW technology that aim to facilitate creativity, information sharing and collaboration among users. The major technical changes of the trends are asynchronous script, data syndication, an open application programming interface and mashup. Although web designers and implementers support the interoperability among these technologies and service, the interoperability is not complied with. It is the same situation in the case of security standardization.

In Web 2.0, composite services are called mashups. A mashup is a web application that combines data from more than one source into a single integrated tool. Figure 1 is an example of the mashup service. Content used in mashups is typically sourced from a third party via a public interface or API. When a non-secure service and a secure service converge into a mashup service, the mashup service is influenced by an attacker. Figure 1 gives an example of why the security levels of every web service and domain conforming to the mashup should be provided equally. If the real estate web site is unsecure, the whole mashup service and domain would not be secure and the other parts of the service network would be gradually affected.

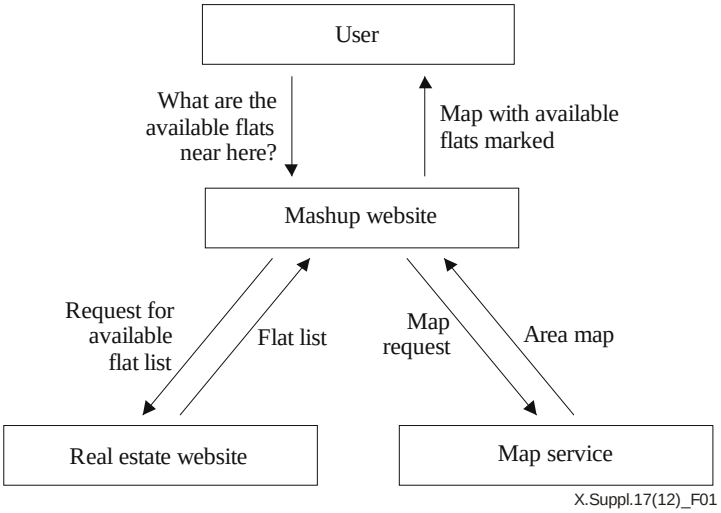

Figure 1 – Example of a mashup service

7 Architecture of enhanced web-based telecommunication services

Enhanced web-based technologies are being applied to telecommunication services since they enable developers to efficiently and cost-effectively develop and deploy new services, and to easily and rapidly integrate content from a variety of sources to form composite services.

Figure 2 illustrates the architecture of an enhanced web-based convergence service. Web 2.0 services provided by the third party on the Internet, and services provided by the network operator in the telecommunication domain, are combined to provide a convergence service using mashup. A user of the mashup client can check the presence of a friend and find their location via the mashup server that invokes the presence server and location server in the telecommunication domain. The mashup client can find their geographic location on the map using the Web 2.0 service that provides a map service. The client can also access the user profile provided via the mashup server. Web protocols such as representational state transfer (REST) [b-Fielding], simple object access protocol (SOAP) [b-W3C] and really simple syndication (RSS) [b-RSS] are used for such mashups.

The core network gateway provides access to the network elements of the network operator. An example of the core network gateway is the Parlay/OSA gateway [b-GSMA] employed to link applications by exploiting the Parlay/OSA APIs with the existing network elements. The Parlay/OSA gateway consists of several functional entities that provide Parlay/OSA interfaces to the applications. The Parlay/OSA gateway is under the control of the network operator or service provider, and is a single point through which all Parlay/OSA interactions pass. If the telecommunication application server does not provide support of a web protocol, then the mashup server can call functional objects using such a gateway.

