基于免疫学原理的混合入侵检测系统的设计与实现*)

傅 涛[1] 孙文静[2] 孙亚民[1] 崔萌萌[3]
(南京理工大学计算机学院 南京 210094)[1] (南京审计学院 南京 210029)[2]
(南京信息工程大学 南京 210044)[3]

摘 要 讨论了基于免疫学的入侵检测系统的架构和各模块的功能,重点研究了本文提出的基于改造开发源代码的入侵检测系统 Snort 的免疫检测器模块的设计,以及免疫检测器的检测流程。以 KDDCup99 数据集为样本,运用本文设计的基于免疫学原理的混合入侵检测系统进行了入侵检测实验,对全部 18 种攻击类型行为的平均检测率为 64.94%,检测结果令人鼓舞。

关键词 入侵检测系统,混合,免疫学

Design and Implementation of Mix Intrusion Detection System Based on Immunology Principle

FU Tao[1] SUN Wen-jing[2] SUN Ya-min[1] CUI Meng-meng[3]
(Nanjing University of Science and Technology, Nanjing 210094, China)[1] (Nanjing Audit University, Nanjing 210029, China)[2]
(Nanjing University of Information Science and Technology, Nanjing 210044, China)[3]

Abstract This paper discusses the architecture of Intrusion Detection System (IDS) based on immunology and functions of each module. It emphasizes on system design of immunization detection module based on the snort which is a kind of open souce IDS and the detection processes of immunization detector. This article takes KDDCup99 dataset as a sample and do the intrusion detection experiment by using principle of immunology. The average detection rate of 18 kinds of intrusion actions is 64.94%, the result is encouraging.

Keywords Intrusion detection system, Mix, Immunology

1 引言

研究发现,生物免疫系统与入侵检测系统具有惊人的相似性,前者保护机体不受诸如病菌、病毒等各种病原体的侵害,而后者则保护计算机系统不受或少受入侵事件的危害或威胁,两者都是在不断变化的环境中维持系统的稳定性。这种相似性使得免疫系统为入侵检测提供了一个自然的研究模板,而且免疫系统在实现过程中表现出的识别、学习、记忆、多样性、自适应、容错及分布式检测等复杂的信息处理能力,正是当前入侵检测领域中所期望得到的。因此,如何将生物免疫的相关机理应用于入侵检测系统,以提高它的检测能力和应变能力就成为当前的热门研究课题。

2 基于免疫学原理的入侵检测系统架构

本文提出的基于免疫学的入侵检测系统(AIIDS)架构如图 1 所示。其检测代理既对未知的入侵方式有学习能力,又能高效率地检测已知的非法网络连接。

该架构包括三个模块:嗅探器模块、基于免疫学的误用检测模块(Snort)、基于免疫学的异常检测模块。

嗅探器模块:负责从网络上获取数据包(含网络上传输的帧、IP 包和报文)。嗅探器将网卡设为杂收(promiscuous)模式,让网卡接收其收到的所有包。如果网络上使用的是交换 HUB,则还需要进行 ARP 欺骗,或者在 HUB 或交换机上设置一个专门的口监听所有的数据包。数据包传递的数据包括自体(正常 TCP/IP 连接)和非自体(非正常 TCP/IP 连接),相对于动物免疫系统的自体成分和非自体成分。网络上获取的数据包用来提供给过滤系统。

过滤系统:对数据源传来的数据进行审计,将无用或多余数据删除。信息流经过过滤后送往检测系统,在需要的时候送到信号发生器。过滤系统发挥着相当于动物免疫系统的皮肤或噬菌细胞的作用。

基于免疫学的误用检测模块(Snort):在本架构中,Snort 发挥着免疫系统中记忆细胞的作用,Snort 将获得的网络数据包按 TCP/IP 协议体系从下到上的顺序进行解析,将网络中传输的数据包还原成基于传输层的连接记录,从中提取出可以用于判断其是否为攻击的特征属性。对于在传输层无法判断的连接记录,则进行高层的协议解析,分解为相应的 FTP, Telnet, HTTP 会话,针对每一种高层协议,提取出可以用于判断其是否为攻击的特征属性。

