الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1453

(2022/01)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

التطبيقات والخدمات الآمنة (2) – أمن التطبيقات (2)

التهديدات الأمنية والمتطلبات الأمنية لأنظمة الإدارة الفيديوية

التوصية ITU-T X.1453

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	X.1030–X.1049
إدارة الأمن	X.1050–X.1069
الخصائص البيومترية	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن الويب	X.1140–X.1149
بروتوكولات الأمن (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230–X.1249
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	X.1350–X.1369
أمن أنظمة النقل الذكية (ITS)	X.1370–X.1399
أمن سجل الحسابات الموزع	X.1400–X.1429
أمن التطبيقات (2)	**X.1450–X.1459**
أمن شبكة الإنترنت (2)	X.1470–X.1489
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1500–X.1519
تبادل مواطن الضعف/الحالة	X.1520–X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
الدفاع السيبراني	X.1590–X.1599
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1600–X.1601
تصميم أمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1640–X.1659
تنفيذ أمن الحوسبة السحابية	X.1660–X.1679
أمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699
الاتصالات الكمومية	
المصطلحات	X.1700–X.1701
مولّد الأعداد العشوائية الكمومية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1710–X.1711
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1712–X.1719
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
حماية البيانات	X.1770–X.1789
أمن شبكات الاتصالات المتنقلة الدولية-2020	X.1800–X.1819

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1453

التهديدات الأمنية والمتطلبات الأمنية لأنظمة الإدارة الفيديوية

ملخص

نظام الإدارة الفيديوية (VMS) هو جوهر أنظمة المراقبة الفيديوية المستخدمة لأغراض السلامة العامة ومراقبة الحركة وما إلى ذلك. وبالدرجة الأولى، يتلقى النظام VMS الفيديو من الكاميرات ويسمح لمستعمل بمشاهدة ذلك الفيديو سواء مباشرة أو من التسجيل. وتتضمن نُهُج النظام VMS الناشئة حالياً المزيد من الذكاء في تصميمها، بما في ذلك التحليل الفيديوي والتحكم في النفاذ.

وبما أن النظام VMS موصول بالشبكة، فإنه يعاني حقاً من العديد من مواطن الضعف، كتلك التي تواجهها خدمات الويب على الإنترنت، ومن ثم ليس من المستبعد أن يكون هدفاً للهجمات السيبرانية.

وتحلل التوصية ITU-T X.1453 التهديدات الأمنية للنظام VMS القائم على منصة المخدم والذي يعمل على شبكة بروتوكول الإنترنت وهي تحدد المتطلبات الأمنية لمواجهة التهديدات الأمنية المحددة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1453	2022-01-07	17	11.1002/1000/14802

مصطلحات أساسية

إطار الأمن، المتطلبات الأمنية، نظام إدارة الفيديو.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع/حقوق تأليف ونشر البرمجيات يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قواعد البيانات المناسبة لدى الاتحاد المتاحة من خلال الموقع الإلكتروني لقطاع تقييس الاتصالات عبر الرابط: http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1453

التهديدات الأمنية والمتطلبات الأمنية لأنظمة الإدارة الفيديوية

1 مجال التطبيق

تحدد هذه التوصية التهديدات الأمنية والمتطلبات الأمنية لنظام الإدارة الفيديوية (VMS) القائم على منصة المخدم الذي يتلقى الفيديو من الكاميرات، وهي نوع من أجهزة إنترنت الأشياء (IoT) التي تسمح للمستخدمين بمشاهدة الفيديو إما مباشرة أو من تسجيل. وتشمل هذه التوصية ما يلي:

- تحليل معمارية النظام VMS القائم على منصة المخدم؛
- تحليل التهديدات الأمنية التي تواجهها أنظمة الإدارة الفيديوية (VMS)؛
- المتطلبات الأمنية لمواجهة التهديدات المحددة.

2 المراجع

يتضمن ما يلي من توصياتٍ لقطاع تقييس الاتصالات بالاتحاد الدولي للاتصالات (ITU-T) وغيرها من المراجع أحكاماً تشكل بالإحالة إليها في النص الحالي أحكام التوصية الحالية. وعند نشر هذه التوصية، كانت إصدارات التوصيات والمراجع المشار إليها سارية المفعول. لكن لمّا كانت جميع التوصيات وغيرها من المراجع تخضع للمراجعة، تُشجَّع الجهات المستعينة بهذه التوصية على بحث إمكانية تطبيق أحدث إصدار من التوصيات وسائر المراجع المسرودة أدناه. وتُنشر بانتظام قائمة بتوصيات قطاع تقييس الاتصالات السارية. والإحالة إلى وثيقة ما في هذه التوصية لا تضفي على الوثيقة في حد ذاتها صفة التوصية.

