工程技术发展
第 3 卷◆第 7 期◆版本 1.0◆2022 年
文章类型：论文 | 刊号（ISSN）：2737-4505(P) / 2737-4513(O)
Engineering Technology Development

针对摄像头网络安全的自动化防护系统

高 健 汤 昕 谷丽蕊
山东高速股份有限公司 山东 济南 250014
DOI:10.12238/etd.v3i7.6014

【摘 要】：近些年，伴随着“智慧小区”“数字城市建设”“新型智慧城市”等多地信息化理论的陆续明确提出，视频监控在安防监控系统、智慧交通、新型智慧城市、智能生活等应用领域越来越广泛。但是，在视频监控系统软件朝着数字化、智能化系统、全面覆盖方位迅速演变的前提下，已有的视频监控机器设备和系统广泛欠缺网络空间安全防护的制度，视频监控系统软件这个全新的基础设施、最大的物联网的应用系统软件，正面临复杂多变的网络和信息安全风险。
【关键词】：摄像头；网络安全；自动化防护
中图分类号：TN915 文献标识码：A

Automatic Protection System for Camera Network Security

Jian Gao, Xin Tang, Lirui Gu
Shandong Expressway Co., Ltd., Shandong Jinan 250014

Abstract: In recent years, along with the "smart community", "digital city construction", "new smart city" and other information theory has been clearly put forward, video surveillance in the security monitoring system, smart traffic, new smart city, smart life and other applications are more and more widely. However, in the video monitoring system software toward digital, intelligent system, comprehensive coverage orientation under the premise of rapid evolution, because of the existing video monitoring equipment and system widely lack of cyberspace security protection system, video monitoring system software, a new infrastructure, one of the biggest application of Internet system software, is facing complex network and information security risks.
Keywords: Camera; Network security; Automatic protection

为了保证视频监控安全性，减少摄像头的网络安全风险和处理维护里的难点痛点，对于摄像头实时、合理、智能化的安全管理十分有必要。文中明确提出对于摄像头现阶段存有的关键风险性搭建安全防范的自动化技术，完成摄像头网络信息安全自动化技术安全防护和安全风险评估，及其资产明细动态化维护。实践活动结果显示，选用该方案可以有效降低摄像头的网络安全风险，实现智能化的安全管理。

1 智慧城市中物联网摄像头的安全现状

伴随着视频监控平台上的订单量大幅度扩展，摄像头机器设备的总数呈指数型增长，但是因为摄像头数量众多且变化大、布署部位普遍、接入方式多种多样、设备型号繁杂等因素，维护面临很大的压力和挑战。互联网侧安全加固工作中全凭人力收集配置扫描仪评定、资产明细靠人力维护，欠缺即时、高效率、自动化监管方式，易导致疏忽、安全风险评估时间长，风险性对话框大，导致对视频监控摄像头的黑客攻击司空见惯，容易造成网络信息安全信息泄漏事情。因而，安全防护系统的高效、方便快捷运维管理是牵制视频监控系统软件预防措施长期性充分发挥的重要因素。

2 摄像头的主要风险

根据目前的维护和攻击情况来看，摄像头目前存在的安全隐患主要有以下 3 个方面：

（1）弱口令。很多客户在设置动态口令时一般仅包括简易数字和字母，密码长度低于 8 位，比如“123”“abc”等，一般很容易被猜测到或者被破解器破译，从而使得客户的终端设备遭遇风险性。但日常维护环节中，为了满足维护便捷不时之需，摄像头的用户名密码能被设为弱口令，或直接沿用厂家的初始密码。网络攻击可以用词典扫描仪和暴力破解密码方法，对 user、admin、root 等各种且简短登录密码开展暴力行为攻克。这些人在获取密码后，运用远程登录协议书 Telnet （Telecommunications Network）、SSH（Secure Shell）或 WEB（World Wide Web）网页页面，获得设备控制管理权限，导致个人隐私泄露。国家互联网应急中心在市场份额排名前列摄像头产品中任意挑选了两个品牌，开展弱口令系统漏洞遍布盲测，结论检测到十几万个弱口令系统漏洞。可以这么说，动态口令是摄像头安全防范的第一道和最直观的预防措施。弱口令变成伤害摄像头安全性口号安全隐患。

（2）端口号暴露面。暴露于网络攻击视野范围内，能够被利用开展侵略的软件、机器设备、信息等，都是属于暴露面。网络攻击一般会让摄像头的协议和端口开展扫描仪，

获得机器设备开摆的端口号和协议书，从这当中探寻已经知道或是不明系统漏洞进行攻击威胁。一部分系统漏洞能够达到远程操作效果，获得控制系统的管理权限，进而执行安全性毁坏，导致个人隐私泄露。如摄像头常见的 HTTP（Hyper Text Transfer Protocol）、HTTPS（Hyper Text Transfer Protocol over SecureSocket Layer）和 RSTP（rapid spanning Tree Protocol）协议书，常见端口号为 80、443、554 等，存有的系统漏洞种类包含指令引入、授权、信息泄漏、跨站脚本攻击、弱口令、文件操作、XSS（Cross Site Scripting）、拒绝服务攻击、文件目录赋值、固定件系统漏洞等。

（3）资产明细不清楚风险性。视频监控在各行各业得到了广泛的应用，机器设备总数呈指数型增长，设备厂家和型号规格也越来越多了。然而由于开发周期长、改造环节多、维护不深层次、管理方法不感兴趣、工作交接不全面、档案资料有丢失、具体内容不健全等因素，导致资产明细没法完全的正确地体现现实中资产状况，还对维护造成了巨大的工作压力。目前靠人力方法维护资产明细的形式，已无法令人满意目前维护要求，造成资产明细动态化维护难以达到。

