Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1453

(01/2022)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Aplicaciones y servicios con seguridad (2) – Seguridad de las aplicaciones (2)

Amenazas y requisitos de seguridad para los sistemas de gestión de vídeo

Recomendación UIT-T X.1453

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web (1)	X.1140–X.1149
Seguridad de las aplicaciones (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1319
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Correo-certificado	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1350–X.1369
Seguridad en los sistemas de transporte inteligente (STI)	X.1370–X.1399
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de las aplicaciones (2)	**X.1450–X.1459**
Seguridad de la web (2)	X.1470–X.1489
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
Ciberdefensa	X.1590–X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
Protección de datos	X.1770–X.1789
SEGURIDAD DE IMT-2020	X.1800–X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1453

Amenazas y requisitos de seguridad para los sistemas de gestión de vídeo

Resumen

Un sistema de gestión de vídeo (VMS) constituye el elemento principal de los sistemas de videovigilancia utilizados para prestar servicios públicos de seguridad y supervisión de tráfico, entre otros. Básicamente, un VMS recibe señal de vídeo de varias cámaras y permite al usuario reproducir esa señal en directo, o mediante una grabación previa de la misma. En la actualidad, el diseño de los VMS incorpora funciones inteligentes cada vez con más frecuencia, en particular para aplicaciones de análisis de vídeo y control de acceso.

Puesto que los VMS poseen conexión a la red, están expuestos a varios tipos de vulnerabilidades, en particular las que plantean los servicios web en Internet, y son susceptibles de ser objeto de ciberataques.

En la Recomendación UIT-T X.1453 se analizan amenazas de seguridad a los VMS que funcionan en plataformas de servidores a través de conexión a una red IP, y se especifican los requisitos de seguridad para hacer frente a amenazas de seguridad específicas.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1453	2022-01-07	17	11.1002/1000/14802

Palabras clave

Marco de seguridad, requisitos de seguridad, sistema de gestión de vídeo.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT T disponibles en el sitio web del UIT T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1453

Amenazas y requisitos de seguridad para los sistemas de gestión de vídeo

1 Alcance

En la presente Recomendación se analizan las amenazas y los requisitos de seguridad relativos a los sistemas de gestión de vídeo (VMS) basados en plataformas de servidores que reciben señales de vídeo de diversas cámaras como dispositivos de Internet de las cosas (IoT), y permiten a los usuarios reproducir esas señales de vídeo en directo o grabadas previamente. Esta Recomendación abarca:

– El análisis de la arquitectura de VMS basados en plataformas de servidores

– El análisis de las amenazas de seguridad a esos VMS

– Los requisitos de seguridad para hacer frente a amenazas específicas.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

La presente Recomendación utiliza el siguiente término definido en otros documentos:

3.1.1 Sistema de videovigilancia [b-ITU-T H.626]: Servicio de telecomunicaciones que se apoya en tecnologías y aplicaciones de vídeo (incluidos audio e imagen) que permiten obtener señales de multimedios a distancia (en particular, audio, vídeo, imagen y señales de alarma) y presentarlos al usuario final de forma sencilla, mediante una red de banda ancha gestionada con arreglo a parámetros de calidad, seguridad y fiabilidad establecidos previamente.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se define el siguiente término:

3.2.1 Sistema de gestión de vídeo: elemento fundamental de los sistemas de videovigilancia que permite a los usuarios reproducir la señal de varias cámaras, grabar y analizar flujos de vídeo, y establecer alertas para la detección de alteraciones de información o de movimiento.

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las abreviaturas y acrónimos siguientes:

DDoS Denegación de servicio distribuida

IDS Sistema de detección de intrusiones

IoT Internet de las Cosas

IP Protocolo Internet

IPS Sistema de prevención de intrusiones

NVR Sistema de grabación de vídeo a través de la red

VMS Sistema de gestión de vídeo

5 Convenios

En la presente Recomendación:

La expresión "**se requiere**" se refiere a un requisito que debe observarse para declarar la conformidad con respecto a la presente Recomendación.