لا يوجد.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلح التالي المعرَّف في وثائق أخرى:

1.1.3 نظام المراقبة الفيديوية (video surveillance) [b-ITU-T H.626]: هو خدمة اتصالات تركز على تكنولوجيا التطبيقات الفيديوية (بما في ذلك الصوت والصورة)، التي تُستخدم لالتقاط الوسائط المتعددة عن بُعد (مثل الصوت والفيديو والصورة وإشارة الإنذار، وما إلى ذلك) وتقديمها إلى المستخدم النهائي على نحو ميسور الاستخدام، استناداً إلى شبكة النطاق العريض المدارة مع ضمان الجودة والأمان والموثوقية.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرِّف هذه التوصية المصطلحات التالية:

1.2.3 نظام الإدارة الفيديوية: وهو جزء جوهري في أي نظام للمراقبة الفيديوية يسمح للمستخدمين بمشاهدة عدة كاميرات وتسجيل وتحليل التدفقات الفيديوية وتضمين إنذارات تنطلق في أحوال العبث في النظام أو الحركة.

4 المختصرات

تستخدم هذه التوصية المختصرات التالية:

DDoS رفض الخدمة الموزّع (*Distributed Denial of Service*)

IDS نظام كشف التسلل (*Intrusion Detection System*)

IoT إنترنت الأشياء (*Internet of Things*)

IP بروتوكول الإنترنت (*Internet Protocol*)

IPS نظام منع التسلل (*Intrusion Prevention System*)

NVR مسجلة فيديوية للشبكة (*Network Video Recorder*)

VMS نظام إدارة فيديوية (*Video Management System*)

5 الاصطلاحات

في هذه التوصية:

تشير عبارة "**يتعين على**" [is required] إلى مطلبٍ "يتعين" الالتزام الصارم به ولا يسمح بالحيْد عنه، في حال زعم الامتثال لهذه التوصية.

وتشير عبارة "**يوصَي بـه**" [is recommended] إلى مطلبٍ "يوصى به" ولكن ليس بصورة مطلقة. وهكذا، لا حاجة لتوفر هذا المطلب لزعم الامتثال لهذه التوصية.

6 نظام الإدارة الفيديوية

ما فتئت إنترنت الأشياء (IoT) تنتشر بسرعة في شتى أنحاء العالم في السنوات القليلة الماضية. ومن شأن أنظمة المراقبة الفيديوية القائمة على إنترنت الأشياء أن تمكّن المستخدمين من مشاهدة ما يحدث في مكان بعيد والتقاط الصور التي قد تهمهم متى أرادوا. وتختلف حالات استخدام هذه الأنظمة على نطاق واسع، من تطبيق القانون ومنع الجريمة إلى السلامة في عمليات النقل ومراقبة الحركة. وأنظمة الإدارة الفيديوية (VMS) هي جوهر أنظمة المراقبة الفيديوية المستخدمة في أنظمة السلامة العامة ومراقبة الحركة. وبالدرجة الأولى، يستقبل النظام VMS الفيديو من الكاميرات ويسمح للمستخدمين بمشاهدة الفيديو إما مباشرة أو من تسجيل. وتتضمن نُهُج النظام VMS الناشئة حالياً المزيد من الذكاء في تصميمها، بما في ذلك التحليل الفيديوي والتحكم في النفاذ.

وبما أن النظام VMS موصول بالشبكة، فإنه يعاني حقاً من العديد من مواطن الضعف، كتلك التي تواجهها خدمات الويب على الإنترنت والتي قد تكون هدفاً للهجوم السيبراني.

