TAICS

TAICS TS-0014-1(E) v1.0 : 2019

Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements

2019/03/26

社團法人台灣資通產業標準協會

Taiwan Association of Informationand Communication Standards

Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements

Published date: 2019/03/26
Approved date: 2018/06/07

Acknowledgements

This standard is formulated by the TAICS-TC5 Network and Information Security Technical Committee.

TC President: Kuang-Chun Hung, General Manager, Onward Security Inc.

TC Vice President: Cheng-Yu Tsai, Section Chief, Institute for Information Industry

TC IoT Security Working Group Leader: Dr. Chuan-Kai Kao, Section Chief, Institute for Information Industry

The list of association members participating in this standard formulation is as follows:

National Chung-Shan Institute of Science and Technology; Industrial Technology Research Institute; Electronics Testing Center, Taiwan; Institute for Information Industry; Telecom Technology Center; Chunghwa Telecom; D-Link Corporation; Onward Security; HTC Corporation; Digicentre Company Limited; National Central University; A Test Lab Technology Corporation; Synology Inc.; Trend Micro Inc.; Gapertise Inc.; and ArcRan Inc.

This standard is supported by the National Communications Commission and Industrial Development Bureau, MOEA, R.O.C..

Contents

Acknowledgements 1
Contents 2
Foreword 3
Introduction 4
1. Scope 6
2. Normative References 7
3. Terms and Definitions 8
4. Security Level 15
4.1 Brief Introduction 15
5. Security Requirements 18
5.1 Physical Layer 18
5.2 System Layer 19
5.3 Communication Layer 21
5.4 Authentication and Authorization 23
5.5 Privacy 25
Appendix A (Normative) Version Requirements of Security Channel 26
Appendix B (Normative) Communication protocols for video surveillance devices 27
Appendix C (Normative) WPA Versions of video surveillance devices 28
Appendix D (Informative) Technical requirements and comparison table of standards 29
References 33
Revision Record 35

Foreword

This is an industry standard regulated and published by the Taiwan Association of Information and Communication Standards (TAICS) with the approval of the TAICS council.

This standard does not suggest all the safety precautions. The related safety maintenance and health operations shall be established and the relevant regulations shall be obeyed before applying this standard.

Part of this standard may involve patents, trademarks, and copyrights. The association is not responsible for the identification of any patents, trademarks, and copyrights.

Introduction

Internet of things (IoT) is the fastest developing industry across the world, and related applications are constantly being innovated. Information security is undeniably the key to the success of IoT technology. Therefore, the Industrial Development Bureau, Ministry of Economic Affairs (MOEA), first sets goals for the environmental standards for IoT security, including video surveillance systems, internet of vehicles (IoV) systems, IoT general systems, auxiliary applications, industrial control systems, medical equipment systems, and point of sale security standards. These standards promote the overall quality of domestic industries and product competitiveness and ensure that consumers are assured information security when they use monitoring devices. The list of all TAICS TS-0014 series standards is available on the TAICS website.

IoT technology, especially video surveillance equipment has moved supply chains toward digitalization. IoT applications have a very extensive scope, including IoV, internet of home, medical networks, and community networks. Consequently, cyberattack events have become commonplace. The frequency and scope of these attacks have been increasing since 2014. At the end of 2016, a malware named Mirai used an Internet protocol (IP) camera as a springboard and created an unprecedented cyberattack.

In view of this, TAICS referred to the international IoT-related cybersecurity standards/guidelines, such as CNS 27001 [1], ANSI/CAN/UL 2900-1: 2017 Standard [2], Groupe Speciale Mobile Association (GSMA) IoT Security Guidelines [3], Open Web Application Security Project (OWASP) Top IoT Vulnerabilities [4], and IoT security guidelines from the Japanese government [5], to establish standards for security quality in domestic video surveillance systems, including (1) physical security, (2) system security, (3) communication security, (4) authentication and authorization mechanism security, and (5) privacy protection. These five security aspects adopt detailed common methods for video surveillance devices.

TAICS TS-0014 series standards correspond to video surveillance systems, including IP cameras, video recorders, and network-attached storage (these devices are generally called video surveillance devices). The TAICS TS-0015 series testing specifications include the testing methods and criteria to verify whether the products meet the norms provided by the TAICS TS-0014 series. “TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System-Part 1: General Requirements” (hereafter referred to as “this/the standard”) includes the “TAICS TS-0014-2 Cybersecurity Standard for Video Surveillance System-Part 2: IP camera” [6], “TAICS

TS-0014-3 Cybersecurity Standard for Video Surveillance System-Part 3: Video Recorder" [7], and "TAICS TS-0014-4 Cybersecurity Standard for Video Surveillance System" [8]. All video surveillance devices must follow the related security regulations in these standards.

