ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T F.743.23 (10/2023)

SERIES F: Non-telephone telecommunication services

Multimedia services

Security requirements for video surveillance systems

ITU-T F-SERIES RECOMMENDATIONS

Non-telephone telecommunication services

TELEGRAPH SERVICE	F.1-F.109
Operating methods for the international public telegram service	F.1-F.19
The gentex network	F.20-F.29
Message switching	F.30-F.39
The international telemessage service	F.40-F.58
The international telex service	F.59-F.89
Statistics and publications on international telegraph services	F.90-F.99
Scheduled and leased communication services	F.100-F.104
Phototelegraph service	F.105-F.109
MOBILE SERVICE	F.110-F.159
Mobile services and multidestination satellite services	F.110-F.159
TELEMATIC SERVICES	F.160-F.399
Public facsimile service	F.160-F.199
Teletex service	F.200-F.299
Videotex service	F.300-F.349
General provisions for telematic services	F.350-F.399
MESSAGE HANDLING SERVICES	F.400-F.499
DIRECTORY SERVICES	F.500-F.549
DOCUMENT COMMUNICATION	F.550-F.599
Document communication	F.550-F.579
Programming communication interfaces	F.580-F.599
DATA TRANSMISSION SERVICES	F.600-F.699
MULTIMEDIA SERVICES	**F.700-F.799**
ISDN SERVICES	F.800-F.849
UNIVERSAL PERSONAL TELECOMMUNICATION	F.850-F.899
ACCESSIBILITY AND HUMAN FACTORS	F.900-F.999

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

Recommendation ITU-T F.743.23

Security requirements for video surveillance systems

Summary

Recommendation ITU-T F.743.23 defines premises unit (PU) device security classification, functional requirements, typical use case and scenario for video surveillance systems. The Recommendation specifies the functional requirements, including PU access security requirements, transmission security requirements, platform security requirements, application security requirements, network security, and security management centre in video surveillance systems.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T F.743.23	2023-10-29	16	11.1002/1000/15618

Keywords

Security requirements, video surveillance.

* 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, 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 F.743.23

Security requirements for video surveillance systems

1 Scope

This Recommendation specifies security requirements for video surveillance systems.

The scope of this Recommendation includes:

– Premises unit (PU) device security classification;
– PU access security requirements;
– Transmission security requirements;
– Platform security requirements;
– Application security requirements;
– Network security requirements;
– Security management centre requirements;
– Typical use case and scenario.

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 H.626] Recommendation ITU-T H.626 (V2) (2019), *Architectural requirements for video surveillance system.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 premises unit (PU) [ITU-T H.626]: A device located at the remote part of a video surveillance system and used to capture multimedia information (such as audio, video, image, alarm signal, etc.) from a surveilled object.

3.1.2 video surveillance system [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 terms:

3.2.1 asset management module: An asset management module deployed on the platform side unifies the management of security information of all access devices on the platform.

3.2.2 asset whitelist: A list of premises unit (PU) devices allowed to access and be accessed by the platform is stored in the asset management module of the platform side, mainly containing device ID, device type, manufacturer, model, firmware version number, etc.

3.2.3 device fingerprint library: A device fingerprint library is deployed in the asset management module on the platform side, which can uniquely identify the information about a device, including media access control address (MAC), device type, manufacturer, model, operating system, etc.

3.2.4 device address feature code: A device address feature code stored in the asset management module of the platform side is formed by the device information such as the Internet protocol (IP) and media access control address (MAC) address of the device, which is used to bind with the device identity document (ID).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DHCP	Dynamic Host Configuration Protocol
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IPC	Internet Protocol Camera
MAC	Media Access Control Address
NFS	Network File System
NVR	Network Video Recorder
POP3	Post Office Protocol-Version 3
PU	Premises Unit
QR	Quick Response
REST	Representational State Transfer
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
RTSP	Real-time Streaming Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TELNET	Teletype Network

5 Conventions

In this Recommendation:

– The keywords "is required to" 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 needs not be present to claim conformance.

– The keywords "can optionally" and "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are 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.

6 PU device security classification

According to the strength of the security protection, the security capability of the premises unit (PU) device is divided into three levels, ranging from low to high: A, B and C. The security classification of the PU device is shown in Table 6-1.