La expresión "**se recomienda**" se refiere a un criterio recomendado, que es, en consecuencia, no obligatorio. Su observancia no es indispensable para declarar la conformidad con respecto a la presente Recomendación.

6 Sistemas de gestión de vídeo

La IoT se ha desarrollado a un ritmo muy rápido en todo el mundo a lo largo de los últimos años. Los sistemas de videovigilancia que soporta la IoT permiten a los usuarios supervisar la actividad que tiene lugar en ubicaciones distantes y obtener, en su caso, imágenes susceptibles de revestir interés. Los casos de utilización de esos sistemas son muy variados, y abarcan la aplicación de la ley y la prevención de delitos, la seguridad en el transporte y la supervisión de tráfico. Los VMS constituyen el elemento principal de los sistemas de videovigilancia utilizados en sistemas públicos de seguridad y supervisión de tráfico. Por lo general, los sistemas VMS reciben la señal de vídeo de varias cámaras y permiten a sus usuarios reproducir esa señal en directo, o mediante una grabación previa de la misma. En la actualidad, el diseño de los VMS incorpora funciones inteligentes cada vez con más frecuencia, en particular para aplicaciones de análisis de vídeo y control de acceso.

Puesto que los VMS poseen conexión a la red, están expuestos a varios tipos de vulnerabilidades, en particular las que plantean los servicios web en Internet, y son susceptibles de ser objeto de ciberataques.

Un sistema habitual de videovigilancia basado en IoT consta de varias cámaras de seguridad, un VMS y dispositivos de cliente para que el usuario pueda reproducir la señal de vídeo. Los VMS permiten a los usuarios grabar y reproducir vídeo en directo de varias cámaras de seguridad, supervisar alarmas, controlar cámaras y obtener grabaciones de archivos. El VMS basado en IoT es más modulares y versátil que un sistema basado en tecnología analógica, y permite a los usuarios controlar dispositivos que forman parte de un sistema de videovigilancia en cualquier lugar de la red.

Los VMS soportan muchas funciones, en particular:

– reproducción simultánea
– grabación de vídeo y audio
– búsqueda y reproducción de vídeo
– análisis de vídeos inteligente
– gestión de cámaras
– gestión de eventos
– gestión de alarmas

Cabe distinguir dos tipos de plataformas de soporte físico de los VMS con conexión a la red, a saber, los VMS basados en plataformas de servidores, con un servidor, o varios, para ejecutar un programa informático de gestión de vídeo, o VMS basados en sistemas de grabación de vídeo a través de la red (NVR). Los VMS utilizan soportes de vídeo lógicos y físicos. Los soportes lógicos de gestión de

vídeo pueden instalarse en soportes físicos de NVR o de servidor. En el primer caso, se utilizan para realizar tareas sencillas, en particular grabación y supervisión de secuencias de vídeo en una zona determinada, y en el segundo caso, para controlar a distancia una gran cantidad de cámaras distribuidas en varios emplazamientos, almacenar o gestionar secuencias de vídeo, así como para llevar a cabo análisis de vídeo inteligentes con objeto de detectar sucesos de forma automática. Por lo general, los VMS basados en NVR incorporan un único NVR útil, al tiempo que los VMS basados en servidores incorporan un servidor, o varios, a fin de controlar una gran cantidad de cámaras y ofrecer servicios analíticos ampliados. En esta Recomendación se abordan únicamente los VMS basados en plataformas de servidores.

Con objeto de analizar la seguridad de los VMS, cabe definir una arquitectura que permite identificar todas las entidades de videovigilancia de un VMS y establecer la relación entre esas entidades. La arquitectura funcional de un VMS para aplicaciones de videovigilancia se muestra en la Figura 1.

