基于 nDPI 的轻量级入侵检测与防御系统的设计与实现

韦 小 刚

(南瑞集团有限公司(国网电力科学研究院有限公司) 江苏 南京 210003)

摘 要 移动互联给人们带来便利的同时,也引入了许多安全风险。针对特定业务的安全防护,因为业务协议单一,业务访问量不大,流量分析及非法协议识别等技术手段可有效检测出网络攻击。采用主流的网络抓包手段,基于 nDPI 深度报检测技术,设计并实现轻量级的入侵检测与防御系统。测试结果表明,该系统可以通过流量检测出异常协议,并追溯到相应终端,从而进行异常终端响应处置,阻断从终端发起的异常连接,从而达到入侵防御的目的。

关键词 入侵检测 入侵防御 流量分析 协议识别

中图分类号 TP393.08 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2019.08.053

DESIGN AND IMPLEMENTATION OF LIGHTWEIGHT INTRUSION DETECTION AND PREVENTION SYSTEM BASED ON NDPI

Wei Xiaogang

(*NARI Group Corporation/State Grid Electric Power Research Institute, Nanjing 210003, Jiangsu, China*)

Abstract While mobile Internet brings convenience to people, it also introduces many security risks. For security protection of specific business, the technical means such as traffic analysis and illegal protocol identification can effectively detect network attacks, because of the simple business protocol and small business access. This paper proposed a lightweight intrusion detection and prevention method, based on nDPI, adopting common network packet capture means for design and implementation of a lightweight intrusion detection and prevention system. The test results show that the system can detect the abnormal protocol through the traffic and trace back to the corresponding terminal, so as to handle the abnormal terminal response and block the abnormal connection initiated from the terminal, thereby achieving the purpose of intrusion prevention.

Keywords Intrusion detection Intrusion prevention Traffic analysis Protocol identification

0 引 言

随着移动信息化技术的广泛应用,移动终端的数量在快速增长,各类移动应用层出不穷,为人们的生产、生活各方面提供了许多便利。但是,提供便利的同时,移动信息化也带来了不少安全风险,如非法终端接入至内网的风险,攻击者利用合法终端对内网系统开展网络攻击。网络攻击的形式多种多样,有 DoS 攻击及端口扫描攻击,这种攻击会导致服务拒绝响应或者服务响应延迟较大,在网络数据传输上表现出来的是流量异常或流量过大。因此,通过对网络流量的分析,开展入侵检测及防御工作,可以有效管理网络环境[1-2],对移动信息化业务的安全运行至关重要。

目前,接入到内网的电力移动业务的流量及协议比较单一,这与网络协议繁多、复杂的移动互联网业务有本质不同。针对这种情况,本文提出一种轻量级的入侵检测与防御方法,基于网络深度数据包检测(network Deep Packet Inspection,nDPI)技术对网络流量进行分析,识别网络协议,分辨出接入到内网的电力移动业务在运行时的异常网络协议,在此基础上,对有异常网络协议的连接进行网络重定向。下面对这套轻量级