A-level devices are recommended to perform two-way authentication with the platform based on the digital certificates to ensure authentic identity.

B-level devices are recommended to perform two-way authentication with the platform based on the digital certificates and sign the video data, which can ensure that authentic identity and video data come from the real device and can verify whether the video content has been tampered with.

C-level devices are recommended to perform two-way authentication with the platform based on the digital certificates, sign and encrypt the video data, which can ensure that authentic identity and video data come from the real device and can verify whether the video content has been tampered with, and can encrypt and protect the video data.

Table 6-1 – PU device security classification

Level	Perform two-way authentication with the platform based on digital certificates	Perform two-way authentication with the platform based on digital certificates and sign the video data	Perform two-way authentication with the platform based on digital certificates, sign and encrypt the video data
A-level	√	-	-
B-level	√	√	-
C-level	√	√	√

7 Functional requirements

7.1 PU access security requirements

PU contains a large amount of video image data and information. Due to the presence of numerous cameras and multiple network branches, there are significant risks associated with the security access control of cameras and other devices. This situation can easily lead to the abuse of network resources and information leakage.

Network cameras are vulnerable to illegal attacks by hackers, and there is a risk of PU device hijacking in video surveillance. Hackers use hijacked PU devices (such as cameras) to launch DDoS attacks and can also use fake devices connected to a video cloud platform to attack internal systems. Therefore, it is recommended to enhance the system-level security of PU device for video surveillance through technical means, including access control, vulnerability assessment, trusted surveillance, equipment authentication, data encryption, and attack protection.

7.1.1 Access control

Security access control achieves effective identification and security management of various types of PU device. It is recommended to support video protocol analysis and establish an [ITU-T H.626]

protocol feature library and device fingerprint library. Only authorised devices are allowed access, and authorised devices are only allowed to transmit authorised data to ensure the security and control of the PU device access process. Furthermore, and prevent illegal private connections, fraudulent use, and timely alarm and make devices knowable and trusted in the network.

The security access control policy is recommended to control access separately according to security requirements and terminal data transmission protocols.

Device access mechanism based on [ITU-T H.626] protocol analysis

For the device access mechanism based on [ITU-T H.626] protocol analysis, it is recommended to support identifying whether an Internet protocol camera (IPC) is accessed using [ITU-T H.626] protocol and extracting the device information of session initiation protocol (SIP) signalling protocol in [ITU-T H.626] protocol, including device ID, device type, manufacturer, model, and firmware version number. Then, it is recommended to identify whether the device information is in the platform-side asset whitelist. If not, it is to alert and block it.

Access mechanism based on device fingerprints collected by the secure access module

The secure access module includes forms such as a secure access gateway or secure plug-in to realise PU device access security and transmission security functions. The secure access gateway is deployed in hardware form behind devices (such as IPC) to realise secure authentication and encrypted transmission of terminals. The secure plug-in is loaded in software form into devices (such as IPC) to achieve secure authentication and encrypted transmission of terminals.

For security IPC, a secure plug-in is recommended to be integrated in the IPC to generate a unique device fingerprint by collecting the MAC address, device type, manufacturer, model, and operating system of the PU device through the secure plug-in.

For other IPC(s), a secure access gateway is recommended to be connected behind the other IPC to generate a unique device fingerprint by collecting the MAC address, device type, manufacturer, model, and operating system of the PU device through the secure access gateway.

It is recommended to upload device fingerprint information to the platform-side asset management module for fingerprint identification of video surveillance device access. If the device fingerprint matches the information in the platform-side device fingerprint library, the PU device is allowed to access the video capability platform, and the device with the wrong fingerprint information should be blocked and alerted in real time.

Access mechanism based on password system

For high security demand scenarios, key information such as a digital ID book is recommended to be written in the IPC to achieve device access using a public key cryptosystem.

Access mechanism based on device address characteristics

For IPC or network video recorder (NVR), it is recommended that access control be performed by collecting device information, such as the Internet protocol (IP) and MAC address of the device, generating a device address feature code, and binding it with the device ID. At the same time, it is stored in the platform-side asset management module to realise device information registration.

