基于骨干网的并行集群入侵检测系统

杨 武[1], 方滨兴[2], 云晓春[1], 张宏莉[1]

(1. 哈尔滨工业大学 国家计算机内容信息安全重点实验室, 黑龙江 哈尔滨 150001,
E-mail:yangwu@pact518.hit.edu.cn; 2. 国家计算机网络与信息安全管理中心, 北京 100031)

摘 要: 骨干网的大流量要求实现骨干网入侵检测系统必须改变传统的入侵检测系统结构模型并采用高效的入侵检测技术. 在对骨干网入侵检测系统的关键技术进行深入研究的基础上,设计并实现了一种适用于骨干网的基于规则的入侵检测系统BNIDS(Backbone Network Intrusion Detection System). 讨论了BNIDS系统的并行集群检测模型、报文捕获机制和基于规则的分析引擎. 试验结果表明,可扩展的BNIDS系统能够对骨干网流量进行实时入侵检测分析.

关键词: 入侵检测;网络安全;负载平衡;报文捕获;多模式匹配
中图分类号: TP393.08 **文献标识码**: A **文章编号**: 0367-6234(2004)03-0273-04

A parallel cluster intrusion detection system for backbone network

YANG Wu[1], FANG Bin-xing[2], YUN Xiao-Chun[3], ZHANG Hong-li[4]

(1. National Computer Content Information Security Key Lab, Harbin Institute of Technology, Harbin 150001, China, E-mail:yangwu@pact518.hit.edu.cn; 2. National Computer Network and Information System Security Administration Center, Beijing 100031, China)

Abstract: In order to change the traditional intrusion detection system architecture model by adopting some efficient intrusion detection techniques in an intrusion detection system (IDS) for backbone network, based on in-depth research on the key techniques of the IDS for backbone network, the design and implementation of a rule-based intrusion detection system for backbone network —BNIDS (Backbone Network Intrusion Detection System), are discussed with emphasis on the parallel cluster detection model, packet capture mechanism and rule-based analysis engine. The results of experiments indicate that the scalable BNIDS can do the real-time intrusion detection in a backbone network.

Key words: intrusion detection; network security; load balance; packet capture; multi-pattern matching

随着Internet的飞速发展,网络攻击事件不断发生. 作为网络安全防护工具防火墙的一种补充措施,网络入侵检测系统正得到迅猛的发展[1]. 近些年,RedCode、Nimda、口令蠕虫等蠕虫病毒的肆虐以及DOS/DDOS等分布式攻击的频繁发生,给世界的经济和人们的生活造成重大的影响. 这些攻击方式的一个显著特点是它们的发生往往会带来骨干网流量出现明显的异常,而这种异常在局部子网中则很难观察到,所以选取骨干网作为入侵监测点十分必要. 由于网络带宽不断增加,骨干网的流量通常达到数Gbps甚至数十Gbps. 在如此高速的网络环境下,将网络数据包全部截获下来很困难,何况还要做复杂的入侵检测分析,因此,要实现基于骨干网的实时入侵检测,必须要改变传统的入侵检测系统结构模型并采用高效的入侵检测技术.

为此,本文在对高效的入侵检测相关技术深入研究的基础上,设计并实现了一种基于骨干网的高性能入侵检测系统BNIDS(Backbone Network Instrusion Detection System).

1 BNIDS的系统结构设计与实现

在骨干网监测点上,使用单节点机采用监听

收稿日期: 20003-05-15.
基金项目: 国家高技术研究发展计划资助项目(2002AA142020).
作者简介: 杨 武(1974-),男,博士研究生;
方滨兴(1960-),男,教授,博士生导师;
云晓春(1971-),男,教授,博士生导师.

