

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1601

(10/2015)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cloud computing security – Overview of cloud computing
security

Security framework for cloud computing

Recommendation ITU-T X.1601

ITU-T

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
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
PKI related Recommendations	X.1340–X.1349
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.1601

Security framework for cloud computing

Summary

Recommendation ITU-T X.1601 describes the security framework for cloud computing. The Recommendation analyses security threats and challenges in the cloud computing environment, and describes security capabilities that could mitigate these threats and address security challenges. A framework methodology is provided for determining which of these security capabilities will require specification for mitigating security threats and addressing security challenges for cloud computing. Appendix I provides a mapping table on how a particular security threat or challenge is addressed by one or more corresponding security capabilities.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1601	2014-01-24	17	11.1002/1000/12036
2.0	ITU-T X.1601	2015-10-29	17	11.1002/1000/12613

Keywords

Cloud computing, confidentiality, data protection, security capabilities, security challenges, security framework, security threats.

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

© ITU 2016

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	3
4	Abbreviations and acronyms	3
5	Conventions	4
6	Overview.....	4
7	Security threats for cloud computing.....	5
	7.1 Security threats for cloud service customers (CSCs)	5
	7.2 Security threats for cloud service providers (CSPs).....	6
8	Security challenges for cloud computing	6
	8.1 Security challenges for cloud service customers (CSCs)	6
	8.2 Security challenges for cloud service providers (CSPs).....	8
	8.3 Security challenges for cloud service partners (CSNs)	10
9	Cloud computing security capabilities.....	10
	9.1 Trust model.....	10
	9.2 Identity and access management (IAM), authentication, authorization and transaction audit.....	11
	9.3 Physical security	11
	9.4 Interface security	11
	9.5 Computing virtualization security	11
	9.6 Network security	12
	9.7 Data isolation, protection and confidentiality protection	12
	9.8 Security coordination.....	12
	9.9 Operational security.....	13
	9.10 Incident management.....	13
	9.11 Disaster recovery	13
	9.12 Service security assessment and audit	13
	9.13 Interoperability, portability and reversibility	14
	9.14 Supply chain security	14
10	Framework methodology	15
	Appendix I Mapping of cloud computing security threats and challenges to security capabilities	17
	Bibliography.....	21

Recommendation ITU-T X.1601

Security framework for cloud computing

1 Scope

This Recommendation analyses security threats and challenges in the cloud computing environment, and describes security capabilities that could mitigate these threats and address security challenges. A framework methodology is provided for determining which of these security capabilities will require specification for mitigating security threats and addressing security challenges for cloud computing.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-NIST-SP-800-53]: Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

3.1.2 capability [b-ISO/IEC 19440]: Quality of being able to perform a given activity.

3.1.3 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.4 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing (3.1.3) invoked using a defined interface.

3.1.5 cloud service customer [b-ITU-T Y.3500]: Party (3.1.17) which is in a business relationship for the purpose of using cloud services (3.1.4).

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.6 cloud service partner [b-ITU-T Y.3500]: Party (3.1.17) which is engaged in support of, or auxiliary to, activities of either the cloud service provider (3.1.7) or the cloud service customer (3.1.5), or both.

3.1.7 cloud service provider [b-ITU-T Y.3500]: Party (3.1.17) which makes cloud services (3.1.4) available.

3.1.8 cloud service user [b-ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer (3.1.5) that uses cloud services (3.1.4).

NOTE – Examples of such entities include devices and applications.

3.1.9 Communications as a Service (CaaS) [b-ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer (3.1.5) is real time interaction and collaboration.

NOTE – CaaS can provide both application capabilities type and platform capabilities type.

3.1.10 community cloud [b-ITU-T Y.3500]: Cloud deployment model where cloud services (3.1.4) exclusively support and are shared by a specific collection of cloud service customers (3.1.5) who

have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.

3.1.11 data controller [b-key definition]: A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

3.1.12 data processor [b-key definition]: In relation to personal data, this means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

3.1.13 hypervisor [b-NIST-SP-800-125]: The virtualization component that manages the guest OSs on a host and controls the flow of instructions between the guest OSs and the physical hardware.

3.1.14 Infrastructure as a Service (IaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer (3.1.5) is an infrastructure capabilities type.

NOTE – The cloud service customer (3.1.5) does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer (3.1.5) may also have limited ability to control certain networking components (e.g., host firewalls).

3.1.15 multi-tenancy [b-ITU-T Y.3500]: Allocation of physical or virtual resources such that multiple tenants (3.1.26) and their computations and data are isolated from and inaccessible to one another.

3.1.16 Network as a Service (NaaS) [b-ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer (3.1.5) is transport connectivity and related network capabilities.

NOTE – NaaS can provide any of the three cloud capabilities types.

3.1.17 party [b- ISO/IEC 27729]: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.18 personally identifiable information [b-ISO/IEC 29100]: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

3.1.19 Platform as a Service (PaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer (3.1.5) is a platform capabilities type.

3.1.20 private cloud [b-ITU-T Y.3500]: Cloud deployment model where cloud services (3.1.4) are used exclusively by a single cloud service customer (3.1.5) and resources are controlled by that cloud service customer (3.1.5).

3.1.21 public cloud [b-ITU-T Y.3500]: Cloud deployment model where cloud services (3.1.4) are potentially available to any cloud service customer (3.1.5) and resources are controlled by the cloud service provider (3.1.7).

3.1.22 security domain [b-ITU-T X.810]: A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain.

3.1.23 security incident [b-ITU-T E.409]: A security incident is any adverse event whereby some aspect of security could be threatened.

3.1.24 service level agreement (SLA) [b-ISO/IEC 20000-1]: A documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.1.25 Software as a Service (SaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer (3.1.5) is an application capabilities type.

3.1.26 tenant [b-ITU-T Y.3500]: One or more cloud service users (3.1.8) sharing access to a set of physical and virtual resources.

3.1.27 threat [b-ISO/IEC 27000]: A potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.28 virtual machine (VM) [b-NIST-SP-800-145]: An efficient, isolated, logical duplicate of a real machine.

3.1.29 vulnerability [b-NIST-SP-800-30]: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 security challenge: A security "difficulty" other than a direct security threat arising from the nature and operating environment of cloud services, including "indirect" threats. See clauses 7 and 8.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
BCP	Business Continuity Plan
CaaS	Communications as a Service
CPU	Central Processing Unit
CSC	Cloud Service Customer
CSN	Cloud Service Partner
CSP	Cloud Service Provider
CSU	Cloud Service User
DNS	Domain Name System
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICT	Information and Communication Technology
IP	Internet Protocol
IT	Information Technology
NaaS	Network as a Service
OS	Operating System
PaaS	Platform as a Service
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
SaaS	Software as a Service
SIM	Subscriber Identity Module