基于免疫学的异常检测系统:该部分将系统正常访问的行为特征与当前访问行为进行对比来检测访问是否为非法访问,其具有能随系统正常访问行为模式的变化而自适应的能力。基于异常检测系统包括以下部分:

(1)向量转换。将不同协议层的网络数据包转换成相应数学向量。由于 TCP/UDP, HTTP, TELNET 协议在网络通信上用得非常多,而且大部分攻击行为是在这些协议下进行的,因此,对这三种协议的数据包进行单独的数值转换,而对其他类型的数据包用同一种数值转换。

(2)行为性质鉴别。含 TCP/UDP 免疫检测、HTTP 免疫检测、TELNET 免疫检测和其他免疫检测四部分,分别与前面的四种数值转换对应,同时将已知的入侵行为输入规则库,其发挥着生物免疫学中阴性选择检测和生物免疫系统的记忆

*)江苏省产业技术研究与开发基金,苏发改高技发[2006]1106 号。傅 涛 博士生,研究方向为计算机网络;孙文静 博士生,研究方向为计算机网络;孙亚民 教授,博士生导师;崔萌萌 讲师,研究方向为信息安全。

细胞的作用。

(3)第一响应代理。当第一响应代理被激活时将引发一系列措施去减缓或阻塞可能的攻击。但它在攻击未被明确确定时作用是受限的,这样设定的目的是在攻击被明确确定前尽量减少对系统的破坏。第一响应代理可做出以下响应:降低优先权、阻塞进程、文件系统保护和入侵活动警告等。在本系统中,第一响应代理发挥着计算机免疫系统中对非本体成分进行反应的作用。

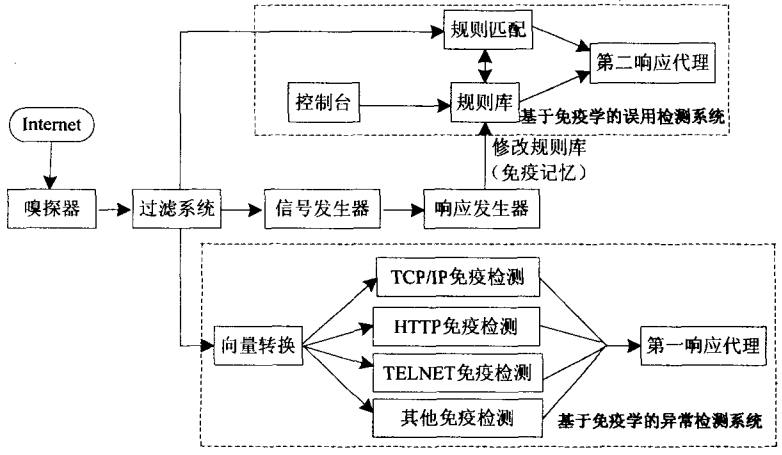

图 1 基于免疫学的混合入侵检测系统的结构

3 免疫检测模块的设计

3.1 模型的物理结构

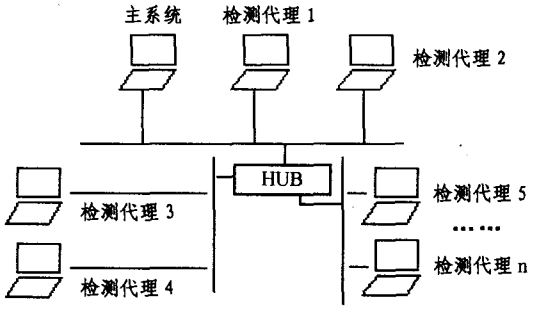

图 2 免疫检测模型的物理结构

图 2 为免疫系统模型的物理结构图。其中,自体定义为计算机间合法的 TCP/IP 连接,可以用计算机通信的路径三元组(源计算机、目的计算机、服务类型)来表示;非自体定义为计算机间非法的 TCP/IP 连接。采用免疫检测器来区分自体和非自体。检测器是一个固定长度为的否定选择算法产生的二进制串。