收稿日期:2018-12-01。国家电网总部科技资助项目(SGGR0000XTJS1800079)。**韦小刚**,高工,主研领域:电力系统信息网络安全。

的入侵检测与防御系统进行详细的阐述。

1 系统设计

1.1 软件流程设计

本文设计的轻量级入侵检测与防御系统主要由网络流量捕获模块、协议识别引擎、响应处置模块组成，基本软件流程图如图 1 所示。

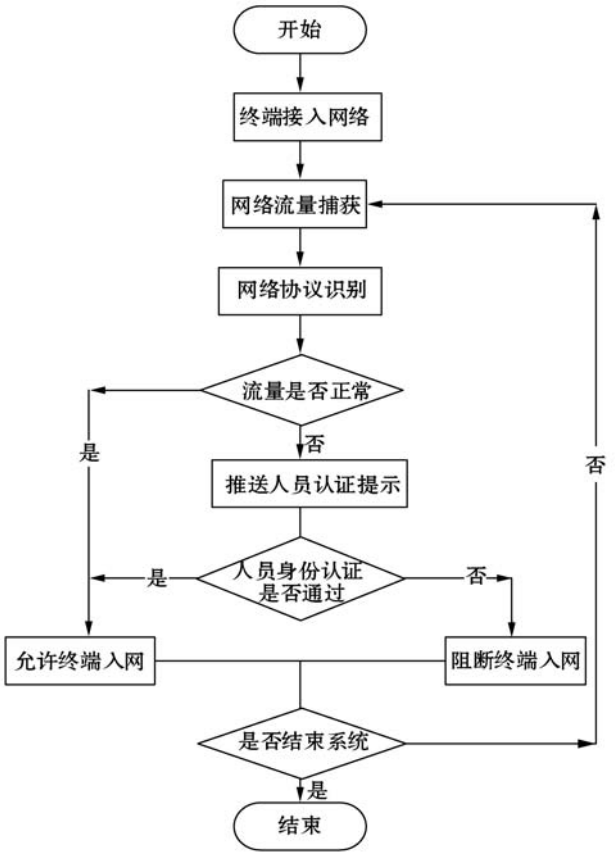

图 1 轻量级入侵检测及防御系统的基本软件流程

网络流量捕获模块是对终端接入网络后产生的流量按照一定的规则进行捕获；协议分析引擎是对捕获到的网络流量进行协议分析，根据既定的协议，可以分辨出业务运行过程中的异常协议，对于协议单一、流程简单的业务来说，这种方式尤为有效；响应处置模块是针对有异常协议的网络流量进行操作，根据认证结果决定是否允许终端入网。

1.2 部署架构设计

系统的部署架构如图 2 所示。各类终端，如 PC 机、笔记本、平板电脑、手机等通过无线网络（如运营商网络或自建 WIFI 网络）访问部署在内网的应用服务器，中间需要经过接入路由器、应用防火墙、接入交换机等多种网络设备。由于无线网络自身存在大量的安全隐患，为了保证内网资源不被攻击者破坏或嗅探，需要对终端访问过程中经过的网络流量进行检测，对检测到的异常进行告警及处置。通过交换机的端口镜像功能把进入应用服务器的流量镜像到入侵检测与防御系统的一个空闲端口供入侵检测与防御系统分析有无异常。

与一般的入侵防御系统串接在关键网络路径上不同的是，本文设计的入侵检测与防御系统采取旁路工作，这样不仅不影响终端访问应用服务器时的数据转发性能，还能避免因为自身的软件缺陷造成网络节点故障，从而直接导致终端无法正常访问应用服务器。此外，认证服务器也是采取旁路工作，接在交换机上，跟入侵检测与防御系统及终端保持网络上贯通。

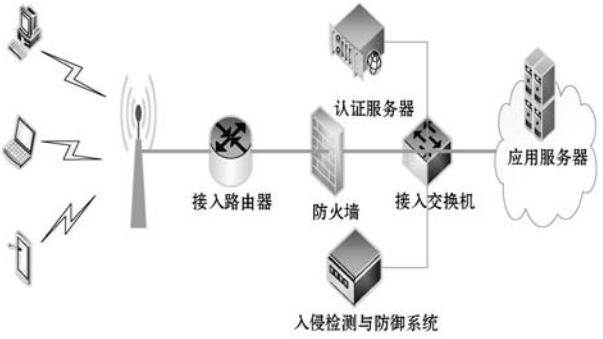

图 2 整体部署架构

2 系统实现

2.1 网络流量捕获模块实现

对网络流量捕获是开展流量监测工作的前提[3-5]，流量捕获的方式很多，本文采用 Linux 系统上 libpcap 库。libpcap（Packet Capture Library）即数据包捕获函数库，是 Unix/Linux 平台下的网络数据包捕获函数库，它是一个独立于系统的用户层包捕获的 API 接口，为底层网络监测提供了一个可移植的框架，Linux 上抓包工具 tcpdump 即基于 libpcap 开发而成。下面是本文对于 libpcap 的使用过程：

