International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1453

(01/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Application Security (2)

Security threats and requirements for video management systems

Recommendation ITU-T X.1453

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.1453

Security threats and requirements for video management systems

Summary

A video management system (VMS) is the core of the video surveillance systems used for public safety, traffic monitoring, etc. Basically, a VMS receives video from cameras and allows a user to view that video either live or recorded. Currently, emerging VMS approaches incorporate more and more intelligence into their design, including video analytics and access control.

As a VMS is networked, it is fully exposed to various vulnerabilities such as those faced by Internet web services and can easily be a target of cyberattacks.

Recommendation ITU-T X.1453 analyses the security threats to server platform based VMSs running on an IP network and specifies security requirements to counteract the identified security threats.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1453	2022-01-07	17	11.1002/1000/14802

Keywords

Security framework, security requirement, video management system.

[*] 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.1453

Security threats and requirements for video management systems

1 Scope

This Recommendation identifies security threats and specifies security requirements for a video management system (VMS) based on a server platform that receives video from cameras, which are one type of Internet of things (IoT) devices, and allows users to view that video either live or recorded. This Recommendation covers the following:

- Analysis of the architecture of a VMS based on a server platform;
- Analysis of security threats faced by such VMSs;
- Security requirements to counteract the identified threats.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 video surveillance system [b-ITU-T H.626]: A telecommunication service focusing on video (including audio and image) application technology, which is used to remotely capture multimedia (such as audio, video, image, alarm signal, etc.) and present them to the end user in a user-friendly manner, based on a managed broadband network with ensured quality, security and reliability.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 video management system: An essential part of any video surveillance system that allows users to view multiple cameras, record and analyse video streams, and set tampering alerts and motion detection alerts.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DDoS	Distributed Denial of Service
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol

IPS	Intrusion Prevention System
NVR	Network Video Recorder
VMS	Video Management System

5 Conventions

In this Recommendation:

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

6 Video management system

The IoT has been growing rapidly across the world over the past few years. IoT based video surveillance systems enable users to view activity taking place in a remote location and to capture at will images that may be of interest. The use cases of these systems vary widely, ranging from law enforcement and crime prevention to safety in transportation and traffic monitoring. VMSs is the core of video surveillance systems used for public safety and traffic monitoring systems. Basically, a VMS receives video from cameras and allows users to view that video either live or recorded. Currently emerging VMS approaches incorporate more and more intelligence into their design, including video analytics and access control.

As VMS is networked, it is fully exposed to various vulnerabilities, such as those faced by Internet web services, and can be a target of cyberattack.

A typical IoT based video surveillance system consists of multiple security cameras, a VMS and client devices for the user to view the video. VMS allows users to record and view live video from multiple security cameras, to monitor alarms, to control cameras and to retrieve recordings from archives. An IoT based VMS is more expandable and flexible than an analogue based system, and it allows users to control devices that make up the video surveillance system anywhere on the network.

VMS can support many different features as follows:

– Simultaneous viewing;

– Recording of video and audio;

– Video search and playback;

– Intelligent video analytics;

– Camera management;

– Event management;

– Alarm management.

There are two different types of hardware platforms for a networked VMS: a VMS based on a server platform involves one or more servers that run a video management software program, or a network video recorder (NVR) based VMS. A VMS is a combination of video software and hardware. Video management software can be mounted on NVR hardware or installed on server hardware. Video management software mounted on an NVR is used to perform simple tasks such as recording and monitoring of video footage in a confined area, whereas video management software installed on a server remotely controls many cameras distributed in various locations, stores and manages video, and also provides intelligent video analytics to automatically detect events. In general, an NVR based VMS refers to a VMS with only one NVR used, whereas a server based VMS refers to a VMS with one or more servers which controls numerous cameras and provides extended analytical services. This Recommendation addresses only VMSs based on server platforms.

To analyse VMS security, an architecture is defined to identify all entities related to the video surveillance based on a VMS and clarify the relationship between the entities. The functional architecture of a VMS for video surveillance applications is shown in Figure 1.