模型由一个主系统和分布在子网的多个检测代理组成,其中主系统可位于任一子网中,一个子网可以有一个或多个检测代理组成。检测代理监测着子网的 TCP/IP 连接,负责子网的入侵检测工作。

3.2 免疫检测器的生成

本文提出了基于改造开发源代码的入侵检测系统 Snort 的免疫检测器模型(图 2)。这里引入了预处理器的概念,预处理器在数据包解码完毕后进行调用,这种特性使得可以很方便地以插件形式将免疫检测器模块加入 Snort 系统,使它具有基于免疫系统的入侵检测的特点。图 3 为免疫检测器的结构图。

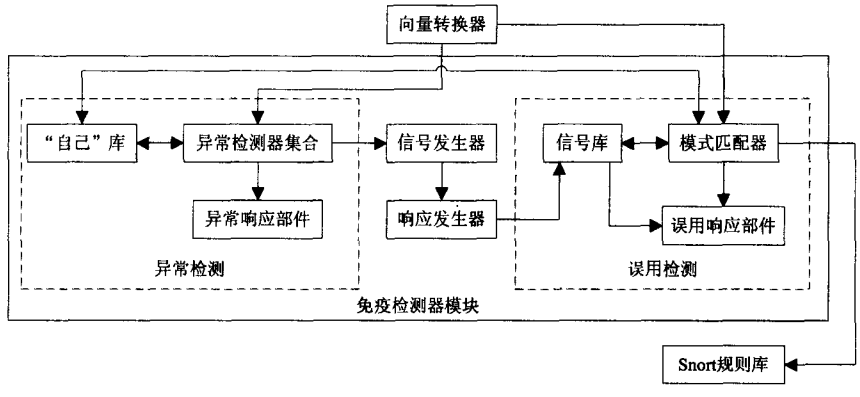

图 3 免疫检测器的结构

各部分的功能是:

(1) 向量转换器。负责将嗅探器 Libpcap 所捕获的数据包在协议解析后进行数值转换,即将不同协议层的网络数据包转换成相应的数学向量。

(2)异常检测器集合。相当于生物免疫系统中 T 细胞的作用,它与预处理器传来的基于不同协议的数学向量进行基于 NA 匹配规则的匹配操作。它还通过周期性的与"自己"库存储的正常网络连接模式进行匹配来检测"自己"是否发生变化,并调整阴性检测器集合的内容。如果异常检测器绑定到不正常网络连接模式,当绑定数量超过一定的阈值时,将激活异常响应部件并将不正常网络连接模式信息传给信号发生器。在本模型中,异常检测器集合发挥着计算机免疫系统中

检测器区分本体成分和非本体成分的作用。

(3)“自己”库。记录了描述正常网络连接模式的集合,发挥着生物免疫系统中 Ts 细胞的作用,当模式匹配器检测到非法网络连接时,就将此非法网络连接模式与“自己”库比较,如果发生匹配,则不引发警报。

(4) 异常响应部件。当异常响应部件被激活时将引发一系列措施去减缓或阻塞可能的不正常的网络连接。但它在攻击未被明确确定时作用是受限的,这样设定的目的是在攻击被明确确定前尽量减少对系统的影响。

(5) 信号发生器。其功能是在异常检测器绑定到不正常网络连接模式的数量超过一定的阈值时将不正常网络连接信息转换为系统受到攻击的信号,并激活响应发生器,通过这种转换可将基于异常检测系统所具有的学习能力引入基于误用检测系统中,可使系统对未来的攻击具有更有效和更精确的检测能力。在本模型中,信号发生器相当于计算机免疫系统中成熟非记忆 B 细胞的作用。

(6) 响应发生器。响应发生器接受系统攻击信号并产生针对这种攻击的对应措施。同时将攻击信号和对应的措施一起送到信号库。

(7) 信号库。信号库负责存储网络非正常连接模式信号和对应的反制措施。它在把攻击信号传送给模式匹配器的同时将对应的反制措施传送给滥用响应部件。通过这种方式本模型可对每一个系统已知的攻击进行检测和作出相应的处理。