ويتكون نظام المراقبة الفيديوية القائم على إنترنت الأشياء عموماً من عدة كاميرات أمنية ونظام إدارة فيديوية وأجهزة عميل لتمكين المستخدم من مشاهدة الفيديو. ويسمح النظام VMS للمستخدمين بتسجيل ومشاهدة الفيديو مباشرة من عدة كاميرات أمنية، لمراقبة الإنذارات والتحكم في الكاميرات واستعادة التسجيلات من الأرشيف. والنظام VMS القائم على إنترنت الأشياء أكثر قابلية للتوسع والمرونة من نظام تماثلي، وهو يسمح للمستخدمين بالتحكم في الأجهزة التي يتكون منها نظام المراقبة الفيديوية في أي مكان على الشبكة.

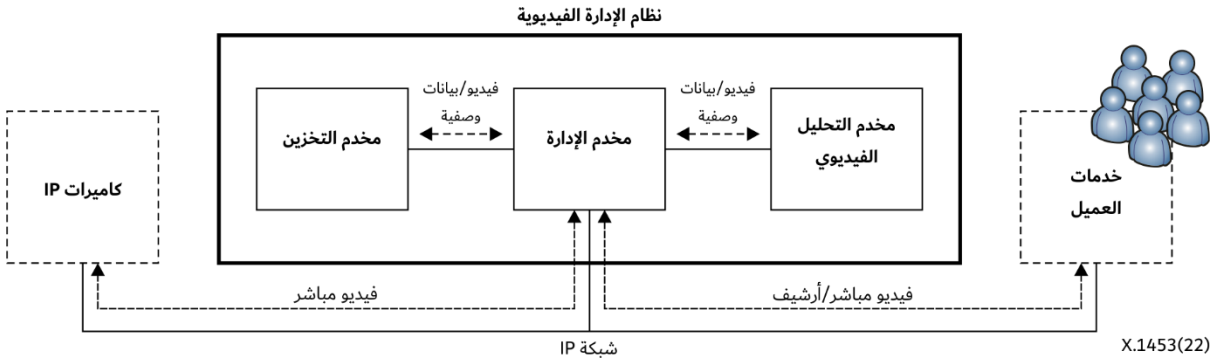
ويمكن أن ينطوي النظام VMS على العديد من الميزات المختلفة على النحو التالي:

- المشاهدة المتزامنة
- تسجيل الفيديو والصوت
- البحث عن الفيديو وتشغيله

- التحليل الفيديوي الذكي
- إدارة الكاميرات
- إدارة الأحداث
- إدارة الإنذارات

وهناك نوعان مختلفان من منصات المعدات لنظام الإدارة الفيديوية VMS الموصول بالشبكة: نظام VMS قائم على منصة مخدم يتضمن واحداً أو أكثر من المخدمات التي تشغل برمجيات للإدارة الفيديوية، أو نظام VMS قائم على مسجل فيديوي للشبكة (NVR). والنظام VMS هو مزيج من البرمجيات والمعدات الفيديوية. ويمكن تثبيت برمجيات الإدارة الفيديوية على معدات المسجل NVR أو تثبيته على معدات المخدم. وتستخدم برمجيات الإدارة الفيديوية المثبتة على المسجل NVR لأداء مهام بسيطة مثل تسجيل مقاطع الفيديو ومراقبتها في منطقة محصورة، بينما تتحكم برمجيات الإدارة الفيديوية المثبتة على المخدم عن بُعد في العديد من الكاميرات الموزعة في مواقع مختلفة، وتختزن الفيديوهات وتديرها، وتوفر أيضاً تحليلات فيديوية ذكية لتحري الأحداث تلقائياً. وعموماً، يشير النظام VMS القائم على المسجل NVR إلى نظام VMS باستخدام مسجل NVR واحد فقط، بينما يشير النظام VMS القائم على مخدم إلى نظام VMS من مخدم واحد أو أكثر يتحكم في العديد من الكاميرات ويوفر خدمات تحليلية واسعة. ولا تتناول هذه التوصية سوى نظام VMS القائم على منصات مخدم.

ولتحليل أمن النظام VMS يتعين وضع معمارية لتحديد جميع الكيانات المتعلقة بالمراقبة الفيديوية على أساس نظام الإدارة الفيديوية وتوضيح العلاقة بين الكيانات. ويوضح الشكل 1 المعمارية الوظيفية للنظام VMS من أجل تطبيقات المراقبة الفيديوية.



