国　际　电　信　联　盟

ITU-T X.1453

(01/2022)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

安全应用和服务（2） – 应用安全（2）

视频管理系统的安全威胁和要求

ITU-T X.1453建议书

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全（1）	X.1140–X.1149
应用安全（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1350–X.1369
智能交通系统（ITS）安全	X.1370–X.1399
分布式账簿技术（DLT）安全	X.1400–X.1429
应用安全（2）	**X.1450–X.1459**
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020安全	X.1800–X.1819

ITU-T X.1453建议书

视频管理系统的安全威胁和要求

摘要

视频管理系统（VMS）是公共安全、交通监控等视频监控系统的核心。基本上而言，VMS从摄像头接收视频，并允许用户实时查看该视频或视频录像。目前新兴的VMS设计方式是将越来越多的智能融入其中，包括视频分析和访问控制。

由于VMS是连网的，会完全在各种漏洞方面不堪一击（如互联网网络服务面临的漏洞），因此很容易成为网络攻击的目标。

ITU-T X.1453建议书分析运行在IP网络上的、基于服务器平台的VMS面临的安全威胁，并对抵制已确定安全威胁的安全要求做出具体规定。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1453	2022-01-07	17	11.1002/1000/14802

关键词

安全框架、安全要求、视频管理系统

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联没有收到实施本建议书可能需要的受专利/软件版权保护的知识产权通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们查询可通过ITU-T网站获得的适当的ITU-T数据库，网址为：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1453建议书

视频管理系统的安全威胁和要求

1 范围

本建议书明确基于服务器平台的视频管理系统（VMS）的安全威胁和安全要求，这些视频管理系统从摄像头（物联网设备的一种）接收视频，并允许用户实时查看该视频或视频录像。本建议书包括以下内容：

– 基于服务器平台的VMS的架构分析

– 此类VMS面临的安全威胁分析

– 抵制已确定威胁的安全要求。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均会得到修订；因此本建议书的使用者应查证是否有可能使用下列建议书和其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

无。

3 定义

3.1 他处定义的术语

本建议书使用以下他处定义的术语：

3.1.1 视频监控系统[b-ITU-T H.626]：一项以视频（包括音频和图像）应用技术为重点的电信业务，用于远程捕获多媒体（如音频、视频、图像、报警信号等）并以用户友好的方式呈现给最终用户，其基础是质量、安全性和可靠性得到保证的受管宽带网络。

3.2 本建议书中定义的术语

本建议书定义了以下术语：

3.2.1 视频管理系统（video management system）：任何视频监控系统的必不可少的部分是允许用户查看多个摄像头、记录和分析视频流，并设置篡改警报和行动发现警报。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

DDoS 分布式拒绝服务

IDS 入侵检测系统

IoT 物联网

IP 互联网协议

IPS 入侵防御系统

NVR 网络录像机

VMS 视频管理系统

5 惯例

在本建议书中：

关键用语**“要求”（is required to**）表明是一项务必严格遵守的要求，若要宣布与本建议书一致，则不允许与该要求有任何偏离。

关键用语**“建议”（is recommended**）表明是一项建议遵守的要求，但并非绝对必要。因此宣布与本建议书一致时不需要表明要满足该要求。

6 视频管理系统

过去几年，物联网（IoT）在全球范围内迅速发展。基于物联网的视频监控系统方便用户查看发生在远程地点的活动情况，并按意愿捕捉他们感兴趣的图像。这些系统的使用案例千差万别，从执法和犯罪预防到交通安全和交通监控，不一而足。视频管理系统（VMS）是用于公共安全和交通监控系统的视频监控系统的核心。基本上而言，VMS接收来自摄像头的视频，并允许用户实时查看视频或视频录像。当前新兴的VMS设计方式将越来越多的智能融入其中，包括视频分析和访问控制。