1. Scope

Video surveillance systems, whose purpose is to monitor specific locations for security maintenance, mainly consist of IP cameras, digital video recorders, network video recorders, and network-attached storage. These systems further comprise (1) dedicated monitoring infrastructure for the installed cameras, local or remote computer devices, mobile devices, and cloud servers and (2) a functional networking environment, including Wi-Fi access points, routers, and switches.

2. Normative References

The following documents are referred to in the text in such a way that some or all of their content constitutes the requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

(1) ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements

(2) CNS 27001: 2013 Information Technology-Security Techniques-Information Security Management Systems-Requirements

(3) NIST SP 800-9 Guide to Computer Security Log Management

3. Terms and Definitions

The following terms and definitions are applicable in the standard.

3.1 Video Surveillance System

The purpose of video surveillance systems is to monitor specific locations for achieving the goal of security maintenance. These systems are commonly used to monitor personnel entrances and exits, garage, parking lots, or other important places. To ensure security, video surveillance systems are mainly composed of the following equipment: IP cameras, video recorders, and network-attached storage.

3.2 IP Camera

Embedded cameras, such as IP cameras, smart cameras, and 3D cameras, used in video surveillance systems are equipped with a networking function.

3.3 Video Recorder

Video recorders, such as digital video recorders (DVRs) and network video recorders (NVRs), used in video surveillance systems are equipped with networking function.

(a) DVR: A DVR is a type of closed-structure image storage and management device that supports image formats such as NTSC and PAL and also supports a wired (e.g., coaxial cable) front camera. Its image storage supports built-in storage media.

(b) NVR: A NVR is a type of open-structure image storage and management device that supports image formats such as H.264 and AVI and also supports both wired (e.g., network line) and wireless (e.g., Wi-Fi) front cameras. Its image storage supports local or remote storage media.

3.4 Network-Attached Storage

Devices dedicated to data storage on the internet run management-related functions, such as data access, and support multiple file transport protocols, which allows different operating systems or computers with different protocols to obtain access to the network-attached storage.

3.5 Embedded Camera

A microprocessor-based camera with a specific function and computing efficiency is mostly embedded in a device consisting of digital hardware and mechanical components.

3.6 Security Vulnerability

A defect in device security threatens the confidentiality, integrity, and availability of the system or application data.

3.7 Common Vulnerabilities and Exposures (CVE)

The CVE is a vulnerability plan sponsored by the US Department of Homeland Security. The plan assigns a globally recognized unique number to each vulnerability.

3.8 National Vulnerability Database (NVD)

The NVD is provided by the National Institute of Standards and Technology (NIST) [9]. The NIST is responsible for the release and update of common vulnerabilities listed in the CVE.

3.9 Common Vulnerability Scoring System (CVSS)

The CVSS is a set of criteria for scoring common vulnerabilities. The severity of the damage caused by the threat, accessibility of the security vulnerability, and degree of difficulty for an attacker to make improper use of the vulnerability are included in the scoring system. The score ranges from 0 to 10, where 0 indicates no risk and 10 indicates critical risk [10].

3.10 Severity Rating

A CVSS rating of 0 indicates no severity, a rating of 0.1 to 3.9 indicates low severity, a rating of 4.0 to 6.9 indicates medium severity, a rating of 7.0 to 8.9 indicates high severity, and a rating of 9.0 to 10 indicates critical severity.

3.11 Sensitive Data

Sensitive data is information built, stored, or transmitted in a device and its affiliated storage media according to the user's behavior or operation of mobile applications. The leakage of this information, including but not limited to personal information, passwords, keys, or geographic locations, may cause damage to the user.

3.12 Personally Identifiable Information

According to Article 2.1, Chapter I of the Personal Information Protection Act [11], personally identifiable information includes the name, date of birth, I.D. card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical records, genetic information, sexual life, health examination, criminal record, contact information, financial conditions, social activities, and other information that may be used to identify a natural person both directly and indirectly.

3.13 Privacy

Privacy refers to private information, all or part of which shall not be publicized. The owner has the right to protect such information. The privacy indicated in this standard includes videos recorded by video surveillance systems and user information.

3.14 Control Programs

Control programs are applications used to control video surveillance device motion or browse surveillance contents, including mobile and desktop applications.