الشكل 1 – معمارية وظيفية مبسطة لنظام الإدارة الفيديوية (VMS)

تشتمل أنظمة المراقبة الفيديوية على خمسة أنواع من الكيانات الرئيسية: الكاميرات ومخدمات التخزين ومخدمات الإدارة ومخدمات التحليل الفيديوي وأجهزة العميل. ويتكون نظام الإدارة الفيديوية الموجود في قلب نظام المراقبة الفيديوية من مخدم إدارة ومخدم تخزين ومخدم تحليل فيديوي. وهناك أربع علاقات بين الكيانات الموضحة في الشكل 1 على النحو التالي: بين الكاميرا ومخدم الإدارة، وبين مخدم الإدارة وجهاز العميل، وبين مخدم الإدارة ومخدم التخزين، وبين مخدم الإدارة ومخدم التحليل الفيديوي.

ويكون توصيل النظام VMS بالكاميرات وأجهزة العميل عبر شبكة ما. ويكون مخدم الإدارة ومخدم التخزين ومخدم التحليل الفيديوي عادةً في نفس الشبكة. وتكون أجهزة العميل عموماً موصولة بشبكة مفتوحة، مثل الإنترنت، من أجل مراقبة موسعة عن بُعد.

ومخدم الإدارة هو مركز النظام VMS. فهو يتحكم ويدير جميع الكيانات في أنظمة المراقبة الفيديوية، بما في ذلك إعدادات الكاميرا ومعلمات التخزين وما إلى ذلك. ويقوم مخدم التخزين بتسجيل الفيديو من الكاميرات المرتبطة به ويختزن البيانات الوصفية التي يستحدثها مخدم التحليل الفيديوي. ويقوم مخدم التحليل الفيديوي بتحليل الأهداف المتحركة في تدفق فيديوي ويستحدث بيانات وصفية لوصف الأنشطة والأحداث المحددة. ويولد مخدم التحليل الفيديوي شكلين من البيانات الوصفية، البيانات الوصفية للأحداث والبيانات الوصفية للإنذارات. ويتألف كل حدث أو إنذار من رسائل بيانات وصفية متعددة تحتوي على نعوت مختلفة بشأن أي تغيير يلاحظ أو مقطع حركة في تدفق فيديوي.

7 التهديدات الأمنية

1.7 التهديدات للواجهة بين مخدم الإدارة والكاميرا

تتمثل المهمة الرئيسية للواجهة بين مخدم الإدارة والكاميرا في التقاط الفيديو من الكاميرا وضبط إعدادات الكاميرا والتحكم في الكاميرا للتدوير والإمالة والتكبير/التصغير. والبيانات المنقولة عبر هذه الواجهة هي الهدف الرئيسي للمهاجم. ويمكن للمهاجم تعطيل خدمة الإدارة الفيديوية باعتراض البيانات وتزويرها وإعادة تشغيلها. وثمة هدف آخر لدى المهاجمين وهو رفض خدمة الإدارة الفيديوية وذلك بشن هجوم رفض الخدمة الموزع (DDoS) على الكاميرات ومخدم الإدارة.

وفيما يلي التهديدات التي تتعرض لها الواجهة بين مخدم الإدارة والكاميرا:

- النفاذ غير المصرح به: هجوم يتمثل في النفاذ إلى الكاميرا باستخدام حساب شخص آخر أو طريقة نفاذ أخرى. وقد يؤدي النفاذ غير المصرح به إلى الكاميرا إلى الكشف عن معلومات حساسة وتعديل الفيديو والاستخدام غير القانوني للموارد. إذ من الممكن، بعد نفاذ المهاجم إلى الكاميرا، جمع بيانات الفيديو بشكل غير قانوني، ويمكن أن تؤدي المراقبة في الوقت الفعلي لبيانات الفيديو إلى شواغل تتعلق بالخصوصية.
- التنصت على الشبكة: هجوم يلتقط بيانات الفيديو المرسلة من الشبكة ويقرأ محتوى الفيديو بحثاً عن معلومات حساسة، مثل الوجوه ولوحات ترخيص السيارات وما إلى ذلك.
- رفض الخدمة: هجوم يحاول تشغيل شفرة خبيثة على مخدم الإدارة أو الكاميرا بهدف إغراق الهدف بفيض من البيانات أو طلبات الخدمة. ويمكن أن يفضي هذا الهجوم إلى إبطاء خدمات الإدارة الفيديوية أو تعطيلها.
- تزوير البيانات الفيديوية: يقوم المهاجم بقطع البيانات الفيديوية، ثم يرسل بيانات فيديوية مزيفة إلى مخدم الإدارة. ويمكن أن يتسبب الهجوم في حدوث تداخل مع التشغيل الاعتيادي لنظام VMS.
- تزوير بيانات التحكم: يقوم المهاجم بقطع بيانات التحكم لضبط إعدادات الكاميرا، ثم يرسل بيانات تحكم مزيفة إلى الكاميرات. ويمكن أن يتسبب الهجوم في حدوث تداخل مع وظائف التحكم الاعتيادية في الكاميرات.
- تهديدات من الداخل: عندما يتعلق الأمر بالناس، هناك دائماً خطر أن يتصرف بعض الأفراد بطريقة ضارة أو دون مبالاة تعرّض خدمة الإدارة الفيديوية للخطر. فالمستخدمون الذين يتقاسمون كلمة سر "المدير" أو يتركون بيانات الاعتماد في أماكن غير آمنة، أو المستخدمون المهملون أو غير المدربين تدريباً كافياً، أو التصرفات الضارة من جانب مستخدمين ساخطين، كل هذا يشكل تهديدات لا بأس بها.