的方式对网络数据进行入侵分析时,即使是采用SMP的计算机,其最大可以处理的数据流量约为110 Mbps,所以单节点处理机无法适应高速骨干网中实时入侵检测的要求. 本文利用负载平衡技术,提出了一种基于骨干网的并行集群分析处理模型,通过采用SPMD的计算模式来对集群系统进行了可伸缩性设计. 在网络流量增大时,可以通过增加处理节点等方法来扩展集群检测系统的数据处理能力. BNIDS的系统结构模型如图1所示. 负载平衡器通过分光器接入骨干网,实现物理层数据流光信号的截获. 为将进入到负载平衡器的数据分流到集群系统中的各个传感器上,负载平衡器需要配置相应的100 Mbps/1 000 Mbps以太端口,将骨干网光信号的数据接入转换成入侵检测系统所要求的以太网卡的数据接入. 负载平衡器除具备基本的数据分流功能外,还可以按照管理器的配置策略进行简单的数据过滤,以减少传感器的数据负载.

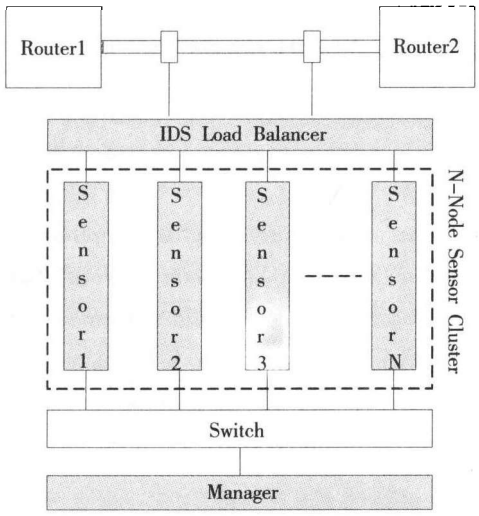

图1 BNIDS的系统结构模型

骨干网中的大部分流量是基于TCP协议的. 针对TCP流量,一种理想的负载平衡算法应满足以下要求:1)数据被近乎均匀地划分到各个节点机上,以保证节点机间的负载均衡;2)任意一个TCP连接的双向数据都被分流到同一节点机上,以保证各节点机间无数据依赖. 但负载平衡算法不应过于复杂,以实现高速骨干网中数据的快速分流. 为此,负载调度器采用了一种基于连接轮转调度的算法,以连接为粒度,对网络数据进行合理、细粒度的分流. 在TCP/IP协议中,四元组(源IP地址、目的IP地址、源端口、目的端口)唯一地确定了一个连接. 连接轮转调度算法描述如下:当连接的第一个数据包(SYN包)到达时,负载平衡器将最近分配的节点机号取模N再加1作为新连接的分流地址(N为节点机数),将报文发送到该节点机,同时负载平衡器在Hash表中记录这个连接(以四元组形式)和相应的节点机号并更新最近分配的节点机号. 这样当这个连接的下一个报文到达时,从Hash表中可以得到原来选定节点机的地址,继续将报文发送到相同的节点. 当连接终止或超时,负载平衡器将这个连接从Hash表中删除.

对于其他的协议类型则通过对二元组(源IP地址、目的IP地址)做简单的散列运算来获取分流地址. 公式为:目的节点机号=(源IP地址⊕目的IP地址) mod N, N为集群系统的节点数. BNIDS系统中的传感器用于捕获以太网数据包、进行协议分析与还原以及规则匹配过程. 管理器接收传感器生成的警报事件并进行综合的分析和结果显示. 传感器的实现框架如图2所示.