（1）*获取网络接口* 确定入侵检测与防御系统上需要监听的网络接口，该接口可以指定或由 libpcap 自动选择，具体函数为 pcap_lookupdev( )。

（2）*打开网络接口* 确定需要监听的网络接口后，需要对该接口进行初始化，具体函数为 pcap_open_live。

（3）*获取数据包* 打开网络接口后就已经开始监听，这是 libpcap 使用过程中的核心部分，可采用函数 pcap_dispatch 来完成获取数据包的任务。

（4）*释放网络接口* 这个功能是在操作完网络接口后对接口进行释放，具体函数为 pcap_close。

2.2 网络协议识别引擎实现

捕获网络流量的目的是进行网络协议识别，分辨

出异常协议,便于后续响应处置,本文基于 nDPI 技术实现网络异常协议识别。nDPI 是由 ntop 维护的一个 openDPI[6-7]的扩展库,从 OpenDPI 发展而来,解决了 OpenDPI 的诸多问题,并具备相当完善的应用层协议识别功能[8-9],几乎成为 DPI 领域的唯一之选。本次系统对 nDPI 源码进行二次开发,针对电力特定的业务,增加可识别到的协议类型,对异常协议进行告警,并通知后续的响应处置模块对产生异常协议的连接及时处理,具体过程如下:

(1) *初始化协议识别引擎*　调用 ndpi_init_detection_module()初始化协议识别引擎的检测模块。

(2) *设置需要识别的协议*　调用 ndpi_protocol_detection_bitmask2()设置协议的掩码,调用 ndpi_load_protocols_file()加载协议文件,通过协议文件指定具体识别哪些协议。

(3) *识别协议*　调用 ndpi_detection_process_packet()可以获得报文的具体信息,包括协议流、报文的详细信息等数据。业务运行过程中,系统根据指定的协议进行协议匹配,无法完成匹配的则为异常协议。针对异常协议,可追溯到具体的终端,从而便于后续的响应处理。

(4) *统计分析*　系统对业务运行过程中识别到的协议进行统计,并对异常协议的处理进行可视化展示。

2.3　响应处置模块实现

对于发起异常协议的终端(PC 机、笔记本、平板电脑、手机等)的系统响应处置如图 3 所示。终端向应用服务器发起访问请求后,本文设计的入侵检测与防御系统通过网络流量捕获模块获取到网络上的流量并进行监测。通过协议识别引擎检测到异常协议后,追溯该异常协议所发起的终端,并向该终端发起网络重定向报文,将终端的访问重定向至认证服务器。认证服务器受到终端发起的请求后,则推送认证提示,只有通过认证的终端才被允许接入网络,认证通不过则被阻断。