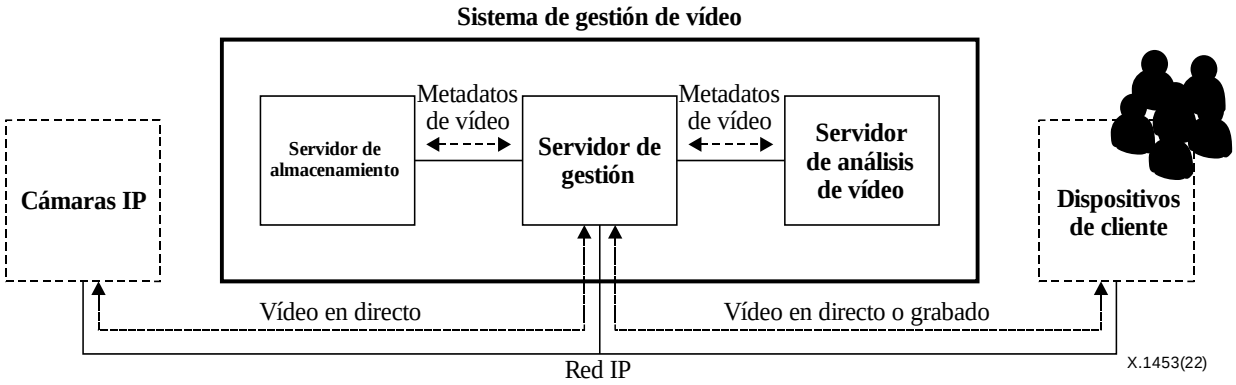

Figura 1 – Arquitectura funcional simplificada de un VMS

Los sistemas de videovigilancia abarcan cinco tipos de entidades principales, a saber, cámaras, servidores de almacenamiento, servidores de gestión, servidores de análisis de vídeo y dispositivos de cliente. Los VMS que constituyen el elemento principal de los sistemas de videovigilancia están integrados por un servidor de gestión, un servidor de almacenamiento y un servidor de análisis de vídeo. Existen cuatro relaciones entre las entidades que se muestran en la Figura 1, a saber, entre cada cámara y el servidor de gestión, entre el servidor de gestión y un dispositivo de cliente, entre el servidor de gestión y el servidor de almacenamiento, y entre el servidor de gestión y el servidor de análisis de vídeo.

Cada VMS está conectado con las cámaras y los dispositivos de cliente a través de una red. El servidor de gestión, el servidor de almacenamiento y el servidor de análisis de vídeo se sitúan, por lo general, en la misma red. Los dispositivos de cliente suelen conectarse a una red abierta, en particular Internet, a fin de ampliar las funciones de supervisión a distancia.

El servidor de gestión es el elemento principal de cada VMS. Controla y gestiona todas las entidades de los sistemas de videovigilancia, en particular la configuración de las cámaras y los parámetros de almacenamiento. El servidor de almacenamiento graba secuencias de vídeo de las cámaras que incorporan funciones de conexión con el mismo y almacena los metadatos generados por el servidor de análisis de vídeo. Dicho servidor analiza objetos en movimiento a través de un flujo de vídeo y genera metadatos para describir las actividades y los sucesos que se identifican. El servidor de análisis de vídeo genera dos tipos de metadatos: metadatos de sucesos y metadatos de alertas. Cada suceso o alerta se compone de varios mensajes de metadatos que contienen atributos de índole diversa, asociados a un cambio detectado, o a un segmento de movimiento de una transmisión de vídeo.

7 Amenazas de seguridad

7.1 Amenazas para la interfaz entre el servidor de gestión y las cámaras

La principal tarea de la interfaz entre el servidor de gestión y las cámaras es obtener la señal de vídeo de éstas, ajustar su configuración y controlarlas para facilitar su rotación e inclinación vertical y fijar su distancia focal. Los datos transferidos a través de esas interfaces constituyen el principal objetivo de posibles atacantes. Éstos pueden alterar adversamente al VMS mediante la interceptación, falsificación o reproducción de datos. Otro objetivo de los atacantes puede consistir en la denegación del VMS por medio de un ataque de denegación de servicio distribuido (DDoS) contra las cámaras y el servidor de gestión.