7.1.2 Vulnerability assessment

It is recommended to support regular vulnerability security scan and weak password scan for PU device to master the security status of devices, while dynamically sorting out asset information.

Vulnerability security scan

Vulnerability security scan is recommended to perform a regular scanning schedule for on-net devices and generate device vulnerability scan reports, with the scope of the scan specified by device type

and IP. The device vulnerability scan report includes information such as vulnerability name, risk level, discovery time, vulnerability port, and vulnerability description. It is recommended to support vulnerability security interface queries for on-net terminals and support retrieval by conditions, including terminal name, belonging group, IP address, MAC address, and terminal type.

Weak password detection

Weak password detection is recommended to perform a regular scanning schedule for on-net devices and generate device weak password scan reports, with the scope of the scan specified by device type and IP. The device weak password scan report includes information such as terminal name, belonging group, IP address, MAC address, and terminal type. It is recommended to support updating and configuring weak password tables.

7.1.3 Trusted surveillance

Based on trusted computing technology, the system's electronic fingerprint is established through a comprehensive collection of IPC system bootloader, operating system core files, and important configuration parameters to realise the security protection of the operating system.

Once a breach of trustworthiness is detected, an alarm message will be sent to the management backend.

7.1.4 Equipment authentication

It is recommended to use a variety of technologies to implement device authentication functions such as password, device fingerprint, password technology, etc., to confirm the authenticity of the PU device identity.

7.1.5 Data encryption

Security IPC is recommended to support data encryption based on password technology through the built-in secure access module.

Other IPC(s) are recommended to support the implementation of data transmission encryption protection through the secure access gateway.

7.1.6 Attack protection

For security IPC, it is recommended to implement a security protection function through the built-in secure access module to block network attacks and abnormal access behaviour against the PU device.

For other IPC, it is recommended to implement security protection function through the secure access gateway to block network attacks and abnormal access behaviour against the PU device.

7.2 Transmission security requirements

It is recommended to use encryption measures to ensure the confidentiality of data and prevent information attacks during data transmission.

It is recommended to encrypt key video service data during transmission by deploying an SIP signalling gateway and video security gateway to prevent data eavesdropping.

7.2.1 Transmission encryption

Transmission encryption is applicable to security IPC and other IPCs.

The security IPC is recommended to embed the secure access module.

Other IPC(s) are recommended to add the secure access gateway.

Both the secure access module and the secure access gateway are embedded with encryption modules to enable encryption of the video data collected by the IPC.

The secure access module and the secure access gateway negotiate with the platform based on the key to establish transmission encryption channels (such as virtual private networks, etc.) to protect the integrity and confidentiality of video streams and signalling during transmission.

7.2.2 Digital signature

It is recommended to embed the secure access module on the security IPC or add the secure access gateway to other IPC(s) to provide two-way identity authentication and video data signature capabilities.

7.3 Platform security requirements

Platform security is the foundation of business application security.

It is recommended to provide access control capability of platform resources and formulate access control policies for tenants' IP addresses, target ports, access protocols and access rights.

It is recommended to use security hardening techniques to protect the platform environment.

It is recommended to provide security protection capability for tenants on public networks.

Platform security includes virtual network security, host-network security, storage security, identity security, and video content filtering.

7.3.1 Virtual network security

It is recommended to control the network traffic of the platform for security access, build an isolated virtual network environment, and timely detect and block malicious threats in the network.

7.3.2 Host-network security

The virtual machine agent security plug-in for host protection is recommended to detect traffic between virtual machines, performance status of virtual machines, and risk status.

It is recommended to detect and alert on the failure of resource isolation between virtual machines for intrusions on critical nodes, and to detect and alert on propagating malicious code infections.

7.3.3 Storage security

Mechanisms such as multi-copy redundancy, data consistency assurance, and virtualisation isolation are recommended to ensure secure and reliable cloud storage.

It is recommended to ensure that memory and storage space are fully cleared when reclaimed.

When a tenant deletes business application data, it is recommended that the platform remove all copies from the cloud storage.

7.3.4 Identity security

When managing devices in the platform remotely, it is recommended to establish a two-way authentication mechanism between the management terminal and the platform.

When a cloud tenant logs into the platform, it is recommended that a two-way authentication mechanism be established between the tenant and the platform.