因而，搞好弱口令和端口号暴露面动态化智能管控，完成资产明细的自动化技术动态性维护，是提高视频监控服务平台摄像头机器设备安全系数最直观、最有效预防措施。

3 摄像头安全防护自动化系统

3.1 构建思路

因为 Python 语言的表达简约、可读性及其扩展性等特点，所以可以根据 python 搭建一个轻量的摄像头机器设备安全防范自动化技术，完成视频监控服务平台摄像头即时、动态变化安全风险评估，及其互联网侧自动化被动安全下达，并通过漏扫采集到的信息，进行摄像头资产的自动办理备案，完成资产明细的自动化技术动态性维护。

（1）采集模块：通过与视频监控平台开发接口，秒级采集注册到平台的摄像头清单，写入数据库。

（2）分析模块：通过对比，输出新注册到平台的摄像头清单，包括非新增摄像头但 IP（Internet Protocol）地址发生变更的部分，并对漏扫模块和加固模块下发任务。

（3）漏扫模块：接收来自分析模块的漏扫任务，主要有全量和增量两类任务。全量漏扫以月为周期，对注册到平台的全景摄像头进行安全评估。增量是对平台新增的注册摄像头进行安全评估，摄像一注册到平台，立即自动触发任务，将采集到的设备信息，写入数据库，完成资产备案，完善资产信息。

（4）自动配置模块：接收来自分析模块的加固配置下发任务，调用接口，完成配置下发。

3.2 具体实现

3.2.1 实时自动化漏扫模块

根据 python 语言开发插口，连接视频监控服务平台，实时采集视频监控软件上已注册的摄像头的 IP 地址信息。对信息进行梳理研究分析，将全新上线的摄像头 IP 地址根据插口输送到安全性漏扫服务平台，全自动开启漏洞扫描系统、弱口令检查等网络信息安全评定每日任务（可以进行周期时间设定，适用秒级、min 级、钟头级、天、月），并回到摄像头型号规格等信息载入数据库系统，进行刚注册的摄像头信息的完善和资产办理备案。完成摄像头发布、安全风险评估、资产办理备案的实时、自动化技术同步，减少风险性对话框，处理资产明细动态性维护的一大难题。

3.2.2 安全配置自动下发模块

通过优化视频监控平台和摄像头中间报文及流媒体播放的互动制度，完成摄像头的降到最低浏览，随后产生固定不动统一的访问策略，启用传输网接口实现自动部署下达。

流媒体播放浏览体制提升：服务平台布署直播服务器，流媒体视频网络服务器接受摄像头的视频采集之后再派发至客户手机客户端或是派发至网络存储器开展视频存储。摄像头不用和用户手机客户端及其服务平台其他作用服务器进行互动，仅需与接入服务器和直播服务器进行报文和流媒体服务器的互动，完成了摄像头由一对多（面对各大网站客户）向一对一（只面对服务平台）的改变，进而压力降了摄像头的网络暴露面。

3.3 人脸检测、编码与识别

人脸检验、编号和检测算法都是基于提升后 Dlib 库达到的。在优化算法选择时，选用较为成熟且精确度相对较高的 HOG 优化算法来进行检验。HOG 算法的流程为：（1）归一色调。因为求得方位梯度不用五颜六色图片，因而应用灰度值图片就可以，而且为了能尽可能变大图片特性，在色调归一化以后应进行一次校准。图片预备处理的办法已经在图像预处理一部分表明，这里就不多说了；（2）梯度计算。针对归一化后图片开展梯度测算，即找出图片的发暗的程度与方位，就获得了梯度以及梯度方位；（3）对凌乱的梯度值开展规范化，也就是把一个区域以中心为起点划分成好几个地区，将每个小地区里的梯度空间向量规范化，那样就把每个小地区里的梯度向量化为了能 9 个矩阵的特征值（bin）；（4）运用滑窗（block），再将上述小地区里的矩阵的特征值开展规范化，就获得了初始图片的 HOG 特征图。将这一特征图与很多人脸数据提取出来的 HOG 特征图进行比较，就可以找出人脸。在图像预处理一部分，大家提及了图像的变小，因此找到属于自己的的人脸数据信息相较于原图像里

的人脸也刚好相距了减少的占比，所以我们然后将所找到人脸坐标乘于对应的占比，就能在原有源图像标明人脸。

4 结语

近年来随着的不断发展，视频监控系统的信息化应用范畴越来越广泛，为各行各业带来了更多的驱动力和机遇。作为服务供应商，在不懈追求更优质、更智能的视频监控系统作用完成的前提下，也同样需要高度重视它所产生的潜在性安全隐患。但日常维护中，通常高度重视服务平台侧的安全防护，而忽略终端设备侧摄像头安全性。摄像头作为视频监控系统不可或缺的一部分，数量多且布署分散化，安全性布署难度系数较大，但一切系统优化并不是靠点射安全性能够确保的，一定要保证整个系统的安全性。依靠程序化交易的力量，针对目前维护难题和攻击状况，打造了摄像头网络信息安全自动化技术防御系统，完成摄像头即时、动态变化安全风险评估，及其互联网侧自动化被动安全下达，并通过漏扫采集到的信息内容，进行资产清单的自动化技术动态性维护，在缓解维护工作压力、提高维护质量的同时，大幅提升了摄像头的安全性和稳定性。

参考文献：

[1]焦伟.电力调度自动化网络安全防护系统的研究与实现[D].华北电力大学,2014.

[2]陈婧雯.电力调度自动化安全防护问题分析[J].科技传播,2013.

[3]张华,张振华.路灯电缆防盗报警系统设计应用[J].供用电.2009,(5).

[4]茹纯亮,双正文,吕霞付.高速公路电缆防盗报警系统信号检测方法的研究[J].电子测试,2008,(12).