

一种基于 HTTP 包识别的网络安全设备联动的方法

孙 利¹, 徐 亮¹, 吴辞文²

(1 黄淮学院, 河南 驻马店 463000; 2 郑州大学 计算机科学系, 河南 郑州 450006)

摘 要: 本文通过在网络侧集线器与用户主机侧交换机之间部署安全联动设备防火墙, 以及并联在集线器与交换机之间的审计系统, 提出一种基于 HTTP 包识别的网络安全设备联动方法. 它基于网络信息安全领域入侵检测与防范技术, 用以在线解决现有网络安全设备联动阻断技术的时效性较差的问题. 最后, 通过实验测试证明该方法实用有效.

关键词: 网络信息安全; 设备联动; 入侵检测; HTTP 包识别; 规则匹配; 阻断处理

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2013)01-0114-04

A Method of Network Security Device Linkage Based on HTTP Packet Recognition

SUN Li¹, XU Liang¹, WU Ci-wen²

(1 Henan Huanghuai University, Zhumadian 463000, China; 2 Department of Computer Science and Technology, Zhengzhou University, Zhengzhou 450006, China)

Abstract: The paper introduces a device linkage system on firewall between the network side and the switch side of user host, and introduces the audit system connected in parallel between the hubs and switches. Then, the paper introduces a method based on HTTP packet recognition network security device linkage, which is a technology of information security intrusion detection and prevention based on the network. It is mainly used to solve the existing network security equipment linkage blocking technology limitation poor problem. Finally, the test result shows that the method is practical and effective.

Key words: network information security; device linkage; intrusion detection; HTTP packet recognition; rule matching; block processing

1 引言

网络信息日益丰富, 如何保证动态变化的网络信息内容的健康合法以及如何对突然出现的不良内容进行判断及阻断, 已经成为安全领域研究中的热点技术.

网络内容审计系统作为旁路监听设备, 一般采用并联到交换机监听口的方式部署, 不会对网络性能造成影响, 可用性强于应用层防火墙. 赵晓明等通过设置入侵检测代理和集中控制服务器, 提出一种分布式的网络安全防护体系^[1]. 但是其问题是只能

提供事后报警, 这种传统的阻断方式是以双向 TCP reset 方式, 具有时间滞后、网络传输率下降、成功率低等问题, 无法精确对不良链接进行隧道包的阻断.

文献[2-4]给出了一种并联设备(如入侵检测系统)与串联设备(防火墙)的联动协议, 通过 server-client 的方式实现设备联动阻断连接的目的. 该方法的缺点在于阻断的滞后性, 即入侵行为已经到达了内部网络之后, 才由入侵检测系统发现, 然后再通知处于网关位置的防火墙对该连接进行阻断, 此时内部网络也许已经有被注入病毒的危险.

而对于网络内容审计而言, 即使旁路部署的审

收稿日期: 2012-05-08; 修回日期: 2012-06-12

基金项目: 国家自然科学基金项目(60920109)

计系统发现了用户访问不良网页,并且通知了防火墙阻断该连接.然而由于浏览器缓存或不良网页频繁变换 IP 等方式,用户还能继续浏览到不良信息,即出现时效性差等问题.本文通过“审计系统—防火墙”安全设备联动缩短检测非法信息的相应时间,其目的是为了解决现有网络安全设备联动在线阻断技术的时效性较差的问题.

2 网络安全设备联动系统

2.1 体系结构

本系统是一种网络安全设备联动的系统,包括:部署在网络侧集线器与用户主机侧交换机之间的防火墙,以及并联在所述集线器与交换机之间的审计系统.数据包从网络侧通过所述集线器后,被审计系统和防火墙同时截获;防火墙判定不是 http 数据包;或者判定是 http 数据包,但未在设定的时间内收到审计系统发来的阻断要求,则向用户主机侧转发该数据包;防火墙判定是 http 数据包,并且在设定的时间内收到审计系统发来的阻断要求,则进行阻断处理,最终达到对不良信息阻断的目的,其检测与处理不良信息的系统体系结构如图 1 所示.