2.7 تهديدات للواجهة بين مخدم الإدارة وجهاز العميل

تتمثل المهمة الرئيسية للواجهة بين مخدم الإدارة وجهاز العميل في توفير الواجهات لمشاهدة الفيديو مباشرة والنفاذ إلى الفيديوهات المسجلة.

وفيما يلي التهديدات التي تتعرض لها الواجهة بين مخدم الإدارة وجهاز العميل:

- النفاذ غير المصرح به: هجوم يتمثل في النفاذ إلى جهاز العميل باستخدام حساب شخص آخر أو طريقة نفاذ أخرى. وقد يؤدي النفاذ غير المصرح به إلى جهاز العميل إلى الكشف عن معلومات حساسة وتعديل الفيديو والاستخدام غير القانوني للموارد. إذ من الممكن، بعد نفاذ المهاجم إلى جهاز العميل، جمع بيانات الفيديو بشكل غير قانوني، ويمكن أن تؤدي المراقبة في الوقت الفعلي لبيانات الفيديو إلى شواغل تتعلق بالخصوصية.
- التنصت على الشبكة: هجوم يلتقط بيانات الفيديو المرسلة من الشبكة ويقرأ محتوى الفيديو بحثاً عن معلومات حساسة، مثل الوجوه ولوحات ترخيص السيارات أو أي نوع آخر من المعلومات الحساسة.
- رفض الخدمة: هجوم يحاول تشغيل شفرة خبيثة على مخدم الإدارة أو أجهزة العميل بهدف إغراق الهدف بفيض من البيانات أو طلبات الخدمة. وقد يؤدي هذا الهجوم إلى إبطاء خدمات الإدارة الفيديوية أو تعطيلها.

- تزوير بيانات الفيديو: يقوم المهاجم بقطع البيانات الفيديوية، ثم يرسل بيانات فيديوية مزيفة إلى أجهزة العميل. ويمكن أن يتسبب الهجوم في حدوث تداخل مع التشغيل الاعتيادي لنظام VMS.
- تزوير بيانات التحكم: يقوم المهاجم بقطع بيانات التحكم لضبط إعدادات الكاميرا، ثم يرسل بيانات تحكم مزيفة إلى مخدم الإدارة. ويمكن أن يتسبب الهجوم في حدوث تداخل مع وظائف التحكم الاعتيادية في الفيديو.
- تهديدات من الداخل: عندما يتعلق الأمر بالناس، هناك دائماً خطر أن يتصرف بعض الأفراد بطريقة ضارة أو دون مبالاة تعرّض خدمة إدارة الفيديو للخطر. فالمستخدمون الذين يتقاسمون كلمة سر "المدير" أو يتركون بيانات الاعتماد في مكان غير آمن، أو المستخدمون المهملون أو غير المدربين تدريباً كافياً، أو التصرفات الضارة من جانب مستخدمين ساخطين، كل هذا يشكل تهديدات لا بأس بها.

3.7 تهديدات للواجهة بين مخدم الإدارة ومخدم التخزين

تتمثل المهمة الرئيسية للواجهة بين مخدم الإدارة ومخدم التخزين في توفير واجهات لتسجيل/مشاهدة الفيديو والبيانات الوصفية.