3.15 Control Management

Control management involves achieving device operation system control through a local or remote network as follows:

(a) By enforcing product maintenance, accessing device resources, surveying screens, or controlling cameras through a control program, website management interface, or command interface.

(b) By setting up the system using a control program, website management interface, or command interface (e.g. IP address).

3.16 Application Program Interface (API)

The API is an interface that connects different parts of the software system. Currently, the most commonly used video surveillance device is the open network video interface forum (ONVIF) application interface. Users access the ONVIF application interface through hypertext transfer protocol (HTTP) to gain control of the related operating applications of IP cameras, such as system information extraction and image surveillance extraction.

3.17 Third-Party Library

A third-party library is a library with a specific function created by other organizations. A system designer refers to a third-party library to accelerate development of or meet the services required by the device.

3.18 Encryption

Encryption involves the use of a math algorithm to modify the original information for making it unreadable.

3.19 Digital Signature

A private key, which produces a specific length of electronic document via a math algorithm, is used as the user's electronic signature. It can be verified with a public key. Digital signatures not only ensure the integrity of the document but also verify the nonrepudiation of the author of the document.

3.20 Security Tunnel

A security tunnel is a protocol for secure end-to-end communication among networks. A secure tunnel is used to maintain both data confidentiality and integrity. For example, the secure sockets layer (SSL) and transport layer security (TLS) are the common communication protocols used currently.

3.21 Secure Domain, Secure World

Secure domain, secure world is an area isolated from the normal operating environment and is only used to enforce security-related operations, such as encryption and decryption, key management, and integrity inspection. It also provides reservation for sensitive data.

3.22 Government Configuration Baseline (GCB)

The GCB of Taiwan includes security settings (e.g., password length and refresh deadline) of communication terminal equipment (e.g., PC) [12] for reducing hacker intrusions and cyberattacks.

3.23 Password

A password is a group of characters that verifies user identity and forwardly controls user access to the system.

3.24 Default Password

The default password is the password set before delivery. The default password is used to login into the video surveillance device when the user connects to the network for the first time without changing any settings.

3.25 Device Authentication

Device authentication indicates that the test object must verify the identity of the connected device to ensure reliable identification of the transfer object. The common methods of authentication include asking the connected device for a username and password or using digital authentication of the device to ensure its identification.

3.26 Security Event Log

The security event log includes a recording of every activity defined by the audit rules. The recording enables users to be aware of threats or the occurrence of attack events. The security events mentioned in this standard refer to a user's behavior of logging in into the system.

3.27 Universal Plug and Play (UPnP)

UPnP enables devices to connect with each other directly and also customizes the configuration for data sharing in local area network environments (e.g., home and company networks).

3.28 Simple Network Management Protocol (SNMP)

The SNMP divides the network equipment area into two parts, manager and agent. The agent indicates the network status data of the domain collected by itself in variables, whereas the manager collects the data returned by the agent through the GET command.

3.29 Bonjour

Bonjour provides the service of auto searching for network equipment in local area network environments (e.g., home, company networks). Bonjour uses an IP protocol so that equipment can discover each other without the use of an IP address or DNS server.

3.30 Wi-Fi-Protected Setup (WPS)

WPS is a protocol launched by the Wi-Fi alliance that simplifies a user's settings on wireless security. After Wi-Fi protected access (WAP) launched the WPS mode, users only had to push the button at the client side to connect without any complicated security settings. In the WPS, connection is achieved through two methods. The first method involves using a PIN to achieve a connection, and the second involves the push-button connection mode, in which the connection is activated by pushing a button.

3.31 Wi-Fi Protected Access (WPA)

WPA includes two standards, namely WPA and WPA2, developed to protect network security and improve the shortcomings of wired equivalent privacy (WEP). WPA adopts a Michael message authentication code and RC4 cryptosystem, whereas WPA2 adopts a counter mode cipher block chaining message authentication code protocol (CCMP) message authentication code and advanced encryption standard (AES) cryptosystem.

3.32 Multifactor Authentication (MFA)

A user is allowed access to a device after multiple authentications. MFA mainly considers three factors of cryptography authentication, namely something you know, something you have, and something you are, thus identifying the same device in different phases.

3.33 Forward Secrecy (FS)

FS ensures that the past communication is safe and communication data is not leaked even if the password or key is leaked.

3.34 Debug Mode

The debug mode is also called the engineer mode. Generally, in the developing or patching stage, products stay in this mode and can access the resources of the system without limit. Moreover, error messages are displayed to the engineers for debugging use.

