医院网络安全态势感知系统构建

莫禹钧 潘愈嘉 黄 捷

（贵港市人民医院 贵港 537100）

〔摘要〕 建立网络安全态势感知系统，从业务逻辑、基础检测、深度监测、报表与日志管理等方面分析系统需求，从威胁情报、流量传感器和安全感知平台 3 个模块介绍系统构建，阐述系统功能与应用效果，指出其应用有助于防止医院因网络攻击造成的严重损失。

〔关键词〕 “互联网 + 医疗”；医院信息网络安全；态势感知系统

〔中图分类号〕R - 056 〔文献标识码〕A 〔DOI〕10. 3969/j. issn. 1673 - 6036. 2018. 12. 006

Building of the Situationl Perception System for Hospital Network Security *MO Yunjun, PAN Yujia, HUANG Jie, Guigang City People's Hospital, Guigang 537100, China*

〔**Abstract**〕 The perception system for network security situation has been built. The paper analyzes system requirements from the aspects like service logic, basic detection, and management of reports and logs, introduces system building from the three modules like threat intelligence, traffic sensor and security perception platform, expounds upon system functions and application effects, as well as points out that the application is conducive to the prevention of serious loss caused to hospitals by network attack.

〔**Keywords**〕 "Internet + medical"; hospital information network security; situational perception system

1 引言

近年来网络攻击入侵频频发生，影响着各个企业网络安全[1]，医院也经常面临来自互联网的攻击威胁。贵港市人民医院已部署安全设备和软件，但仍有部分攻击绕过防护进入医院内部，对重要数据或资产造成威胁[2]。传统安全防御体系中的设备遍布 2 ~ 7 层，应用层设备主要是入侵检测系统（Intrusion Detection System，IDS），入侵防御系统（Intrusion Prevention System，IPS）和审计[3]。IDS、IPS 主要原理是依靠已知特征、行为的模式匹配来对攻击行为进行检测[4]，所以对基于未知漏洞、恶意代码等未知行为的攻击无法检测。而利用黑白名单、签名和规则来发现安全威胁的传统安全防御体系无法应对不断发展的网络威胁和信息环境。因此亟需一种可以应对未知威胁的技术来快速准确地发现网络攻击入侵痕迹，及时解除威胁。网络安全态势感知系统可以使安全管理员及时找到潜伏在网络中的安全攻击威胁，能够在早期快速发现恶意攻击行为，精确定位受害目标和攻击源头，可以使入侵途径和攻击者背景进行研究判断以及溯源[5]，从源头上发现医院网络中的安全隐患，尽可能地减少安全攻击威胁对医院造成的损失。

2 系统需求

2.1 业务逻辑

支持自动识别医院网络中主机的内网和外网网

〔修回日期〕 2018 - 09 - 10

〔作者简介〕 莫禹钧，工程师，发表论文 6 篇。

段；根据流量内容自动识别医院网络网段 IP 是终端还是服务器。自动识别非法资产并根据流量探测出非法资产的操作系统、开放端口等基础信息；自动识别合法服务器并通过流量分析识别出合法服务器开放的服务、端口和端口传输的协议和应用等。持续检测业务资产存在的风险，及时发现业务漏洞和安全隐患。能够自动识别所有访问关系并归类访问请求属于正常、风险还是违规访问等。

2.2 基础检测

支持 IP 碎片重组、传输控制协议（Transmission Control Protocol，TCP）流重组、应用层协议识别与解析；有多种入侵攻击监测模式和统一资源定位地址（Uniform Resourse Locator，URL）监测模式。通过模式匹配生成事件，可提取 URL 和域名记录在特征事件触发时利用源 IP 地址、源端口、目的 IP 地址，目的端口和传输层协议录制原始报文。能够进行异常会话检测，对外联行为分析、间歇会话连接、加密通道分析、异常域名分析、上下行流量分析等的多场景网络异常通信行为进行分析检测。Web 应用安全检测，针对浏览器/服务器（Browser/Server，B/S）架构应用，范围包括 PHP、ASP、JSP 等脚本语言编写的 WebShell 后门脚本上传，检测结构化查询语言（Structured Query Language，SQL）注入、跨站脚本攻击（Cross Site Scripting，XSS）、系统命令注入、跨站点请求伪造（Cross Site Request Forgery，CSRF）攻击、恶意爬虫攻击以及文件包含、目录遍历、信息泄露等攻击。敏感数据泄密检测，可对敏感信息自定义，通过文件类型和敏感关键字对信息过滤和检测。

2.3 深度检测

支持以会话级视图展示网络流量，利用网络流量的正常行为特性建立正常流量模型，判断流量是否出现异常，通过网络水平、网络垂直、IP 地址及端口扫描实现网络蠕虫、IP 协议异常报文、TCP 异常报文和地址解析协议（Address Resdution Protocol，ARP）欺骗检测等。可进行黑链、口令暴力破解、弱密码扫描及终端病毒和恶意软件检测、新爆发的高危漏洞进行检测。