(8) 模式匹配器。接收预处理器传来的数学向量并与信号库存储的模式进行匹配,如果超过一定的激活门限,则将信号库中存储的相应的非正常连接模式信号和对应的反制措施按照 Snort 的规则库的规则编写规范,这相当于检测器从非记忆状态转化为记忆状态。

(9) 滥用响应部件。该部件被激活时接收攻击所匹配的网络连接模式信息,并从信号库中查询相应的处理措施,然后对不正常网络连接行为进行处理。

(10) 规则库。当模式匹配器与信号库匹配检测到一个非法网络连接模式,同时与“自己”库进行匹配,如未发生匹配则引发滥用检测事件。此时模式匹配器将信号库中存储的这个非法网络连接模式和处理方法,按照 Snort 规则库的规范写入 Snort 规则库。这个过程就是免疫记忆的过程,所以 Snort 规则库相当于起到生物免疫系统的记忆细胞的作用。

3.3 免疫检测器的检测流程

(1) 向量转换器将网络连接模式信息并行地传到异常检测器集合和模式匹配器,同时开始异常检测和滥用检测。

(2) 异常检测器集合与网络连接模式信息进行匹配,如匹配次数超过一定阈值,则激活信号发生器将网络连接模式信息传给信号发生器并激活异常响应部件,使异常响应部件展开一系列措施去减缓或阻塞可能的不正常的网络连接。

(3) 信号发生器被激活后将非法网络连接模式信息传给响应发生器,响应发生器接受这种信息并产生针对这种非法网络连接模式信息的处理措施。并将这两者传给信号库。系统在此步骤中实现检测器从未成熟到成熟的非记忆状态的转换。

(4) 当模式匹配器通过与信号库的交互检测到一次非法网络入侵,且和“自己”库比较,未发生匹配,则触发滥用响应部件对此进行反应。同时将此种非法网络连接模式和处理方法依据 Snort 规则库的规范写入规则库。此过程实现检测器由成熟的非记忆状态转化为记忆状态。

4 实验及测试结果分析

4.1 实验数据

实验数据采用 KDDCup99 数据集。该数据集分成具有标识的训练数据和未加标识的测试数据。测试数据和训练数据有着不同的概率分布,测试数据包含一些未出现在训练数据中的攻击类型,这使得入侵检测更具有现实性。在训练数据集中包含了 1 种正常的标识类型 normal 和 22 种训练攻击类型(表 3)。另外有 14 种攻击类型仅出现在测试数据集中。

表 1 KDDCup99 入侵检测实验数据的标识类型

标识类型	含义	具体分类标识
Normal	正常记录	normal
DOS	拒绝服务攻击	back, land, neptune, pod, smurf, teardrop
Probing	监视和其他探测活动	ipsweep, nmap, portsweep, satan
R2L	来自远程机器的非法访问	ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster
U2R	普通用户对本地超级用户特权的非法访问	buffer _ overflow, loadmodule, perl, rootkit

本文实验中使用 KDDCup99 中的网络入侵检测数据包 kddcup_data_10percent 进行实验。

kddcup_data_10percent 数据包是对 kddcup_data 数据包 10%的抽样,10%抽样的结果是仅仅减少了 7 个类型记录的个数,对所包含的记录类型个数并没有改变。

4.2 实验结果与分析

文本实验结果如表 2 所示。

表 2 实验检测结果统计

类型	具体类型	测试包中数据量	正确检测数据量	检测率
DOS	back	1098	549	50%
	land	9	9	100%
	neptune	58001	57235	98.8%
	pod	87	87	100%
	smurf	164091	0	0%
	teardrop	12	8	66.7%
Probing	ipsweep	306	102	33.3%
	nmap	84	25	29.8%
	portsweep	354	118	33.3%
	satan	1633	1149	70.4%
R2L	ftp_write	3	2	66.6%
	guess_passwd	4367	4367	100%
	imap	1	1	100%
	multihop	18	16	88.9%
	phf	2	2	100%
	spy		无	
	warezmaster			
	warezclient	1602	713	44.5%

