International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1643

(01/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cloud computing security – Cloud computing security best practices and guidelines

Security requirements and guidelines for virtualization containers in cloud computing environments

Recommendation ITU-T X.1643

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	**X.1640–X.1659**
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1643

Security requirements and guidelines for virtualization containers in cloud computing environments

Summary

Recommendation ITU-T X.1643 analyses security threats and challenges for virtualization containers in cloud computing environments and specifies a reference framework with security guidelines for virtualization containers in the cloud.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1643	2022-01-07	17	11.1002/1000/14804

Keywords

Cloud computing, security guidelines, virtualization container.

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T X.1643

Security requirements and guidelines for virtualization containers in cloud computing environments

1 Scope

This Recommendation analyses security threats and challenges for virtualization containers in cloud computing environments and specifies a reference framework with security guidelines for virtualization containers in the cloud.

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.1162] Recommendation ITU-T X.1162 (2008), *Security architecture and operations for peer-to-peer networks.*

[ITU-T X.1255] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information.*

[ITU-T X.1279] Recommendation ITU-T X.1279 (2020), *Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms.*

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*

[ITU-T X.1605] Recommendation ITU-T X.1605 (2020), *Security requirements of public Infrastructure as a Service (IaaS) in cloud computing*.

[ITU-T Y.3508] Recommendation ITU-T Y.3508 (2019), *Cloud computing – Overview and high-level requirements of distributed cloud*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation 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 cloud service image [ITU-T Y.3508]: An executable code with state information of a virtual machine (see clause 3.1.10) or container (see clause 3.1.11).

3.1.3 execution environment [b-ITU-T Y.4500.1]: Logical entity that represents an environment capable of running software modules.

3.1.4 gateway [b-ITU-T H.350.4]: A device that translates from one protocol to another. Often gateways translate between the IP network and the public switched voice network to allow integration of the two.

3.1.5 orchestration [b-ITU-T Y.3100]: In the context of IMT-2020, the processes aiming at the automated arrangement, coordination, instantiation and use of network functions and resources for both physical and virtual infrastructures by optimization criteria.

3.1.6 overlay network [b-ITU-T X.1162]: An overlay network is a virtual network that runs on top of another network. Like any other network, the overlay network comprises a set of nodes and links between them. Because the links are logical ones, they may correspond to many physical links of the underlying network.

3.1.7 registry [b-ITU-T X.1255]: A mechanism for registering metadata about digital entities and storing metadata schemas, and which provides an ability to search the registry for persistent identifiers based on the use of the metadata schemas.

3.1.8 spoofing [b-ITU-T X.1279]: The pretence assumed by an entity to be a different entity, by presenting a recorded image or other biometric data sample, or an artificially derived biometric characteristic, in order to impersonate an individual.

3.1.9 transport layer security [b-ITU-R BT.1699]: A protocol used to send and receive encoded data over the Internet. This protocol supports a combination of various security technologies including shared key cryptosystem, digital certificates, hash functions to prevent eavesdropping, message forgery, and spoofing.

3.1.10 virtual machine (VM) [b-ITU-T Q.1743]: A software program that simulates a hypothetical computer central processing unit. The programs executed by a virtual machine are represented as byte codes, which are primitive operations for this hypothetical computer.

3.1.11 virtualization container [b-ITU-T L.1362]: Partition of a compute node that provides an isolated virtualized computation environment.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 node failure: An error where one or multiple network nodes could not be accessed in an orchestration system.

3.2.2 packet sniffing attack: A method of tapping each packet as it flows across the network illegally.

3.2.3 virtualization container bridge network mode: A network mode that allocates an individual namespace and an Internet protocol (IP) address to each virtualization container and allows the virtualization container to communicate with the host directly.

3.2.4 virtualization container escape attack: Attacker illegally gets the 'executing' authority of a virtualization container and uses this authority to get higher authority of the virtualization container's host virtual machine (VM) or physical host server.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL Access Control List

API Application Programming Interface

CPU Central Processing Unit

DDOS Distributed Denial of Service

DOS Denial of Service

DTLS Datagram Transport Layer Security

IaaS Infrastructure as a Service

IP Internet Protocol

IPsec IP security protocol

MITM Man-in-the-Middle

OS Operating System

TLS Transport Layer Security

VM Virtual Machine

VXLAN Virtual extensible Local Area Network

5 Convention

In this Recommendation:

The keyword "**may**" indicate an optional requirement which is permissible, without implying any sense of being recommended.