It is recommended to unify the management of privileged accounts such as platform operation and maintenance management to reduce the risk of privileged accounts being abused.

7.3.5 Video content filtering

It is recommended to provide the ability to detect viruses, remote control Trojans, attack software packets, etc. that are entrapped in the network traffic of video transmission.

It is recommended to transmit video data according to the pre-registered video data format. It is recommended to support real-time analysis and filtering of transmitted video data, blocking and alarming of video data that does not conform to the format.

7.4 Application security requirements

The platform carries various cloud applications. It is recommended to strictly control access to the application to prevent illegal theft of video resources.

Application security requirements include video leak proof and authorisation management.

7.4.1 Video leak proof

It is recommended to support the encryption of sensitive video data during video access.

It is recommended to implement features such as user authentication access, video data encryption, watermark loading (text watermark, quick response (QR) code watermark, dot matrix watermark, etc.), and screenshot prohibition.

Automatic encryption

When the surveillance video is downloaded locally, it is recommended to automatically encrypt it to ensure that it can only be opened on the downloaded computer.

Screenshot control

It is recommended to block all kinds of screenshot software and screen recording software to avoid taking screenshots and recording screens while playing surveillance video.

Watermark loading

It is recommended to provide a watermark loading function, including an invisible dot matrix watermark, visible text watermark, and visible QR code watermark, which can be loaded with self-defined text description, date, time, source IP, MAC address and username to avoid screen recording and ensure the traceability of surveillance video data.

7.4.2 Authorisation management

Authorisation management includes examining and approving surveillance video data and surveillance video data control.

Examine and approve surveillance video data

When someone wants to access surveillance video, it is recommended to support the management and recording of the surveillance video access process, including request, approval, and authorisation management.

Surveillance video data control

When someone is authorised to access surveillance video, it is recommended to restrain the video visitor by setting a password, limiting the access time and the number of times, and loading a watermark on the surveillance video to ensure the security of the surveillance video.

7.5 Network security requirements

Network security recommends communicating through authorised interfaces provided by edge devices.

It is recommended that only authorised devices can connect to the internal network, and that internal users can only connect to the external network after authorisation.

Network security requirements include access control and network protection.

7.5.1 Access control

It is recommended to monitor various access operations occurring on the network and the data packets transmitted on the network.

It is recommended to analyse protocol behaviour and network traffic data to discover security risks and perform timely access control and alerts according to security policies.

It is recommended to identify and control the application-layer protocol to achieve malicious code protection and application attack protection. The specific protocol control requirements are as follows:

– It is recommended to only allow SIP, real-time transport protocol (RTP), real-time streaming protocol (RTSP), real-time transport control protocol (RTCP) and hypertext transfer protocol secure (HTTPS) protocols access, filter the signalling and parameter keywords of these protocols, and only allow three business services and ports: SIP signalling control, RTP and RTSP media transmission, and Representational state transfer (REST) intelligent analysis data transmission.

– It is recommended to prohibit hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), file transfer protocol (FTP), teletype network (TELNET), secure shell (SSH), network file system (NFS), post office protocol-version 3 (POP3), dynamic host configuration protocol (DHCP), and other unnecessary protocols access.

7.5.2 Network protection

It is recommended to provide the application layer intrusion prevention function to analyse messages from header to content and match them with pre-defined attack characteristics to discover and block hidden attack messages in the data flow. At the same time, it is recommended to analyse the interaction behaviour of protocols and discover abnormal network protocol messages to detect attack behaviour. When a security threat is detected, it can respond in real time and defend automatically.

It is recommended to monitor attacks at the application layer of the platform including port scanning, trojan horse attacks, denial of service attacks, buffer overflow attacks, IP fragmentation attacks and network worms.

When an attack is detected, it is recommended to record the attack source IP, attack type, attack purpose, attack time, and provide an alert in case of a serious intrusion.

7.6 Security management centre requirements

It is recommended to monitor the status of video surveillance devices in real time in order to detect abnormal devices and provide early warning.

It is recommended to unify the security management of the platform and provide security situational awareness capability.

