



专题:业务平台安全

网络视频监控系统信息安全机制解析

张艳霞¹, 李洪², 陈军³, 杨晓光³

(1. 中国电信股份有限公司上海研究院 上海 200122;

2. 中国电信集团公司网络运行维护事业部 北京 100032;

3. 中国电信股份有限公司北京研究院 北京 100035)

摘要:信息安全机制是网络视频监控系统安全体系中的核心部分,其安全性包括业务数据安全性和音视频媒体数据安全性,对此,业界有多种解决方案和算法标准,选择了监控业界两个代表性网络视频监控标准的信息安全机制进行解读,分析了主流解决方案和算法,最后提出了通用的视频监控的信息安全机制建议。

关键词:网络视频监控;数据安全;加密;信令

doi: 10.3969/j.issn.1000-0801.2013.08.011

Research on Information Security Mechanism Used in Network Video Surveillance System

Zhang Yanxia¹, Li Hong², Chen Jun³, Yang Xiaoguang³

(1. Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China;

2. Network Operation & Maintenance Division, China Telecom Corporation, Beijing 100032, China;

3. Beijing Research Institute of China Telecom Co., Ltd., Beijing 100035, China)

Abstract: Information security mechanism is a key part of security network video surveillance system, including service data security and multimedia data security, and there are a lot of security solutions and specifications now. Two typical specifications on the network video surveillance system were selected to analyze their information security mechanism and the encryption algorithm, and the suggestions on common data protection mechanism were given out.

Key words: network video surveillance, data security, encryption, signaling

1 引言

网络视频监控系统是基于IP网的图像远程监控、传输、存储、管理的视频监控系统,将分散、独立的图像采集点进行联网,实现跨区域的统一监控、统一存储、统一管理、资源共享。

典型网络视频监控系统主要由前端监控设备(摄像机、视频服务器/编码器)、监控中心(中心服务器)、监控客户端(监控工作站)3部分组成。通过对网络视频监控系统所

面临的安全状况的分析,网络视频监控系统的安全性在总体结构上分为4个层次:物理安全、接入安全、传输和网络安全、业务安全 and 数据安全。

其中,网络视频监控系统数据安全是指应对用户和权限等业务信息和音视频媒体信息有加密保护措施,包括业务数据的安全性和媒体数据的安全性,业务数据包括用户信息、实时浏览、存储、回放以及数据配置(如设备信息查询、云台功能查询、通道名称设置)等;媒体数据包括各通道传输的视频数据、音频数据以及静态的录像文件等。



视频监控系统面临的数据安全威胁大体分类如下:

- 拒绝服务攻击,导致视频监控系统的业务系统无法正常提供服务;
- 漏洞威胁攻击,导致视频监控系统的业务系统无法正常提供服务,数据安全(机密性、完整性和可用性)被破坏;
- 病毒蠕虫,带来的数据完整性和可用性损失以及可能的网络可用性损失;
- 口令猜测,导致视频监控系统的资源被滥用、业务系统等无法正常提供服务,数据安全(机密性、完整性和可用性)受到破坏;
- 视频监控系统的信令/视频数据的不安全远程传输,导致数据安全(机密性、完整性和可用性)受到破坏。

针对上述数据安全威胁,在数据安全的具体技术和设备要求方面,监控业界不同公司的安全策略不同,下面针对业界关于网络视频监控系统的的社会安全机制和方案进行分析。

2 视频监控系统的社会安全分类

通常,视频监控系统业务数据和媒体数据采用分离的通道进行操作,其传输通道类型可分为信令流和媒体流。

(1)信令流加密

业务数据加密是指每个控制命令或者参数设置命令都必须进行加密处理,采取加密业务信令通道的办法来保证信息的安全性,保证数据鉴别、防篡改、防窥视、鉴别来源、防止非法访问、防伪造。

系统对信令进行加密,所有信令都使用加密技术,为了支持加密技术,需增加会话准备操作,进行握手交换标识,以读取密码生成密钥,进而对分组进行加密。

(2)媒体流加密

对于视频流的实时加密流程与信令流类似,同样需要进行交换标识,以读取密码生成密钥。

视频流和视频控制信令应以不同的物理通道进行传输,视频控制信令通过信令流传输,视频流通过媒体流传输。

视频控制协议是视频监控终端与视频设备(视频管理服务器/监控平台、DVR、摄像头等设备)间的控制指令集,即建立视频监控图像连接的基本指令集。为保证通信中指令集不包含网络攻击指令、其他非法字符集或嵌入机密数

据向外泄露,视频传输系统应具备视频协议安全控制功能,对所有视频监控交互指令进行严格安全过滤,阻断非法数据传输和网络攻击的入侵。

3 视频监控信息社会安全机制的标准情况

针对网络视频监控系统安全机制,业界主要有 ONVIF (Open Network Video Interface Forum, 开放型网络视频产品接口开发论坛)、中华人民共和国公安部(以下简称公安部)《城市监控报警联网系统技术标准安全技术要求》、CCSA《电信网视频监控系统安全要求》等标准,此外运营商和厂商各自制定了针对自己系统的安全标准和解决方案,其中 ONVIF 和《城市监控报警联网系统技术标准安全技术要求》是业界采用比较多的监控标准。

ONVIF 成立于 2008 年 5 月,由安讯士网络通讯公司联合博世集团及索尼公司三方携手共同成立,关注 IP 视频监控,目标是实现一个网络视频框架协议,使不同厂商所生产的网络视频产品(包括摄录前端、录像设备等)完全互通。ONVIF 规范向视频监控引入了 Web Services 的概念,设备的实际功能均被抽象为 Web Services 的服务,视频监控系统的控制单元以客户端的身份出现,通过 Web 请求的形式完成控制操作。

由于 ONVIF 基于 Web Services,Web Services 主要利用 HTTP 和 SOAP 使数据在 Web 上传输,其在信息安全方面主要有以下要求:

- 获取或设置访问安全策略;
- 服务器端 HTTPS(secure hypertext transfer protocol,安全超文本传输协议)认证;
- 客户端 HTTPS 认证;
- 密钥生成和证书下载功能;
- IEEE 802.1x supplicant 认证;
- IEEE 802.1x CA 认证;
- IEEE 802.1x 配置。

在信息安全性方面,ONVIF 规范支持摘要认证和 WS-安全框架。

在用户认证方面,最基本验证包括 HTTP 摘要认证和 WSS 摘要认证(用户名令牌描述(username token profile)),高级验证包括 TLS-based access。

在用户认证通过后,通过“获取或设置访问安全策略”实现基于用户的权限控制,以授权其能访问的前端监控设备。

用户名令牌描述必须使用随机数和时间戳作为定义(根据 WS-username token),因为系统为每个摄像头设备提供不同证书不太现实,因此系统对客户端使用用户名令牌描述和主要权限验证,这样就需使用密码加密算法,算法主要采用 SHA-1 函数和 HMAC 算法。举例来说,某一用户 A,其用户名令牌为 UA,P_UA,该用户要访问的终端设备为 NEP,则 $PE_UA = \text{base64}(\text{HMAC_SHA-1}(UA + P_UA, NEP + \text{"ONVIF password"})$) 即为其客户端配置的用户证书和设备权限验证,其中 HMAC_SHA-1 是一种安全的基于加密散列(Hash)函数和共享密钥的消息认证协议,它可以有效地防止数据在传输过程中被截获和篡改,维护了数据的完整性、可靠性和安全性。

在信息的安全通信层面,ONVIF 规范定义了两种通信层面的安全架构:传输层安全(transport layer security, TLS)和消息层安全。

传输层安全协议用于保护 ONVIF 提供的所有服务,同时还需要保护媒体流的 RTP(real-time transport protocol,实时传输协议)/RTSP/HTTPS。

- 设备应该支持 TLS 1.0、TLS 1.1,可以支持 TLS 1.2;加密算法支持 TLS_RSA_WITH_AES_128_CBC_SHA、TLS_RSA_WITH_NULL_SHA。
- 客户端应支持 TLS 1.1、TLS 1.0,加密算法支持 TLS_RSA_WITH_AES_128_CBC_SHA、TLS_RSA_WITH_NULL_SHA。
- 服务器端认证:设备支持 X.509(X.509 是由国际电信联盟(ITU-T)制定的数字证书标准)服务器认证, RSA key 长度至少为 1 024 bit;客户端支持 TLS 服务器认证。
- 客户端认证:支持 TLS 的设备应该支持客户端认证,客户端认证功能可以在设备管理命令中禁止和启用。支持 TLS 的设备应该在证书请求中支持 RSA 认证类型,而且应该支持 RSA 客户端认证和签名验证。

信息层面的安全,规范采用基于端口的安全框架 IEEE 802.1x,支持 EAP-PEAP/MSCHAPv2、EAP-MD5、EAP-TLS 和 EAP-TTLS。TLS 允许点对点的保密性和完整性,但是在有中间通信节点的情况下,TLS 不能提供端到端的安全,此外,为了实现用户基本权限控制,Web Services 需要验证每个 SOAP 消息的来源。

在信息安全方面,公安部《城市监控报警联网系统技

术标准安全技术要求》对此有具体的信息安全章节要求,该标准是由全国安全防范报警系统标准化技术委员会制定的,其成立于 1987 年,负责我国安全防范技术领域国家标准、行业标准的制定、修订工作和对口国际电工委员会/报警技术委员会(IEC/TC79)的工作。

其信息安全技术要求的主要内容总结如下。

- 公钥基础设施,包括证书认证机构(CA)和 3 种证书类型(用户证书、设备证书和 CA 证书),证书的载体可通过移动存储介质、硬盘、智能卡、USBKey、专用加密设备,其中 USBKey 为 USB 接口带有算法的令牌,专用加密设备如加密机,用于产生、存储和管理密钥和公钥证书。
- 用户身份认证可采用 USBKey、静态口令、动态口令、智能卡、人体生物特征等。
- 对标准 SIP 设备的认证,采用数字证书的认证方式。
- 在数据的加密保护方面,针对静态存储文件、传输内容、信令数据定义了可支持的加密算法:DES、3DES、AES(advanced encryption standard,高级加密标准)(128 bit)、RSA(1 024 bit 或 2 048 bit)、安全多用途网际邮件扩充协议(S/MIME)等。
- 对信息的完整性采用数字摘要、数字时间戳及数字水印等技术防止信息的完整性被破坏。数字摘要支持信息摘要 5(MD5)、安全散列算法 1(SHA-1)、安全散列算法 256(SHA-256)等算法。

上述两个标准对业界视频监控数据安全机制的实现有着重要的指导意义,涵盖了监控业界主流解决方案。

4 视频监控信息安全机制的对比

以业界一个典型安全的监控系统厂商为例,通常其会支持多种信息安全方案,包括视频编解码算法支持高等级加密算法;支持传输数据加密,防止恶意登录后的浏览;图像码流包含数字水印,防止替换和篡改;在信息安全传输协议方面通常支持 HTTPS 传输,确保传输安全等。

监控厂商采用哪一种信息安全机制标准,与监控系统的实际应用场景和系统架构有密切关系。

以 ONVIF 规范为例,ONVIF 规范核心聚焦点在于网络视频传送设备与网络视频客户端之间的接口,因此其典型应用场景是:

- 前端监控设备 PU 上线后,向平台 CMU 发送 hello 消息;



- 平台 CMU 需要搜寻设备时,向前端监控设备 PU 发送 probe 消息;
- 平台 CMU 与前端监控设备 PU 进行信令交互,请求能力集,获取配置;
- 客户端 CU 上线,向平台 CMU 注册,建立连接;
- 平台 CMU 与客户端 CU 进行信令交互,传输设备列表;
- 在平台 CMU 的协调下,客户端 CU 同前端监控设备 PU 建立连接传输码流。

由上述场景可见,ONVIF 平台 CMU 的功能在于协调 CU 同前端监控设备 PU 建立连接传输码流,其针对信息安全的研究也主要侧重于系统信息安全认证和获取,包括业务信令数据的安全认证、密钥生成和证书下载功能,为此,ONVIF 定义了用户证书和生成机制,以实现客户端与网络视频产品之间安全的授权访问。

此外,在协议架构方面,ONVIF 是基于 Web Services 协议的,因此其在信息的安全传输方面使用 IEEE 802.1x 验证服务器和 HTTPS 保护机制,以保证信息点到点的安全传输。由于 ONVIF 平台不负责音视频媒体流的转发,是客户端到摄像头点到点直连访问音视频,因此,ONVIF 信息安全标准不涉及音视频媒体数据的加密、完整性保护和传输。

公安部《城市监控报警联网系统标准》行业标准对全国平安城市工程的建设和监控系统相关设备的开发起着规定指导性的作用,需涵盖国内绝大部分安全防范用视频监控系统的技术要求,因此该系列标准针对城市监控报警联网系统,从视频编解码、信息传输和控制、视频的存储和播放、平台系统、卡口监控和比对、设备接入和使用、安全和测试、工程验收等做了较为技术性的详尽要求。

因此,与 ONVIF 规范不提供完全的服务器端证书机构(CA)不同,公安部《城市监控报警联网系统技术标准安全技术要求》定义了基于专门证书认证机构认证体系,定义了3种证书类型(用户证书、设备证书和CA证书),并统一了证书的格式,定义了证书的载体,用户可采用公安部、国家密码管理局等国家有关机构认证通过的硬件加密机(即黑盒子),用于产生、存储和管理密钥和公钥证书。

此外,与 ONVIF 规范侧重于业务信令数据的安全认证不同,《城市监控报警联网系统技术标准安全技术要求》在业务信令数据和音视频媒体数据加密和完整性方面皆定义了可支持的加密算法要求。

5 监控系统采用的主流算法

从具体的加密算法方面,针对信令流和媒体流加密,监控系统一般使用 DES、3DES、AES(128 bit)、RSA(1 024 bit 或 2 048 bit)等加密算法。

DES、3DES 是对称加密算法,即加密和解密使用相同密钥的算法,DES 使用一个 56 bit 的密钥,3DES 使用两个独立密钥对明文运行 DES 算法 3 次,从而得到 112 bit 有效密钥强度;一般监控系统可采用 DES、3DES 算法保证信令流和媒体流的安全性。

AES 为对称加密算法,支持长度为 128 bit、192 bit 和 256 bit 的密钥长度,其中 128 bit 密钥长度的 AES 是最常采用的版本,也是监控系统中采用较多的一种算法。

RSA 是非对称加密算法,是目前最优秀的公钥方案之一,但是 RSA 的缺点是运算代价很高,尤其是速度较慢,较对称密码算法慢几个数量级,因此 RSA 一般用于对 AES 密钥的安全传输。由于 AES 加密算法是公开的,信息的保密依赖于 AES 密钥的保密,因此,对于 AES 密钥的安全传输,可采用 RAS 非对称加密算法。

监控系统中的数据除了通过信令流和媒体流传输外,还有很多静止的数据,如存储的录像文件、音频数据,为保证安全性,同样也需要加密处理,针对录像文件加密的方法有很多,可采用 3DES、AES(128 bit)、SCB2 等。

此外,在监控系统中,为了确保图片和视频数据的安全可靠,监控系统可采用数字摘要、数字时间戳及数字水印等技术防止信息的完整性被破坏。

数字摘要就是采用单项散列函数将需要加密的明文“摘要”成一串固定长度(128 bit)的密文,数字摘要可采用信息摘要 5(MD5)、安全散列算法 1(SHA-1)、安全散列算法 256(SHA-256)等算法。

数字时间戳是用来证明消息的收发时间的,用户首先将需要加时间戳的文件经加密后形成文档,然后将摘要发送到专门提供数字时间戳服务的权威机构,该机构对原摘要加上时间后,进行数字签名,用私钥加密,并发送给原用户。

数字水印技术,即在抓拍照片或视频编码过程中加入隐藏标记,防止该照片或视频在传输、存储、处理过程中被恶意篡改,确保数据的保密性,水印制作方案采用密码学中的加密体系来加强,在水印嵌入、提取时采用一种密钥甚至几种密钥联合使用。

在数据安全传输协议方面,监控系统通常用到 HTTPS、IEEE 802.1x(基于端口的网络接入控制)协议、TLS 协议、SRTP(secure real-time transport protocol,安全实时传输控制协议)。

HTTPS 是监控系统中应用较多的安全传输协议,是由 SSL+HTTP 构建的可进行加密传输、身份认证的网络协议,一般应用于业务数据信令流的加密。

IEEE 802.1x 协议使用标准安全协议(如 RADIUS)提供集中的用户标识、身份验证、动态密钥管理和记账,客户端通过认证获得身份验证,为会话生成唯一密钥,该密钥可用于监控系统消息安全传输。

TLS 协议使得当服务器和客户机进行通信时,确保没有第三方能窃听或盗取信息。TLS 协议包括 TLS 记录协议和 TLS 握手协议;TLS 记录协议可使用如数据加密标准(DES)保证连接安全。TLS 握手协议使服务器和客户机在数据交换之前进行相互鉴定,并协商加密算法和密钥。

视频流在传输层的加密也可使用 SRTP 对传输通道进行加密,SRTP 是在 RTP 基础上所定义的一个协议,旨在为单播和多播应用程序中的实时传输协议的数据提供加密、消息认证、完整性保护和重放保护功能。

6 安全机制的应用建议

通常,一个监控系统应根据加密等级和系统架构的不同采用相应的安全机制。

对于一般的安全监控系统,要求支持业务数据访问权限进行安全认证和授权,实现业务信令流的加密和传输。访问权限的安全认证可采用口令、数字证书或数字摘要等标准算法,信令流的加密算法根据业界标准可采用 DES、3DES、AES(128 bit)等算法,信令流的安全传输可根据监控架构协议采用不同的通信安全协议,如 HTTPS、IEEE 802.1x 等。

对于需要高度安全和保密的系统,不但需要支持信令流的加密,还需要对传输的媒体流进行加密,一般厂商的视频编解码芯片均可支持高等级音视频加密算法,如 DES、3DES、AES(128 bit)等。此外,视频加密可以采用视频关键帧或全数据加密两种方式。关键帧是反映一组镜头中的主要信息内容的一帧图像,由于视频监控系统摄像头一般是固定安装的,其所涉及的场景范围有限,因此,各帧图像冗余信息很多,采用全数据视频流加密耗费芯片资源,加密费用很高,采用关键帧加密可以减少很多工作量。

媒体流和信令流数据的加密,不论采用何种加密算法,均涉及密钥的管理问题。

在不采用专门证书认证机构的认证体系下,监控平台、前端监控设备、监控客户端必须具备采用统一的加解密模块和密钥产生模块的能力,为了调试或其他选择,视频监控平台、监控终端和客户端都必须支持统一的开关,方便开启或关闭命令加密功能。

考虑到视频监控平台可分为多级监控平台,因此不同的监控平台的服务器应该使用不同的密钥,每个监控平台服务器定期随机产生一个密钥,该监控平台服务器下的所有终端设备可以获得该密钥,终端设备使用该密钥对发送出去的数据加密,对接收的数据解密,保障信息在传输过程中的安全性。

视频监控系统之间需要经过信任操作才能互通,一般的信任操作由双方执行,请求方信任受信方,受信方的请求可以被请求方接受。对等地,受信方也要执行信任操作,以监控系统通常采用的 AES 加密为例,其原理如下。

视频监控平台服务器定期随机产生一个 AES 加密/解密密钥,分别使用各个终端或客户端用户密码对 AES 加密密钥进行加密,形成传输密钥发往各个设备,各个设备对传输密钥的内容进行解密,即可获取 AES 加密/解密密钥。在以后的监控过程中,所有设备就可以使用该 AES 加密/解密密钥对信令和媒体码流进行加密和解密。

对于监控系统中静止的数据,如存储的录像文件、音频数据,为保证安全性,需要加密处理,可采用通用的针对录像文件加密的方法,如 3DES、AES(128 bit)、SCB2 等。

为了确保图片和视频数据的安全可靠,监控系统还可采用数字摘要、数字时间戳及数字水印等技术防止信息的完整性被破坏。

7 结束语

综上所述,网络视频监控系统的安全性是个复杂的体系,要保证视频监控的安全运行,还需要考虑多级安全认证机制、关键数据容灾/备份、网络私密保护(VLAN/VPN)、网元自动化运行管理等多种因素。本文针对监控系统中最关键的数据安全,选择监控业界两个代表性标准的信息安全机制进行解读,对主流解决方案进行了对比,分析了监控系统采用的主流算法,最后提出了视频监控的安全机制应用建议。

(收稿日期:2013-08-10)