Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1453

(01/2022)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Applications et services sécurisés (2) – Sécurité des applications (2)

Menaces et exigences de sécurité pour les systèmes de gestion vidéo

Recommandation UIT-T X.1453

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile (1)	X.1140–X.1149
Sécurité des applications (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1350–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1399
Sécurité de la technologie des registres distribués (DLT)	X.1400–X.1429
Sécurité des applications (2)	**X.1450–X.1459**
Sécurité de la toile (2)	X.1470–X.1489
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
Cyberdéfense	X.1590–X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
Protection des données	X.1770–X.1789
SÉCURITÉ DES IMT-2020	X.1800–X.1819

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1453

Menaces et exigences de sécurité pour les systèmes de gestion vidéo

Résumé

Un système de gestion vidéo (VMS) est l'élément central des systèmes de vidéosurveillance utilisés pour la sécurité du public, la surveillance du trafic, etc. En principe, un système VMS reçoit des vidéos provenant de caméras et permet à un utilisateur de visualiser ces vidéos, qu'il s'agisse de vidéos en direct ou de vidéos enregistrées. À l'heure actuelle, les méthodes qui se font jour dans le domaine des systèmes VMS intègrent de plus en plus l'intelligence dès la conception, y compris pour l'analyse vidéo et le contrôle d'accès.

Étant donné qu'il fonctionne en réseau, un système VMS est exposé en tout point à différentes vulnérabilités, telles que celles auxquels sont confrontés les services web Internet, et peut être facilement la cible de cyberattaques.

La Recommandation UIT-T X.1453 contient une analyse des menaces de sécurité pour les systèmes VMS fondés sur la plate-forme du serveur fonctionnant sur un réseau IP et indique les exigences de sécurité permettant de remédier aux menaces de sécurité recensées.

Historique

Édition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T X.1453	2022-01-07	17	11.1002/1000/14802

Mots clés

Système de gestion vidéo, cadre de sécurité, exigence de sécurité.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

À la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1453

Menaces et exigences de sécurité pour les systèmes de gestion vidéo

1 Domaine d'application

La présente Recommandation identifie les menaces de sécurité et expose les exigences de sécurité pour un système de gestion vidéo (VMS) fondé sur une plate-forme du serveur qui reçoit des vidéos provenant de caméras, qui sont un type de dispositif de l'Internet des objets (IoT), et permet à un tiers de visionner ces vidéos, qu'il s'agisse de vidéos en direct ou de vidéos enregistrées.

Cette Recommandation couvre les aspects suivants:

– Analyse de l'architecture d'un système VMS fondé sur une plate-forme du serveur.

– Analyse des menaces de sécurité auxquelles sont confrontés ces systèmes VMS.

– Exigences de sécurité permettant de remédier aux menaces recensées.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une recommandation.

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise le terme suivant défini ailleurs:

3.1.1 système de vidéosurveillance [b-UIT-T H.626]: un service de télécommunication qui se fonde sur une technologie d'application vidéo (comprenant l'audio et l'image) généralement utilisée pour saisir à distance des signaux multimédias, par exemple des signaux audio, vidéo, d'images et d'alarmes, et les présenter à l'utilisateur final de manière conviviale, via un réseau large bande géré dont la qualité, la sécurité et la fiabilité sont garanties.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 système de gestion vidéo: un élément essentiel de tout système de vidéosurveillance, qui permet aux utilisateurs de visualiser plusieurs caméras, d'enregistrer et d'analyser des flux vidéo et de définir des alertes de falsification et des alertes de détection de mouvement.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

DDoS déni de service réparti (*distributed denial of service*)

IDS système de détection des intrusions (*intrusion detection system*)

IoT Internet des objets (*Internet of things*)

IP protocole Internet (*Internet protocol*)

IPS système de prévention des intrusions (*intrusion prevention system*)

NVR enregistreur vidéo réseau (*network video recorder*)

VMS système de gestion vidéo (*vidéo management system*)

5 Conventions

Dans la présente Recommandation:

L'expression "**il est nécessaire**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité à la présente Recommandation.