A continuación, se enumeran las principales amenazas a la interfaz entre el servidor de gestión y las cámaras:

- Acceso no autorizado: ataque que facilita el acceso a una cámara a través de la cuenta de otra persona o mediante otro método de acceso. Un acceso no autorizado a la cámara puede provocar la divulgación de información sensible, modificar vídeos, o utilizar recursos de forma ilícita. Por ejemplo, una vez que un atacante haya accedido a una cámara, podría obtener ilícitamente datos de vídeo, y la supervisión en tiempo real de los mismos podría conllevar problemas de privacidad.
- Espionaje de red: conlleva ataques que permiten obtener datos de vídeo transmitidos a través de la red y acceder al contenido de vídeo para recabar información sensible, en particular, rostros de personas, matrículas de coches, etc.
- Denegación de servicio: se produce a raíz de un ataque que tiene por objeto ejecutar un código malicioso en el servidor de gestión o en las cámaras, con la finalidad de saturar su capacidad de funcionamiento mediante peticiones de datos o de servicio masivas. Este tipo de ataques puede dificultar o interrumpir el funcionamiento de los VMS.
- Falsificación de datos de vídeo: un atacante podría bloquear los datos de vídeo, falsificarlos y enviarlos posteriormente al servidor de gestión. El ataque podría dificultar el funcionamiento habitual del VMS.
- Falsificación de datos de control: un atacante podría bloquear los datos de control para ajustar la configuración de la cámara, falsificarlos, y enviarlos posteriormente a las cámaras. El ataque podría dificultar las funciones habituales de control de las cámaras.
- Amenazas internas: los ataques de seres humanos pueden conllevar el riesgo de un comportamiento malicioso o irresponsable de los mismos, susceptible de dificultar el VMS. Cabe destacar los usuarios que comparten una contraseña de "administrador" o guardan sus credenciales en lugares inseguros, los usuarios irresponsables o insuficientemente formados, o las acciones maliciosas de usuarios descontentos.

7.2 Amenazas para la interfaz entre el servidor de gestión y los dispositivos de cliente

La principal tarea de la interfaz entre el servidor de gestión y el servidor de almacenamiento es la de permitir la visualización de vídeo en directo y acceder a archivos de vídeo grabados.

A continuación, se enumeran las principales amenazas a la interfaz entre el servidor de gestión y el dispositivo de cliente:

- Acceso no autorizado: ataque que facilita el acceso a un dispositivo de cliente a través de la cuenta de otra persona o mediante otro método de acceso. Un acceso no autorizado a un dispositivo de cliente puede provocar la divulgación de información sensible o utilizar recursos de forma ilícita. Por ejemplo, una vez que un atacante haya accedido a un dispositivo de cliente, podría obtener ilícitamente datos de vídeo, y la supervisión en tiempo real de los mismos podría conllevar problemas de privacidad.

- Espionaje de red: conlleva ataques que permiten obtener datos de vídeo transmitidos a través de la red y acceder al contenido de vídeo para recabar información sensible, en particular, rostros de personas y matrículas de coches, u otro tipo de información sensible.
- Denegación de servicio: se produce a raíz de un ataque que tiene por objeto ejecutar un código malicioso en el servidor de gestión o en los dispositivos de cliente, con la finalidad de saturar su capacidad de funcionamiento mediante peticiones de datos o de servicio masivas. Este tipo de ataques puede dificultar o interrumpir el funcionamiento del VMS.
- Falsificación de datos de vídeo: un atacante podría bloquear los datos de vídeo, falsificarlos y enviarlos posteriormente a los dispositivos de cliente. El ataque podría dificultar el funcionamiento habitual del VMS.
- Falsificación de datos de control: un atacante podría bloquear los datos de control para ajustar la configuración de la cámara, falsificarlos, y enviarlos posteriormente al servicio de gestión. El ataque podría dificultar la supervisión de vídeo habitual por el usuario.
- Amenazas internas: los ataques de seres humanos pueden conllevar el riesgo de un comportamiento malicioso o irresponsable de los mismos, susceptible de dificultar el VMS. Cabe destacar los usuarios que comparten una contraseña de "administrador" o guardan sus credenciales en lugares inseguros, los usuarios irresponsables o insuficientemente formados, o las acciones maliciosas de usuarios descontentos.