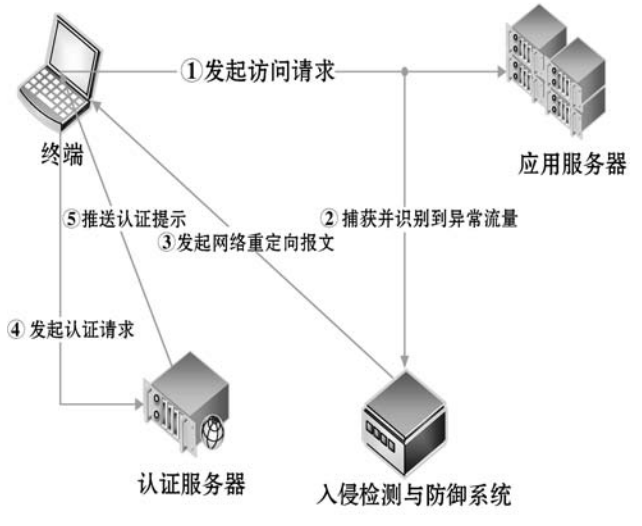

图 3　响应处置流程示意图

3　系统测试

设置协议文件时,可指定具体的网络协议及端口,也可指定协议中包含的 IP 地址,甚至是可指定具体的网站名,系统可以采用字符串匹配的方式识别出相应协议。图 4 为系统检测后的统计分析结果之一,其中 HTTP 和 ICMP 为协议文件中指定的协议,13.9% 是协议文件中未指定的协议,进一步分析后,最终有13.5% 的流量被系统认为协议异常,将会进行后续的响应处置。在实际的电力业务运行过程中,协议类型单一,通过本文设计的系统比较容易区分出与业务无关的其他协议,承载这些无关协议的流量将会被网络重定向,以便进一步检查终端使用人员是否有攻击行为。

图 4　初步统计分析结果

4　结　语

本文考虑到现有入侵检测系统及防御系统实施部署的复杂性,面向电力业务的实际运行特点,对入侵检测及防御功能合二为一,提出了一种轻量级的入侵检测与防御系统的设计、实现方案,并给出了运行测试结果,系统经过权威检测机构检测误报率及漏报率均为 0%,现场试点过程中的运行稳定。本系统的设计与实现对网络流量监测、协议分析及异常终端的响应处置等都有较高的参考价值。

参　考　文　献

[1] 周杨. 协议分析技术在入侵检测系统中的应用[J]. 计算机系统应用,2011,20(6):161-164.

[2] 袁春蕾,欧阳志友,王垄. 基于 nDPI 的流量监控分析实验平台研究[J]. 实验技术与管理,2015,32(3):97-100.

[3] 龚俭,王卓然,苏琪. 面向网络安全事件的入侵检测与取证分析[J]. 华中科技大学学报(自然科学版),2016,44(11):30-33.

[4] 张宇. 企业信息网网络入侵检测系统设计与实现[D]. 成都:电子科技大学,2018.

[5] 宋晓燕. 网络应用层流量监控系统的研究与设计[D]. 西安:西安科技大学,2016.

(下转第 333 页)

电极利用率、提高液滴操作的并行处理和减小生化实验完成时间的影响能力越高,比如,在 3 min 时限内,用 TS 在 10×10、11×11 和 12×12 芯片完成生化实验的时间分别比 TS* 减少了 10.58%、7.12% 和 4.19%。

5 结　语

本文利用功能模块的动态重构特性,在某个操作执行的过程中,适时改变其绑定的功能模块在片上的位置,增大液滴操作的并行处理,同时结合改进的禁忌搜索算法来实现功能模块的动态移位以及数字微流控生化检验的架构级调度和几何级布局,以达到提高电极利用率,最小化生化检验完成时间的目的。通过人体体液体外诊断实验的仿真,对多个算法进行比较,仿真结果验证了本文算法的有效性和可行性。而且该算法同样也可用于其他生化实验的实施,对数字微流控生化检验的系统综合具有一定的参考价值。

参 考 文 献

[1] Choi K, Ng A H C, Fobel R, et al. Digital Microfluidics [J]. Annual Review of Analytical Chemistry, 2012, 5(1): 413 – 440.

[2] Srinivasan V, Pamula V K, Fair R B. An integrated digital microfluidic lab-on-a-chip for clinical diagnostics Oil human physiological fluids [J]. Lab Chip, 2004, 4(4): 310 – 315.

[3] Kaler K, Prakash R. Droplet Microfluidics for Chip-Based Diagnostics[J]. Sensors, 2014, 14(12):23283 – 23306.

[4] Jebrail M J, Bartsch M S, Patel K D. Digital microfluidics: a versatile tool for applications in chemistry, biology and medicine[J]. Lab on a Chip, 2012, 12(14):2452 – 2463.