The keywords "**shall**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**should**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "**shall not**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

6 Overview

This Recommendation specifies a virtualization container security framework shown as Figure 6-1 which includes user-layer security, access-layer security, resource-layer security, service-layer security, security management and security services.

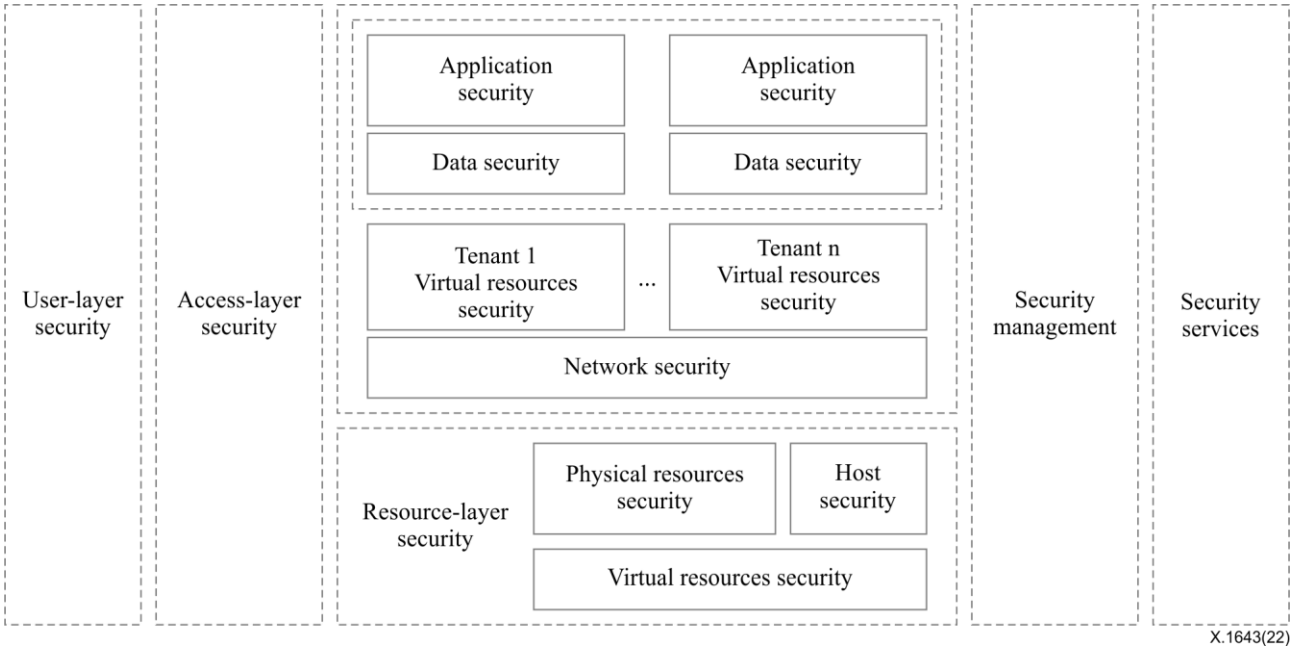

Figure 6-1 – Virtualization container security framework

The purpose of using this framework is to:

– ensure the reliability and stability of the virtualization container in a cloud computing environment,

– protect virtualization container security by protecting the security of all the component elements, e.g., user-layer, access-layer, resource-layer, etc., and

– provide security management and security services to virtualization container service clients.

Referring to Figure 6-1:

a) **User-layer security** manages user's roles, identification information and operations in order to ensure user access control over virtualization containers, to authenticate users and to audit user operations.

b) **Access-layer security** includes access control mechanisms, such as Web access, application programming interface (API) access.

c) **Resource-layer security**: Resource layer security is divided into physical resource security, host security and virtual resource security.

   i. **Physical resource security** refers to the security of the hardware resources of the virtualization container, such as the security of computing resources (central processing unit (CPU), or memory), the network resources (router, switch), storage resources, etc.

   ii. **Host security** refers to the host server that the virtualization container is implemented on, such as the security of the host operation system (OS), VM, etc.

   iii. **Virtual resource security** refers to the security of the virtual components of virtualization, such as virtual computing, virtual network, virtual storage, etc.

d) **Security management** refers to security management functions of a virtualization container in a cloud computing environment, including identity management, authentication management, security policies management, security operations management, maintenance management, etc.

e) **Security services** provides virtualization container security capabilities to users in the form of services.