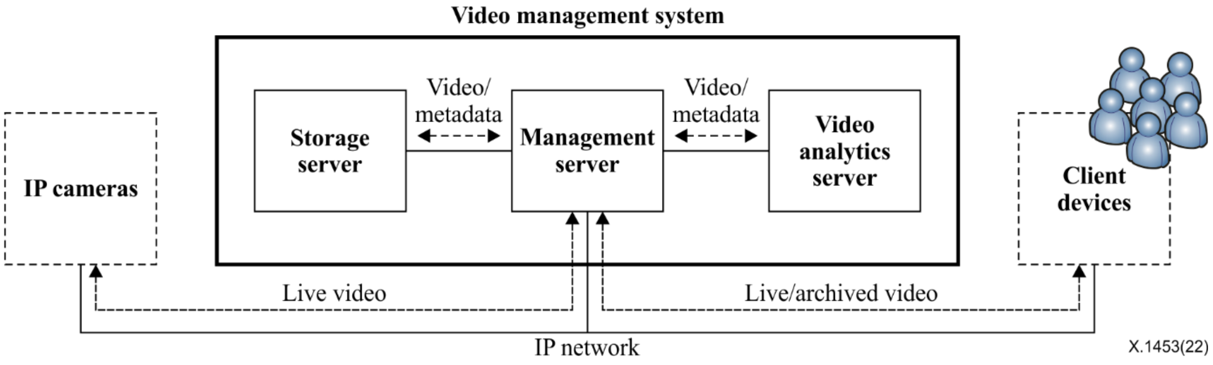

Figure 1 – Simplified functional VMS architecture

Video surveillance systems have five types of major entities: cameras, storage servers, management servers, video analytics servers and client devices. A VMS at the core of a video surveillance system is composed of a management server, a storage server and a video analytics server. There are four relationships between the entities shown in Figure 1, as follows: between a camera and the management server, between the management server and a client device, between the management server and the storage server, and between the management server and the video analytics server.

The VMS is connected to the cameras and client devices via a network. The management server, the storage server and the video analytics server are usually located in the same network. The client devices are typically connected to an open network, such as the Internet, for extended remote monitoring.

The management server is the centre of the VMS. It controls and manages all entities in video surveillance systems, including camera settings and storage parameters. The storage server records video from the cameras that are attached to them and stores the metadata created by the video analytics server. The video analytics server analyses moving objects in a video stream and creates metadata to describe the activities and events that are identified. The video analytics server generates two forms of metadata, event metadata and alert metadata. Each event or alert is composed of multiple metadata messages that contain various attributes about a detected change or motion segment in a video feed.

7 Security threats

7.1 Threats to the interface between the management server and camera

The main task of the interface between the management server and camera is to collect video from the camera, adjust the camera settings and control the cameras to rotate, tilt and zoom. Data transferred via these interfaces is an attacker's main target. An attacker can damage the VMS by intercepting, falsifying and replaying the data. Another target for attackers is the denial of the VMS by launching a distributed denial of service (DDoS) attack against the cameras and the management server.

Threats to the interface between management server and camera are as follows:

- Unauthorized access: An attack that gains access to the camera using someone else's account or another access method. Unauthorized access to the camera can cause disclosure of sensitive information, video modification and illegal use of resources. For example, once an attacker has accessed the camera, video data can be illegally collected, and real-time monitoring of the video data can result in privacy concerns.

- Network eavesdropping: An attack that captures video data transmitted from the network and reads the video content in search of sensitive information such as faces and car licence plates.
- Denial of service: An attack that tries to run malicious code on the management server or the cameras with the objective of flooding the target with massive data or service requests. With this attack, VMSs can be slowed down or stopped.
- Falsification of video data: An attacker blocks the video data, and then sends falsified video data to the management server. The attack can cause interference with the normal operation of the VMS.
- Falsification of control data: An attacker blocks the control data for adjusting camera settings, and then sends falsified control data to the cameras. The attack can cause interference with the normal camera control functions.
- Insider threats: Where humans are involved, there is always a risk of individuals acting in a malicious or careless manner that puts the VMS at risk. Users sharing an "administrator" password or leaving credentials in unsecure locations, careless or inadequately trained users, or malicious actions by disgruntled users will always pose a significant threat.

7.2 Threats to the interface between the management server and client device

The main task of the interface between the management server and client device is to provide interfaces to view live video and access recorded videos.