2.4 威胁情报关联

通过流量采集设备采集医院网络中的原始流量，结合云端的威胁情报库，评估安全事件的可信度、威胁度和风险值。通过大数据关联分析发现医院网络中的失陷主机、安全威胁，识别业务潜在安全风险和高级持续性威胁行为（Advanced Persistent Threat，APT）。支持有效攻击和被利用漏洞检测，进而对攻击进行溯源，利用图关联分析，将攻击者的 IP、域、病毒、黑客工具、攻击手段、黑客位置、历史攻击记录等所有信息关联起来，还原呈现整个攻击场景，形成攻击事件。

2.5 流量记录、报表与日志管理

支持还原和记录医院网络中的通信行为，供安全管理员取证分析，还原内容包括 TCP 会话记录、Web 访问记录、SQL 访问记录、域名服务（Domain Name Service，DNS）解析记录、文件传输行为、轻型目录访问协议（Lightweight Directory Access Protocol，LDAP）登录行为等。可提供 Word 或 PDF 格式文档报表形式的可视化风险报告；通过 Syslog 服务接收和存储第 3 方设备的日志并提供详细的字段搜索功能。

3 系统构建

3.1 概述

医院内网和外网在逻辑上进行隔离，网关分别部署在不同的核心交换机上。构建安全态势感知系统，系统接入拓扑，见图 1。流量传感器以旁路方式接入核心交换机，分别在内网和外网核心交换机上建立镜像组，流量传感器所接端口是镜像组的目的端口，而核心交换机下联汇聚交换机的端口全部作为镜像组的源端口，这样实施不用中断网络，既不影响各个业务科室的用户，也不影响现有的网络结构，即使设备或系统出现异常也不会影响医院网络和系统，防止产生单点故障。而安全态势感知平台则通过网络双绞线与流量传感器直接相连，接收

流量传感器传输的流量信息，同时接入外网交换机连接互联网，获取云端的威胁情报。

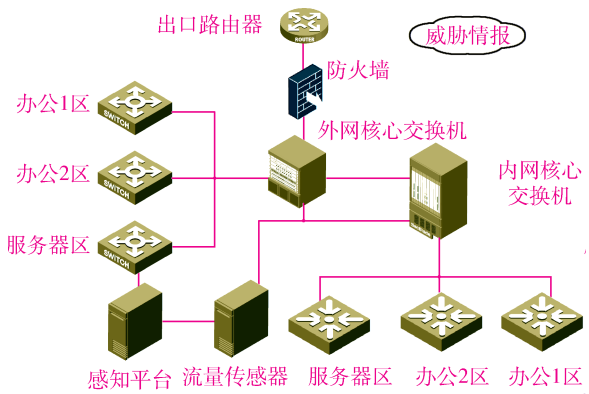

图 1 安全感知系统接入拓扑

3.2 威胁情报

该模块是来自互联网大数据的分析成果，可以对新型木马、APT 攻击、特种免杀木马等未知威胁进行规则化描述。主要是利用人工智能自我学习的自动化数据处理技术进行精细分析以确认攻击源手段、攻击对象及目的，通过多维度信息融合实现基于攻击场景的事件关联、交叉关联和启发式关联，从而评估攻击事件的可信度、威胁度和风险值，找出攻击源的原型，包括实现形态、编码风格等。通过特征找到攻击源，最终确保准确发现未知威胁并形成云端威胁情报库，供安全感知平台系统使用。

3.3 流量传感器

获得医院网络链路中数据的复制信息，主要作用是监听、检测医院网络中的数据流及用户或服务器的网络行为，同时采集 TCP 行为。流量传感器利用医院网络流量镜像识别内部用户和业务资产、业务的访问关系，根据获取到的网络流量对医院网络初步识别攻击、异常行为和检测违规行为。

3.4 安全态势感知平台

负责存储流量传感器传输的流量日志和告警日志，安全感知平台不但能快速处理分析所有数据并提供检索支持，还可以将本地数据的日志和威胁情报结合并进行关联性分析以产生告警信息，对其中的攻击源攻击受害主机的整个过程进行还原并提供界面展示，也能以文档形式导出。总的来说安全态势感知平台负责存储所有流量数据并进行预处理和提供检索。

4 系统功能

4.1 可视化展示全网资产和访问关系

系统主动识别并通过列表展示全院网络业务资产，发现新增资产，同时将资产的开放端口、可登录的 Web 后台等基础信息在界面展示；图形可视化展示全院网络业务对象的访问关系，包括用户对业务、业务对业务、业务与互联网 3 者关系的完全展示及搜索功能。展示当前业务所有的访问关系，标明是否违规、被攻击、被登录、对外攻击等，给失陷、高危、低危等不同等级的访问源和访问目的使用不同的颜色标识。展示用户访问业务、使用应用、协议和端口，判断这些访问是否属于攻击、违规、远程登录等行为。医院安全管理员可轻松识别出网络中的访问关系已对哪些业务造成影响，也可判断当前用户或资产是否已经失陷或可疑。