7 Security challenges and threats for virtualization container in cloud computing

7.1 Security challenges and threats for virtualization container execution environment

The virtualization container execution environment is the first area which needs protection because it is typically the least secure and easiest place to insert malicious code. Besides, more threats can take place here, for example, malicious or moronic source code changes, malicious or mistaken alterations to automated build controllers, error-laden configuration scrips, and the addition of insecure libraries or insecure versions of existing code.

7.2 Security challenges and threats for virtualization container during runtime

7.2.1 Security challenges and threats for virtualization container runtime monitoring

Virtualization containers are ephemeral, but this core value makes monitoring it difficult. In addition, monitoring tools have no visibility or awareness inside the virtualization container at API level, which makes it more difficult to monitor virtualization container behaviours during its runtime.

7.2.2 Security challenges and threats for virtualization container runtime isolation

Isolation is a core security mechanism of virtualization containers. Referring to [ITU-T X.1605], virtual machine (VM) escape, which means vulnerabilities of interfaces between the VMs that attackers could exploit to control the VM or the host of VM, was one of the main security challenges to infrastructure as a service (IaaS) in cloud computing. Similarly, with insecure isolation, a virtualization container engine could suffer from a virtualization container escape attack, i.e., attackers could exploit a compromised virtualization container to attack other virtualization containers that share the same host OS, and further attack the underlying host OS or host directly.

Improper handlings after virtualization container execution may also introduce other critical secure threats: 1) it could leak sensitive residual information to attackers; 2) if it could not release the computing or network resources properly, other virtualization containers might not acquire needed resources.

7.3 Security challenges and threats for registry of virtualization container

As defined in [ITU-T X.1255], registry is a mechanism for registering metadata about digital entities and storing metadata schemas, and which provides an ability to search the registry for persistent identifiers based on the use of the metadata schemas. In addition, the registry of a virtualization container contains important identification information for authorization. With either misconfigured security controls or vulnerability exploitation, attackers could potentially gain access to the registry of a virtualization container illegally and alter or delete the content entirely. Outdated software may have vulnerabilities and registry may suffer from these vulnerabilities as attackers could exploit their vulnerabilities to gain access via backdoor attacks. In addition, mismanaged configurations could also be exploited by attackers to hijack the registry of the virtualization container.

7.4 Security challenges and threats for cloud service image

As defined in [ITU-T Y.3508], cloud service image is an executable code with state information of virtual machines or virtualization containers, and includes operating systems, libraries, data files, applications, etc. Because virtualization containers are deployed based on cloud service images, the cloud service image security is the precondition of the virtualization container security. Cloud service images face following major threats:

a) Software of cloud service images may contain vulnerabilities that can be exploited by attackers.

b) With improper configuration, the cloud service image integrity check could fail to be verified. In addition, the accountability of validating the cloud service image integrity depends on application scenarios wherein cloud service providers are responsible if users deploy virtualization containers based on cloud service images provided by cloud service providers; whereas users are responsible if deployed virtualization containers are based on cloud service images from elsewhere, such as downloading from a registry.

c) Cloud service image files may be tampered stealthily. For example, attackers could implant backdoor or malicious software into cloud service image files during upload or download.

7.5 Security challenges and threats for operating system (OS)

In the virtualization containerized environment, all the virtualization containers "share" the kernel and other host resources with the host system. Therefore, the underlying host OS represents the most critical target for attacks. If the OS is compromised, all the virtualization containers are compromised as well. Additionally, host-based controls and security policies can be applied on each virtualization container. Moreover, virtualization containers escape attacks that happen via bugs in the application code and can bypass the engine and access the host OS and the kernel that controls all the other applications.