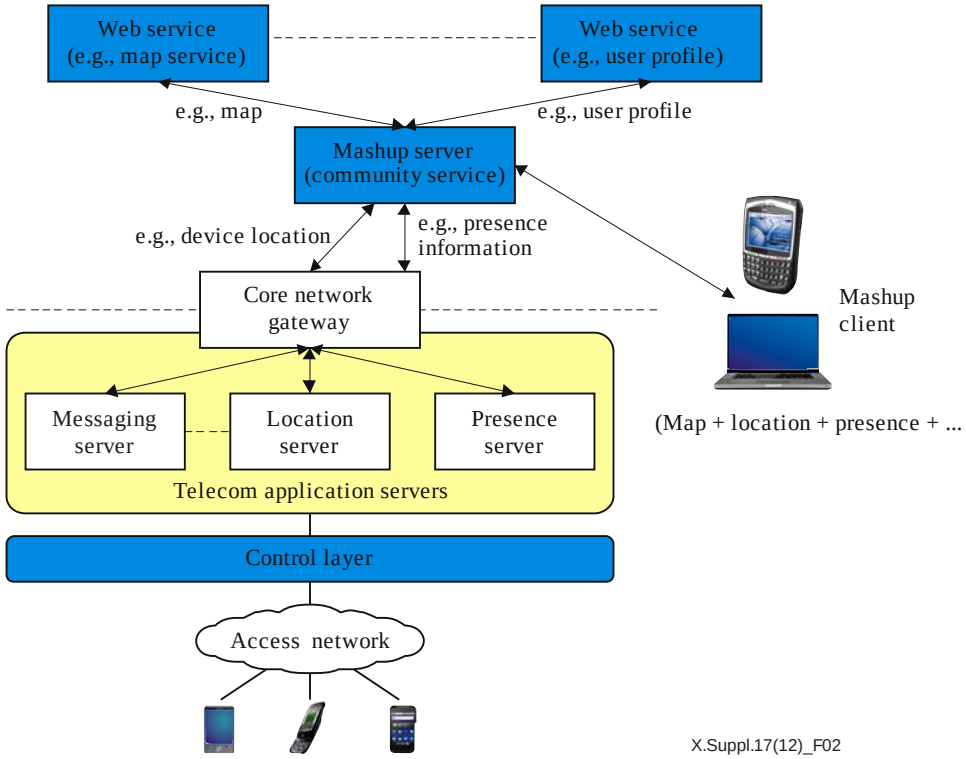

Figure 2 – Architecture of the enhanced web-based convergence service

8 Threats of enhanced web-based telecommunication services

Threats have been classified into five categories: general security threats, security threats to asynchronous script, security threats to web APIs, security threats to data syndication and security threats to mashups.

8.1 General security threats

8.1.1 Denial of service (DoS)

Denial of service occurs when an entity fails to perform its proper function or acts in a way that prevents other entities from performing their proper functions. One example of denial of service would be overwhelming the server with requests that either require excessive processing or consume excessive resources.

8.1.2 Eavesdropping

Eavesdropping involves viewing information that should not be viewed, either by examining messages in transit or by examining the content stored in a server.

8.1.3 Man-in-the-browser

A Man-in-the-browser (MitB) attack will be successful irrespective of whether security mechanisms, such as secure socket layer (SSL)/public key infrastructure (PKI) and/or two or three factor authentication solutions, are in place or not.

8.1.4 Man-in-the-middle

A form of Internet threat related to man-in-the-middle (MitM) is a Trojan that infects a web browser and has the ability to modify pages, modify transaction content or insert additional transactions, all in a completely covert fashion that is invisible to both the user and the host application. A man-in-the-middle attack is an attack whereby an attacker is able to read and modify, at will, the messages between two parties without either party knowing that the link between them has been compromised.

8.1.5 Masquerade

In a masquerade, an entity pretends to be a different entity. An authorized entity with few privileges may use a masquerade to obtain extra privileges by impersonating an entity having such privileges.

8.1.6 Modification of messages

The modification of a message occurs when the content of a data transmission is altered undetected, thereby resulting in an unauthorized effect.

8.1.7 Repudiation

A repudiation attack happens when an application does not adopt controls to properly track and log users' actions, thus permitting malicious manipulation or forging the identification of new actions. This attack can be used to change the authoring information of actions executed by a malicious user in order to log wrong data to log files. Its usage can be extended to general data manipulation in the name of others, in a similar manner as spoofing mail messages. If this attack takes place, the data stored on log files can be considered invalid or misleading.

8.1.8 Replay

A replay occurs when a message, or part of it, is repeated to produce an unauthorized effect.