ويكون مخدم الإدارة ومخدم التخزين عادة في نفس الشبكة أو موصولين عبر خط مخصص. وحتى لو كان مخدم الإدارة موصولاً بالشبكة العمومية فقط، يمكن للمتسلل استغلال مواطن الضعف الأمنية لدى مخدم الإدارة للنفاذ بشكل غير قانوني إلى مخدم التخزين.

وفيما يلي التهديدات التي تتعرض لها الواجهة بين مخدم الإدارة ومخدم التخزين:

- النفاذ غير المصرح به: هجوم يتمثل في النفاذ إلى مخدم الإدارة باستخدام حساب شخص آخر أو طريقة نفاذ أخرى للنفاذ إلى البيانات المختزنة في مخدم التخزين. ويمكن أن يؤدي النفاذ غير المصرح به إلى مخدم التخزين إلى الكشف عن معلومات حساسة واستخدام غير قانوني للموارد.
- الكشف عن البيانات: هجوم يتمثل في النفاذ غير القانوني إلى محتوى الفيديو المختزن في المخدم يقرأ المعلومات الحساسة، مثل الوجوه ولوحات ترخيص السيارات. ويمكن للمهاجم الكشف عن البيانات غير المشمولة الحماية.
- دس البيانات وتعديلها: هجوم يتمثل في تعديل بيانات الفيديو المختزنة بشكل غير قانوني وذلك بتضمينها بيانات شائبة، مما يؤدي إلى إضعاف موثوقية المعلومات الفيديوية.
- تهديدات من الداخل: عندما يتعلق الأمر بالناس، هناك دائماً خطر أن يتصرف بعض الأفراد بطريقة ضارة أو دون مبالاة تعرّض خدمة إدارة الفيديو للخطر. فالمستخدمون الذين يتقاسمون كلمة سر "المدير" أو يتركون بيانات الاعتماد في مكان غير آمن، أو المستخدمون المهملون أو غير المدربين تدريباً كافياً، أو التصرفات الضارة من جانب مستخدمين ساخطين، كل هذا يشكل تهديدات لا بأس بها.

4.7 تهديدات للواجهة بين مخدم الإدارة ومخدم التحليل الفيديوي

تتمثل المهمة الرئيسية للواجهة بين مخدم الإدارة ومخدم التحليل الفيديوي في بث الفيديو لتحليل الأهداف المتحركة في بيانات الفيديو والبيانات الوصفية لوصف الأنشطة والأحداث المحددة في مخدم التحليل الفيديوي.

ويكون مخدم الإدارة ومخدم التحليل الفيديوي عادة في نفس الشبكة أو موصولين عبر خط مخصص. وحتى عندما يكون مخدم الإدارة فقط موصول بالشبكة العمومية، يمكن للمتسلل استغلال مواطن الضعف الأمنية لدى مخدم الإدارة للنفاذ بشكل غير قانوني إلى مخدم التحليل الفيديوي.

وفيما يلي التهديدات التي تتعرض لها الواجهة بين مخدم الإدارة ومخدم التحليل الفيديوي:

- النفاذ غير المصرح به: هجوم يتمثل في النفاذ إلى مخدم الإدارة باستخدام حساب شخص آخر أو طريقة نفاذ أخرى للنفاذ إلى البيانات المختزنة في مخدم التحليل الفيديوي. ويمكن أن يؤدي النفاذ غير المصرح به إلى مخدم التحليل الفيديوي إلى حدوث أعطال، مما يقلل من موثوقية مخدم التحليل الفيديوي.

- الكشف عن البيانات: هجوم يتمثل في النفاذ بشكل غير قانوني إلى محتوى الفيديو المختزن على المخدم يقرأ معلومات حساسة مثل الوجوه ولوحات ترخيص السيارات وما إلى ذلك. ويمكن للمهاجم الكشف عن البيانات غير المشمولة بالحماية.
- دس البيانات وتعديلها: هجوم يتمثل في تعديل بيانات الفيديو أو البيانات الوصفية بشكل غير قانوني وذلك بإدخال بيانات شائبة، مما يؤدي إلى إضعاف موثوقية مخدم التحليل الفيديوي. مثال ذلك، عندما يَنفُذ المهاجم بشكل غير قانوني إلى مخدم الإدارة، يمكنه الحصول بشكل غير قانوني على أذونات لشخص غير مرخص له باستبدال بيانات وجه الشخص المرخص له المختزن ببيانات وجه شخص غير مرخص له.
- تهديدات من الداخل: عندما يتعلق الأمر بالناس، هناك دائماً خطر أن يتصرف بعض الأفراد بطريقة ضارة أو دون مبالاة تعرّض خدمة إدارة الفيديو للخطر. فالمستخدمون الذين يتقاسمون كلمة سر "المدير" أو يتركون بيانات الاعتماد في مكان غير آمن، أو المستخدمون المهملون أو غير المدربين تدريباً كافياً، أو التصرفات الضارة من جانب مستخدمين ساخطين، كل هذا يشكل تهديدات لا بأس بها.