7.6 Security challenges and threats for orchestration management system of virtualization container

As defined in [b-ITU-T Y.3100], orchestration is the processes aiming at the automated arrangement, coordination, instantiation and use of network functions and resources for both physical and virtual infrastructures by optimization criteria, and it is a typical technology used in virtual networks (such as cloud computing environments). In a cloud virtualization container environment, an orchestration management system enables management of large-scale virtualization containers that are deployed in the cloud, and this faces several security challenges and threats as follows:

a) Privilege abuse: If the security policy of the orchestration management system does not follow the least privilege principle, users could make use of it and operate virtualization containers beyond their own privileges, which results in significant security consequences.

b) Unauthorized access to open API: Open APIs and other publicly accessible network resources such as network ports on the Internet expose new attacking surfaces. Attackers could exploit vulnerabilities of open APIs, such as improper authentication, authorization, integrity check, etc., and gain access to the virtualization container orchestration, and further operate or modify its virtualization containers.

c) Node failure management: Node failure means one or multiple network nodes could not be accessed in an orchestration management system. Inappropriate handling of node failure could interfere with other regular nodes and the orchestration management. Attackers could make use of it maliciously and lower the performance of orchestrations.

d) Configuration management: An orchestration management system of a virtualization container introduces different configurations on a huge amount of assets, and various types of services, which demands a high-level secure policy of configuration management. Misconfiguration could enlarge attacking surfaces, and result in significant security risks. For example, attackers could penetrate into the internal orchestration software through publicly accessible virtualization container applications.

7.7 Security challenges and threats for virtualization container network

A virtualization container network could run under two typical network modes, the virtualization container bridge network mode and the virtualization container overlay network mode, to communicate with other virtualization containers on the same host, across different hosts, or within virtualization containers.

The virtualization container bridge network mode allocates individual namespace and an Internet protocol (IP) address to each virtualization container and allows the virtualization container to communicate with the host directly.

As defined in [ITU-T X.1162], an overlay network is a virtual network that runs on top of another network. Like any other network, the overlay network comprises a set of nodes and links between them. Because the links are logical ones, they may correspond to many physical links of the underlying network. In a cloud virtualization container environment, a virtualization container overlay network connects distributed virtualization containers. Specifically, it builds a virtual overlay network on top of the underlay network of each host by the virtual extensible local area network (VXLAN) technique, to enable interconnecting virtualization containers and allow virtualization containers communicate across hosts.

The common security challenges and threats for both of these two network modes of virtualization container includes:

– **Denial of service (DoS)/ distributed denial of service (DDoS) attack**

  A virtualization container network faces DoS/DDoS attack threats from both internal and external networks:

a) DoS/DDoS threats from internal networks: An attacker might exploit compromised virtualization containers to launch DoS/DDoS attacks on other virtualization containers on the same network, to overwhelm the computing resources of targets such as bandwidth, CPUs, etc.

b) DoS/DDoS threats from external networks: Virtualization containers on the same host share the same physical network adapters. Additionally, if an attacker launches DoS/DDoS attacks on a target virtualization container by sending a large volume of data packets from botnet hosts, it might not only damage the target virtualization container, but also overwhelm the network bandwidth of the host machine, resulting in DoS/DDoS attacks on the host and on other virtualization containers as well.

– **Man-in-the-middle attack**

Virtualization containers under various network modes do not provide encryption mechanisms initially, this results in virtualization containers that are actually vulnerable to man-in-the-middle (MITM) attack. For example, as defined in [ITU-T X.1279], spoofing is the pretence assumed by an entity to be a different entity, by presenting a recorded image or other biometric data sample, or an artificially derived biometric characteristic, in order to impersonate an individual, and it is a typical security threat. An attacker could exploit a comprised virtualization container and perform spoofing attacks on a target virtualization container on the same virtual network. In addition, if successful the attacker can actually hijack the normal network traffic of a virtualization container, and afterwards perform a series of man-in-the-middle attacks.

Applications within virtualization containers may choose to do their own encryption using protocols such as transport layer security (TLS), or datagram transport layer security (DTLS). In these cases, an implementer who understands that the traffic within the virtualization container or, the traffic moving between virtualization containers, may choose not to duplicate the provision of encryption. The goal of this approach is to maximize protection of the inter-virtualization container traffic while minimizing the computational overhead associated with encrypting the same traffic more than once.