6 Système de gestion vidéo

L'IoT est en plein essor ces dernières années à travers le monde. Les systèmes de vidéosurveillance basés sur l'IoT permettent aux utilisateurs de visualiser les activités qui se déroulent à distance et de capturer lorsqu'ils le souhaitent des images susceptibles de présenter un intérêt. Les cas d'utilisation de ces systèmes varient considérablement, allant de l'application de la loi et de la prévention de la criminalité à la sécurité dans les systèmes de transport et à la surveillance du trafic. Les systèmes VMS sont au cœur des systèmes de vidéosurveillance utilisés pour les systèmes de sécurité du public et de surveillance du trafic. En principe, un système VMS reçoit des vidéos provenant de caméras et permet à un tiers de visualiser ces vidéos, qu'il s'agisse de vidéos en direct ou de vidéos enregistrées. À l'heure actuelle, les méthodes qui se font jour dans le domaine des systèmes VMS intègrent de plus en plus l'intelligence dès la conception, y compris pour l'analyse vidéo et le contrôle d'accès.

Étant donné qu'ils fonctionnent en réseau, les systèmes VMS sont exposés en tout point à différentes vulnérabilités, telles que celles auxquels sont confrontés les services web Internet, et peuvent être facilement la cible de cyberattaques.

Un système de vidéosurveillance type basé sur l'IoT se compose de plusieurs caméras de sécurité, d'un système VMS et de périphériques clients permettant à l'utilisateur de visualiser la vidéo. Le système VMS permet aux utilisateurs d'enregistrer et de visualiser des vidéos en direct à partir de plusieurs caméras de sécurité, de surveiller les alarmes, de contrôler les caméras et de récupérer des enregistrements à partir d'archives. Un système VMS basé sur l'IoT est plus extensible et flexible qu'un système analogique; il permet aux utilisateurs de contrôler les appareils qui composent le système de vidéosurveillance n'importe où sur le réseau.

Le système VMS peut prendre en charge de nombreuses fonctionnalités différentes telles que:

– la visualisation simultanée;
– l'enregistrement vidéo et audio;
– la recherche et lecture vidéo;
– l'analyse vidéo intelligente;
– la gestion des caméras;
– la gestion des événements;
– la gestion des alarmes.

Il existe deux types de plates-formes matérielles pour un système VMS en réseau: un système VMS fondé sur une plate-forme du serveur implique un ou plusieurs serveurs qui exécutent un logiciel de gestion vidéo ou un système VMS fondé sur un enregistreur vidéo réseau (NVR). Un système VMS

est une combinaison de logiciel et de matériel vidéo. Le logiciel de gestion vidéo peut être monté sur du matériel NVR ou installé sur du matériel serveur. S'il est monté sur un matériel NVR, le logiciel est utilisé pour effectuer des tâches simples comme enregistrer et surveiller des séquences vidéo dans une zone confinée; s'il est installé sur un matériel serveur, il contrôle à distance plusieurs caméras réparties dans divers emplacements, stocke et gère la vidéo, et fournit également des analyses vidéo intelligentes pour détecter automatiquement les événements. En général, un système VMS monté sur du matériel NVR fait référence à un système VMS qui utilise un seul enregistreur NVR, tandis qu'un système VMS installé sur du matériel serveur fait référence à un système VMS qui utilise un ou plusieurs serveurs pour contrôler plusieurs caméras et fournir des services analytiques étendus. Cette recommandation ne concerne que les systèmes VMS fondés sur les plates-formes du serveur.

Aux fins de l'analyse de la sécurité des systèmes VMS, une architecture est mise en place. Celle-ci vise à identifier toutes les entités liées à la vidéosurveillance fondée sur le système VMS et à clarifier les relations entre les entités. L'architecture fonctionnelle d'un système VMS pour les applications de vidéosurveillance est illustrée à la Figure 1.

