基于指纹技术的专网资产互联网暴露面探测手段的研究

曾　杰，史裕饶，王　晨

（天津市公安局交通警察总队科技和设施保障支队，天津 300220）

摘　要　本文基于物联网最新的技术，针对安全监管需求，参考国家网络安全法律法规、政策要求、等保2.0网络安全建设标准以及公安部对专网的建设要求，从“底数清、情况明、能处置”等维度，利用专有终端（摄像头、红绿灯、电子眼）指纹识别技术、网络空间资产主动探测技术、网络空间资产被动探测技术、电子警务系统专项识别技术，构建了一套集控管于一体的设备专网资产互联网暴露面探测方法，结合网络空间资源测绘方法，识别专网资产暴露风险。

关键词　指纹技术；专网资产；互联网暴露面；网络空间资源

中图分类号：TP393.03　　**文献标识码**：A　　**文章编号**：1007-0745(2023)03-0028-03

在信息技术和互联网高速发展的今天，云计算、大数据、移动互联、物联网已深入我国各个行业每一个角落。

天津交管设备专网是基于物联网及传统IT网络架构的公共交通安全业务管理专网。交通管理监控、违章抓拍、交通信号控制等业务系统均利用此专网，随着纳入的设备越来越多，专网得到了快速的发展，海量数据实现了网络上的交换和使用。但与此同时，网络空间安全形势日益严峻，如何确保专网资产不暴露在互联网上，减少暴露面，进而更有效、更有针对性地进行安全防护已提上日程。

本文研究利用专有终端（摄像头、红绿灯、电子眼）指纹识别技术、网络空间资产主动探测技术、网络空间资产被动探测技术、电子警务系统专项识别技术，构建了一套集控管于一体的设备专网资产互联网暴露面探测方法，结合网络空间资源测绘方法，识别专网资产暴露风险，以此来提升设备专网边界的完整性。

1 国内外研究现状和发展趋势

网络空间资源测绘是资产互联网暴露面探测的技术核心支撑，主要对网络空间中的各类资源及其属性进行探测、融合分析和绘制。

1.1 国外研究现状

代表性工作包括美国国防部高级研究计划局的“X计划”、美国国土安全部的“SHINE计划”、美国国家安全局的“藏宝图计划”。

1.1.1 2013年DARPA制定X计划

允许美国军方作战人员规划网络战，允许他们根据各类关键性网络“地形”进行作战规划，具体包括邮件与文件服务器、路由器及网关等需要着重防御的网络组成要素，同时以出色的可视化效果审视各关键性网络地形要素的活动、运行情况及状态。[1]

1.1.2 SHINE计划

项目名称为SHINE（SHodan INtelligence Extraction），负责单位为DHS下属ICS-CERT（工业控制系统应急小组），参与人员为Bob Radvanovsky & Jake Brodsky（Shodan两位开发者），起止时间为2008年中期-2014年1月31日，关注点为美国本土关键基础设施相关设备网络可达及安全态势。成果是将46万联网设备（截止到2012.12，到2014年共发现219万联网设备）降低到7200个。本项目涉及技术包括网络空间资产主动探测技术、网络空间资产被动探测技术、工业系统设备指纹识别技术以及SCADA蜜网的开发。

1.1.3 藏宝图计划

藏宝图计划的目标是要识别互联网地图上的任何时间、任何地点的任何设备。藏宝图计划由NSA和CSS（中央安全局）两个部门共同负责，共同合作成立NTOC（威胁作战中心），由NSA负责维护运行，搜集全球互联网情报，用于建立态势感知能力。[2]

1.2 国内研究现状和发展趋势

目前，在网络空间可视化领域，依旧处于起步阶段，

对于监管单位，对其辖管的资产暴露面缺乏完善的自动化检测及分析，仅通过梳理互联网出口很难真实、清晰地反映互联网暴露面风险。

在传统的网络安全业务上，统计、分析等工作多是以文本、图表等方式进行查询与显示。但随着物联网时代的来临，IOT 设备被越来越多地应用于当前的信息采集建设中，由此带来了更大的资产监管挑战，采集的数据信息量大、种类繁多、表现形式复杂，在网络空间与地理空间上缺乏直观的映射关系，难以直观地找到暴露的出口，需要一种手段，全面地提供信息支持。