4.2 风险告警和分析

系统自动判断业务系统或资产是否已被攻击，通过邮件告警等方式向医院安全管理员告知重要安全事件。将目标系统或资产发起和遭受的攻击、异常活动整合成安全事件，使安全管理员直观了解到目标主机正在进行或遭受的攻击。通过攻击链来展示主机被入侵后发起的威胁活动情况，直观展示被入侵后的主机是否被利用、产生威胁以及威胁程度是否逐步升级等。

4.3 全局视角风险态势感知

系统结合失陷主机、安全事件、业务资产脆弱性等方面综合分析，对全院网络的安全态势进行整体评价，帮助医院安全管理员掌握网络整体安全态势并辅助进行安全决策分析，将所有风险业务、风险用户及其安全事件、举证、风险和建议以 Word 或 PDF 文档形式导出，形成详细报告供安全管理员审阅并采取相应措施。同时还可将可视化风险报告以 PDF 报表

形式对全院网络的安全情况进行评估，展示并说明网络中存在的风险业务、风险用户、攻击、后门等问题，方便领导了解全院网络总体安全情况。

5 应用效果

一般情况下如果大量终端未同时出现症状，医院管理员很难发现内网中存在的攻击，如基于“永恒之蓝”漏洞发展的变种病毒，目前变种形式已经越来越多，有些只是潜伏在内网中，不会造成大规模明显的不良反应，不易被发现。而通过安全态势感知系统能很容易地发现网络中各种攻击，了解具体攻击程度，使医院系统在未出现大规模中毒之前将病毒提前清理掉。在构建安全态势感知系统后，经过对一段时间的流量采集分析，平台发出一些告警，遍布 3 个阶段：尝试入侵但未成功、入侵成功和入侵成功后将终端变成僵尸主机，告警类型包括网络漏洞、网络攻击、黑市工具、僵尸网络、流氓推广、网络蠕虫和木马等。每个告警详细记录攻击事件的过程、程度和目前状态并展示攻击原理，提出处理建议等。其中发现最严重的是基于“永恒之蓝”漏洞的变种病毒，已经有数 10 台终端失陷，沦为僵尸主机，严重威胁医院网络安全。根据处理建议采取一系列针对性措施，包括在防火墙上限制外来攻击者 IP 访问、及时更新相关补丁、对内网的僵尸主机进行逐一查杀等。安全态势感知系统使医院安全管理员能够更有针对性地实现精准预防及查杀，主动发现网络中存在的威胁，及时采取相应措施，有助于防止医院因病毒攻击造成的严重损失。

6 结语

安全态势感知系统满足新等保 2.0 对网络攻击检测和分析要求，特别是针对未知的新型网络攻击和 APT 攻击。网络安全态势感知系统的构建标志着医院从被动防护向主动防御的转变，医院不再以防范为中心，更加强调检测与响应。下一步将通过感知系统与下一代防火墙、杀毒软件等安全设备和软件的联动实现整个主动式体系，为建设完整的主动式防御体系奠定坚实基础。

参考文献

1 刘剑，苏璞睿，杨珉，等. 软件与网络安全研究综述［J］. 软件学报，2018，29（1）：42－68.
2 徐影. 面向大型企业信息安全建设的虚拟化威胁感知技术［J］. 电信科学，2016，32（12）：149－156.
3 张杰. 基于云模型的半监督聚类入侵防御技术研究［D］. 镇江：江苏科技大学，2014.
4 刁振军. 融合 Snort 和代理的网络异常检测与防御系统研究［J］. 电子设计工程，2018，26（1）：43－47.
5 王龙海. 面向武警总队信息网的安全态势感知研究［D］. 北京：国防科学技术大学，2011.

（上接第 24 页）

参考文献

1 杨杰，周小四，沈利. 家庭远程医疗监护报警和咨询智能系统［J］. 高技术通讯，2012，12（6）：1－6.
2 金纯，蒋小宇，罗祖秋. ZigBee 与蓝牙的分析与比较［J］. 信息技术与标准化，2014（6）：17－20.
3 赵泽，崔莉. 一种基于无线传感器网络的远程医疗监护系统［J］. 信息与控制，2006，35（2）：265－269.
4 杨顺，章毅，陶康. 基于 ZigBee 和以太网的无线网关设计［J］. 计算机系统应用，2010，19（1）：194－197.
5 石道生，任毅，罗惠谦. 基于 Zigbee 技术的远程医疗监护系统设计与实现［J］. 武汉理工大学学报，2008，30（3）：396－397.
6 潘巨龙，李善平，吴震东. 基于无线传感器网络的社区保健检测系统［J］. 中国计量学院学报，2007，6（18）：136－140.
7 陈荷燕. 无线远程生理参数传输系统研究［D］. 南京：南京航空航天大学，2006：12－16.
8 许剑，卢建刚. 多参数无线医疗监护系统的设计与开发［J］. 中国医疗器械杂志，2005，29（6）：406－409.
9 李迎春，朱诗兵，陈刚. 无线传感器网络体系结构研究［J］. 山西电子技术，2009，18（4）：71－73.
10 齐妍妍. 脉搏信号去噪及特征提取方法的研究［D］. 北京：北京工业大学，2012：25－26.