8.2 Security threats to asynchronous script

Asynchronous script is a group of interrelated web development techniques used for creating interactive web applications or rich Internet applications. With asynchronous script, web applications can retrieve data from the server asynchronously in the background without interfering with the display and behaviour of the existing page. This feature is enabled by XMLHttpRequest and JavaScript object notation [b-JSON]. XMLHttpRequest is an API that allows client-side scripting language to make HyperText Transfer Protocol (HTTP) connections to remote servers and to exchange data, such as plain text, eXtensible Markup Language (XML) or JSON. JSON is a lightweight, text-based, language-independent data-interchange format. It defines a small set of formatting rules to create a portable representation of structured data.

8.2.1 Exploiting silent transactions

Any system that silently processes transactions using a single submission is dangerous to the client. For example, if a normal web application allows a simple uniform resource locator (URL) submission, a preset session attack will allow the attacker to complete a transaction without the user's authorization. In asynchronous scripting language, the transaction is silent; it happens with no user feedback on the page, so an injected attack script may be able to behave maliciously in the client's web applications or browser without authorization.

8.2.2 Cross-site request forgery (CSRF)

A cross-site request forgery (CSRF) attack causes a victim to unwillingly submit one or more HTTP requests to a vulnerable website. A typical cross-site request forgery attack compromises data integrity; it gives an attacker the ability to modify information stored by a vulnerable website. When a web application requires user authentication, it often does not require the user to type in their password for every HTTP request. Instead, web applications track users' authentication states between multiple HTTP requests by tokens such as session cookies or the HTTP authorization header. However, there can be a problem with this approach; modern web browsers memorize the tokens associated with URLs and automatically attach the token when a new HTTP request is issued to the server, even if the request is not intended by the user. Cross-site request forgeries take advantage of this browser behaviour. With CSRF, a user just needs to visit a malicious website the web pages of which can include scripting language logic that issues (potentially hidden) HTTP requests to other web servers (such as the user's bank), and those HTTP requests might be authorized by the web server because of the presence of the tokens. CSRF enables various kinds of attacks, such as sending e-mail from a web-based mail service, posting a comment to a blog on the user's behalf, altering a user's buddy list in a social networking service (SNS) or changing settings in a home router.

8.2.3 Cross-site scripting (XSS)

A cross-site scripting (XSS) attack is a type of attack where trusted content is injected with malicious code. XSS attacks can be used to steal session cookies, access restricted information, rewrite parts of the page or even act as a user of the browser.

8.2.4 JSON hijacking

JavaScript object notation (JSON) hijacking builds upon cross-site request forgery attacks and compromises confidentiality; an attacker can read a victim's information. JSON is used for communicating information in scripting language and is based on two types of data structures: arrays and objects. JSON array is directly vulnerable to JSON hijacking.

8.2.5 Malformed scripting language object serialization

Scripting language supports object-oriented programming (OOP) techniques. It has many different built-in objects. A new object can be created using new *object()* or simple in-line code. The programmer can either assign a variable to the *objects()* to process it or make an *eval()*. If an attacker sends a malicious "subject" line embedded with script, then the reader becomes a victim of cross-site scripting attacks. A scripting language object can have both data and methods. Improper usage of scripting language object serialization can open up a security hole that can be exploited by a crafty packet injection code.

8.2.6 Script injection in a document object model

Once this serialized stream of objects is received in the browser, developers make certain calls to access the document object model (DOM). The objective is to "repaint" or "recharge" the DOM with new content. This can be done by calling *eval()*, a customized function, or *document.write()*. If these calls are made on untrustworthy information streams, the browser would be vulnerable to DOM manipulation vulnerability. There are several *document.*()* calls that can be utilized by attack agents to inject XSS into the DOM context.

8.3 Security threats to web application programming interfaces

Both SOAP and REST are platform-neutral protocols for communicating with remote services. Clients can use SOAP and REST to interact with remote services without the knowledge of their underlying platform implementation. REST web APIs use HTTP alone to interact with XML or

JSON payloads. SOAP is a protocol for exchanging XML-based messages over computer networks, normally using HTTP/hypertext transfer protocol security (HTTPS).