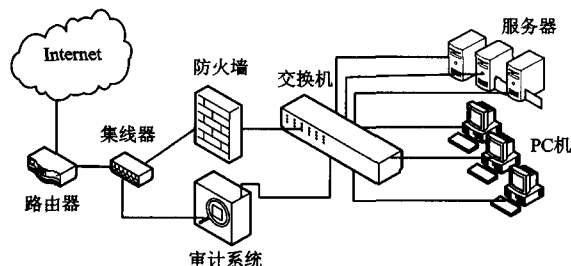


图 1 系统的体系结构

2.2 联动步骤

网络的入侵检测与隔离协议(Intrusion Detection and Isolation Protocol, IDIP)是 NAI Labs、Boeing Phantom Works 和 U. C. Davis 共同开发的一个用于入侵检测系统中快速、自动响应入侵攻击的协议,它支持各种网络组件之间信息的相互交换.但目前的通信机制无论针对何种布局,都局限于一种或一类统一的安全防护系统^[5-6].因而,通过数据包到达用户主机之前被审计系统和防火墙截获后,防火墙判定是否 http 数据包,并且在设定的时间内收到审计系统发来的阻断要求,进行联动对比,对异常数据包进行阻断处理.具体步骤:

(1)审计系统和防火墙同时截获数据包,分析数据包 http 属性,并判断在设定的时间内收到审计系统发来的阻断要求;

(2)审计系统判断是否发出阻断要求:拆接数据包、根据内容规则进行匹配、联动处理;

(3)分析到达防火墙时间、审计系统处理时间;

(4)拆接数据包的过程需要通过防火墙与审计系统共同完成,进行规则匹配分析;

(5)阻断处理.分析数据包,进行丢包处理或替代后转发处理;

(6)网络安全设备联动.分析在防火墙中设定的所述时间大于审计系统处理的时间与阻断请求从审计系统到达防火墙的时间之和,进行联动阻断处理.

3 设备联动机制的实施

为了更具体地解决网络旁路审计设备通过防火墙的并行联动实现在线阻断不良链接的时效性问题,通过网络安全设备联动的具体实施方式,以及若干实施实例具体加以说明.

3.1 防火墙的过滤

该方法中通过防火墙判断数据包(过程 S1~S5),如果该包是 http 协议的数据包,则做暂缓处理,将数据包暂存到一个暂存器中(FIFO 原则),假设该 http 数据包标示为 x ,达到一定时间后(标记为 t_x ,一般为数百毫秒级),如未收到审计系统的阻断要求,则进行正常转发处理,同时清除暂存记录,如该段时间内收到审计系统发来的阻断要求,则进行丢包或替代后转发处理,同时清除暂存记录.如果该包不是 http 协议的数据包,则进行正常转发处理.如图 2 所示,表示防火墙对数据包的阻断处理过程.

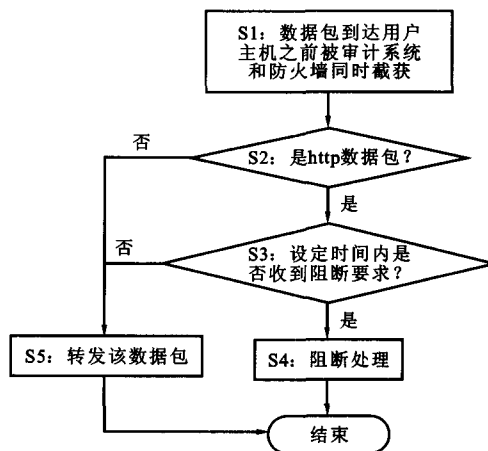


图 2 防火墙对数据包的阻断处理过程

3.2 审计系统对数据包的处理

路由器通过进程交换、快速交换、优化的分布式交换或其他方式传递数据包,包的捕获结合轮询和

中断的优点,即通过使内核空间和用户空间共享一段内存区域的方式捕获数据包。

基于局域网之间 IDC(Internet Data Center,即互联网数据中心)中可能存在非法信息、图像等内容,参照国内外各主流安全厂商的分布式系统和网站内容审计系统的设计,用于测试 IDC 网站内容审计系统依据以下原则:

① 具有可扩充性,有利于系统随着 IDC 规模增大升级改造;

② 能够直接监控 10 G bit/s 骨干链路,具有至少 5 Gbit/s 的吞吐能力,以学校信息中心骨干网络进行测试;