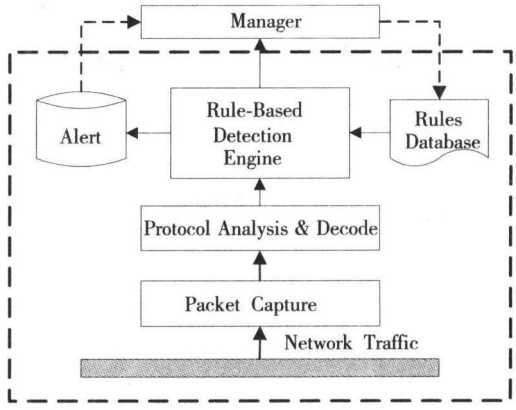

图2 传感器结构

1.1 基于零拷贝技术的报文捕获机制

传统的网络入侵检测系统一般是通过调用报文捕获函数库Libpcap[2]来捕获网络链路层数据帧. 在大流量网络环境下,基于Libpcap的捕包机制效率低下,往往会出现大量丢包的现象. 造成这种现象的主要原因是数据包的传输总是通过操作系统内核来完成,这包括了一些关键路径如系统调用和数据拷贝等过程. 系统调用相当于一个中断号为0x80的中断,在网络流量很大时,系统调用消耗在中断现场保存与进程切换上的CPU时间就相当可观. 内存带宽是系统主要的性能瓶颈之一,多次的数据内存拷贝操作要消耗大量的CPU周期和内存资源,从而严重地增加了系统的处理开销.

为了提高入侵检测系统的捕包性能,有必要减少报文传输过程的中间环节,绕过操作系统内核,减少或消除数据拷贝次数,降低系统有限资源的消耗. 为此设计了基于零拷贝技术的高效报文捕获机制 - Libcapture. 图3对Libcapture与传统

libpcap 捕包机制进行对比. 从图中可以看出 Libcapture 由 3 个部分组成：内核管理模块 - Kernel Manager、改进的网卡驱动程序 - New NIC Driver、虚拟网络接口 - VNI(Virtual Network Interface). 其中 VNI 位于系统的用户态，为应用程序提供访问网络接口硬件的 API 函数库，其他两部分位于系统核心态，Kernel Manager 负责用户空间的虚拟地址 - 物理地址转换并创建共享缓冲环. Kernel Manager 仅在打开虚拟网络接口时使用. New NIC Driver 则通过和 Kernel Manager 的交互获取网卡异步 DMA 操作所需的物理地址转换表，并启动 DMA 直接在用户缓冲区和网络接口硬件之间传输网络数据包.

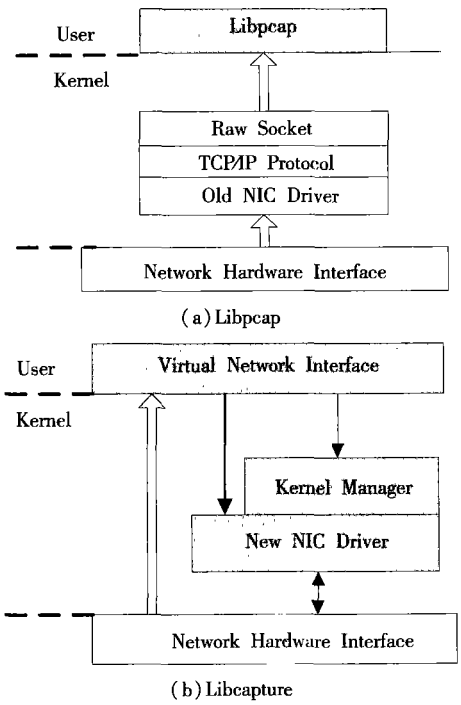

图3　Libpcap 和 Libcapture 捕包机制的对比

1.2　基于规则的检测引擎设计

网络入侵检测系统常用的检测分析技术包括异常检测和滥用检测. 基于规则的检测引擎能够综合滥用检测和异常检测这两种检测方法的优点，在保证检测准确性的同时提高了检测未知攻击和多态攻击的能力. 在 BNIDS 系统的实现中采用了一种与 snort[3] 中的规则描述语言类似的语法. 一条规则分为规则头和规则选项两部分. 规则头包括源地址、目的地址、源端口和目的端口以及所属协议和匹配动作. 规则选项部分使用一些关键字组合来描述攻击特征，如关键字 content 描述了数据包载荷中需进行模式搜索的特征字符串.

