Computer Science and Application 计算机科学与应用, 2023, 13(10), 1817-1823
Published Online October 2023 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2023.1310180

Hans汉斯

视频监控存在风险隐患及防护对策研究

戈西伟[1]，白　玲[2]，陈宝海[1]，朱　琳[1]，霍爱国[1]

[1]中国人民解放军63726部队，宁夏 银川
[2]中国人民解放军32032部队，北京

收稿日期：2023年9月6日；录用日期：2023年10月5日；发布日期：2023年10月13日

摘　要

近年来，视频网络监控的发展越来越广泛，网络设施也在不断升级，从目前信息化发展的趋势来看，网络监控系统的结构和配置都发生了巨大的变化，结合某单位营区视频监控系统的安全需求和使用需求，对整个系统安全风险进行分析，制定各阶段安全管控点的安全防控措施，形成“事前检测 + 事中防护 + 事后追溯”的全生命周期视频监控信息安全防护。

关键词

视频监控，风险隐患，安全防护

Research on Risks and Hidden Dangers in Video Surveillance and Protective Measures

Xiwei Ge[1], Ling Bai[2], Baohai Chen[1], Lin Zhu[1], Aiguo Huo[1]

[1]Chinese People’s Liberation Army 63726 Unit, Yinchuan Ningxia
[2]Chinese People’s Liberation Army 32032 Unit, Beijing

Received: Sep. 6th, 2023; accepted: Oct. 5th, 2023; published: Oct. 13th, 2023

Abstract

In recent years, the development of video network monitoring has become increasingly widespread, and network facilities are constantly upgrading. From the current trend of information technology development, the structure and configuration of network monitoring systems have undergone significant changes. Based on the security and usage requirements of a certain unit's

文章引用: 戈西伟, 白玲, 陈宝海, 朱琳, 霍爱国. 视频监控存在风险隐患及防护对策研究[J]. 计算机科学与应用, 2023, 13(10): 1817-1823. DOI: 10.12677/csa.2023.1310180

camp video monitoring system, the entire system security risk is analyzed, and security prevention and control measures for each stage of security control points are formulated, Form a full lifecycle video surveillance information security protection system that includes "pre detection, in-process protection, and post traceability".

Keywords

Video Monitoring, Risk Hazards, Safety Protection

1. 引言

高清网络视频监控设备，在近几年快速扩张使用的趋势下，是一个很重要发展阶段，从标清到高清的跨越，实现了视频监控从“看得见”到“看得清”的转变[1]。也正是高清视频监控的分辨率在不断提高，信息化项目的大力推进，视频监控数据存储量日益大幅增加，在海量信息数据存储下导致自身的安全问题也越来越多。第一，视频监控内容更广泛、信息数据更敏感，容易吸引黑客的注意，视频监控数据一旦被攻击，严重影响部队营区的安全，甚至造成国家重大的经济损失和政治影响，对于黑客来说在攻击过程中获得数据越多，黑客的效率就越高，得到的诉求就越大[2]。第二，视频监控系统是部队营区安防系统的重要组成部分，虽然视频监控系统在系统安全设计、建设、维护等方面的使用上相对稳定可靠，但从安防领域高度来看，黑客活动仍然日趋频繁，WEB 应用攻击、网站攻击、互联网恶意软件呈大幅增长态势，专业人士对视频监控系统的安全意识还比较薄弱，信息安全整体还面临严峻挑战[3]。

2. 视频监控现状

安防监控技术是保证营区周边、重要场所等安全的重要技防手段，线路敷设点多线长，覆盖面及其宽广，营区内部、营区门口、营区周边、营区外道路等，安装设备较为多样，有监控摄像头、人脸识别机、车辆识别等设备，为确保信息数据存储的安全，在存储手段上不会使用云存储(互联网)，主要存储手段为 NVR、硬盘录像机等硬件设备，在网络传输上主要有内部局域网、涉密信息网等，网络的延伸到营区门口、周边路口、重要仓库、重点要害部位等场所，摄像机的使用类型上多为智能数字型网络摄像机，效果清晰，智能数据准确。高清、智能、多维，是当下安全防范技术的主流，我们可以更准确的提取到所需要的信息。Smart 265 编码技术、目标结构化算法、车牌识别算法、人脸识别算法、视频检索引擎、多传感器融合等技术已全部应用到智慧营区中，覆盖点位多、面积广、功能全、算法新，在方便工作的同时也带来了诸多的安全隐患[3]。图 1 所示视频监控使用需求示意图。