4. Security Levels

Security levels are a combination of security requirements that address various security risks at product deployment. Thus, security levels can be utilized to reduce or eliminate the threats to information security.

4.1 Brief Introduction

A summary of security levels is presented in Table 1, where the first column refers to security aspects, namely (1) physical security, (2) system security, (3) communication security, (4) authentication and authorization mechanism security, and (5) privacy protection. The second column refers to the goals of security requirements in each security aspect. The third column refers to security levels, each of which is a combination of security requirements that must be met to cope with various security risks, whose details are described in chapter 5.

Table 1 Summary of security levels

Security aspects	Goals of security requirements	Security levels		
		Level 1	Level 2	Level 3
Physical security	5.1.1. Access Control of Physical Interfaces	5.1.1.1	-	-
	5.1.2. Warning of Physical Abnormal Behavior	-	5.1.2.1 5.1.2.2	-
	5.1.3. Physical Protection	5.1.3.1	-	-
	5.1.4. Secure Boot	-	-	5.1.4.1
System security	5.2.1. Operating System and Security of Network Services	5.2.1.1	-	5.2.1.2
	5.2.2. Security of Network Service Ports	5.2.2.1	-	-
	5.2.3. Update Security	5.2.3.1 5.2.3.2 5.2.3.3	-	-
	5.2.4. Security of Sensitive Data in Storage	5.2.4.1 5.2.4.2	5.2.4.3	5.2.4.4
	5.2.5. Security of Website Management Interface	5.2.5.1	-	-
	5.2.6. Security of Management Applications	5.2.6.1 5.2.6.2 5.2.6.3	-	-
	5.2.7. Logs and Warnings	5.2.7.1 5.2.7.2	5.2.7.4	-

Security aspects	Goals of security requirements	Security levels		
		Level 1	Level 2	Level 3
		5.2.7.3		
Communication security	5.3.1. Security of Sensitive Data in Transmission	5.3.1.1	-	5.3.1.2
	5.3.2. Communication Protocols and Configuration Security	5.3.2.1 5.3.2.2	5.3.2.3	-
	5.3.3. Wi-Fi Communication Security	5.3.3.1 5.3.3.2	5.3.3.3	5.3.3.4
Authentication and authorization mechanism security	5.4.1. Security Authentication	5.4.1.1 5.4.1.2	5.4.1.3 5.4.1.4	5.4.1.5 5.4.1.6
	5.4.2. Password Authentication	5.4.2.1 5.4.2.2 5.4.2.3 5.4.2.4	-	5.4.2.5 5.4.2.6
	5.4.3. Security Authorization	5.4.3.1 5.4.3.2	-	-
Privacy protection	5.5.1. Protection of Access of Privacy	5.5.1.1 5.5.1.2 5.5.1.3	-	-
	5.5.2. Privacy Transmission Protection	Refer to 5.3.1.1	-	Refer to 5.3.1.2

4.1.1 Security aspects

(a) Physical security: Involves the prevention of product dismantling or the control of accessing removable media and the debug port.

(b) System security: Involves the protection of operating systems, network services, update services, and firmware.

(c) Communication security: Involves the safeguarding of sensitive data and the exploration of unknown cybersecurity vulnerabilities in used protocols (specified in Appendix B).

(d) Authentication and authorization mechanism security: Involve the enforcement of privileges of individual identities at user interfaces.

(e) Privacy protection: Involves the nondisclosure of the private information stored on video surveillance devices, such as users' personal video data.

4.1.2 Goals of security requirements

The goals of security requirements are the terms to be examined in each security aspect and shall include one or more security requirements.

4.1.3 Formation of security levels

Security levels are divided into three categories, namely Level 1, Level 2, and Level 3, according to the associated cybersecurity risks and implementation complexities. The level number indicates the increasing significance of the required security, with lower security levels being met first to satisfy a higher one.

5. Security Requirements

This chapter describes in detail the common methods employed for satisfying the security functions of video surveillance. All video surveillance devices (each referred to as “target product” hereafter) shall meet all the stated requirements accordingly.

5.1 Physical Security

5.1.1 Access control of physical interfaces

5.1.1.1 The target product only provides limited access rights to the user, which means that the target product shall default to “no access to target product’s debug mode” through a physical interface.

5.1.2 Warning of physical abnormal behavior

5.1.2.1 The target product shall record the plug-ins and unplugs of physical ports.

5.1.2.2 The target product shall have a related warning mechanism when the network connection is lost by the physical layer.

5.1.3 Physical protection

5.1.3.1 The exterior of the target product shall not have a design that can enable resetting the default password by hand.