③ 采用模块化软件结构,各功能模块可依据实际需要选用,便于以后新功能模块开发,同时也能够在现有系统上增加;

④ 采用全旁路部署模式。

基于此,在对 http 数据包监测和阻断过程中,通过对域名、符号、图像特征、关键字等的处理,通过并联在集线器与交换机之间的审计系统,数据包从网络侧通过集线器后,由审计系统和防火墙同时截获,其审计系统结构设计如图 3 所示。

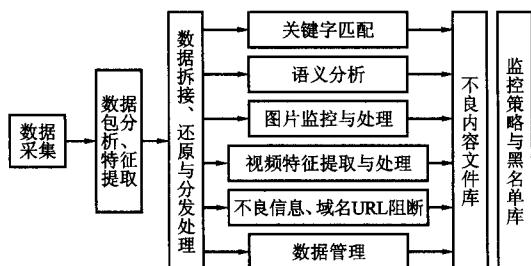


图3 审计系统内部结构设计

3.3 数据包的拆接

数据包从网络侧通过集线器后,被审计系统和防火墙同时截获,分析网络安全设备的处理时间,其过程如图 4 所示。

防火墙判断数据包是否是 http 数据包,若防火墙判定不是 http 数据包,则向用户主机侧正常转发该数据包。判定是 http 数据包,则做暂缓处理,将数据包暂存到一个暂存器中(可为先入先出存储器 FIFO 原则),之后若未在设定的时间 t_x 内收到审计系统发来的阻断要求,则向用户主机侧正常转发该数据包,同时清除暂存记录;之后若在设定的时间 t_x 内收到审计系统发来的阻断要求,则进行丢包或替代后转发等阻断处理,同时清除暂存记录。

数据包拆接的过程中,审计系统判断是否发出阻断要求的逻辑为:拆接数据包时以拆接所得内容

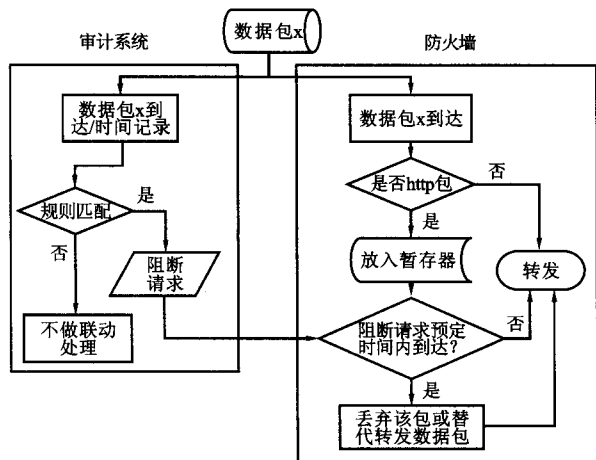


图4 数据包的拆接处理过程

与预设的内容规则进行规则匹配,拆接时间为 m_x (通常为数百毫秒),发现违反规则,则向防火墙发出阻断请求,该请求从审计系统到达防火墙的时间为 n_x (一般小于 10 毫秒),未发现违反规则,则不做联动处理。在防火墙中设定的时间 t_x 应大于审计系统处理的时间与阻断请求从审计系统到达防火墙的时间之和($t_x > m_x + n_x$)。上述处理过程均以毫秒级计算,所以,网页延时数百毫秒对用户体验影响不大。

3.4 应用效果

由于系统结构中防火墙与审计系统并联于校园网信息中心机房,所以可提供同时截获 http 数据包。然后,通过防火墙的判断数据包协议类型机制,以及定时缓存 http 数据包并等待审计系统的阻断要求机制,达到了在线阻断不良链接,不会被用户主机侧接收的效果,进而体现了阻断技术的时效性。

4 设备联动的性能测试及分析

4.1 测试环境与过程

(1) 实验测试环境

实验测试环境建立在校园信息中心机房,共建立 10 台机器,其中 1 台为服务器。配置:9 台为 PC 机,CPU 为 Intel(R) Core(TM)2 Duo CPU E7500 2.93 GHz,机器内存 2GB,Windows XP 操作系统;服务器 CPU 为 Intel Xeon E5620 2.4 GHz(1 个)1 台,内存 2 * 2GB,安装 Linux 5.0 操作系统。