3. 视频监控存在的风险隐患

现在的高清摄像头都是基于 IP 网络进行传输，前端模块也是网络模块，网络容易被黑客攻击，而且摄像头是全天 24 小时工作，多数摄像头的安装位置远离营区、有的远离监控值班室、还有有的存在监控盲区，监控值班人员不能 24 小时实时监控所有监控画面，更不能全面及时的掌握设备运行情况，这样就给黑客攻击带来了可乘之机。

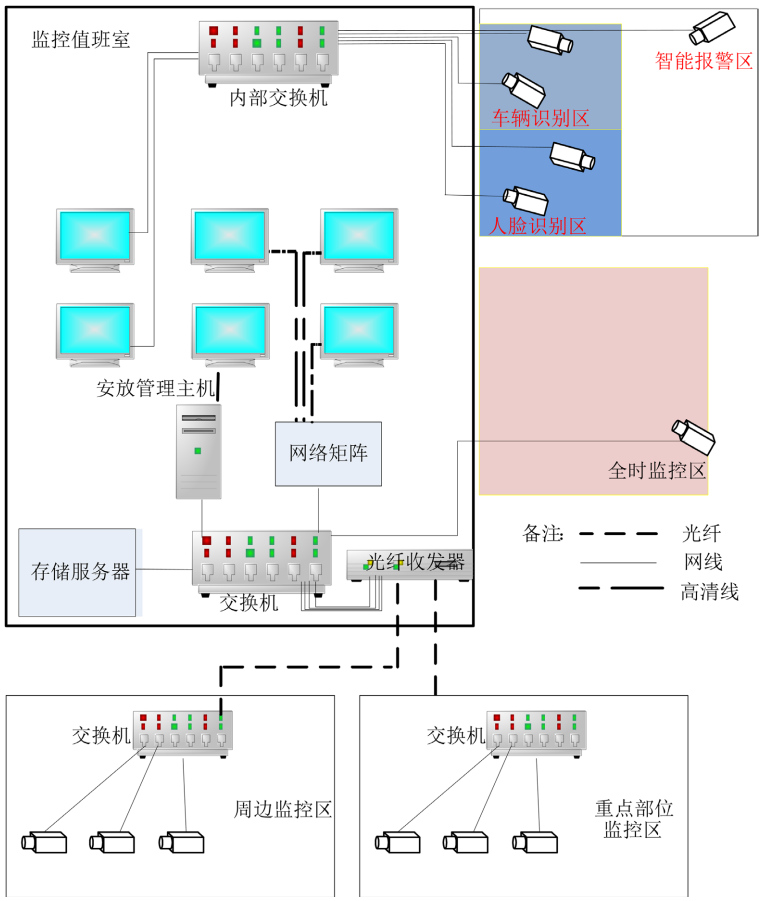

Figure 1. Schematic diagram of video surveillance usage requirements
图 1. 视频监控使用需求示意图

3.1. 视频监控前端存在的隐患

目前摄像头前端采用的都是网络模块传输数据，使用起开方便、接入灵活，数据采集是全天候 24 小时，但是采集装置在传输中存在多方面的安全隐患，现在使用的传输系统没有相应的安全管控，这也成为网络传输中存在的薄弱环节。

摄像头前端视频采集的安全风险主要有以下方面影响：1) 网络摄像头是传统摄像头的升级版，设备硬件和网络技术由内置的硬件平台、内置的 Linux 系统和内置的 web 服务组件组成。USB 接口主要用于摄像头收集图像和安装 WiFi 无线网卡，网络摄像头可能缺少密码、缓冲区溢出、未经授权的访问、拒绝服务命令注入等功能，无线网卡可以连接手机、笔记本等设备来控制摄像头，这样就造成安全风险[4]。图 2 海康摄像头内部组件界面。

2) 通过共有的网络接口收集设备信息和数据信息，网络摄像头的端口基本一致，但是海康摄像头端口相对固定，如 554 端口用于远程控制客户端，浏览器访问端口 80 和 8000 等可以远程登录控制、操作参数等，攻击者可以通过端口扫描、IP 地址搜索软件等方式，可以快速发现在网络中激活、运行的设备信息，黑客就可以通过笔记本等外联设备对服务器进行远程访问、攻击、破坏。如果攻击者成功破解网络摄像头的前端设备后，轰击着就可以对控制中心的所有设备轻松的掌控操作，顺利的获取监控中心的敏感信息，甚至可以被用作入侵和攻击网络的跳板，进行信息数据的收集的系统木马病毒的植入等操作[4]。图 3 海康前端摄像头默认端口。