我国学者提出，通过网络空间可视化表达，提供资源、产权、监管、司法等涉网国内经济、政治、文化、法治的基础和保障，也是国家治理体系和治理能力现代化在网络空间中进行建设和实施的基本要素和重要保障 [3]。

目前在我国网络安全领域，有部分平台提供了网络空间资产的基础探测能力，基于专用的测绘引擎，zoomeye 可以提供全球 42 亿 IP 地址的网络空间资产发现能力 [4]，hunter 可以提供超 5 亿 IP 数，65 亿资产总数 [5]，因此具备利用现有基础扩充对专网互联网暴露面测绘分析的基础。

2 技术路线

在为保障业务系统的正常运行，经过多年的建设，天津市公安交通管理局建设了一张纯物理专网，通过设备的专网专用，陆续建设了道路违法停车、高点监控、鹰眼监控、黄标车违法抓拍、各类电子警察等一系列智能交通设施，在网络安全层面，也率先引入链路即安全的运营理念，为交管业务开展提供了坚实的网络环境保障。

但在整体建设中，各区接入网络的建设情况不尽相同，引入了包括 MV 链路、MSTP 链路等多种专线的接入形式，还有部分点位存在 4/5G 接入的情况，同时各区承建的运营商单位，在对于各自建设的接入网络的管理上，较纯物理专网而言，在配置管理及网络路由管理上有更大的暴露风险，因此需要采取本文中的解决思路，进行统一监管。

针对安全监管需求，参考国家网络安全法律法规、政策要求、等保 2.0 网络安全建设标准以及公安部对专网的建设要求，从“底数清、情况明、能处置”等维度，采用网络空间资产主动探测技术、网络空间资产被动探测技术以及网络空间资产指纹识别技术，设计一套符合专网网络的互联网暴露面监测的基于指纹技术的专网资产互联网暴露面探测手段。

3 基于指纹技术的专网资产互联网暴露面探测手段设计

天津市公安交通管理局的业务系统中应用了监控资产、信号灯资产、违停抓拍等物联网资产模块，由于在建设的最初设计中，专网环境不应存在互联网出口，因此无法采用 IP 地址的监控手段，对交管专网中的资产进行互联网暴露面分析，针对该组网模型的特点，设计基于指纹技术的专网资产互联网暴露面探测方法。该方法将采用网络空间资产主动探测技术、网络空间资产被动探测技术以及资产指纹识别技术，实现对天津市公安交通管理局专网设备指纹识别和互联网暴露面分析，避免出现因建设过程中出现的专网资产异常暴露在互联网上的情况，切实保障专网的封闭网络环境。

3.1 网络空间资产主动探测技术

网络空间资产主动探测技术是通过主动向目标网络资产发送构造的数据包 [6]，并从返回数据包的相关信息（包括各层协议内容、包重传时间等）中提取目标信息，来实现对开放端口及服务等网络资产信息的主动探测。

3.2 网络空间资产被动探测技术

网络空间资产被动探测技术是通过网络旁路侦听的方式 [7]，被动采集目标网络的流量，对流量中的数据包中的相关字段 IP、端口号、协议号等内容进行分析，从而实现对网络资产信息的被动探测采集。

3.3 网络资产指纹识别技术

网络资产指纹识别技术凭借网络资产探测的主动扫描探测技术和被动流量分析技术，得到目标指纹，与系统内置的资产特征指纹库对比，完成网络资产的匹配，确定资产指纹信息。资产识别结果的准确性由指纹特征提取与匹配的精确度决定，指纹特征由对大量资产指纹进行相同内容提取，特有内容区分，以确定资产信息与特征的对应关系，以组成资产特征指纹库。目标指纹达成匹配条件则可获得相应资产组件的设备类型，组件名称，厂商信息、型号版本等数据。

3.4 判定资产符合性技术

通过网络空间主动探测技术和被动探测技术，获取设备专网中目标指纹，对指纹按内容差异进行大致分类，提取同类指纹之间相同内容，提取可确定资产

组件的关键字，例如服务器字段、标题字段、UA字段、厂商、cookie等；区分关键字内差异内容，例如型号、版本信息等；有序组合相关关键字，组成完整特征，实现与资产的唯一对应关系。