8.3.1 Injection flaws

Injection occurs when user-supplied data are sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

8.3.2 Session hijacking and theft

Some web-service providers use session identifiers during communication to identify the service requesters. An attacker can steal and use the identifier information to hijack a session between the web services provider and the consumer.

8.4 Security threats to data syndication

RSS is a family of web feed formats used to publish frequently updated works such as blog entries, news headlines, audio and video in a standardized format and used for data syndication in web services (WSs). RSS formats use XML.

8.4.1 Masquerade of anonymous user

Rogue routers or unauthorized anonymous users might masquerade as valid users. Furthermore, malicious users of the system may try impersonating an honest web-based telecommunication services user. Passive adversaries can eavesdrop on the messages sent over web-based telecommunication services links.

8.4.2 RSS injection

RSS injection is a type of attack where the RSS feed is injected with malicious code. If the RSS reader can display rich content and run scripts, the same problems arise that exist while using the web browser.

8.4.3 XML message injection and manipulation

An attacker can modify parts of the XML messages or attachments to cause endless loops or failure of an XML parser. The attacker can also make use of recursive elements, XPath expression or unrelated message attachments, to perform unintended processing that leads to service failure. This attack usually comes after a man-in-the-middle attack.

8.5 Security threats to mashup

Mashup is a web application that combines data from more than one source into a single integrated tool. Content used in mashups is typically sourced from a third party via a public interface or API (e.g., SOAP or REST). Other methods of sourcing content for mashups include web feeds (e.g., RSS). Mashups provide additional opportunities for all of the above attack scenarios if proper security policies are not in order.

Mashup applications often allow arbitrary third-party mashup components. If a malicious site is able to entice mashup users to embed their mashup component, and if the mashup application does not offer sufficient protection, then the user and the mashup application's website are vulnerable. A malicious mashup component can inject malicious code into the application to achieve all kinds of attacks, including XSS, CSRF and DoS, and might be able to steal sensitive user information. If the mashup application provides simple server-side asynchronous script proxy services, then a malicious client-side mashup component can pass the user's private data to a foreign web server via the mashup application's asynchronous script proxy service.

9 Security objectives of enhanced web-based telecommunication services

9.1 Access control

This service provides protection against unauthorized use of resources accessible via the API. This protection service may be applied to various types of access to a resource (e.g., the use of a communications resource; the reading, writing, or deletion of an information resource; the execution of a processing resource) or to all accesses to a resource.

9.2 Authentication

Authentication is required to confirm the identities of the communicating entities. Authentication ensures the validity of the claimed identities of the entities participating in communication, and provides assurance that an entity is not attempting a masquerade or an unauthorized replay of a previous communication. Authentication techniques may be required as part of access control.

9.3 Authorization

Authorization is required to grant rights and access rights of users to access secure web-based telecommunication services. Authorization and authentication are tightly coupled but authorization systems depend on secure authentication systems to ensure that users are who they claim to be and thus prevent unauthorized users from doing something to secured resources.

9.4 Availability

Availability is recommended and ensures that there is no denial of authorized access to several kinds of resources due to events impacting the network traffic. Availability also allows users to receive an application service from anywhere and at any time on web entities with the ability of such service.

9.5 Communication security

Communication security is recommended and ensures that information flows between authorized end-points only. Communication security ensures that the information is neither diverted nor intercepted as it flows between these end-points.

9.6 Data confidentiality

Data confidentiality is recommended to protect data that are being transported, processed or stored by a network service against unauthorized access or viewing.

9.7 Data integrity

Data integrity is recommended and ensures the correctness or accuracy of data. Data are protected against unauthorized modification, deletion and replication, providing an indication of these unauthorized activities.

9.8 Guarantee of efficiency

In order to apply real-time telecommunication, security services are efficient so that they do not delay the transmission or operations. Therefore, web-based secure telecommunication services are light-weight.

9.9 Non-repudiation

Non-reputation is recommended to provide the means for preventing an individual or an entity from denying having performed a particular action related to data, by making available proof of various network-related actions.