5.7 العلاقة بين التهديدات الأمنية والكيانات داخل/خارج نظام الإدارة الفيديوية

تستهدف التهديدات الأمنية أماكن محددة بين الكيانات المبينة في الشكل 1. وتظهر علاقة التهديدات والكيانات الأمنية داخل/خارج نظام الإدارة الفيديوية في الجدول 1، حيث تشير الحلقة في الخلية إلى أن الكيان مرتبط بتهديد أمني معين.

الجدول 1 – العلاقة بين المتطلبات الأمنية والكيانات

كيانات / تهديدات	بين VMS والكاميرات	VMS		بين VMS وأجهزة العميل
		بين مخدم الإدارة ومخدم التخزين	بين مخدم الإدارة ومخدم التحليل الفيديوي	
تنصت على الشبكة	○			○
نفاذ غير مرخص	○	○	○	○
رفض الخدمة	○			○
الكشف عن البيانات		○	○	
دس البيانات وتعديلها	○	○	○	○
تهديدات من الداخل	○	○	○	○

8 المتطلبات الأمنية

1.8 السرية

تضمن سرية البيانات عدم تمكن كيانات غير مخوّلة من قراءة محتوى البيانات. وحتى في حالة التنصت على بعض البيانات وكشف المهاجم عنها، يمكن ضمان سريتها.

والسرية مطلوبة للبيانات الحساسة، سواء فيما يخص تخزينها أو إرسالها. وتشمل البيانات الحساسة البيانات الفيديوية وبيانات الأوامر التي تتحكم في تشغيل الكاميرات والبيانات المختزنة في مخدم التخزين وما إلى ذلك.

- السرية مطلوبة للحرص على أن البيانات الفيديوية المنقولة على الشبكة لا يمكن قراءتها من جانب كيانات غير مصرح لها.
- السرية مطلوبة للحرص على أن بيانات الأوامر التي تتحكم في تشغيل الكاميرات المنقولة على الشبكة لا يمكن قراءتها من جانب كيانات غير مصرح لها.
- السرية موصى بها للتأكد من أن البيانات المختزنة على مخدم التخزين ومخدم التحليل الفيديوي لا يمكن قراءتها من جانب كيانات غير مصرح لها.

2.8 السلامة

تتمثل السلامة في ضمان عدم اختلاف البيانات، بعد نقلها، عن تلك التي كانت في المصدر. ويتعين عدم تغيير البيانات الأصلية المختزنة بعد النفاذ المصرح به.

- السلامة مطلوبة للتأكد من أن البيانات الفيديوية المنقولة من الكاميرا هي بيانات أصلية دون تزوير.
- يوصى بالسلامة للتأكد من أن البيانات الفيديوية المختزنة هي بيانات أصلية دون تزوير.
- يوصى بالسلامة للتأكد من أن البيانات الفيديوية المرسلة لأغراض التحقيق الجنائي، وما إلى ذلك، هي بيانات أصلية دون أي تغيير.

3.8 استيقان المستخدم والجهاز

الاستيقان مطلوب لتأكيد هويات المستخدمين والأجهزة. ومن شأن الاستيقان التحقق من صحة الهويات المزعومة للكيانات المشاركة في المراقبة الفيديوية والحرص على أن أي كيان غير مصرح له لا يحاول التنكر في هيئة كيان مرخص له.

- استيقان المستخدم مطلوب للتأكد من أن المستخدم مدير شرعي مسموح له بالنفاذ إلى المخدمات في نظام VMS للإدارة الفيديوية المركزية.
- استيقان المستخدم مطلوب للتأكد من أن المستخدم هو مستخدم شرعي لجهاز العميل وأنه يسمح له بمشاهدة البيانات الفيديوية عن بُعد.
- استيقان الجهاز موصى به للتأكد من أن الجهاز هو جهاز عميل شرعي يسمح بتوصيله عن بُعد بالنظام VMS.
- استيقان الجهاز موصى به للتأكد من أن الكاميرا هي كاميرا شرعية يُسمح بتوصيلها بالنظام VMS.