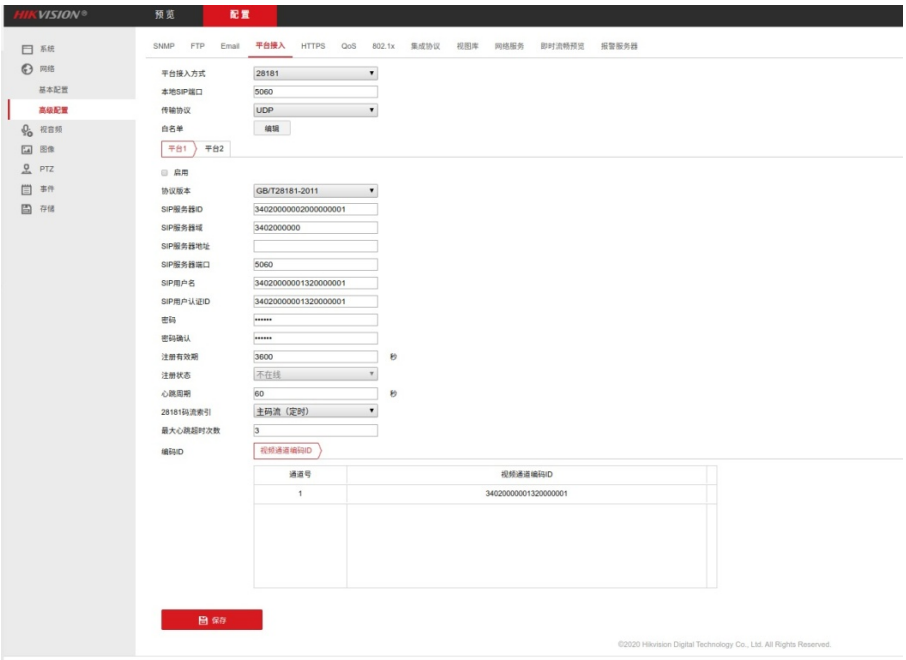

Figure 2. Internal component interface of Hikvision camera
图 2. 海康摄像头内部组件界面

Figure 3. Default ports for Hikvision front end cameras
图 3. 海康前端摄像头默认端口

3.2. 监控中心模块存在安全风险

监控中心模块是网络视频监控系统的核心，主要有图像监控设备、存储服务器等，具有视频回放、设备访问、网络传输、视频存储等功能，监控中心存储许多易受入侵的重要数据，控制设备的权限、设置入侵漏洞等设备信息。1) 摄像头前端和后端的视频数据采集后，监控中心仅用于简单的权限识别和管理，没有集中的存储机房，或者存储设备放置随意，且没有专门的加密设备和安全认证机制提供的设备或者通过安检合格的设备，客户端和用户的数据信息，不能完全保证最终数据信息的合法性，不能及时阻止非法访客的入侵攻击[5]；2) 监控中心管理平台在出厂时就缺乏安全性，导致用户名和密码默认存储在数据库中，能够让系统管理员以外的人员可以轻松地窃取、访问包含管理员用户名和密码的数据库。造成随意访问系统或者进行非法操作，比如，黑客提高用户的权限；对远程控制视频采集设备的接口控

制，策略的加固等相关信息和参数修改；3) 网络服务器的视频监控管理员不具备安全意识，通常使用相同的用户名，比如用户名 admin，便于维护人员管理管理，密码通常是原始设备密码或非常简单的密码，或者添加设备时使用存储激活密码，如 123456、888888 等，没有做到存储设备与监控设备密码分离，在添加设备时与存储激活密码一致，密码过于简单，而且没有做到 3 个月更新一次密码，造成密码泄露扩散，这些都是安全风险存在的隐患。

4. 视频监控系统安全防护措施

当前视频监控系统主要存在前端设备、终端设备、网络传输、操作系统、设备应用、数据存储、安全管理等方面的安全风险，目前的防护设备主要有入侵检测、防火墙、终端防病毒等，不能满足日益增长的巨大风险隐患，特别是针对部队营区视频监控系统，随着信息化建设的不断升级，网系之间的融合，光纤入户等问题凸显[6]。针对现有问题及时建立基于安全态势感知的主动安全防御系统，通过现在的智慧图像人工智能整合技术，形成正向的安全闭环保护，在视频监控事件发生前后，形成有效的信息安全管理措施。一是对视频监控系统中的资产进行实时检测和统计，及时掌握前端设备、中心管理、后端设备等资产的组成底数和分布使用情况，利用有效的漏洞扫描工具检测资产漏洞，定期更新设备密码，通过特殊符号 + 大小写字母 + 数字方式增加密码强度。二是通过部署安全网关、应用防火墙、终端杀毒软件、单项网闸等安全防护设备，从主机层、网络层、应用层、数据层，形成 7 * 24 小时综合保护态势，确保设备运行、网络传输、数据加密保护的安全性。