The particular security threats that virtualization container bridge network mode and virtualization container overlay network mode face are described in clauses 7.7.1 and 7.7.2.

7.7.1 Virtualization container bridge network mode

Under the virtualization container bridge network mode, a virtualization container connects to a virtual network by its virtual network interface, which allow the virtualization container to communicate with the host directly and act as the initial gateway. Network packets of a virtualization container will be first sent to the initial gateway and then routed to other virtualization containers. Virtualization containers under the same virtual network are interconnected.

Without a network security policy for the virtualization container bridge network mode, there is no network access control between virtualization containers. If there is no firewall and other network defensive mechanisms, an attacker sits in one virtualization container and can easily launch various attacks to other virtualization containers, for example by, spoofing, packet sniffing attack, etc., this results in severe consequences, such as sensitive information leakage, etc.

Therefore, there are network security risks under the virtualization container bridge network mode without an effective network access control policy between virtualization containers on the same host.

7.7.2 Virtualization container overlay network mode

The virtualization container overlay network mode does not have initial network access control policy for virtualization containers. Also, because VXLAN network traffic is not encrypted by default, it needs to utilize other tunnelling protocols, such as the IP security protocol (IPsec), etc., to encrypt the VXLAN network traffic and ensure the data transfer security.

8 Security requirements and guidelines for virtualization containers in cloud computing environments

This clause provides security requirements and guidelines according to the security challenges and threats for virtualization containers that are described in clause 7.

8.1 Security requirements and guidelines for virtualization containers during runtime

a) When making an update to applications or services, running virtualization containers shall be stopped and replaced with new virtualization containers.

b) Tools should be used to look for common vulnerabilities in the runtimes deployed. Any instances at risk shall be upgraded.

c) No unauthorized users shall have access to the virtualization container daemon.

8.2 Security requirements and guidelines of registry of virtualization containers

a) The server that hosts the registry should be locked down in order to mitigate the risk of attack there.

b) Development tools, the orchestration management system and virtualization containers should be configured to only connect to registries over encrypted channels.

c) Registries should be pruned of unsafe, vulnerable cloud service images that shall no longer be used.

d) All access to registry should require authentication to ensure that only cloud service images from trusted entities can be added to it.

8.3 Security requirements and guidelines of cloud service images of virtualization containers

a) The purpose of cloud service images is to create an application or service virtualization container. Cloud service images for other tasks shall not be used.

b) Cloud service image signatures should be validated before cloud service images execution to ensure cloud service images come from trusted sources and have not been tampered with.

c) Continuous monitoring and maintenance of registries should be implemented to ensure cloud service images within them are maintained and updated as vulnerabilities and configuration requirements change.

d) Accessing cloud service images should use immutable names that specify discrete versions of cloud service images.

8.4 Security requirements and guidelines of the host OS of virtualization containers

a) Attack vectors should be minimized by eliminating all but the essentials from the host environment.

b) Virtualization containerized and non-virtualization containerized workloads shall not be mixed on the same host instance.

c) The version of host OS should be validated by implementing management practices and tools.

d) All authentication to the OS should be audited.

e) Virtualization containers should run with the minimal set of file system permissions required. Any file changes in the host OS of virtualization container should only be made with the authorisation policies.

8.5 Security requirements and guidelines of the orchestration management system of virtualization containers

a) An orchestration management system should be installed from an official, trusted, up-to-date source.

b) The orchestration management system should be configured to provide high availability and automatic failover to the extent possible.

c) The orchestration management system should use a least a privilege access model where the user is only granted the ability to perform the specific actions on the specific host, virtualization container and cloud service image.

d) Strong authentication methods, such as requiring multifactor authentication instead of just a password, should be used for administrative accounts of the orchestration management system.

e) The orchestration management system should be configured to separate network traffic into discrete virtual networks by sensitivity levels.

f) The orchestration management system should be configured to isolate deployments to specific sets of hosts by sensitivity levels.