其中,配置 1 台华为赛门铁克 Secoway USG2220 防火墙、1 台 BDS3000-SG3 审计系统、IPtables、1 台集线器、1 台 H3C LS-3100-26TP-SI-H3 工作组交换机、1 台 H3C ER6300 路由器,共同构成实验测试环境,参考文献[7]配置网络系统。

(2) 测试步骤

控制每个入侵检测系统 (Intrusion Detection System, IDS) 节点的“审计系统—防火墙”联动模块每隔 $\Delta t(\text{ms})$ 向“审计系统—防火墙”联动模块发送 1 条不同攻击者 Alert 发来的警告信息,共 3000 条,这里可定义联动模块检测到来自外部网络的非法信息频率 $f=1/\Delta t$ 。这样对这些外部非法信息进行分析处理,生成新的规则,并分发到“审计系统—防火墙”节点的对应联动模块。

这里为了最大限度降低自身性能对整体数据传输、通信机制性能瓶颈效应的影响,其分析处理采用最简单的将攻击者 http 数据包加入黑名单的处理方式^[8-9]。

4.2 测试结果及分析

(1) 测试结果

假设防火墙接收来自审计系统发来的阻断信息的条数平均值为 N ,则可定义阻断响应速度为 V ,则在所处的局域网系统中“审计系统—防火墙”安全设备联动间隔 Δt 内,则 $V=N/2 \cdot (t_x-1000/f)$, Δt 取 1, 2, ..., 6 (ms), 可以得出实验测试数据,如表 1 所示。

表 1 测试数据

次序 项目	1	2	3	4	5	6
$f/(\text{次}/\text{ms})$	1	0.5	0.33	0.25	0.2	0.17
$t_x/(\text{ms})$	1253	2321	3427	4365	5341	6512
$N/\text{条}$	1321	1853	2147	2302	2954	3000
$V/(\text{条}/\text{ms})$	2.61	2.89	2.51	3.15	4.33	2.93
丢包率 (%)	0.224	0.160	0.115	0.062	0.012	0.003

(2) 结果分析

从实验结果可以看出,联动模块检测到来自外部网络的非法信息频率低于或接近于 0.2 次/ms 时,阻断响应速度有所降低,在高速的网络状态,防火墙与审计系统相互联动的速率维持较好的状态,接收外网的非法信息频率高于 0.2 次/ms 时,阻断相应速度都能够达到 2.5 条/ms 上,如图 5、图 6 所示,说明通过防火墙与审计系统联动机制提高了对非法信息的检索与鉴别的速度。

基于以上思想,比较网络攻击频率数据特征的判别,以及网络攻击频率混沌特性,在实际操作时本文采用了两种与网络非法信息攻击的平均值对比,通过“审计系统—防火墙”联动足够阻断不良信息的侵扰^[10]。通过定时缓存 http 数据包并等待审计系统的阻断要求机制,达到了在线阻断不良链接,不会被