4.1. 设备入网前安全检测

通过专业的监测设备进行安全检测，主要是摄像头前端各类感知设备，包括监控摄像机组件、报警探测器组件、环境感知组件、门禁机设备等，所有的组件、设备要根据安全管理要求，对场景进行部署安装，在部署安装前对设备组件的嵌入式系统、WEB 端口的应用漏洞进行重点检测，通过数据结果分析被测系统存在隐患，统计出详实的检测结果，及时发现监控系统 WEB 应用所存在的安全隐患，针对检测结果和存在的安全隐患制定相应的补救措施和安全建议。

在入网使用前对终端设备进行全面的病毒查杀，包括存储服务器、硬盘录像机、监控终端等设备，在操作系统上安装最新杀毒软件，进行全面的病毒查杀和漏洞扫描工作，及时发现病毒文件和系统漏洞，做好全面的有效处理，确实让系统运行安全、设备运行稳定，为安防系统提供智能、稳定、有效的信息数据来源。

4.2. 数据传输中的安全防护

4.2.1. 防火墙技术

在服务器的出入口处安装网络防火墙，做好端口的限制策略防护，在确保信息网络抗攻击能力的同时，加强对基础网络的安全控制和数据监控，有效提升基础网络的安全性，从而为上层应用提供安全的运行环境。防火墙的应用可以最大限度的保障网络正常运行，主要提高网络的安全性、强化网络的安全策略、防止信息泄露，同时具有信息认证、抗网络攻击、IP/MAC 地址绑定等功能，有效防止陌生地址攻击有效数据，保证访问的权限。图 4 IP/MAC 地址绑定。

4.2.2. 单项网闸技术

单项网闸技术是安全隔离与信息单向访问导入的集成，采用模块化设计，单项网闸可以设置连接信任及不可信网络，对访问请求进行预处理，以实现安全应用数据的剥离。能够对当前设备系统信息与状态进行监控，能够监控 UDP 单播任务、UDP 组播任务、自定义协议过滤、带宽配额任务等，可根据配

置的策略及时对业务数据放行、拦截，并可通过日志记录的方式向管理员提出警示，可以对非法 IP 的访问提供详细的记录，防止 IP 盗用，实现信息数据单项访问策略配置，如有攻击者系统会实时向管理员发出报警信息并对攻击者进行拦截，保证信息数据的安全。图 5 网闸功能界面。

Figure 4. IP/MAC address binding
图 4. IP/MAC 地址绑定

Figure 5. Gateway function interface
图 5. 网闸功能界面

4.3. 事后事件追溯

通过运维审计系统实现对所有的前端设备、终端设备、网络设备、安全设备、应用系统的操作行为全面的记录，包括登录时 IP、登录用户、登录时间、操作命令等内容实行全方位的审计，审计后的结果可以对设备日志、操作系统日志、应用系统日志进行全面的查看分析判断，有效的对各种安全威胁、异常行为事件进行处理，确实提高信息数据的安全[6]。

5. 结束语

部队营区是一个特殊的环境，网络视频监控系统在部队的使用中逐渐占据重要地位，它具有系统规模大、部署分散、承载网接入和内容敏感等特点，为了保护国家的财产安全及部队内部的人身、信息的

安全，建设一套智能化的监控系统是非常必要的，按照高标准的安全防范系统设计建设一套应用实际需求服务，而且在技术上要有一定的前瞻性和可扩展性，确保在一定时间内不会落后，还得考虑到数字化特性，在使用方便的同时更要做好网络的规划和信息传输安全策略防护，保证信息数据传输的安全。

参考文献

[1] 高万河. 网络视频监控系统的现状及发展趋势[J]. 信息与电脑(理论版), 2017, 375(5): 178-179.

[2] 陶槊, 王晓芳, 陈滨. 视频监控系统安全传输复合加密算法设计[J]. 安庆师范大学学报(自然科学版), 2021, 27(2): 37-43.

[3] 官清珍. 视频监控技术的概述与发展[J]. 中国安防, 2010(1): 51-54.

[4] 孔晓东. 智能视频监控技术研究[D]: [博士学位论文]. 上海: 上海交通大学, 2008: 3.

[5] 朱秀昌. 视频监控技术的智能化趋势[J]. 中兴通讯技术, 2010, 16(6): 32-34.

[6] 甄伟. 谈数字化综合安防系统的构建[J]. 科技资讯, 2011(20): 70-71, 99.