7.6.1 Asset management

It is recommended to collect PU device information through active scanning, passive listening, manual setting, establish a device fingerprint database (mainly containing an IP address, MAC address, device type, manufacturer, model, hostname, operating system, etc.) and conduct classification statistics to realise unified asset management of devices.

7.6.2 Key infrastructure

For high security level scenarios, it is recommended to provide full life-cycle management of encryption and decryption keys (including symmetric keys, asymmetric keys, digital certificates, etc.).

It is recommended to provide encryption capability for cloud platform and application data.

7.6.3 Security situational awareness

It is recommended to dynamically integrate information on platform assets, attacks, threats and vulnerabilities, and analyse them using big data technology to grasp the overall security status of the platform.

It is recommended that security situation reports be generated automatically on a regular basis to judge and warn of current network and future threats. The security situation report includes statistics of relevant data, including the number of security vulnerabilities, attack IP, attacked assets, attacked domain names, attack events, attack threat levels, etc.

Appendix I

Typical use case and scenario

(This appendix does not form an integral part of this Recommendation.)

I.1 PU authentication

Step 1: Bob is the administrator of the video surveillance platform at X museum. He logs into the video surveillance platform using his account and password in the X museum's dedicated virtual network environment. He can see all the devices currently connected to the platform in the asset management module of the platform. The asset management module contains an asset whitelist and device details, etc. The X museum video surveillance platform is pre-set to allow access only to IPC with [ITU-T H.626] protocol.

Step 2: Alice wants to connect the A-level IPC at the new point of the X museum to the video surveillance platform. She requests Bob to add the IPC to the platform asset whitelist and provides Bob with the IPC's device ID, device type, manufacturer, model, firmware version number, etc.

Step 3: After Bob adds the IPC to the platform asset whitelist, Alice connects the A-level IPC into the platform in the virtual network environment dedicated to the X museum. The video surveillance platform first identifies whether the IPC uses the [ITU-T H.626] protocol to access, and after successful identification extracts the device information in the [ITU-T H.626] standard SIP signalling protocol, including device ID, device type, manufacturer, model number, and firmware version number, and matches this information with the platform side asset whitelist. After successful matching, the IPC is successfully connected to the X museum video surveillance platform.

Figure I.1 illustrates this scenario.

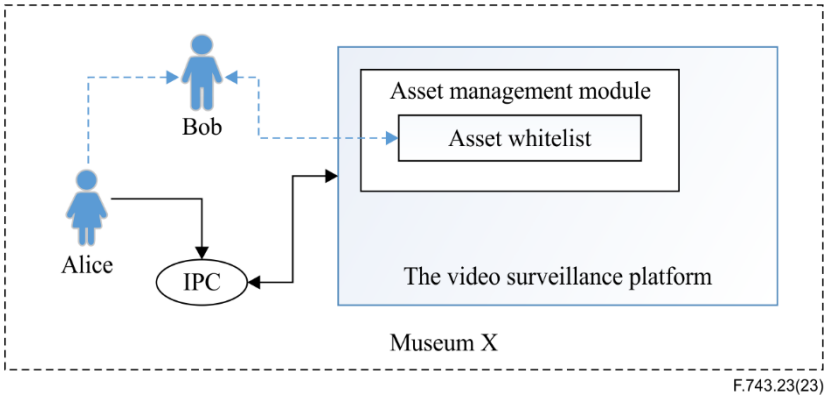

Figure I.1 – PU authentication

I.2 Security hardening of video surveillance systems

Step 1: Company M is a leading company in the industry. Company M is at location G and the factory is at location H. Company M uses the video surveillance system to view the operation of the factory in real time. Since the factory involves M company's commercial secrets, M company proposes to strengthen the security of the video surveillance system.

Step 2: Company M first reinforces the security of the IPCs in the factory. The security capability of the current IPCs in the factory are all B-level. For security IPC, secure access module is added, and for other IPC(s), a secure access gateway is installed to block network attacks and abnormal access behaviours against the PU devices and to realise the security protection function for the IPCs. Among them, the secure access module and secure access gateway are

embedded with encryption modules to realise the encryption of the video data collected by the IPCs, making the security capability of the factory's IPCs reach the C-level. The secure access module and secure access gateway negotiate with the platform based on keys to establish transmission encryption channels (such as VPN, etc.) to protect the integrity and confidentiality of IPC video streams and signalling in the transmission process. Besides, company M encrypts the IPC's video data during transmission by deploying an SIP signalling gateway and video security gateway to prevent the data from being eavesdropped.

