

Recommendation

ITU-T X.1646 (05/2025)

SERIES X: Data networks, open system communications and security

Cloud computing security – Cloud computing security best practices and guidelines

Security threats to be identified in the domain of security as a service

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	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
Overview of cloud computing security	X.1600-X.1601
Cloud computing security requirements, security capabilities	X.1602-X.1629
Cloud computing security controls	X.1630-X.1639
Cloud computing security best practices and guidelines	X.1640-X.1659
Other cloud computing security	X.1660-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1839
METaverse AND DIGITAL TWIN SECURITY	X.2000-X.2199
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249

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

Recommendation ITU-T X.1646

Security threats to be identified in the domain of security as a service

Summary

Security as a service (SecaaS) is a cloud service category in which the capabilities provided to the cloud service customer are the integration of a suite of security services with the existing operating environment of the cloud service provider. During the development, delivery, use and support of SecaaS, there are security challenges. This Recommendation provides an overview of SecaaS and identifies security threats in the domain of SecaaS provided from public cloud with multi-tenant environments.

Recommendation ITU-T X.1646 followed the structure of security requirements for virtualized services defined in Technical Report ITU-T XSTR-XAASL, *Framework for security standardization for virtualized services*. Security threats in the domain of SecaaS are identified in the following areas: architecture, identity and access management, software isolation and application programming interface (API)-related issues, isolation of instances, data protection, availability, incident response, management, orchestration and deployment.

History*

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1646	2025-05-29	17	11.1002/1000/16383

Keywords

Security as a service, security threat.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and 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 <https://www.itu.int/ITU-T/ipr/>.

© ITU 2025

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.....	1
4 Abbreviations and acronyms	2
5 Conventions	2
6 Overview of SecaaS.....	3
7 Security threats in the domain of SecaaS	3
7.1 Security threats in the domain of architecture	3
7.2 Security threats in the domain of identity and access management (IAM)....	5
7.3 Security threats in the domain of software isolation and API-related issues.....	7
7.4 Security threats in the domain of isolation of instances	9
7.5 Security threats in the domain of data protection.....	10
7.6 Security threats in the domain of availability.....	13
7.7 Security threats in the domain of incident response.....	14
7.8 Security threats in the domain of management, orchestration and deployment	14
Bibliography.....	22

Recommendation ITU-T X.1646

Security threats to be identified in the domain of security as a service

1 Scope

Security as a service (SecaaS) is a cloud service category in which the capabilities provided to the cloud service customer (CSC) are the integration of a suite of security services with the existing operating environment. This Recommendation provides an overview of SecaaS and identifies security threats in the domain of SecaaS provided from public cloud with multi-tenant environments.

Security threats in the domain of SecaaS are identified in the following areas: architecture, identity and access management (IAM), software isolation and application programming interface (API) related issues, isolation of instances, data protection, availability, incident response (IR), management, orchestration and deployment.

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.

- [[ITU-T X.1045](#)] Recommendation ITU-T X.1045 (2019), *Security service chain architecture for networks and applications*.
- [[ITU-T X.1601](#)] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.
- [[ITU-T Y.3525](#)] Recommendation ITU-T Y.3525 (2020), *Cloud computing – Requirements for cloud service development and operation management*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 cloud service customer** [b-ITU-T Y.3500]: A party which is in a business relationship for the purpose of using cloud services.
- 3.1.2 cloud service partner** [b-ITU-T Y.3500]: A party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.
- 3.1.3 cloud service provider** [b-ITU-T Y.3500]: A party which makes cloud services available.
- 3.1.4 security as a service (SecaaS)** [b-ITU-T Y.3500]: The capabilities provided to the cloud service customer are the integration of a suite of security services with the existing operating environment by the cloud service provider (CSP).

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CD	Continuous Delivery/Deployment
CI	Continuous Integration
CSC	Cloud Service Customer
CSN	Cloud Service Partner
CSP	Cloud Service Provider
IAM	Identity and Access Management
IR	Incident Response
JWT	JSON Web Token
LLM	Large Language Model
ML	Machine Learning
RBAC	Role-Based Access Control
SFC	Service Function Chain
SSC	Security Service Chain
SSRF	Server-Side Request Forgery
XSS	cross-Site Scripting

5 Conventions

This Recommendation uses the following conventions:

- The keywords "is required" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.
- The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.
- The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this Recommendation and its appendices, the words shall, shall not, should and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Overview of SecaaS

Security as a service (SecaaS) is a cloud service category in which the capabilities provided to the cloud service customer are the integration of a suite of security services with the existing operating environment of the cloud service provider, as shown in Figure 6-1. Although SecaaS can be provided from a public cloud or a private cloud, this Recommendation only covers security threats in the domain of SecaaS provided from a public cloud with multi-tenant environments. The potential source of attack may include malicious cloud service customer (CSC), cloud service partner (CSN), cloud service provider (CSP) staff, and people who can access security services remotely or physically.

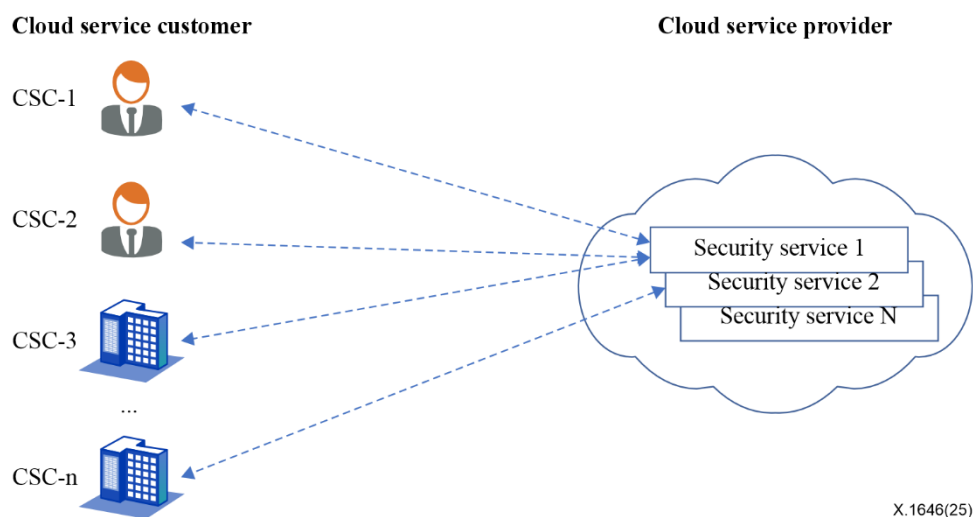


Figure 6-1 – Overview of SecaaS

7 Security threats in the domain of SecaaS

7.1 Security threats in the domain of architecture

Security services may be built based on cloud-native architecture, which may involve container infrastructure, microservices, serverless architecture, etc. Security threats in the domain of cloud-native architecture include the following:

Label: T-Architecture-1

Name: Security threat caused by container vulnerabilities

Description: When security services are hosted in containers, if there are container vulnerabilities, attackers may leverage the vulnerabilities to escape the container and/or even attack the host OS.

Condition: Security services are hosted in containers and there are vulnerabilities in the containers.

Source of attack: Malicious CSC or CSN.

Impact: Attackers may leverage the vulnerabilities to escape the container and/or even attack the host OS.

Label: T-Architecture-2

Name: Security threat caused by insecure container images

Description: Security services may use container images to build and deploy applications. If a CSP/CSN uses unverified container images or container images with malicious software to build and deploy applications, attackers may attack vulnerable applications.

Condition: CSP/CSN uses unverified container images or container images with malicious software to build and deploy applications.