1.2.1　高效灵活的规则描述语言

BNIDS 系统的规则描述语言能够用尽可能少的要素以及尽量简单的语法来描述一些常见的网络攻击事件. 相对于 Snort 规则只能描述基于数据包的特征匹配而言，这种规则语言不仅能够描述用于滥用检测的模式特征(pattern)而且还可以描述用于异常检测的正常模式简档(profile).

为进行协议分析和状态检查，定义了规则选项“tcp_flow: client_to_server, established”. 这个选项表示待检测的数据包是客户端请求并且经过了 TCP 状态检查.

规则语言能够描述应用层协议规范，这样当数据包载荷不符合规则所描述的协议规范时就认为发生了异常. 例如规则语言定义了关键字 within 来描述数据包中两处不同的内容匹配之间的距离. 这样规则“alert tcp any any - > $ HOME_NET 143 (content:"LOGIN "; content:!"|0a|"; within:100;)”可以用来表示如果在命令字符 LOGIN 之后紧随一定数量的字节(< =100)而没有发现行终止符就报警，这表明出现了一种新的 IMAP 缓冲区溢出攻击.

针对 DOS/DDOS 类型的攻击，可以定义关键字 counter 来描述一段时间内出现的某一类型数据包的数量. 规则选项“counter: $ THRESHOLD, $ PERIOD”表示在规定的 $ PERIOD 时间内，某一类型的数据包计数超过域值 $ THRESHOLD.

1.2.2　多规则的高速模式匹配算法

BNIDS 采用了一种高性能的多规则检测引擎来负责对数据包进行规则匹配. 该检测引擎分为两个阶段. 第一阶段是基于规则内容的多模式匹配搜索过程；第二阶段在完成规则内容匹配后验证其他规则选项以确定该规则是否真正匹配当前数据包.

多模匹配算法是基于规则的检测引擎的核心，其性能对网络入侵检测系统的整体性能影响较大. 许多研究者对入侵检测中的模式匹配算法进行了深入的分析并提出了一些高性能多模式匹配算法. Aho - Corasick[4] 算法是一种使用有限状态自动机的并行搜索匹配算法. Aho - Corasick 算法与 BM 算法相结合的 AC - BM 算法[5]，利用了 BM 算法的跳转搜索方式，但要求模式集中的模式具有共同的前缀才具有较高的性能. Mike Fisk[6] 等人提出了搜索模式集的 SBMH 算法，表明在规则数较少时，SBMH 优于 Aho - Corasick 算法. 但当规则数超过 100 条时，Aho - Corasick 算法优于 SBMH 算法.

随着攻击特征库的不断增大，要求匹配算法具有良好的可扩展性. 在 BNIDS 中采用的是经过改进的 Aho - Corasick 算法. 该算法利用多个模式

串构建一个有限状态自动机并且通过使用该自动机来发现在对文本字符串的一次扫描过程中所有模式匹配的情况. 改进的 Aho - Corasick 算法分为两步进行:首先对入侵检测的多条规则中的特征模式串进行预处理,通过这些特征模式串构建有限状态自动机的状态以及状态转换函数;第二步进行网络数据包的匹配过程,当匹配搜索进行到有限状态机的终止状态时,检查匹配的模式串列表以确定其对应的规则选项是否匹配该数据包. 该算法模式匹配过程的时间复杂度是 O(n)(n 为数据包长度),且与规则数目的多少无关.

2 试验结果与分析

两台机器采取背靠背的方式连接,一台作为大流量发包机,另一台作为捕包机(配置如下:CPU - PIII1G × 2,内存 - 2G,网卡 - Intel Pro1000 千兆以太网卡). 测试在不同报文尺寸的情况下,两种不同的捕包机制 Libpcap 与 Libcapture 的报文捕获性能. 结果如图 4 所示. 从图 4 中可以看出,由于采用零拷贝技术消除了用户层和内核之间的内存拷贝操作,随着接收报文长度的增加,Libcapture 的峰值处理带宽也不断提高. Libpcap 的峰值带宽随报文尺寸的变化不大,这是使用传统内核协议栈所带来的结果. 在相同报文尺寸的条件下,Libcapture 的峰值带宽要比 Libpcap 高许多. 这表明 Libcapture 是一种高性能的报文捕获机制.