7.3 Amenazas para la interfaz entre el servidor de gestión y servidor de almacenamiento

La principal tarea de la interfaz entre el servidor de gestión y el servidor de almacenamiento es la de permitir la grabación y visualización de señales de vídeo, incluidos sus metadatos.

El servidor de gestión y el servidor de almacenamiento suelen estar situados en la misma red, o conectados a través de una línea específica. Aunque sólo esté conectado a la red pública el servidor de gestión, un ciberatacante podría aprovechar las vulnerabilidades de seguridad del servidor de gestión para acceder de forma ilícita al servidor de almacenamiento.

A continuación, se enumeran las principales amenazas a la interfaz entre el servidor de gestión y el servidor de almacenamiento:

- Acceso no autorizado: ataque que facilita el acceso al servidor de gestión a través de la cuenta de otra persona o mediante otro método de acceso para acceder a datos almacenados en el servidor de almacenamiento. Un acceso no autorizado al servidor de almacenamiento puede provocar la divulgación de información sensible, o utilizar recursos de forma ilícita.
- Divulgación de datos: ataque que permite acceder de forma ilícita a contenido de vídeo almacenado en el servidor y obtener información sensible, en particular, rostros de personas y matrículas de coches. Un atacante podría divulgar datos que no estén protegidos.
- Introducción y modificación de datos: ataque que permite modificar de forma ilícita datos de vídeo almacenados mediante la introducción en los mismos de datos alterados, con objeto de menoscabar la calidad de la información de vídeo.
- Amenazas internas: los ataques de seres humanos pueden conllevar el riesgo de un comportamiento malicioso o irresponsable de los mismos, susceptible de dificultar el VMS. Cabe destacar los usuarios que comparten una contraseña de "administrador" o guardan sus credenciales en lugares inseguros, los usuarios irresponsables o insuficientemente formados, o las acciones maliciosas de usuarios descontentos.

7.4 Amenazas para la interfaz entre el servidor de gestión y el servidor de análisis de vídeo

La principal tarea de la interfaz entre el servidor de gestión y el servidor de análisis de vídeo es transmitir vídeo para analizar objetos en movimiento en los datos de vídeo, así como metadatos para describir las actividades y los eventos identificados en el servidor de análisis de vídeo.

El servidor de gestión y el servidor de análisis de vídeo suelen estar ubicados en la misma red o conectados a través de una línea específica. Aunque sólo esté conectado a la red pública el servidor de gestión, un ciberatacante podría aprovechar las vulnerabilidades de seguridad del servidor de gestión para acceder de forma ilícita al servidor de análisis de vídeo.

A continuación, se enumeran las principales amenazas a la interfaz entre el servidor de gestión y el servidor de análisis de vídeo:

- Acceso no autorizado: ataque que facilita el acceso al servidor de gestión a través de la cuenta de otra persona o mediante otro método de acceso para acceder a datos almacenados en el servidor de análisis de vídeo. Un acceso no autorizado al servidor de análisis de vídeo puede provocar un funcionamiento inadecuado del sistema, y en particular, del servidor de análisis de vídeo.
- Divulgación de datos: ataque que permite acceder de forma ilícita a contenido de vídeo almacenado en el servidor y obtener información sensible, en particular, rostros de personas y matrículas de coches. Un atacante podría divulgar datos que no estén protegidos.
- Introducción y modificación de datos: ataque que permite modificar de forma ilícita datos o metadatos de vídeo mediante la introducción de datos alterados, con objeto de menoscabar el funcionamiento del servidor de análisis de vídeo. Por ejemplo, una vez que un atacante ha accedido de forma ilícita al servidor de gestión, podría sustituir los datos faciales almacenados de una persona autorizada por los datos faciales de otra persona no autorizada.
- Amenazas internas: los ataques de seres humanos pueden conllevar el riesgo de un comportamiento malicioso o irresponsable de los mismos, susceptible de dificultar el VMS. Cabe destacar los usuarios que comparten una contraseña de "administrador" o guardan sus credenciales en lugares inseguros, los usuarios irresponsables o insuficientemente formados, o las acciones maliciosas de usuarios descontentos.