Threats to the interface between management server and client device are as follows:

- Unauthorized access: An attack that gains access to the client device using someone else's account or another access method. Unauthorized access to the client device can cause disclosure of sensitive information and illegal use of resources. For example, once an attacker has accessed the client device, video data can be illegally collected and real-time monitoring of the video data can result in privacy concerns.
- Network eavesdropping: An attack that captures video data transmitted from the network and reads the video content in search of sensitive information such as faces, car licence plates or any other kind of sensitive information.
- Denial of service: An attack that tries to run malicious code on the management server or the client devices with the objective of flooding the target with massive data or service requests. With this attack, a VMS can be slowed down or stopped.
- Falsification of video data: An attacker blocks the video data, and then sends falsified video data to the client devices. The attack can cause interference with the normal operation of the VMS.
- Falsification of control data: An attacker blocks the control data for adjusting camera settings, and then sends falsified control data to the management server. The attack can cause interference with the user's normal video monitoring.
- Insider threats: Where humans are involved, there is always a risk of individuals acting in a malicious or careless manner that puts the VMS at risk. Users sharing an "administrator" password or leaving credentials in unsecure locations, careless or inadequately trained users, or malicious actions by disgruntled users will always pose a significant threat.

7.3 Threats to the interface between the management server and storage server

The main task of the interface between the management server and storage server is to provide interfaces to record/view the video and the metadata.

The management server and the storage server are usually located in the same network or are connected via a dedicated line. Even if only the management server is connected to the public network, a hacker can exploit the security vulnerabilities of the management server to illegally access the storage server.

Threats to the interface between management server and storage server are as follows:

- Unauthorized access: An attack that gains access to the management server using someone else's account or another access method to access data stored in the storage server. Unauthorized access to the storage server can cause the disclosure of sensitive information and illegal use of resources.
- Disclosure of data: An attack that illegally accesses video content stored in the server and reads sensitive information such as faces and licence plates. An attacker can disclose data that have not been protected.
- Injection and modification of data: An attack that illegally modifies the stored video data by injecting them with impure data, degrading in this way the reliability of the video information.
- Insider threats: Where humans are involved, there is always a risk of individuals acting in a malicious or careless manner that puts the VMS at risk. Users sharing an "administrator" password or leaving credentials in unsecure locations, careless or inadequately trained users, or malicious actions by disgruntled users will always pose a significant threat.

7.4 Threats to the interface between the management server and video analytics server

The main task of the interface between management server and video analytics server is to transmit video to analyse moving objects in video data, and metadata to describe the activities and events that are identified in the video analytics server.

The management server and the video analytics server are usually located in the same network or are connected via a dedicated line. Even only the management server is connected to the public network, an attacker can exploit the security vulnerability of the management server to illegally access the video analytics server.

Threats to the interface between the management server and video analytics server are as follows:

- Unauthorized access: An attack that gains access to the management server using someone else's account or another access method to access data stored in the video analytics server. Unauthorized access to the video analysis server can lead to malfunctions, which reduces the reliability of the video analysis server.
- Disclosure of data: An attack that illegally accesses video content stored on the server and reads sensitive information such as faces and licence plates. An attacker can disclose data that have not been protected.
- Injection and modification of data: An attack that illegally modifies the video data or metadata by injecting them with impure data, degrading in this way the reliability of the video analysis server. For example, once an attacker has illegally accessed the management server, the attacker can illegally obtain permissions for an unauthorized person by replacing the stored authorized person's facial data with an unauthorized person's facial data.
- Insider threats: Where humans are involved, there is always a risk of individuals acting in a malicious or careless manner that puts the VMS at risk. Users sharing an "administrator" password, or leaving credentials in unsecure locations, careless or inadequately trained users, or malicious actions by disgruntled users will always pose a significant threat.

7.5 Relationship between security threats and entities inside/outside VMS

The security threats target specific places between the entities in Figure 1. The relationship of security threats and entities inside/outside VMS is shown in Table 1, where an open circle in a cell indicates that the entity is related to the particular security threat.