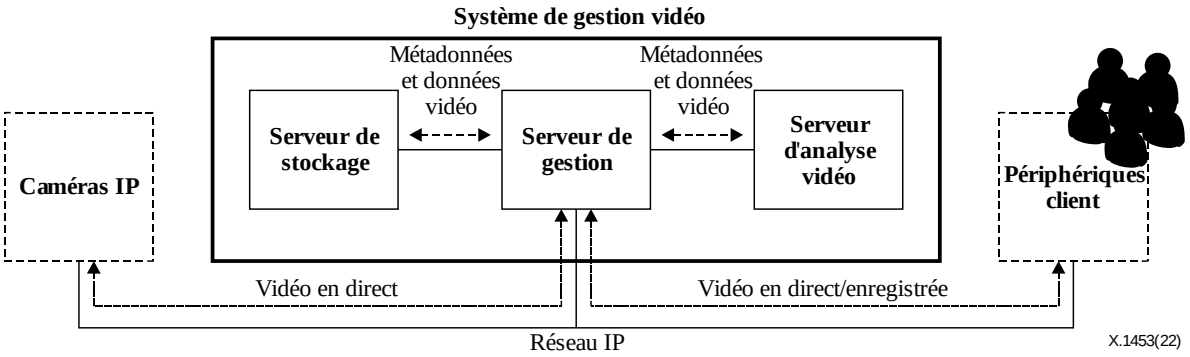

Figure-1 – Architecture fonctionnelle simplifiée d'un système VMS

Les systèmes de vidéosurveillance comportent cinq composantes majeures: les caméras, les serveurs de stockage, les serveurs de gestion, les serveurs d'analyse vidéo et les dispositifs client. Le système VMS qui se trouve au cœur du système de vidéosurveillance comprend un serveur de gestion, un serveur de stockage et un serveur d'analyse vidéo. On observe quatre types de relations possibles entre les composantes représentées sur la Figure 1, à savoir: entre une caméra et le serveur de gestion, entre le serveur de gestion et un périphérique client, entre le serveur de gestion et le serveur de stockage, et entre le serveur de gestion et le serveur d'analyse vidéo.

Le système VMS est connecté aux caméras et aux périphériques client via un réseau. Le serveur de gestion, le serveur de stockage et le serveur d'analyse vidéo se trouvent souvent placés sur le même réseau. Les périphériques client sont généralement connectés à un réseau ouvert, tel que l'Internet, pour une surveillance à distance étendue.

Le serveur de gestion constitue le centre du système VMS. Il contrôle et gère toutes les composantes des systèmes de vidéosurveillance, y compris les paramètres de caméra et les paramètres de stockage. Le serveur de stockage enregistre la vidéo depuis les caméras qui lui sont rattachées et stocke les métadonnées créées par le serveur d'analyse vidéo. Le serveur d'analyse vidéo analyse les objets en mouvement dans le flux vidéo et crée des métadonnées pour décrire les activités et les événements recensés. Le serveur d'analyse vidéo génère deux formes de métadonnées: des métadonnées d'événement et des métadonnées d'alerte. Chaque événement ou alerte est composé de plusieurs messages de métadonnées qui contiennent divers attributs concernant un changement ou un segment de mouvement détecté dans un flux vidéo.

7 Menaces de sécurité

7.1 Menaces pesant sur l'interface entre le serveur de gestion et la caméra

L'interface qui fait le lien entre le serveur de gestion et la caméra a pour tâche principale de collecter la vidéo de la caméra, d'ajuster les paramètres de la caméra et de contrôler la rotation, l'inclinaison et le zoom de la caméra. Les données transférées via ces interfaces sont la cible principale de l'auteur d'une attaque. Ce dernier peut altérer le service VMS par interception, falsification et répétition de ces données. Les auteurs d'attaques visent également le déni du service VMS au moyen d'attaques par déni de service réparti (DDoS) contre les caméras et le serveur de gestion.