由于VMS是连网的，会完全在各种漏洞方面不堪一击（如互联网网络服务面临的漏洞），因此可能成为网络攻击的目标。

典型的基于物联网的视频监控系统由多个安全摄像头、一个VMS和供用户查看视频的客户端设备组成。VMS允许用户记录和查看来自多个安全摄像头的实时视频，监控警报，控制摄像头，并从档案中检索记录。基于物联网的VMS比基于模拟技术的系统更具可扩展性和灵活性，方便用户在网络上的任何地方控制组成视频监控系统的设备。

如下所示，VMS可支持许多不同功能特性：

– 同时查看；
– 视频和音频记录；
– 视频搜索和回放；
– 智能视频分析；
– 摄像头管理；
– 事件管理；
– 警报管理。

连网VMS有两种不同类型的硬件平台：基于服务器平台的VMS涉及一个或多个运行视频管理软件程序的服务器，或是基于网络录像机（NVR）的VMS。VMS结合使用视频软件和硬件。视频管理软件可安装在NVR硬件或服务器硬件上。安装在NVR的视频管理软件用于执行简单的任务，如在有限的区域内记录和监控视频镜头，而安装在服务器上的视频管理软件则远程控制分布在不同地点的许多摄像头、存储和管理视频，并提供智能视频分析以自动发现事件。通常而言，基于NVR的VMS是指仅使用一个NVR的VMS，而基于服务器的VMS是指具有一个或多个服务器的VMS，且控制着多个摄像头并提供扩展的分析服务。本建议书仅阐述基于服务器平台的VMS。

为了分析VMS的安全性，现定义了相关框架，以确定基于VMS的与视频监控相关的所有实体，并阐明实体之间的关系。用于视频监控应用的VMS的功能架构如图1所示。

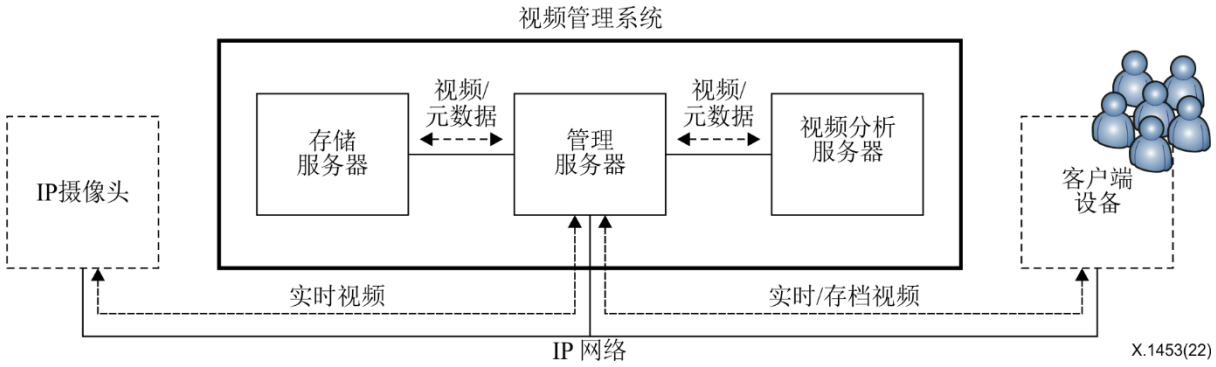

图1 – 简化的功能视频管理系统（VMS）架构

视频监控系统有五种主要实体：摄像头、存储服务器、管理服务器、视频分析服务器和客户端设备。作为视频监控系统核心的VMS由管理服务器、存储服务器和视频分析服务器组成。图1所示的实体之间有四种关系，具体为：摄像头与管理服务器之间、管理服务器与客户端设备之间、管理服务器与存储服务器之间以及管理服务器与视频分析服务器之间的关系。

VMS通过网络与摄像头和客户端设备连接。管理服务器、存储服务器和视频分析服务器通常位于同一网络中。客户端设备通常连接至开放网络（如互联网），用于大范围远程监控。

管理服务器是VMS的核心。它控制和管理视频监控系统中的所有实体，包括摄像头设置、存储参数等。存储服务器记录来自与之连接的摄像头的视频，并存储由视频分析服务器创建的元数据。视频分析服务器分析视频流中的移动对象，并创建元数据来描述所确定的活动和事件。视频分析服务器生成两种形式的元数据，事件元数据和警报元数据。每个事件或警报由多个元数据消息组成，这些消息包含有关视频源中检测到的变化或活动片段的各种属性。

7 安全威胁

7.1 管理服务器与摄像头之间接口面临的威胁

管理服务器与摄像头之间的接口的主要任务是从摄像头收集视频，调整摄像头设置并控制摄像头的旋转、倾斜和缩放。通过这些接口传输的数据是攻击者的主要目标。攻击者可以通过截取、篡改和重放数据来破坏视频管理服务。攻击者的另一个目标是通过对摄像头和管理服务器发起分布式拒绝服务（DDoS）攻击来拒绝视频管理服务。

对管理服务器与摄像头之间接口的威胁如下：

- 未经授权的访问：利用他人账户或其他访问方法获得摄像头访问权限的攻击。未经授权访问摄像头可能会导致敏感信息泄露、视频修改和非法使用资源。例如，一旦攻击者访问了摄像头，则视频数据可能会被非法收集，对视频数据的实时监控可能会导致出现（泄露）隐私问题。

- 网络窃听：一种捕获从网络传输的视频数据并读取视频内容以搜索人脸、汽车牌照等敏感信息的攻击。
- 拒绝服务：试图在管理服务器或摄像头上运行恶意代码的攻击，目的是用大量数据或服务请求淹没目标。这种攻击可使视频管理服务放缓速度或完全停止。
- 伪造视频数据：攻击者拦截视频数据，然后将经伪造的视频数据发送至客户端设备。攻击会干扰VMS的正常运行。
- 篡改控制数据：攻击者拦截用于调整摄像头设置的控制数据，然后向摄像头发送经篡改的控制数据。攻击会干扰摄像头的正常控制功能。
- 内部威胁：在涉及人的地方，总是存在个人以恶意或粗心的方式行事的风险，从而使视频管理服务面临风险。共享“管理员”密码或在不安全的地方留下凭据的用户、粗心或训练无素的用户，或心怀不满的用户的恶意行为，总是会带来严重威胁。

7.2 管理服务器与客户端设备之间接口面临的威胁

管理服务器与客户端设备之间的接口的主要任务是提供查看实时视频和访问录制视频的接口。

对管理服务器与客户端设备之间接口的威胁如下：

- 未经授权的访问：使用他人账户或其他访问方法获得客户端设备访问权限的攻击。未经授权访问客户端设备可能会导致敏感信息泄露和资源非法使用。例如，一旦攻击者访问了客户端设备，则视频数据就会被非法收集，对视频数据的实时监控会导致出现（泄露）隐私问题。
- 网络窃听：一种捕获从网络传输的视频数据并读取视频内容以搜索敏感信息（如人脸、汽车牌照或任何其他类型的敏感信息）的攻击。
- 拒绝服务：试图在管理服务器或客户端设备上运行恶意代码的攻击，目的是用大量数据或服务请求淹没目标。这种攻击可使视频管理服务放缓速度或完全停止。
- 伪造视频数据：攻击者拦截视频数据，然后将经伪造的视频数据发送至客户端设备。攻击会干扰VMS的正常运行。
- 篡改控制数据：攻击者拦截用于调整摄像头设置的控制数据，然后向管理服务器发送经篡改的控制数据。
- 内部威胁：在涉及人的地方，总是存在个人以恶意或粗心的方式行事的风险，从而使视频管理服务面临风险。共享“管理员”密码或在不安全的地方留下凭据的用户、粗心或训练无素的用户，或心怀不满的用户的恶意行为，总是会带来严重威胁。

7.3 管理服务器与存储服务器之间接口面临的威胁

管理服务器与存储服务器之间的接口的主要任务是提供记录/查看视频和元数据的接口。

管理服务器与存储服务器通常位于同一网络中，或者通过专用线路连接。即使只有管理服务器与公共网络连接，黑客也可以利用管理服务器的安全漏洞非法访问存储服务器。

对管理服务器与存储服务器之间接口的威胁如下：

- 未经授权的访问：利用他人账户或其他访问方法访问存储在存储服务器中的数据、从而获得对管理服务器的访问权的攻击。未经授权访问存储服务器可能会导致敏感信息泄露和资源非法使用。
- 数据泄露：非法访问存储在服务器中的视频内容并读取人脸、车牌等敏感信息的攻击。攻击者可能泄露未受保护的数据。
- 数据注入和修改：通过注入不纯数据非法修改存储的视频数据的攻击，这种行为降低了视频信息的可靠性。
- 内部威胁：在涉及人的地方，总是存在个人以恶意或粗心的方式行事的风险，从而使视频管理服务面临风险。共享“管理员”密码或在不安全的地方留下凭据的用户、粗心或训练无素的用户，或心怀不满的用户的恶意行为，总是会带来严重威胁。

7.4 管理服务器与视频分析服务器之间接口面临的威胁

管理服务器与视频分析服务器之间的接口的主要任务是传输视频以分析视频数据中的移动对象，以及传输元数据以描述在视频分析服务器中确定的活动和事件。

管理服务器和视频分析服务器通常位于同一网络中，或者通过专用线路连接。即使只有管理服务器与公共网络连接，攻击者也可以利用管理服务器的安全漏洞非法访问视频分析服务器。

对管理服务器与视频分析服务器之间接口的威胁如下：

- 未经授权的访问：利用他人账户或其他访问方法访问存储在视频分析服务器中的数据、从而获得对管理服务器的访问权的攻击。未经授权访问视频分析服务器可能会导致故障，从而降低视频分析服务器的可靠性。
- 数据泄露：非法访问存储在服务器上的视频内容并读取人脸、车牌等敏感信息的攻击。攻击者可能泄露未受保护的数据。
- 数据注入和修改：通过注入不纯数据非法修改视频数据或元数据的攻击，这种行为降低了视频分析服务器的可靠性。例如，一旦攻击者非法访问了管理服务器，则攻击者即可以通过用未授权人员的面部数据取代存储的经授权人员的面部数据来非法获得未授权人员的权限。
- 内部威胁：在涉及人的地方，总是存在个人以恶意或粗心的方式行事的风险，从而使视频管理服务面临风险。共享“管理员”密码或在不安全的地方留下凭据的用户、粗心或训练无素的用户，或心怀不满的用户的恶意行为，总是会带来严重威胁。

7.5 安全威胁与VMS内部/外部实体之间的关系

安全威胁针对的目标是图1中实体之间的特定位置。表1显示安全威胁与VMS内部/外部实体之间的关系，其中小格中的空心圆表示该实体与特定的安全威胁相关。

表1 – 安全要求与实体之间的关系

实体 / 威胁	VMS与摄像头之间	VMS		VMS与客户端设备之间
		管理服务器与存储器之间	管理服务器与视频分析服务器之间	
网络窃听	○			○
未经授权的访问	○	○	○	○
拒绝服务	○			○
数据泄露		○	○	
数据的注入和修改	○	○	○	○
内部威胁	○	○	○	○

8 安全要求

8.1 保密性

保密性旨在确保未得到授权的实体不能读取数据内容。即使某些数据被窃听，攻击者泄露了这些数据，也可以确保其保密性。

存储或传送敏感数据都需要保密性。敏感数据包括视频数据、控制摄像头操作的命令数据、存储在存储服务器上的数据等。

- 要求具有保密性，以确保网络上传输的视频数据不会被未经授权的实体读取。
- 要求具有保密性，以确保控制网络上传输的摄像头操作命令数据不会被未经授权的实体读取。
- 建议具有保密性，以确保存储在存储服务器和视频分析服务器上的数据不会被未经授权的实体读取。

8.2 完整性

完整性确保数据一旦传送即与源头数据保持一致。要求授权访问后原始存储的数据不得被更改。

- 要求保持完整性，以确保从摄像头传输的视频数据是未经伪造的原始数据。
- 建议保持完整性，以确保存储的视频数据是未经伪造的原始数据。
- 建议完保持整性，以确保导出的、用于刑事调查等的视频数据是未经更改的原始数据。

8.3 用户和设备身份验证（authentication）

要求进行身份验证以确认用户和设备的身份。身份验证可确保参与视频监控的实体的声明身份的有效性，并保证未经授权的实体不会试图伪装成经授权实体行事。

- 要求进行用户身份验证，以确保用户是合法的管理员，可以访问VMS中的服务器，以进行集中视频管理。
- 要求进行用户身份验证，以确保用户是客户端设备的合法用户，并允许用户远程查看视频数据。
- 要求进行设备身份验证，以确保设备是被允许远程连接到VMS的合法客户端设备。
- 建议进行设备身份验证，以确保摄像头是被允许连接到VMS的合法摄像头。

8.4 访问控制

要求进行访问控制，以确保仅允许授权用户访问参与视频监控的适当资源。尽管管理员是被允许维护和控制视频监控系统特权组的成员，但建议为每个用户授予不同的访问权限。

- 要求进行访问控制，以确保仅允许授权用户根据其在视频监控系统中的访问权限访问管理服务器。访问类型包括实时视频监控、录制视频回放和远程摄像头控制。
- 要求进行访问控制，以确保仅允许授权的客户端设备用户根据其访问权限访问视频监控。访问类型包括实时视频监控和录制视频回放。

8.5 入侵防御

要求开展入侵防御来保护VMS的实体、存储的视频数据和服务免受内部和外部的企图非法访问的影响。VMS中的入侵防御可分为逻辑方法和物理方法两类。逻辑入侵防御方法保护系统资源免受使用基于IP的网络的攻击。物理入侵防御方法保护系统资源免受物理非法访问影响。

- 要求开展逻辑入侵防御来确保系统资源免受使用基于IP的网络的攻击，从而使视频监控正常运行。用于逻辑入侵防御的网络安全系统包括入侵发现系统（IDS）和入侵防御系统（IPS）。最好使用专用的网络安全系统，而不是在VMS内部实施的系统。
- 要求开展物理入侵防御来确保只有通过用户身份验证确认的合法用户才可进入安装有VMS的安全运营中心。

8.6 安全性要求与安全威胁之间的关系

表2表明安全性要求与安全威胁之间的关系，其中小格中的空心圆表示为了消除或减缓某一具体威胁而需得到满足的特定安全性要求。

表2 – 安全性要求与威胁之间的关系

			安全性要求				
			保密性	完整性	用户/设备身份验证	访问控制	入侵防御
安全威胁	VMS	未经授权的访问			○	○	
		数据泄露	○				
		修改/注入		○			
		内部威胁			○	○	
		DOS					○
	VMS与摄像头之间	未经授权的访问			○	○	
		窃听	○				
		DOS					○
		修改/注入		○			
		内部威胁			○	○	
	VMS与客户端设备之间	未经授权的访问			○	○	
		窃听	○				
		DOS					○
		修改/注入		○			
		内部威胁			○	○	

参考资料

[b-ITU-T H.626] ITU-T H.626建议书（2019年），视频监控系统的架构要求。

ITU-T 系列建议书

A 系列	ITU-T 工作的组织
D 系列	资费及结算原则和国际电信/ICT 的经济和政策问题
E 系列	综合网络运行、电话业务、业务运行和人为因素
F 系列	非话电信业务
G 系列	传输系统和媒介、数字系统和网络
H 系列	视听及多媒体系统
I 系列	综合业务数字网
J 系列	有线网络和电视、声音节目及其他多媒体信号的传输
K 系列	干扰的防护
L 系列	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
M 系列	电信管理，包括 TMN 和网络维护
N 系列	维护：国际声音节目和电视传输电路
O 系列	测量设备的技术规范
P 系列	电话传输质量、电话设施及本地线路网络
Q 系列	交换和信令，以及相关的测量和测试
R 系列	电报传输
S 系列	电报业务终端设备
T 系列	远程信息处理业务的终端设备
U 系列	电报交换
V 系列	电话网上的数据通信
X 系列	**数据网、开放系统通信和安全性**
Y 系列	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
Z 系列	用于电信系统的语言和一般软件问题

瑞士印刷
2022年，日内瓦