7.5 Amenazas de seguridad a entidades del VMS o a entidades ajenas al mismo

Las amenazas de seguridad pueden afectar a interfaces específicas entre entidades, según se especifica en la Figura 1. La relación entre esas amenazas de seguridad y las entidades del VMS, u otras entidades ajenas al mismo, se muestra en el Cuadro 1, en el que se representa mediante un círculo en cada celda que la entidad de que se trata guarda relación con una amenaza de seguridad específica.

Cuadro 1 – Relación entre requisitos de seguridad y entidades

Entidades / Amenazas	Entre el VMS y las cámaras	VMS		Entre el VMS y los dispositivos de cliente
		Entre el servidor de gestión y el servidor de almacenamiento	Entre el servidor de gestión y el servidor de análisis de vídeo	
Espionaje de red	○			○
Acceso no autorizado	○	○	○	○
Denegación de servicio	○			○

Cuadro 1 – Relación entre requisitos de seguridad y entidades

Amenazas \ Entidades	Entre el VMS y las cámaras	VMS		Entre el VMS y los dispositivos de cliente
		Entre el servidor de gestión y el servidor de almacenamiento	Entre el servidor de gestión y el servidor de análisis de vídeo	
Revelación de datos		○	○	
Introducción y modificación de datos	○	○	○	○
Amenazas internas	○	○	○	○

8 Requisitos de seguridad

8.1 Confidencialidad

La confidencialidad impide el acceso de entidades no autorizadas a contenidos de información. Aun en el caso de que un ciberatacante revele determinados datos de forma ilegítima, su confidencialidad puede garantizarse.

La confidencialidad es necesaria para proteger información sensible, ya sea para su almacenamiento o su transmisión. Los datos sensibles abarcan, en particular, datos de vídeo, instrucciones de control del funcionamiento de las cámaras e información incluida en el servidor de almacenamiento.

- La confidencialidad es necesaria para impedir el acceso de entidades no autorizadas a datos de vídeo transmitidos a través de la red.
- La confidencialidad es necesaria para impedir el acceso de entidades no autorizadas a datos de control del funcionamiento de cámaras.
- Se recomienda que los datos almacenados en el servidor de almacenamiento y en el servidor de análisis de vídeo sean confidenciales, a fin de evitar el acceso de entidades no autorizadas a los mismos.

8.2 Integridad

La verificación de la integridad de los datos permite garantizar que una vez que éstos se hayan transmitido no difieran de los datos de origen. Los datos originales almacenados no deben modificarse después de un acceso autorizado a los mismos.

- La integridad es necesaria para impedir la falsificación de los datos de vídeo originales transmitidos desde las cámaras.
- Se recomienda garantizar la integridad de los datos de vídeo almacenados originales y evitar su falsificación.
- Se recomienda garantizar la integridad de los datos de vídeo exportados para que, en el marco de su análisis para esclarecer delitos, se trabaje con datos originales que no hayan sido objeto de alteración.

8.3 Autenticación de usuarios y dispositivos

Las tareas de autenticación son necesarias para verificar la identidad de usuarios y dispositivos. La autenticación permite comprobar la identidad de las entidades que realizan actividades de videovigilancia e impide que entidades no autorizadas se hagan pasar por entidades autorizadas.