3.4.1 定制的入库操作

将特征相关信息进行完善补充，如服务类型、设备类型、主机信息及其他额外信息。将天津市公安交通管理局设备专网网络资产指纹对应特征为基础建立匹配库，服务于专有终端（摄像头、红绿灯、电子眼）等。

3.4.2 org上的查找流程

利用搜索工具进行专网资产指纹信息查找。选择查询类型，如组件名、设备类型、专有服务、关键字等；输入对应查询内容；选择多个查询条件间的查询逻辑。

3.5 基于指纹技术的专网资产互联网暴露面探测应用

针对专网资产进行对应指纹的定向开发，建立设备专网网络资产指纹特征匹配库。通过网络空间主动探测技术和被动探测技术，获取天津市公安交通管理局设备专网中专有设备信息，将探测获取的资产信息与设备网络资产指纹特征匹配库进行匹配，从而得到天津市公安交通管理局设备专网专有设备的指纹信息。该指纹信息包括设备操作系统、设备信息、厂商信息、IP地址、端口、服务组件等资产数据。当通过互联网上的探测节点，结合指纹信息可以在全网中收集到的资产库进行匹对，如果发现存在指纹相同的资产，即可说明，某个专网的接入侧节点存在异常，可能存在互联网暴露风险，结合IP地理位置信息，可以进行准确的通报，结合人工的手段，将该风险进行排查整改。

4 应用实践

获得指纹：

1. 根据专网的专用ip库，通过网络空间主动探测技术和被动探测技术，匹配系统内资产特征指纹库获得目标指纹。

2. 根据已匹配出的资产设备类型与指纹本身内容差异进行大致分类，提取同类指纹之间相同内容，寻找可确定资产组件的关键字。

以某品牌电警设备为例，通过交互流量抓取，结合页面爬取，获取到对应品牌的强关联信息，也就是设备的指纹信息：

（1）指纹：Apache。

（2）指纹：XXX XXX httpd。

（3）指纹：XXX IP XXX httpd。

3. 截取指纹内关键字部分，进一步对比，确定差异内容。

4. 编写特征指纹，补充资产组件相关信息。

通过分析，共获取一组指纹信息，确定三个指纹规则。

5. 用特征指纹构成专网专用资产指纹特征库，利用专用ip库进行测试，测算识别率，确保指纹提取正确性。

根据指纹特征，在互联网上，通过指纹信息进行空间资产检索，典型操作如下：

（1）在搜索框中输入专网资产指纹信息，并进行搜索。

（2）在发现存在该类型资产后，进行下钻，通过相关其开放的服务和端口，评估其暴露在互联网上后，可能对专网造成的影响。

（3）通过组件可能存在的漏洞，判断是否有漏洞被利用的风险。

（4）通过高精地理位置信息，确认其资产归属地，推送至相关单位进行整改。

通过相关信息的整理分析，可以实现针对暴露在互联网上的资产进行梳理，为优化专网的安全使用环境提供信息情报指引，从互联网监测层面找到专网的暴露风险，丰富专网安全监测运维手段，避免专网中存在未知的互联网边界出口，形成入侵的脆弱点，确保专网专用，降低因大规模建设过程中的人为因素导致专网设备异常暴露在互联网上的异常事件发生。

参考文献：

[1] 黄维真，何荷．“X计划”：美军网络作战路线图[J]. 环球军事，2013(19):23-25.

[2] 杨望，杨燕婷（整理）. 从美国网空系统看中国高校安全[J]. 中国教育网络，2019(02):24-25.

[3] 郭启全，高春东，郝蒙蒙，等．发展网络空间可视化技术支撑网络安全综合防控体系建设[J]. 中国科学院院刊，2020,35(07):917-924.

[4] 知道创宇：ZoomEye网络空间雷达系统[DB/OL].https://www.knownsec.com/#/product/zoomeye.

[5] 奇安信：网络空间测绘平台[DB/OL].https://hunter.qianxin.com/home/helpCenter?r=1-2.

[6] 王宸东，郭渊博，甄帅辉，等．网络资产探测技术研究[J]. 计算机科学，2018(12):24-31.

[7] 同[6].