5.1.4 Secure boot

5.1.4.1 The target product shall support secure boot and shall not be booted using unauthorized firmware, drivers, or operating systems to make ensure of the integrity and reliability of the system.

5.2 System Security

5.2.1 Operating system and security of network services

5.2.1.1 The operating system and network service of the target product shall not have CVE with a critical severity rating as per the CVSS v3 severity rating.

5.2.1.2 The operating system and network service of the target product shall not have CVE with a high severity rating as per the CVSS v3 severity rating.

5.2.2 Security of network service ports

5.2.2.1 The network service activated by the target product shall be necessary for the main service provided by the supplier to prevent the possibility of products being invaded upon enabling the network interface. Moreover, the supplier shall label the accessibility of the network service in the target product document to avoid the activation of an unclaimed network service.

5.2.3 Update security

5.2.3.1 Firmware shall be equipped with an update mechanism

(a) If the target product supports offline manual updates, the updated files shall be encrypted to ensure confidentiality by adopting an encryption algorithm approved by FIPS 140-2 Annex A [14], or the source code of the target product firmware and other files during installation shall not have decrypted plain text or sensitive data.

(b) If target product supports online updates, the update route shall pass through the security channel and the version of the security channel shall meet the requirements of “Appendix A.” Moreover, the key exchange protocol shall support FS. The identification process shall verify the validity and legality of this security channel certificate (e.g., issuer organization, expiry date, format error, and signature).

5.2.3.2 The target product shall have the ability to verify the integrity and nonrepudiation of the firmware update file.

5.2.3.3 The target product shall have the ability to recover a failed firmware update to normal operation when the update operation is aborted.

5.2.4 Security of sensitive data in storage

5.2.4.1 The access to sensitive data of the target product shall have an authority control mechanism.

5.2.4.2 The authentication factors, keys for encrypting/decrypting (not including the public key for asymmetric encryption), and personal data in the target product shall not be stored in plain text. The encryption algorithm used to protect data shall be authorized by FIPS 140-2 Annex A.

5.2.4.3 The target product shall provide the process of key management to ensure the quality of key management.

5.2.4.4 Sensitive data shall be stored in the security domain of the target product, which is isolated from the normal operating environment.

5.2.5 Security of the website management interface

5.2.5.1 The website management interface of the target product shall not exist in the injection and cross-site scripting attack of OWASP web top 10 [15].

5.2.6 Security of management applications

5.2.6.1 An API shall be equipped with a mechanism for authentication according to the requirements in 5.4.1.1 and 5.4.1.2.

5.2.6.2 Password authentication for an API shall meet all the requirements in 5.4.2.

5.2.6.3 The access control of the API shall meet all the requirements in 5.4.3.

5.2.7 Logs and warnings

5.2.7.1 Logs of security events and the revealing function shall be maintained. The access behavior of users shall be clearly recorded to check if any unauthorized or abnormal

logins have occurred. The content of logs shall include a full timestamp, user identity, and the result of enforcement for subsequent review.

5.2.7.2 Logs of security events shall have access control, which shall not allow access without authorization.

5.2.7.3 Logs of security events shall be equipped with a log rotate mechanism.

5.2.7.4 The warning function shall be provided by the target product to avoid situations where the logs of security events cannot be saved.

5.3 Communication Security

5.3.1 Security of sensitive data in transmission

5.3.1.1 The transmission of sensitive data shall pass the security tunnel by default, and the version of the security tunnel shall meet the requirements of "Appendix A." Moreover, the protocol of key exchange shall support FS, whereas the process of identity authentication shall verify the validity and legality of this security channel certificate (e.g., issuer organization, expiry date, format error, and signature, and so forth).

5.3.1.2 The strength of the encryption algorithm used by the security channel shall be equal to or higher than AES-256.

5.3.2 Communication protocols and configuration security

5.3.2.1 The target product shall provide a function that allows users to turn on/off "Network device information inquiry" automatically, such as UPnP, SNMP, and Bonjour.

5.3.2.2 Accessing the debug mode of the target product through the network in default shall not be allowed.

5.3.2.3 Improper error handling shall not exist in the communication protocol of the target product mentioned in Appendix B, including the fields of message length, message

identifier, and key agreement attribute, and so forth, so that the target product does not crash or the service does not terminate.

5.3.3 Wi-Fi communication security

5.3.3.1 The target product shall provide the WPS PIN function, which users can turn on/off, and the default mode of the function shall be off.

5.3.3.2 The Wi-Fi security mechanism shall adopt WPA by default, and the version of WPA shall meet the requirements of “Appendix C.”