Step 3: Company M conducts security access control for the network traffic of the video monitoring platform and builds an isolated virtual network environment. At the same time, company M sets multiple platform administrators for the video surveillance platform and divides the authority, and each administrator is responsible for an area in the factory. All platform administrators have to log into the platform in the virtual network environment and verify their identity with the platform. After successful verification, the administrators can only view and manage the devices and video files within their authority, and company M manages these platform management accounts uniformly to reduce the risk of abuse of privileged accounts.

Figure I.2 illustrates this scenario.

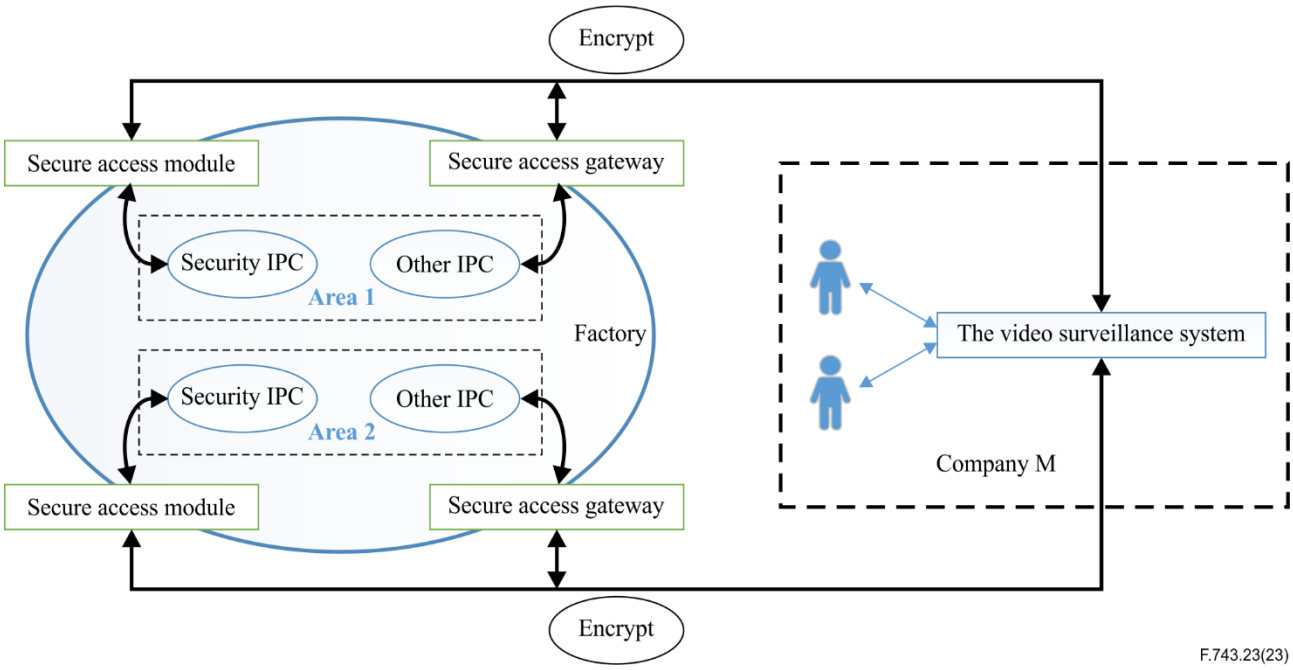

Figure I.2 – Security hardening of video surveillance systems

I.3 Detect and block malicious threats and send alerts

Step 1: Company E provides a common video surveillance management platform called the Q platform. Company A and company B are tenants of the Q platform. Company A and company B connect each company's IPCs to the Q platform for management. Company A and company B are independent of each other on the Q platform. Company E can only see tenant information on the Q platform but cannot view and manage customer's devices and video files.

Step 2: John is the platform administrator of company A and Smith is the platform administrator of company B. John and Smith log into the Q platform in their respective companies' isolated virtual network environment. They can only see and manage their own company's devices and video files on the Q platform.