Les menaces pesant sur l'interface entre le serveur de gestion et la caméra sont les suivantes:

- Accès non autorisé: attaque consistant à obtenir l'accès à la caméra en utilisant le compte d'un tiers ou une autre méthode d'accès. L'accès non autorisé à la caméra peut entraîner la divulgation d'informations sensibles, la modification de la vidéo et l'utilisation illicite de ressources. Par exemple, dès lors qu'il a réussi à accéder à la caméra, l'auteur d'une attaque peut recueillir illégalement des données vidéo et la surveillance en temps réel de ces données vidéo peut entraîner des problèmes de confidentialité.
- Écoute illicite du réseau: attaque consistant à intercepter des données vidéo transmises depuis le réseau et à lire le contenu vidéo pour trouver des informations sensibles comme des visages et des plaques d'immatriculation.
- Déni de service: attaque tentant d'exécuter un code malveillant sur le serveur de gestion ou les caméras dans le but d'inonder la cible avec un grand nombre de données ou de demandes de service. Les services VMS, face à cette attaque, peuvent être ralentis voire arrêtés.
- Falsification des données vidéo: l'auteur d'une attaque bloque les données vidéo et envoie de fausses données au serveur de gestion. L'attaque peut provoquer des interférences avec le fonctionnement normal du système VMS.
- Falsification des données de contrôle: l'auteur d'une attaque bloque les données de contrôle pour ajuster les paramètres de la caméra et envoie de fausses données aux caméras. L'attaque peut provoquer des interférences avec les fonctions normales de commande de la caméra.
- Menaces internes: lorsqu'une activité implique une intervention humaine, le risque est toujours présent que des personnes fassent preuve de malveillance ou de négligence et ainsi fragilisent le service VMS. Les utilisateurs qui communiquent les mots de passe "administrateur" ou qui ne protègent pas leurs justificatifs d'identité en lieu sécurisé, les utilisateurs négligents ou mal formés ou encore des actions malveillantes de la part d'utilisateurs aigris représenteront toujours une menace importante.

7.2 Menaces pesant sur l'interface entre le serveur de gestion et le dispositif client

L'interface qui fait le lien entre le serveur de gestion et le dispositif client a pour tâche principale de fournir des interfaces permettant de regarder des vidéos en direct et d'accéder aux vidéos enregistrées.

Les menaces pesant sur l'interface entre le serveur de gestion et le dispositif client sont les suivantes:

- Accès non autorisé: attaque consistant à obtenir l'accès au dispositif client en utilisant le compte d'un tiers ou une autre méthode d'accès. L'accès non autorisé au dispositif client peut entraîner la divulgation d'informations sensibles et l'utilisation illicite de ressources. Par exemple, dès lors qu'il a réussi à accéder au dispositif client, l'auteur d'une attaque peut recueillir illégalement des données vidéo et la surveillance en temps réel de ces données vidéo peut entraîner des problèmes de confidentialité.
- Écoute illicite du réseau: attaque consistant à intercepter des données vidéo transmises depuis le réseau et à lire le contenu vidéo pour trouver des informations sensibles comme des visages, des plaques d'immatriculation, etc.

- Déni de service: attaque tentant d'exécuter un code malveillant sur le serveur de gestion ou les dispositifs client dans le but d'inonder la cible avec un grand nombre de données ou de demandes de service. Un service VMS, face à cette attaque, peut être ralenti voire arrêté.
- Falsification des données vidéo: l'auteur d'une attaque bloque les données vidéo et envoie de fausses données aux dispositifs client. L'attaque peut provoquer des interférences avec le fonctionnement normal du système VMS.
- Falsification des données de contrôle: l'auteur d'une attaque bloque les données de contrôle pour ajuster les paramètres de la caméra et envoie de fausses données au serveur de gestion. L'attaque peut provoquer des interférences avec la vidéosurveillance normale de l'utilisateur.
- Menaces internes: lorsqu'une activité implique une intervention humaine, le risque est toujours présent que des personnes fassent preuve de malveillance ou de négligence et ainsi fragilisent le service VMS. Les utilisateurs qui communiquent les mots de passe "administrateur" ou qui ne protègent pas leurs justificatifs d'identité en lieu sécurisé, les utilisateurs négligents ou mal formés ou encore des actions malveillantes de la part d'utilisateurs aigris représenteront toujours une menace importante.