5.3.3.3 Improper error handling shall not exist in the Wi-Fi protocol of the target product mentioned in Appendix B, including the fields of message length, message identifier, and key agreement attribute, and so forth, so that the target product does not crash or the service does not terminate.

5.3.3.4 The authentication mechanism of the Wi-Fi shall support 802.1X port-based network access control.

5.4 Authentication and Authorization mechanism security

5.4.1 Security authentication

5.4.1.1 Before accessing the target product resources, passing through the authentication mechanism (which prevents replay attacks) shall be required.

5.4.1.2 The authentication error message shall not show the name of the legal user.

5.4.1.3 The target product shall have the function of uploading certificates to increase the cybersecurity of the credential authentication mechanism.

5.4.1.4 Every time the target product resets the factory settings, the certificate key (including Secure Shell (SSH) and TLS) shall change, which ensures the uniqueness of every product key and reduces the possible risk of key leakage.

5.4.1.5 Target product shall adopt MFA.

5.4.1.6 The connected video surveillance products shall support mutual authentication to ensure the validation of the connected device.

5.4.2 Password authentication

5.4.2.1 Each product shall have different default passwords. If the target product is accessed successfully for the first time, the password shall be forced to change.

5.4.2.2 The principal of the password strength basically refers to the password principal category of the GCB, and the length of the password shall be at least longer than eight characters.

5.4.2.3 The principal of password strength basically refers to the password principal category of the GCB, and the characters in the password shall match three of the following four types of characters: (1) English capital letters (A to Z), (2) English lower case letters (a to z), (3) decimal digits (0 to 9), and (4) non-English characters (e.g., !, $, #, and %).

5.4.2.4 The target product shall limit the frequency and number of times for entering a password. It shall also perform the following tasks:

(a) Lock the account if login fails up to five times.

(b) Lock the account within a certain period of time.

(c) Reset the counter of failed login attempts at least after a certain period of time.

5.4.2.5 The principal of password strength basically refers to the password principal category of the GCB, and the user's account name and password shall not include more than three consecutive and identical characters.

5.4.2.6 The principal of password strength basically refers to the password principal category of the GCB, and the password history policy shall be enforced.

5.4.3 Security authorization

5.4.3.1 The target product shall classify the user according to their roles, such as general user and system administrator, and so forth. It shall also define each permission in target product document to ensure the permission of each role is matched with the one claimed in target product document.

5.4.3.2 There shall be a limit to the idle time for users to set the target product's authorization behavior. If the remote connection is timed out, lost, or ended, a new authentication is required.

5.5 Privacy Protection

5.5.1 Privacy access protection

5.5.1.1 Private information stored in the target product shall only be accessed by authorized individuals.

5.5.1.2 Users shall have the rights to delete the private information they have saved.

5.5.1.3 Every time a new login event occurs, the target product shall issue a warning message automatically.

5.5.2 Privacy transmission protection

5.5.2.1 The requirements of privacy transmission protection are in accordance with the requirements of “5.3.1 Security of Sensitive Data in Transmission.”

Appendix A
(Normative)
Version Requirements for the Security Channel

HTTP is combined with the TLS or SSL protocols to establish security channels for preventing transmitted data from being stolen. However, after Google pointed out the cybersecurity vulnerabilities in SSL in October 2014, TLS has completely replaced SSL. However, an existing function of TLS 1.0 allows it to be degraded to SSL 3.0, which makes TLS 1.0 unreliable as well. Therefore, the version of the security channel this standard shall follow is TLS v1.2 or higher.

Appendix B
(Normative)
Communication Protocols for Video Surveillance Devices

B.1 Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP):

The RTP and RTCP are defined in RFC 3550 [16] and are commonly applied to video streaming systems, video conferencing, and push-to-talk systems. They define the standard format of packets used to deliver audio and video through the network. RTCP is not used for data transmission, but it supports RTP to pack and send media data. RTCP provides statistics and transmission control information periodically by out-of-band on an RTP conference connection. The main function of this protocol is to provide feedback on the quality of service.

B.2 Real-time Streaming Protocol (RTSP)

The RTSP is defined in RFC 2326 [17] and is used for controlling data for immediate use, such as playing, recording, and pausing video/audio multimedia. This, immediate video/audio control can be achieved between the user end and media server.

B.3 TLS

The TLS protocol is defined in RFC 5246[18]. It establishes a security channel between two applications through the network and can prevent eavesdropping and tampering during data exchange.