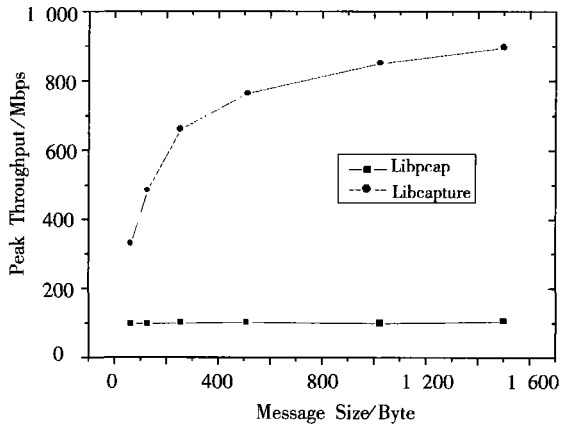

图 4 Libpcap 与 Libcapture 的报文捕获性能

利用 MIT Lincon Lab[7] 提供的 1998 入侵检测训练数据集,选取一天的流量数据(容量大约 160MB 的 Tcpdump 文件). 从入侵检测系统规则库中选取 1000 条规则. 测试在不同规则数目情况下整个数据集的模式匹配时间(实验机配置:CPU - PIII1G × 2,内存 - 2G,硬盘 - 18GSCSI,操作系统 - Linux - 2.4.10),如表 1 所示. 结果表明采用改进的 Aho - Corasick 算法后,入侵检测系统模式匹配的时间不依赖于规则数目的变化而变化,从而保证了系统具有较好的匹配性能.

表 1 模式匹配时间与规则数目的关系表

规则数目	系统运行时间/s	模式匹配时间所占百分比/%	模式匹配时间/s
14	7.288	55.94	4.08
200	7.818	53.21	4.16
450	10.821	37.73	4.08
700	11.314	37.12	4.19
1 000	17.193	23.54	4.04

3 结 语

通过采取分流的策略降低骨干网入侵检测系统中单个节点的处理负载,综合采用基于零拷贝技术的报文捕获机制以及高速多规则匹配算法来提高单节点的数据分析处理能力,从而提高了骨干网入侵检测系统的性价比. 实践表明具有可扩展性的 BNIDS 系统能够对骨干网流量进行实时复杂的入侵分析.

参考文献:

[1] AXELSSON S. Intrusion detection systems: a survey and taxonomy[R]. Technical Report 99 - 15, Dept. of Computer Engineering, Chalmers University, 2000.

[2] Libpcap [EB/OL]. http://www.tcpdump.org/release/libpcap - 0.7.2.tar.gz.

[3] ROESCH M. Snort-lightweight intrusion detection for network[A]. Proceedings of LISA'99: 13th System Administration Conference[C]. Washington: Seattle, 1999.

[4] AHO A V, CORASICK M J. Efficient string matching: an aid to bibliographic search[J]. Communications of the ACM, 1975, 18(6): 333 - 340.

[5] MCALERNEY J, COIT C, STANIFORD S. Toward faster pattern matching for intrusion detection[A]. DARPA Information Survivability Conference and Exposition[C]. [s.l.]:[s.n.],2001.

[6] FISK M, VARGHESE G. Fast content-based packet handling for intrusion detection [R]. Technical Report CS2001 - 0670, San Diego: Department of Computer Science and Engineering, 2001.

[7] GRAF I, LIPPMANN R, CUNNINGHAM R, *et al*. Results of DARPA 1998 offline intrusion detection evaluation[EB/OL]. http://ideval.ll.mit.edu/results - html - dir, 1998.

(编辑 王小唯)