7.3 Menaces pesant sur l'interface entre le serveur de gestion et le serveur de stockage

L'interface qui fait le lien entre le serveur de gestion et le serveur de stockage a pour tâche principale de fournir des interfaces permettant d'enregistrer/de consulter les vidéos et les métadonnées.

Le serveur de gestion et le serveur de stockage sont souvent situés sur le même réseau ou sont connectés via une ligne dédiée. Dans le cas où seul le serveur de gestion est raccordé au réseau public, un pirate peut exploiter les failles de sécurité sur le serveur de gestion pour accéder illégalement au serveur de stockage.

Les menaces pesant sur l'interface entre le serveur de gestion et le serveur de stockage sont les suivantes:

- Accès non autorisé: attaque consistant à obtenir l'accès au serveur de gestion en utilisant le compte d'un tiers ou une autre méthode pour accéder aux données enregistrées sur le serveur de stockage. L'accès non autorisé au serveur de stockage peut entraîner la divulgation d'informations sensibles et l'utilisation illicite de ressources.
- Divulgation des données: attaque consistant à obtenir illégalement l'accès au contenu vidéo stocké sur le serveur et à lire des informations sensibles telles que des visages et des plaques d'immatriculation. L'auteur d'une attaque peut divulguer des données non protégées.
- Injection et modification des données: attaque consistant à modifier illégalement les données vidéo enregistrées en y injectant des données impures, ce qui réduit ainsi la fiabilité des informations vidéo.
- Menaces internes: lorsqu'une activité implique une intervention humaine, le risque est toujours présent que des personnes fassent preuve de malveillance ou de négligence et ainsi fragilisent le service VMS. Les utilisateurs qui communiquent les mots de passe "administrateur" ou qui ne protègent pas leurs justificatifs d'identité en lieu sécurisé, les utilisateurs négligents ou mal formés ou encore des actions malveillantes de la part d'utilisateurs aigris représenteront toujours une menace importante.

7.4 Menaces pesant sur l'interface entre le serveur de gestion et le serveur d'analyse vidéo

L'interface qui fait le lien entre le serveur de gestion et le serveur d'analyse vidéo a pour tâche principale de transmettre des vidéos afin d'analyser les objets en mouvement dans les données vidéo de même que les métadonnées pour décrire les activités et les événements recensés sur le serveur d'analyse vidéo.

Le serveur de gestion et le serveur d'analyse vidéo sont souvent situés sur le même réseau ou sont connectés via une ligne dédiée. Dans le cas où seul le serveur de gestion est raccordé au réseau public, un pirate peut exploiter les failles de sécurité sur le serveur de gestion pour accéder illégalement au serveur d'analyse vidéo.

Les menaces pesant sur l'interface entre le serveur de gestion et le serveur d'analyse vidéo sont les suivantes:

- Accès non autorisé: attaque consistant à obtenir l'accès au serveur de gestion en utilisant le compte d'un tiers ou une autre méthode pour accéder aux données enregistrées sur le serveur d'analyse vidéo. L'accès non autorisé au serveur d'analyse vidéo peut entraîner des dysfonctionnements réduisant ainsi la fiabilité du serveur d'analyse vidéo.
- Divulgation des données: attaque consistant à obtenir illégalement l'accès au contenu vidéo stocké sur le serveur et à lire des informations sensibles telles que des visages et des plaques d'immatriculation. L'auteur d'une attaque peut divulguer des données non protégées.
- Injection et modification des données: attaque consistant à modifier illégalement les données vidéo enregistrées en y injectant des données impures, ce qui réduit ainsi la fiabilité du serveur d'analyse vidéo. Par exemple, dès lors qu'il a réussi à accéder au serveur de gestion, l'auteur d'une attaque peut illégalement obtenir des autorisations pour une personne non autorisée en remplaçant les données faciales de la personne autorisée stockées par les données faciales d'une personne non autorisée.
- Menaces internes: lorsqu'une activité implique une intervention humaine, le risque est toujours présent que des personnes fassent preuve de malveillance ou de négligence et ainsi fragilisent le service VMS. Les utilisateurs qui communiquent les mots de passe "administrateur" ou qui ne protègent pas leurs justificatifs d'identité en lieu sécurisé, les utilisateurs négligents ou mal formés ou encore des actions malveillantes de la part d'utilisateurs aigris représenteront toujours une menace importante.

7.5 Relations entre les menaces de sécurité et les composantes intérieures/extérieures au système VMS

Les menaces de sécurité se concentrent sur certaines portions entre les composantes, comme le montre la Figure 1. Les relations entre les menaces de sécurité et les composantes intérieures/extérieures au système VMS sont présentées dans le Tableau 1. La présence d'un rond dans une cellule indique que cette composante est liée à la menace de sécurité considérée.

Tableau 1 – Relations entre les exigences de sécurité et les composantes de sécurité

Composantes / Menaces	Entre le système VMS et les caméras	VMS		Entre le système VMS et les dispositifs client
		Entre le serveur de gestion et le serveur de stockage	Entre le serveur de gestion et le serveur d'analyse vidéo	
Écoute illicite du réseau	○			○
Accès non autorisé	○	○	○	○
Déni de service	○			○
Divulgation des données		○	○	
Injection et modification des données	○	○	○	○
Menaces internes	○	○	○	○

8 Exigences de sécurité

8.1 Confidentialité

La confidentialité garantit que le contenu des données ne peut être lu par des entités non autorisées. Si certaines données sont interceptées et qu'un attaquant les divulgue, leur confidentialité peut tout de même être assurée.

La confidentialité doit être assurée pour les données sensibles, qu'elles soient stockées ou transmises. Les données sensibles incluent les données vidéo, les données de commande supervisant le fonctionnement des caméras et les données enregistrées sur le serveur de stockage.

- La confidentialité est requise pour garantir que les données vidéo transmises sur le réseau ne peuvent être lues par des entités non autorisées.
- La confidentialité est requise pour garantir que les données de commande supervisant le fonctionnement des caméras transmises sur le réseau ne peuvent être lues par des entités non autorisées.
- La confidentialité est recommandée pour garantir que les données enregistrées sur le serveur de stockage et le serveur d'analyse vidéo ne peuvent être lues par des entités non autorisées.

8.2 Intégrité

L'intégrité garantit qu'après leur transfert, les données ne sont pas différentes de ce qu'elles étaient à la source. Les données originales stockées ne doivent pas avoir changé après un accès autorisé.

- L'intégrité est requise pour garantir que les données vidéo transmises depuis la caméra sont des données originales non falsifiées.
- L'intégrité est recommandée pour garantir que les données vidéo enregistrées sont des données originales non falsifiées.
- L'intégrité est recommandée pour garantir que les données vidéo exportées à des fins d'enquête judiciaire, etc. sont des données originales qui n'ont pas été altérées.

8.3 Authentification de l'utilisateur et du dispositif

L'authentification est requise pour confirmer l'identité des utilisateurs et des dispositifs. L'authentification assure la validité des identités déclarées des entités participant à la vidéosurveillance et donne l'assurance qu'une entité non autorisée ne tente pas d'usurper l'identité d'une entité autorisée.