- La autenticación de usuario permite garantizar que un usuario sea un administrador legítimo, autorizado para acceder a los servidores del VMS en labores de gestión de vídeo centralizada.
- La autenticación de usuario permite garantizar asimismo que un usuario sea un usuario legítimo de un dispositivo de cliente se le autorice a consultar datos de vídeo a distancia.
- Se recomienda la autenticación de dispositivos para velar por que éstos sean dispositivos de cliente legítimos, con autorización para establecer una conexión a distancia con el VMS.
- Se recomienda la autenticación de dispositivos para garantizar que cada cámara se use de forma lícita al conectarse con el VMS.

8.4 Control de acceso

Las tareas de control de acceso permiten garantizar que sólo usuarios autorizados puedan acceder a los recursos adecuados en el marco de actividades de videovigilancia. Pese a que los administradores formen parte de un grupo con privilegios de mantenimiento y control de un sistema de videovigilancia, se recomienda conceder a cada usuario un derecho de acceso diferente.

- El control de acceso permite garantizar que sólo los usuarios autorizados puedan acceder al servidor de gestión, con arreglo a sus privilegios de acceso al sistema de videovigilancia. Los tipos de acceso incluyen la supervisión de vídeo en tiempo real, la reproducción de grabaciones de vídeo y el control de cámaras a distancia.
- El control de acceso permite garantizar que sólo los usuarios autorizados de los dispositivos de cliente puedan acceder al sistema de videovigilancia, con arreglo a sus privilegios de acceso. Los tipos de acceso incluyen la supervisión de vídeo en tiempo real y la reproducción de grabaciones de vídeo.

8.5 Prevención de intrusiones

La prevención de intrusiones permite proteger las entidades del VMS, los datos de vídeo almacenados y sus correspondientes servicios frente a intentos de acceso ilícito, tanto internos como externos. La prevención de intrusiones en los VMS puede tener lugar a nivel lógico o físico. El método de prevención de intrusiones a nivel lógico permite proteger los recursos de sistema frente a ataques a través de redes IP. El método de prevención de intrusiones a nivel físico permite proteger los recursos de sistema frente a accesos ilícitos a nivel físico.

- La prevención de intrusiones a nivel lógico garantiza la protección de los recursos de sistema frente a ataques a través de redes IP, a fin de facilitar un funcionamiento adecuado de los sistemas de videovigilancia. Los sistemas de seguridad de red utilizados para la prevención de intrusiones a nivel físico incluyen el sistema de detección de intrusiones (IDS) y el sistema de prevención de intrusiones (IPS). Conviene utilizar un sistema de seguridad de red específico, en lugar de un sistema implantado en el marco del VMS.
- La prevención de intrusiones a nivel físico garantiza que sólo los usuarios lícitos identificados mediante técnicas de autenticación puedan acceder al centro de operaciones de seguridad en el que se ha instalado el VMS.

8.6 Relación entre requisitos de seguridad y amenazas para la misma

La relación entre requisitos de seguridad y amenazas para la misma se muestra en el Cuadro 2, en el que se representa, mediante un círculo en cada celda, un requisito de seguridad específico con objeto de suprimir o mitigar una amenaza concreta.

Cuadro 2 – Relación entre requisitos de seguridad y amenazas para la misma

			Requisitos de seguridad				
			Confidencialidad	**Integridad**	**Autenticación de usuarios y dispositivos**	**Control de acceso**	**Prevención de intrusiones**
Amenazas de seguridad	VMS	Acceso no autorizado			○	○	
		Divulgación de información	○				
		Alteración o introducción de datos		○			
		Amenazas internas			○	○	
		DOS					○
	Entre el VMS y las cámaras	Acceso no autorizado			○	○	
		Espionaje	○				
		DOS					○
		Alteración o introducción de datos		○			
		Amenazas internas			○	○	
	Entre el VMS y los servicios de cliente	Acceso no autorizado			○	○	
		Espionaje	○				
		DOS					○
		Alteración o introducción de datos		○			
		Amenazas internas			○	○	

Bibliografía

[b-ITU-T H.626] Recomendación UIT-T H.626 (2019), *Requisitos de arquitectura para sistemas de videovigilancia*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2022