Table 1 – Relationship between security requirements and entities

Entities / Threats	Between VMS and cameras	VMS		Between VMS and client devices
		Between the management server and the storage server	Between the management server and the video analytics server	
Network eavesdropping	○			○
Unauthorized access	○	○	○	○
Denial of service	○			○
Disclosure of data		○	○	
Injection and modification of data	○	○	○	○
Insider threats	○	○	○	○

8 Security requirements

8.1 Confidentiality

Confidentiality ensures that data content cannot be read by unauthorized entities. Even if some data are eavesdropped and an attacker discloses it, their confidentiality can be ensured.

Confidentiality is required for sensitive data, whether for storage or transmission. Sensitive data include video data, command data controlling the operation of cameras and data stored on the storage server.

- Confidentiality is required to ensure that video data transmitted on the network cannot be read by unauthorized entities.
- Confidentiality is required to ensure that command data controlling the operation of cameras transmitted on the network cannot be read by unauthorized entities.
- Confidentiality is recommended to ensure that data stored on the storage server and the video analytics server cannot be read by unauthorized entities.

8.2 Integrity

Integrity ensures that data, once transmitted, do not differ from that at the source. It is required that the original stored data should not be changed after authorized access.

- Integrity is required to ensure that the video data transmitted from camera are original data without forgery.
- Integrity is recommended to ensure that the stored video data are original data without forgery.
- Integrity is recommended to ensure that the exported video data for criminal investigation, etc. are original data that have not been altered.

8.3 User and device authentication

Authentication is required to confirm the identities of users and devices. Authentication ensures the validity of the claimed identities of the entities participating in video surveillance and provides assurance that an unauthorized entity is not attempting to masquerade as an authorized entity.

- User authentication is required to ensure that a user is a legitimate administrator allowed to access the servers in the VMS for central video management.
- User authentication is required to ensure that a user is a legitimate user of a client device and is allowed to remotely view the video data.
- Device authentication is recommended to ensure that a device is a legitimate client device allowed to remotely connect to the VMS.
- Device authentication is recommended to ensure that a camera is a legitimate camera allowed to be connected to the VMS.

8.4 Access control

Access control is required to ensure that only authorized users are allowed to access appropriate resources participating in video surveillance. Even though administrators are involved in the privileged group that is permitted to maintain and control the video surveillance system, it is recommended that each individual user be granted a different access right.

- Access control is required to ensure that only authorized users are allowed to access the management server according to their access privileges in the video surveillance system. The types of access include real-time video monitoring, recorded video playback and remote camera control.
- Access control is required to ensure that only authorized client device users are allowed to access the video surveillance according to their access privileges. The types of access include real-time video monitoring and recorded video playback.

8.5 Intrusion prevention

Intrusion prevention is required to protect the entities of the VMS, the stored video data and the services from internal and external illegal access attempts. Intrusion prevention in a VMS can be categorized into the logical method and the physical method. The logical intrusion prevention method protects system resources from attacks that use an IP based network. The physical intrusion prevention method protects system resources from physical illegal access.

- Logical intrusion prevention is required to ensure that system resources are protected from attacks that use an IP based network, allowing the video surveillance to operate normally. Network security systems used for logical intrusion prevention include an intrusion detection system (IDS) and intrusion prevention system (IPS). It is better to use a dedicated network security system rather than a system implemented inside the VMS.
- Physical intrusion prevention is required to ensure that only legitimate users identified through user authentication can enter the security operation centre where the VMS has been installed.

8.6 Relationship between security requirements and security threats

The relationship between security requirements and security threats is shown in Table 2, where an open circle in a cell indicates that a particular security requirement should be satisfied in order to remove or mitigate the specific threat.

Table 2 – Relationship between security requirements and threats

			Security requirements				
			Confidentiality	Integrity	User/device authentication	Access control	Intrusion prevention
Security threats	VMS	Unauthorized access			○	○	
		Disclosure of data	○				
		Modification/injection		○			
		Insider threats			○	○	
		DOS					○
	Between VMS and cameras	Unauthorized access			○	○	
		Eavesdropping	○				
		DOS					○
		Modification/injection		○			
		Insider threats			○	○	
	Between VMS and client devices	Unauthorized access			○	○	
		Eavesdropping	○				
		DOS					○
		Modification/injection		○			
		Insider threats			○	○	

Bibliography

[b-ITU-T H.626] Recommendation ITU-T H.626 (2019), *Architecture requirements for video surveillance system*.

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