Appendix C
(Normative)
WPA Versions of Video Surveillance Devices

WPS is a mechanism to ensure secure Wi-Fi transmission. It implements IEEE 802.11i to solve the cybersecurity problems caused by WEP. WPA is also vulnerable to cyberattacks. The version that this standard shall currently use is Wi-Fi-protected access v2 or above.

Appendix D
(Informative)
Technical Requirements and Comparison of Standards

Table D.1 Technical requirements and comparison of standards

Technique requirements	Term corresponds to OWASP [3]	Term corresponds to ONVIF [19, 20]
5.1.1.1	I10: Poor Physical Security Ensuring only required external ports such as USB are required for the product to function. Ensuring the product has the ability to limit administrative capabilities.	-
5.1.2.1 5.1.2.2	-	-
5.1.3.1	I2: Insufficient Authentication/Authorization Ensuring that password recovery mechanisms are secure.	-
5.1.4.1	I9: Insecure Software/Firmware Implement the secure boot if possible (chain of trust).	-
5.2.1.1 5.2.1.2	-	-
5.2.2.1	I3: Insecure Network Services Ensuring only necessary ports are exposed and available.	-
5.2.3.1	I9: Insecure Software/Firmware Ensuring the device has the ability to update (very important, needs a secure update mechanism). Ensuring the update file is encrypted using accepted encryption methods. Ensuring the update file is transmitted via an encrypted connection. Ensuring the update file does not expose sensitive data.	Core Spec. – Ver. 16.12 4.5.5 Firmware Upgrade
5.2.3.2	I9: Insecure Software/Firmware Ensuring the update is signed and verified before allowing the update to be uploaded and applied.	-
5.2.3.3	N/A	-
5.2.4.1	I8: Insufficient Security Configurability Ensuring the ability to separate normal users from administrative users.	-
5.2.4.2	I8: Insufficient Security Configurability	-

Technique requirements	Term corresponds to OWASP [3]	Term corresponds to ONVIF [19, 20]
	Ensuring the ability to encrypt data at rest or in transit.	
5.2.4.3	N/A	-
5.2.4.4	I8: Insufficient Security Configurability Ensuring the ability to encrypt data at rest or in transit. I2 Insufficient Authentication/Authorization Ensuring credentials are properly protected.	-
5.2.5.1	I1: Insecure Web Interface Ensuring web interface is not susceptible to XSS, SQLi or CSRF.	-
5.2.6.1 5.2.6.2	I2: Insufficient Authentication/Authorization Ensuring that the strong passwords are required The app authentication is required.	-
5.2.6.3	I2: Insufficient Authentication/Authorization Ensuring granular access control is in place when necessary. I8: Insufficient Security Configurability Jump to: navigation, search Ensuring the ability to separate normal users from administrative users.	-
5.2.7.1	I8: Insufficient Security Configurability Ensuring the ability to enable logging of security events.	-
5.2.7.2	-	-
5.2.7.3	-	-
5.2.7.4	I8: Insufficient Security Configurability Ensuring the ability to notify end users of security events	-
5.3.1.1 5.3.1.2	I4: Lack of Transport Encryption Ensuring data is encrypted using protocols such as SSL and TLS while transiting networks. Ensuring only accepted encryption standards are used and avoid using proprietary encryption protocols. Ensuring the message payload encryption. Ensuring the secure encryption key handshaking. Ensuring received data integrity verification. I8: Insufficient Security Configurability Ensuring the ability to encrypt data at rest or in transit.	-
5.3.2.1	I3: Insecure Network Services	-

Technique requirements	Term corresponds to OWASP [3]	Term corresponds to ONVIF [19, 20]
	Ensuring network ports or services are not exposed to the network via UPnP for example.	
5.3.2.2	I10: Poor Physical Security Ensuring the product has the ability to limit administrative capabilities	-
5.3.2.3	I3: Insecure Network Services Ensuring services are not vulnerable to buffer overflow and fuzzing attacks.	-
5.3.3.1 5.3.3.2	I8: Insufficient Security Configurability Ensuring the ability to encrypt data at rest or in transit.	-
5.3.3.3	I3: Insecure Network Services Ensuring services are not vulnerable to buffer overflow and fuzzing attacks.	-
5.3.3.4	-	-
5.4.1.1	I2: Insufficient Authentication/Authorization The app authentication is required.	Core Spec. – Ver. 16.12 5.12.1 Authentication 5.12.3 Username token profile Advanced Security Service Spec. – Ver. 1.3 4.2 Certificate-based Client Authentication
5.4.1.2	I7: Insecure Mobile Interface Ensuring user accounts cannot be enumerated using functionality such as password reset mechanisms	-
5.4.1.3 5.4.1.4	-	-
5.4.1.5	I2: Insufficient Authentication/Authorization Implement two factor authentications where possible. I7: Insecure Mobile Interface Implementing two factor authentications if possible.	-
5.4.1.6	I2: Insufficient Authentication/Authorization The device authentication is required.	-
5.4.2.1	I1: Insecure Web Interface Default passwords and ideally default usernames to be changed during initial setup. I7: Insecure Mobile Interface Default passwords and ideally default usernames to be changed during initial setup.	-