Step 3: Q platform provides periodic vulnerability security scan and weak password detection for all devices accessing the platform, specifies the scanning scope by terminal type and IP address, and generates a terminal vulnerability scan report and terminal weak password scan report. The content of the terminal vulnerability scan report includes information such as vulnerability name, risk level, discovery time, vulnerability port, and vulnerability description. The terminal weak password scan report includes the terminal name, belonging group, IP address, MAC address, terminal type, and weak password type.

Step 4: One day, Q platform performed regular security scans and found that a device in company A had a weak password, and immediately generated an alert message and a weak password scan report and sent it to John. John received the alert message and rectified the device based on the device information in the weak password scan report, instantly changing the default password of the device and securing the device.

Step 5: One day, Q platform performed a regular security scan and found that company B's device had a remote code executable vulnerability, and immediately generated an alert message and vulnerability scan report and sent it to Smith. After receiving the alert message, Smith immediately analysed the vulnerability and initiated a vulnerability fix to ensure the security of the device.

Figure I.3 illustrates this scenario.

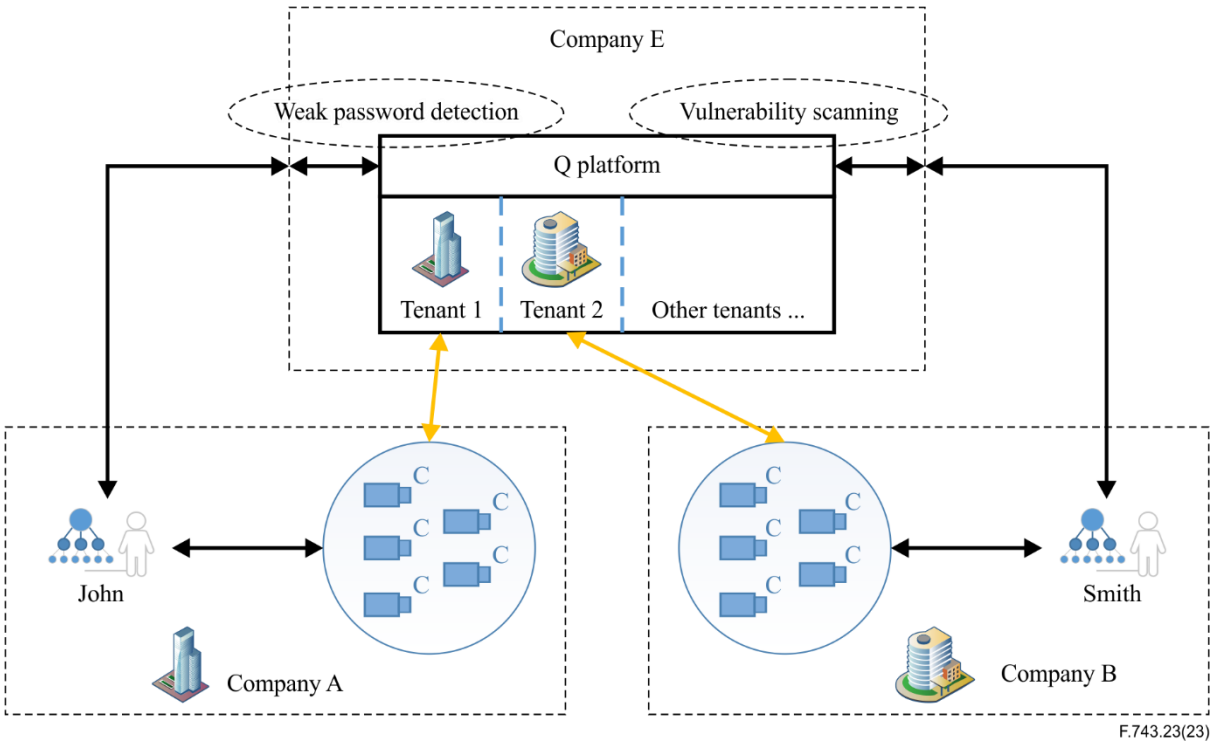

Figure I.3 – Detect and block malicious threats and send alerts

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

Published in Switzerland
Geneva, 2023