用户主机侧接收的效果,进而改善了阻断技术的时效性。

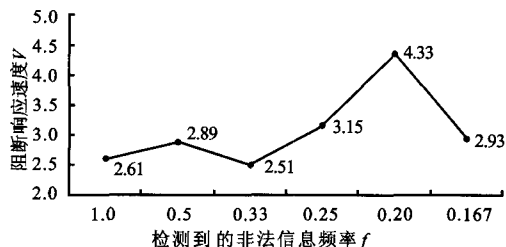


图 5 阻断响应速度与检测到非法信息频率关系

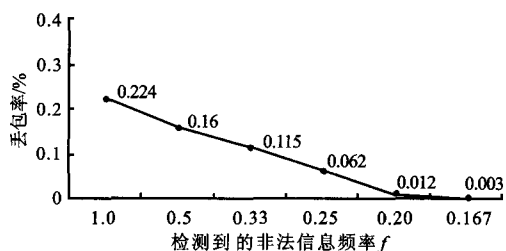


图 6 丢包率与检测到非法信息频率关系

5 结束语

信息安全领域的技术人员可以对该方法进行各种改动和变型,而不脱离“审计系统—防火墙”设备联动的应用范围、技术领域,适用于现有的 IPv4 与 IPv6 网络。由于现有网络信息安全技术固有的缺陷,该方法还不能完全解决阻断技术中非法信息通过数据传输延迟的时差问题避开安全设备的监测。但在规模不大的局域网中,比如在局域网监测系统中,本方法利用入侵攻击的特征、人员监控可以较好地改善在线阻断响应速度与网络延迟的矛盾,解决了 Linux 捕获 http 数据包的瓶颈,以及审计系统中数据流高速处理的丢包问题,从而在改善阻断技术的时效性问题上起到关键性作用。

参考文献:

- [1] 孙勇,张恒,马严,等. 基于 IPv6 的入侵检测与防火墙联动系统[J]. 计算机工程, 2008(11):152-154.
- [2] 张月国,铁玲,薛质,等. 基于 SNMP 协议的网络安全设备联动策略机制[J]. 信息安全与通信保密, 2003(12):36-37.
- [3] 夏高,刘斌. 用于高速网络入侵检测系统的并行 TCP/IP 协议栈[J]. 清华大学学报:自然科学版, 2011(07):942-948.
- [4] 赵晓明,张新霞. 基于网络信息安全内容审计系统及相关技术研究[J]. 航空计算技术, 2006(9):127-130.

(下转第 122 页)

和(8)起到了决定的作用,从而使得收敛曲线继续快速下降;这个过程一直持续到算法收敛为止,此时收敛曲线变得平滑。

5 结束语

本文提出了一种混沌和声算法求解连续函数优化问题。为了提升求解效果,新算法在基本和声算法基础上进行了三方面改进:第一,引入了佳点集初始化操作,增强了初始种群的均匀性;第二,在生成新候选和声向量时,引入了一种自适应的学习机制;第三,设计了一种混沌局部搜索算子,用于提升较优和声向量的质量。五个标准测试函数的仿真实验结果证明:新算法无论是求解质量还是收敛速度都显著优于基本和声算法。

参考文献:

- [1] Geem Z W, Kim J H. A new heuristic optimization algorithm: harmony search[J]. Simulation, 2001, 76 (2):60-68.
- [2] Mahdavi M, Fesanghary M, Damangir E. An improved harmony search algorithm for solving optimization problems[J]. Applied Mathematics and Computation, 2007, 188(2):1567-1579.
- [3] Pan Q K, Suganthan P N, Tasgetiren M F, et al. A self-adaptive global best harmony search algorithm for continuous optimization problems [J]. Applied Mathematics and Computation, 2010, 216 (3): 830-848.
- [4] Wang C M, Huang Y F. Self-adaptive harmony search algorithm for optimization[J]. Expert Systems with Applications, 2010, 37(4):2826-2837.
- [5] Omran M G H, Mahdavi M. Global-best harmony search[J]. Applied Mathematics and Computation, 2008, 198(2):643-656.
- [6] 张铃,张钊. 佳点集遗传算法[J]. 计算机学报, 2001, 24(009):917-922.
- [7] LiMingxing, Heng Ping, Dong Peiwu. Research on artificial neural network method for credit application [J]. Research Information Ltd(RIL) UK, 2004(2): 127-131.
- [8] 张中辉,操家庆,梁意文. 基于联动机制的入侵防御系统[J]. 计算机时代,2006(7):28-30.
- [9] 宁海滨. 基于校园网的入侵检测系统设计与实现[D]. 北京:北京大学,2008.
- [10] 刘文星. 网络攻击频率混沌时间序列预测[D]. 长沙:国防科学技术大学,2008.
- [11] 潘炜,李伟华. 网络安全联动模型的设计与应用[J]. 计算机科学,2006(5):113-116.

作者简介:

闫涛 男,(1970—),本科,副教授.研究方向为数据挖掘。

作者简介:

孙利 男,(1972—),硕士,副教授.研究方向为计算机网络与安全。

徐亮 男,(1978—),硕士,讲师.研究方向为数字图像处理与可视化技术研究。

吴辞文 男,(1975—),博士研究生,讲师.研究方向为计算机网络与应用。

(上接第 117 页)