8.6 Security requirements and guidelines of virtualization containers in different network modes

8.6.1 Inter virtualization container traffic restriction for virtualization container bridge network mode

In bridge network mode, the default initial security configuration of the virtualization container does not control and restrict network access. In order to prevent potential DoS/DDoS threats, there should be network access control policies according to actual requirements, including:

a) Inter virtualization container communication shall be prohibited completely if possible. In specific application scenarios, if all virtualization containers on the host do not need network communication with each other, virtualization container to virtualization container communication could be prohibited by changing the default security configuration.

b) Inter virtualization container access control policies should be implemented: In a virtualization container cloud environment where multi-tenancy exists, there may be a situation where a single virtualization container occupies many hosts to overwhelm the bandwidth of other virtualization containers. In order to ensure regular communication between virtualization containers and avoid abnormal traffic that are caused by DoS/DDoS attacks, restriction mechanisms on the communication traffic between virtualization containers should be implemented.

c) Encryption mechanisms and policies should be implemented, e.g., to utilize IPsec protocol to encrypt the traffic and ensure the confidentiality of inter virtualization container communication, thus preventing network sniffing or man-in-the-middle attacks.

8.6.2 Inter virtualization container access control

a) Access control for virtualization container bridge network mode

In bridge network mode, the default initial security configuration of virtualization containers allows virtualization containers to connect to the same virtual network and communicate with each other directly. Therefore, in order to prevent abnormal accesses, access control mechanisms and policies should be configured on demand. Including:

1) Different virtual networks for virtualization containers should be configured to achieve network isolation between different virtualization containers. This will block

communication traffic with other networks and achieve the isolation purpose between virtualization container networks.

2) Access control based on whitelist policy should be implemented to ensure the network security between virtualization containers, communication between virtualization containers should be prohibited by default, and then configure the access control rules on demand. Access control based on whitelist policy reduces the attack surface by minimization strategy.

b) Access control for virtualization container overlay network mode

In virtualization container overlay network mode, different virtualization containers can access each other directly on the same subnet and host. Access control list (ACL) access rules should be added manually in the host access control policies, or a firewall should be deployed on the host, to control access from external hosts to internal virtualization container applications.

In a large virtualization container cloud environment, it might not be practical to update firewall rules manually due to the frequent dynamic updates of microservices [b-ITU-T J.1301]. It is recommended to utilize some tools to manage the process automatically, such as virtualization container micro-segmentation which is a virtualization container firewall technique that provides fine-grained network segmentation isolation mechanisms and can perform segmentation isolation for a single virtualization container, virtualization containers in a same subset network, or virtualization container applications, and can implement network access control policies accordingly.

Bibliography

[b-ITU-T H.350.4] Recommendation ITU-T H.350.4 (2011), *Directory services architecture for SIP*.

[b-ITU-T J.1301] Recommendation ITU-T J.1301 (2021), *Specification of cloud-based converged media service to support Internet protocol and broadcast cable television – Requirements*.

[b-ITU-T L.1362] Recommendation ITU-T L.1362 (2019), *Interface for power management in network function virtualization environments – Green abstraction Layer version 2*.

[b-ITU-T Q.1743] Recommendation ITU-T Q.1743 (2016), *IMT-Advanced references to Release 11 of LTE-Advanced evolved packet core network*.

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

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T X.1162] Recommendation ITU-T X.1162 (2008), *Security architecture and operations for peer-to-peer networks*.

[b-ITU-T X.1251] Recommendation ITU-T X.1251 (2019), *A framework for user control of digital identity*.

[b-ITU-T X.1255] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information*.

[b-ITU-T X.1279] Recommendation ITU-T X.1279 (2020), *Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms*.

[b-ITU-T X.1604] Recommendation ITU-T X.1604 (2020), *Security requirements of Network as a Service (NaaS) in cloud computing*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[b-ITU-T Y.4500.1] Recommendation ITU-T Y.4500.1 (2018), *oneM2M – Functional architecture*.

[b-ITU-R BT.1699] Recommendation ITU-R BT.1699 (2013), *Harmonization of declarative application formats for interactive TV*.

[b-ISO/IEC 19944] ISO/IEC 19944:2016, *Information technology – Cloud services and devices: Data flow, data categories and data use*.

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology –Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27729] ISO/IEC 27729:2012, *Information and documentation – International standard name identifier (ISNI)*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology –Security techniques – Privacy framework*.

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, 2022