9.10 Privacy

Privacy is recommended and refers to the right of individuals to control or influence which information related to them may be collected and stored, and to whom such information may be disclosed.

9.11 Secure remote backup of device

Secure remote backup of device is recommended to provide a means to store and retrieve securely the system configuration to/from a remote server when the device is exchanged or crashed, etc., because the configurations could have user privacy information.

9.12 Secure user management

In the case of anonymous users, the use of telecommunication service is made possible without any registration process other than open personal information. Nonetheless, the information is validated.

9.13 Separating key management

Separating key management is recommended to protect encryption keys from unauthorized disclosure and misuse among key management entities: users, delivery systems and administrators, by dividing critical functions to ensure that no one individual has enough information or access privilege to perpetrate fraud.

9.14 Trust service

Trust service is recommended to establish secure relationships among key entities related to web services (e-commerce, e-business and system). This forms the measurement basis for the delivery of the related service(s). Because many systems are interconnected, errors in one system often have a domino effect on other systems as well – even beyond the entity's boundaries.

9.15 Relationship between security objectives and security threats

Each security objective is a countermeasure against certain security threats. The relationship between security objectives and security threats is shown in Table 1. The letter 'X' in a cell formed by the intersection of this table's columns and rows designates that a particular security objective is provided in order to remove or mitigate a specific threat.

Table 1 – Relationship between security objectives and security threats

Objectives / Threats	Access control	Authentication	Authorization	Availability	Communication security	Data confidentiality	Data integrity	Guarantee of efficiency	Non-repudiation	Privacy	Secure remote backup of device	Security user management	Separating key management	Trust service
Cross-site request forgery (CSRF)		X	X			X	X		X					
Cross-site scripting (XSS)		X										X		X
Denial of service	X			X				X		X				X
Eavesdropping						X								
Exploiting silent transaction											X	X	X	
Injection flaws														X
JSON hijacking			X		X									X
Malformed scripting language object serialization		X					X					X		X
Man-in-the-browser		X			X									
Man-in-the-middle		X				X	X							
Masquerade		X												X
Masquerade of anonymous user	X													
Modification of messages						X	X							
Repudiation		X							X					
Replay					X				X					
RSS injection		X				X	X							
Scalable mashup		X												X
Script injection in DOM	X						X							
Session hijacking and theft	X		X											
XML message injection and manipulation		X				X	X		X					

Bibliography

[b-ITU-T M.3030] Recommendation ITU-T M.3030 (2002), *Telecommunication Markup Language (tML) framework*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2012) | ISO/IEC 9594-8, *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.802] Recommendation ITU-T X.802 (1995), *Information technology – Lower layers security model*.

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[b-ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

[b-ITU-T X.812] Recommendation ITU-T X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*.

[b-ITU-T X.813] Recommendation ITU-T X.813 (1996) | ISO/IEC 10181-4:1997, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.

[b-ITU-T X.814] Recommendation ITU-T X.814 (1995) | ISO/IEC 10181-5:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework*.

[b-ITU-T X.815] Recommendation ITU-T X.815 (1995) | ISO/IEC 10181-6:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework*.

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

[b-JSON] JSON (JavaScript Object Notation), based on: ECMA (1999), *ECMAScript Language Specification*, Standard ECMA-262, 3rd edition.
<http://www.json.org>

[b-OWASP] The Open Web Application Security Project (2010), *Top 10 Web Application Security Risks for 2010*.
<https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project>

[b-GSMA] GSM Association et al. (2008), *OneAPI Initiative*.
<http://oneapi.gsma.com/>

[b-Fielding] Fielding, R.T. (2000), Representational State Transfer (REST), In: *Architectural Styles and the Design of Network-based Software Architectures* [Dissertation], Irvine, University of California, Irvine.
<http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm>

[b-RSS] RSS Advisory Board (2009), *RSS 2.0 Specification*.
<http://www.rssboard.org/rss-specification>

[b-W3C] W3C (2007), *SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)*.
<http://www.w3.org/TR/soap12-part1/>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012