[5] Chakrabarty K. Design, testing, and applications of digital microfluidics-based biochips [C]//Proceedings of the 18th International Conference on VLSI Design held jointly with 4th International Conference on Embedded Systems Design, Washington, DC, USA, January 3 – 7, 2005: 221 – 226.

[6] Chakrabarty K, Su F. Design automation challenges for microfluidics-based biochips [C]//Design, Test, Integration, and Packaging of MEMS/MOEMS. Montreux, Switzerland, Jun 1 – 3, 2005: 260 – 265.

[7] Chakrabarty K, Su F. System-level design automation tools for digital [C]//CODES + ISSS, Jersey City, New Jersey, USA, 2005: 201 – 206.

[8] Chakrabarty K, Zeng J. Design automation for microfluidics-based biochips[J]. ACM Journal on Emerging Technologies in Computing Systems, 2005, 1(3): 186 – 223.

[9] Ren H, Fair R B. Micro/nano liter droplet formation and dispensing by capacitance metering and electro wetting actuation [C]//Proceedings of the 2nd IEEE Conference on Nanotechnology, 2002 IEEE-NANO Munich: IEEE, 2002: 369 – 372.

[10] Paik P, Pamula V K, Fair R B. Rapid droplet mixers for digital microfluidic systems[J]. Lab on a Chip, 2003, 3(4): 253 – 259.

[11] Pollack M G, Shenderov A D, Fair R B. Electrowetting-based actuation of droplets for integrated microfluidics[J]. Lab on a Chip, 2002, 2(2):96 – 101.

[12] Glover E. Tabu search: Part I[J]. ORSA Journal on Computinn, 1989, 1(3): 190 – 206.

[13] 贺一. 禁忌搜索及其并行化研究[D]. 重庆:西南大学, 2006.

[14] Su F, Hwang W L, Chakrabarty K. Droplet Routing in the Synthesis of Digital Microfluidic Biochips[C]//Proceedings of the Conference on Design, Automation and Test in Europe, DATE 2006, Munich, Germany, March 6 – 10, 2006. IEEE, 2006: 73 – 78.

[15] Ding J, Chakrabarty K, Fair R B. Scheduling of microfluidic operations for reconfigurable two-dimensional electrowetting arrays[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits, and Systems, 2001, 20(12):1463 – 1468.

[16] Su F, Chakrabarty K. Architectural-Level Synthesis of Digital Microfluidics-Based Biochips [C]//Proceedings of the 2004 IEEE/ACM International conference on Computer-aided design. IEEE, 2004: 223 – 228.

(上接第 319 页)

[6] 景鹏. 天地一体化网络中深度包检测应用开发[D]. 北京:北京交通大学,2017.

[7] 刘永明,王渊. 基于 DPI 和 DFI 的非法业务识别技术[J]. 软件导刊,2015,14(12):177 – 179.

[8] Deri L, Martinelli M, Bujlow T, et al. nDPI: Open-source high-speed deep packet inspection[C]// 2014 International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE, 2014.

[9] 卓中流. 匿名网络追踪溯源关键技术研究[D]. 成都:电子科技大学,2018.

(上接第 324 页)

[14] 钟成, 李兴华, 宋园园, 等. 无线网络中基于共享密钥的轻量级匿名认证协议[J]. 计算机学报, 2018, 41(5): 191 – 205.

[15] 江英华, 张仕斌, 昌燕, 等. 具有双向身份认证的量子密钥分发协议[J]. 量子电子学报, 2018(1):49 – 53.

[16] 陈晓峰. 基于纠缠交换的具有双向认证的多方量子密钥分发[J]. 韶关学院学报, 2016, 37(10): 20 – 24.

[17] 陈晓峰, 刘晓芬. 基于单粒子态的双向认证多方量子密钥分发[J]. 量子电子学报, 2017, 34(3): 369 – 373.