4.8 التحكم في النفاذ

التحكم في النفاذ مطلوب لضمان السماح للمستخدمين المصرح لهم فقط بالنفاذ إلى الموارد المناسبة المشاركة في المراقبة الفيديوية. وعلى الرغم من أن المسؤولين يشاركون في المجموعة ذات الامتيازات المسموح لها بالحفاظ على نظام المراقبة الفيديوية والتحكم فيه، فمن الموصى به منح كل مستخدم حق نفاذ مختلف.

- التحكم في النفاذ مطلوب لضمان السماح للمستخدمين المصرح لهم فقط بالنفاذ إلى مخدم الإدارة وفقاً لامتيازات النفاذ الخاصة بهم في نظام المراقبة الفيديوية. وتشمل أنواع النفاذ المراقبة الفيديوية في الوقت الفعلي والتشغيل الفيديوي المسجل والتحكم في الكاميرا عن بُعد.
- التحكم في النفاذ مطلوب لضمان السماح لمستخدمي جهاز العميل المصرح لهم فقط بالنفاذ إلى المراقبة الفيديوية وفقاً لامتيازات النفاذ الخاصة بهم. وتشمل أنواع النفاذ المراقبة الفيديوية في الوقت الفعلي والتشغيل الفيديوي المسجل.

5.8 منع التسلل

منع التسلل مطلوب لحماية كيانات نظام الإدارة الفيديوية والبيانات الفيديوية المختزنة والخدمات من محاولات النفاذ غير القانونية الداخلية والخارجية. ويمكن تصنيف منع التسلل في النظام VMS في فئتين: الطريقة المنطقية والطريقة المادية. فطريقة منع التسلل المنطقية تحمي موارد النظام من الهجمات التي تستخدم شبكة قائمة على بروتوكول الإنترنت. بينما تحمي طريقة منع التسلل المادية موارد النظام من النفاذ المادي غير القانوني.

- منع التسلل المنطقي مطلوب لضمان حماية موارد النظام من الهجمات التي تستخدم شبكة قائمة على بروتوكول الإنترنت، مما يسمح للمراقبة الفيديوية بالعمل بشكل اعتيادي. وتشمل أنظمة أمن الشبكات المستخدمة لمنع التسلل المنطقي نظام كشف التسلل (IDS) ونظام منع التسلل (IPS). ومن الأفضل استخدام نظام أمن شبكة مخصص بدلاً من نظام يثبت داخل النظام VMS.

- منع التسلل المادي مطلوب لضمان أن المستخدمين الشرعيين فقط، الذين تم تحديدهم من خلال استيقان المستخدم، يمكنهم النفاذ إلى مركز العمليات الأمنية حيث تم تثبيت النظام VMS.

6.8 العلاقة بين المتطلبات الأمنية والتهديدات الأمنية

يبين الجدول 2 العلاقة بين المتطلبات الأمنية والتهديدات الأمنية، حيث تشير الحلقة في الخلية إلى ضرورة استيفاء شرط أمني محدد من أجل إزالة تهديد محدد أو التخفيف من حدته.

الجدول 2 – العلاقة بين المتطلبات الأمنية والتهديدات الأمنية

			المتطلبات الأمنية				
			السرية	السلامة	استيقان المستعمل/الجهاز	التحكم في النفاذ	منع التسلل
تهديدات أمنية	VMS	نفاذ غير مرخص			○	○	
		كشف عن البيانات	○				
		تعديل/إدخال		○			
		تهديدات من الداخل			○	○	
		رفض الخدمة					○
	بين VMS والكاميرات	نفاذ غير مرخص			○	○	
		تنصت	○				
		رفض الخدمة					○
		تعديل/إدخال		○			
		تهديدات داخلية			○	○	
	بين VMS وأجهزة العميل	نفاذ غير مرخص			○	○	
		تنصت	○				
		رفض الخدمة					○
		تعديل/إدخال		○			
		تهديدات داخلية	○		○	○	

بيبليوغرافيا

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

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2022