Technique requirements	Term corresponds to OWASP [3]	Term corresponds to ONVIF [19, 20]
5.4.2.2 5.4.2.3 5.4.2.4 5.4.2.5 5.4.2.6	I1: Insecure Web Interface Ensuring weak passwords are not allowed. Ensuring account lockout after 3 -5 failed login attempts. I2: Insufficient Authentication/Authorization Ensuring that the strong passwords are required. Ensuring options are available for configuring password controls. I7: Insecure Mobile Interface Ensuring account lockout after a 3 - 5 failed login attempts. I8: Insufficient Security Configurability Ensuring the ability to force strong password policies.	-
5.4.3.1 5.4.3.2	I2: Insufficient Authentication/Authorization Ensuring granular access control is in place when necessary. I8: Insufficient Security Configurability Ensuring the ability to separate normal users from administrative users.	Core Spec. – Ver. 16.12 5.12.2 User-based access control
5.5.1.1 5.5.1.2	I5: Privacy Concerns Ensuring only authorized individuals have access to collected personal information.	-
5.5.1.3	I8: Insufficient Security Configurability Ensuring the ability to notify end users of security events	-
5.5.2.1 5.5.2.2	I4: Lack of Transport Encryption Ensuring the message payload encryption. I5: Privacy Concerns Ensuring any data collected is properly protected with encryption.	-

References

[1] CNS 27001 資訊技術-安全技術-資訊安全管理系統-要求事項

[2] ANSI/CAN/UL 2900-1:2017 Software Cybersecurity for Network Connectable Products, Part 1: General Requirements

[3] GSMA corp., IoT Security Guidelines for Endpoint Ecosystems

[4] Open Web Application Security Project (OWASP) org., Top IoT Vulnerabilities [viewed 2018-05-16]. Available at https://www.owasp.org/index.php/Top_IoT_Vulnerabilities

[5] 経済産業省, 総務省, IoT セキュリティガイドライン ver 1.0

[6] TAICS TS-0014-2(E) v2.0:2018 Video Surveillance System Cybersecurity Standard-Part 2: IP Camera

[7] TAICS TS-0014-3(E) v1.0:2018 Video Surveillance System Cybersecurity Standard–Part3: Video Recorder

[8] TAICS TS-0014-4(E) v1.0:2018 Video Surveillance System Cybersecurity Standard–Part4: Network Attached Storage

[9] National Institute of Standards and Technology(NIST), National Vulnerability Database, https://nvd.nist.gov/vuln/full-listing

[10] First, Common Vulnerability Scoring System v3.0 Specification, https://www.first.org/cvss/specification-document

[11] 行政院法務部, 個人資料保護法, Dec., 2015

[12] 行政院國家資通安全會報技術服務中心, 政府組態基準 Microsoft Windows 8.1 (V1.3)

[13] National Institute of Standards and Technology(NIST), "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", October 2, 2012.

[14] National Institute of Standards and Technology(NIST), Annex A: Approved Security Functions for FIPS PUB 140-2: Security Requirements for Cryptographic Modules, May 10, 2017

[15] Open Web Application Security Project (OWASP) org., OWASP Top Ten 2017 Project [viewed 2018-05-16]. Available at https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project

[16] RFC 3550, RTP: A Transport Protocol for Real-Time Applications

[17] RFC 2326, Real Time Streaming Protocol (RTSP)

[18] RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2

[19] Open Network Video Interface Forum(ONVIF), Core Specification Version 16.12, Dec., 2016.[20] Open Network Video Interface Forum(ONVIF), Advanced Security Service Version 1.3, Feb., 2016.

Revision Record

Version	Date	Abstract
v1.0	2018/06/08	v1.0 Chinese version published
v1.0(E)	2019/03/26	v1.0 English version published

台灣資通產業標準協會

Taiwan Association of Information and Communication Standards

地　址・台北市中正區重慶南路二段51號8樓之一
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw