视频监控系统的安全风险分析及防范对策

李 杰*
杭州海康威视系统技术有限公司 浙江 杭州 310051

摘 要：视频监控系统作为重要的安防组成系统之一，被广泛应用于公共安全的各个领域，其自身的安全问题需要引起关注。本文对视频监控系统的发展和组成进行了阐述，分析了其目前面临的主要安全风险隐患，并对其原因进行了分析，最后针对这些问题提出了相应的防范对策和建议。

关键词：视频监控；安全；风险分析
DOI：https://doi.org/10.37155/2717-5316-0210-25

引言

由于现代科学技术的快速发展，网络视频监控技术应用越来越广，网络视频监控系统所造成的数据安全问题也越发明显。这个数据安全问题也被犯罪分子盯上，其通过视频监控系统来危害家庭、企业和政府，甚至威胁到国家安全。所以，当前最为重要的问题就是提高网络视频监控系统的安全性。现在，人们的安全意识逐渐增强，我们在肯定视频监控系统对社会的安全与进步做出巨大贡献的同时，也要重视它存在的问题，通过综合治理和提早防范等方式，对可能存在的安全风险问题加以控制。

1 网络视频监控系统的组成

1.1 视频前端组成

视频监控前端主要包括网络摄像机、高清云台、视频编码器等前端设备，实现视音频信息的实时采集和压缩编码。

1.2 视频传输组成

视频传输主要包括网络交换机、路由器、防火墙、光端机、网闸等设备，实现视频从前端到本级中心及上下级中心间的网络传输。

1.3 视频中心管理组成

中心管理部署统一的管理平台，主要包括图像中心管理服务器、录像存储服务器、视频回放服务器、设备接入服务器、媒体转发服务器、视频存储系统等集中管理设备，主要实现：（1）视频源接入管理；（2）视频录像、存储、检索、回放以及转发管理；（3）客户端管理；（4）用户身份鉴别、权限管理；（5）日志管理[1]。

1.4 视频应用终端组成

视频应用终端主要包括服务管理终端、监视终端、视频分配器、视频解码器、视频矩阵切换、分布式拼控输入输出、大屏幕等后端显示控制设备，实现视频的监控、投放、录像等功能。

2 网络视频监控系统存在的安全问题

2.1 视频前端设备存在入侵风险

视频前端设备有着全天不间断运行、设备数量多等特点，因用户安全意识薄弱，设置的密码较简单，这使得犯罪分子容易入侵前端设备，也能够通过相关漏洞来盗取高危敏感数据。

2.2 视频传输安全风险

视频摄像机拍摄的视频需要通过网络方式进行传输，由于视频实时性要求高，且传输数量大等多方面因素，很多场所在进行视频传输过程中，未对传输的数据采取必要的加密措施，这就造成了安全隐患。传输线路极易遭到犯罪分子的接入攻击，可能对传输的视频信息进行截取、解码，从而造成监控系统内的数据信息泄露。

*通讯作者：李杰，1982年，男，汉族，浙江宁波，杭州海康威视系统技术有限公司，硕士研究生，研究方向：智慧城市、应急指挥、雪亮工程，主要从事大项目规划设计。

2.3 视频存储安全风险

监控系统的视频图像主流的方法多是采用AVI、MP4等标准格式进行存储在硬盘上，数据量大，一般难以对所有视频数据都进行加密存储。非法人员可以通过非法入侵监控系统，访问硬盘获取存储数据，造成存储的数据信息面临泄露的安全风险，甚至黑客还可能通过技术手段，替换掉硬盘中的存储数据，对存储数据进行干扰和破坏[2]。

2.4 应用软件和数据容易遭受攻击

随着大数据时代的到来，视频监控的功能不再局限于还原现场事件发生情况这么简单，视频监控的价值更侧重于数据深度挖掘和软件应用，而这也使得安防应用软件和视频监控数据成为了不法分子的首选目标。我们在通过大数据来检索实用信息的同时，有些敏感数据很容易被不法分子利用。来自内部的网络攻击风险同样不可忽视，假如内部网络存在计算机病毒或木马等恶意程序就有可能造成内部视频监控网络直接与外界建立联系，从而导致视频监控和敏感信息的泄露。

2.5 运维监管安全风险

视频监控系统最终需要人来执行运维和监管过程。在安装运维过程中，通过建设单位派施工人员来进行安装和运行维护，尤其是一些具有保密性质的单位，如果不法分子利用施工人员的身份在系统建设过程中，直接在系统内部安装恶意软件，窃取视频监控数据信息，将会造成重大的信息泄露事故。而在系统运行和监控过程中，如果运维管理不到位，操作人员不熟悉各项操作，就不能及时发现问题及解决问题，也将给安全监管带来风险[3]。

3 网络视频监控系统安全问题的原因分析

网络视频监控系统一旦大规模部署，其安全风险会立刻显现，针对上述情况，分析其原因，主要含以下三方面内容：（1）网络摄像机及系统独特的安全威胁，公众和行业的认知程度偏低，有待进一步提高。（2）传统网络与信息安全领域缺乏针对性强的安全设备和解决方案，只能部分涵盖智能视频监控设备，无法满足其在隐私保护方面的独特需求。（3）自身资源受限，网络视频监控系统其计算、存储和网络传输受到限制，为了避免自身功能受影响，通常不会部署花费代价较高的专用安全防护技术和设备。

4 网络视频监控系统安全防护建议

4.1 对承建单位及人员进行资质条件审核

重要场所，尤其是涉密场所内的视频监控系统，需要对承建单位和建设人员进行资质条件审核，签订保密承诺协议。尤其在视频监控涉及到的保密要害区域，安全防护等级需要调整至最高级别，必要条件下，应该内部人员经培训上岗后，代替建设单位的操作人员完成建设。在建设施工过程中，需要本单位人员全程跟踪监管，系统安装部署完成之后，需要经安全部门专业人员进行检测合格后，方能投入使用[4]。

4.2 对资产进行分析与统计

首先对网络视频监控系统进行资产分析与统计，掌握视频前端、网络传输、后端平台等各类资产的组成与分布情况，然后使用专用的漏洞扫描工具检测资产存在的漏洞，并对安全漏洞进行加固，定期升级设备固件、更新并增强密码强度，同时加强前后端设备的统一安全认证机制。

4.3 终端应用的安全防护措施

从终端安全管控、恶意代码防护、数据防泄密等多个方面进行防护，主要技术手段有安全配置、漏洞修复、补丁升级、病毒清除等。同时，还可采用数字签名、字符叠加水印等技术手段，对终端视频图像数据进行标记，并在系统平台记录图像调用和录像下载的日志，万一出现数据泄露，即可通过有关标记，对终端视频图像数据追踪溯源。

4.4 网络边界的安全防护措施

在纵向边界的防护上，可配备防火墙、网闸等安全设备或其他安全技术手段，防止来自上下级网络间的非法访问。在横向边界的防护上，可通过防火墙、网闸等安全边界设备实现视频监控系统平台之间的互联互通。保密要求高的视频监控系统还应采用单向传输的模式，做到数据“只进不出”，防止数据泄露。

4.5 数据中心的安全防护措施

可从网络基础安全和主机安全等方面进行防护。其中网络基础安全防护主要有准入控制、访问控制、入侵防范等

防范措施；主机安全防护主要是加强物理环境和系统运行环境的安全防护能力，如防盗窃、防破坏、恶意代码防护等措施。

4.6 加强系统日志审计

建立日志审计系统，收集操作系统、数据库和应用软件的日志，及时响应并分析系统安全事件，实现系统安全运行管理，集中分析以发现潜在的攻击和入侵行为，做好相应部署。

4.7 安全监控措施

对监控系统应用安全进行7X24h监控，特别是要重点关注木马监测、篡改监测、可用性监测、关键字监测等，主动发现应用系统的安全隐患，及时发现出现的安全事件，及时响应和处理。

4.8 系统安全管理的安全防护措施

视频监控系统安全中最重要的安全元素：管理安全。技术上再成熟、防护再安全的系统，如果操作者和使用者不能很好的管理和操作，系统的安全性是无法保证的，当前安防行业内出现的安全事件的很大一部分原因就是用户使用操作错误或不当操作造成的，相关人员安全培训不到位也是一方面。要做好安全制度措施，根据网络视频监控系统信息安全总体规划，编制并维护信息安全相关的制度、流程、预案和作业指南，定期组织信息安全方面的测试与应急演练。另外系统管理员要养成良好的安全习惯，形成规范的安全操作流程，在设备软件版本更新之后及漏洞补丁发布之后及时升级安防系统软件。

5 结束语

总之，网络视频监控被大范围的应用到了社会各行业当中，在网络技术不断发展的今天，安防监控领域所推进的将是整个行业的进步，但在发展的同时，也要对视频监控的安全风险进行防范。相信在不久的将来，网络视频监控技术将获得更加广泛的应用和发展，为用户提供更加可靠、安全的服务

参考文献：

[1]张晓琳.视频监控产业发展之现状挑战及展望[J].中国安防,2020,(8):24-27.

[2]陶槊,魏海利.视频监控系统数据安全风险的技术解决[J].池州学院学报,2020,(3):49-51.

[3]杜庆灵.平安城市视频监控系统网络安全研究[J].科技与创新,2019.

[4]于胜.电力系统视频监控网络信息安全风险及GB 35114实施意义[J].自动化系统技术及应用,2019.

[5]吴欣欣,王鹏程.计算机网络安全中虚拟网络技术的应用研究[J].计算机产品与流通,2020(1):37.