- L'authentification de l'utilisateur est requise pour garantir qu'un utilisateur est un administrateur légitime autorisé à accéder aux serveurs du système VMS pour la gestion vidéo centralisée.
- L'authentification de l'utilisateur est requise pour garantir qu'un utilisateur est un utilisateur légitime d'un dispositif client et qu'il est autorisé à visualiser à distance les données vidéo.
- L'authentification du dispositif est recommandée pour garantir qu'un dispositif client est un dispositif client légitime habilité à se connecter à distance au système VMS.
- L'authentification du dispositif est recommandée pour garantir qu'une caméra est une caméra légitime habilitée à être connectée au système VMS.

8.4 Contrôle d'accès

Le contrôle d'accès est requis pour garantir que seuls les utilisateurs agréés sont autorisés à accéder aux ressources appropriées participant à la vidéosurveillance. Même si les administrateurs sont impliqués dans le groupe privilégié autorisé à maintenir et à contrôler le système de vidéosurveillance, il est recommandé d'accorder à chaque utilisateur un droit d'accès différent.

- Le contrôle d'accès est nécessaire pour garantir que seuls les utilisateurs agréés sont autorisés à accéder au serveur de gestion en fonction de leurs privilèges d'accès dans le système de vidéosurveillance. Les types d'accès incluent la vidéosurveillance en temps réel, la lecture de vidéos enregistrées et le contrôle de caméra à distance.
- Le contrôle d'accès est nécessaire pour garantir que seuls les utilisateurs des dispositifs client agréés sont autorisés à accéder à la vidéosurveillance en fonction de leurs privilèges d'accès. Les types d'accès incluent la vidéosurveillance en temps réel et la lecture de vidéos enregistrées.

8.5 Prévention des intrusions

La prévention des intrusions est nécessaire pour protéger les entités du système VMS, les données vidéo stockées et les services contre les tentatives d'accès illégales internes et externes. La prévention des intrusions dans un système VMS peut être classée en deux catégories: la méthode logique et la méthode physique. La méthode logique de prévention des intrusions protège les ressources système des attaques utilisant un réseau IP. La méthode physique de prévention des intrusions protège les ressources système contre les accès physiques illicites.

- La prévention logique des intrusions est nécessaire pour garantir que les ressources système sont protégées contre les attaques utilisant un réseau IP, permettant ainsi à la vidéosurveillance de fonctionner normalement. Les systèmes de sécurité réseau utilisés pour la prévention logique des intrusions incluent un système de détection d'intrusion (IDS) et un système de prévention d'intrusion (IPS). Il est préférable d'utiliser un système de sécurité réseau dédié plutôt qu'un dispositif mis en place à l'intérieur du système VMS.
- La prévention physique des intrusions est nécessaire pour garantir que seuls les utilisateurs agréés identifiés par l'authentification de l'usager peuvent pénétrer le centre des opérations de sécurité dans lequel le système VMS a été installé.

8.6 Relations entre les exigences de sécurité et les menaces de sécurité

Les relations entre les exigences de sécurité et les menaces sont présentées dans le Tableau 2. La présence d'un rond dans une cellule indique que cette exigence de sécurité devrait être respectée pour supprimer ou atténuer la menace considérée.

Tableau 2 – Relations entre les exigences de sécurité et les menaces

			Exigences de sécurité				
			Confidentialité	**Intégrité**	**Authentification de l'utilisateur/ du dispositif**	**Contrôle de l'accès**	**Prévention des intrusions**
Menaces de sécurité	Système VMS	Accès non autorisé			○	○	
		Divulgation des données	○				
		Modification/injection		○			
		Menaces internes			○	○	
		DOS					○
	Entre le système VMS et les caméras	Accès non autorisé			○	○	
		Écoute illicite	○				
		DOS					○
		Modification/injection		○			
		Menaces internes			○	○	
	Entre le système VMS et les dispositifs client	Accès non autorisé			○	○	
		Écoute illicite	○				
		DOS					○
		Modification/injection		○			
		Menaces internes			○	○	

Bibliographie

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

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2022