由表 2 可见,系统对于 land, neptune , pod, guess_passwd, imap, phf, multihop 共 7 种攻击行为的平均检测率为 98.24%;对其它 11 种攻击类型行为的平均检测率为 43.76%;全部 18 种攻击类型行为的平均检测率为 64.94%。

将攻击行为分为 DOS, Probing, R2L 三类,实验系统对三类型攻击行为的检测率分别为 62.93%, 41.67%和 83.33%,

系统相对于全部样本的平均检测率、误报率分别为 60.47% 和 30.65%(表 3)。

表 3 各类攻击事件检测统计结果

攻击类别	检测率	平均检测率	误报率
DoS	69.23%		
Probing	41.67%	60.47%	30.65%
R2L	83.33%		

表 4 DARPA 入侵检测系统评测大会评测结果

系统	检测率
Forensics	55.56%
Expert1	50.30%
Expert2	46.83%
Dmine	40.20%

表 4 为 1999 年美国 DARPA 入侵检测系统运用 KDD-Cup99 中的网络入侵检测数据包的非抽样数据的评测结果。

比较不难发现,本文设计的基于免疫学原理的混合入侵检测系统在检测性能方面较美国 DARPA 入侵检测系统稍好,有进一步完善之必要。

参 考 文 献

[1] 刘克胜,曹先彬,郑浩然,等. 基于免疫算法的 TSP 问题求解. 计算机工程,2000,26(1):1-2

[2] 陈波,于怜. 基于人工免疫的网络入侵检测[J]. 计算机工程与应用,2002,22:165-167

[3] Dipankar D, Yu S, Majumdar N S. MILA-Multilevel Immune Learning Algorithm// the Proceedings of GECCO. 2003

[4] Kim, Bentley. Immune Memory in the Dynamic Clonal Selection Algorithm// 1st International Conference on Artificial ImmuneSystems (ICARIS-2002). University of Kent at Canterbury, UK, 2002.9

[5] Xie Gang, Xu Xingying, Xie Kerning, et al. Clone mind evolution algorithm. Lecture Notes in Computer Science, v 3611, n PART II, Advances in Natural Computation // First International Conference, ICNC 2005. Proceedings, (EI: 05439427285, SCI: 000232222500132),2005: 945-950

(上接第 49 页)

(5)为检验条件,通过分析各参数之间的关系,从而确定合理的"分层组合导引协调树"的结构。

4.5 MSMIPS 协商控制的策略

"软件人"之间的协商控制采用部分——全局规划(Partial Global Planning,PGP)策略,它是一种典型的分布式协商技术,其特点是每个 SM 都能收集目前的状态,又能收集其他 SM 的目标信息。因此,PGP 提供了 SM 间的灵活协调,保证了各 SM 间的交互。PGP 通过不同局部计划间的交互,可以避免 SM 间的任务冗余,特别是当多个 SM 计划具有相同的中间目标时会发出告警通知。每个 SM 都维护自身的 PGP,独立且异步地使用 PGP 来协调各自的行为,从而实现全局任务。

结束语 本文研究的目的在于,将群体"软件人"智能检测技术和先进的分布式体系结构相结合,构建一种新型的入侵防御系统体系结构。为了实现此目的,提出了基于群体"软件人"入侵防御系统的智能协商控制模型及相应的算法。该模型充分利用各个"软件人"之间相互协作却又相互独立的特性,系统结构具有很好的伸缩性、灵活性、扩展性、自学习能力、容错能力、分布式控制和攻击预防能力等。它能有效地解决传统入侵检测技术对异构系统和大规模高速网络检测的明显不足,以及在不同的入侵检测系统之间数据量大且集中、负载不均衡、不能协同工作等。本课题下一步的研究方向包括:1)将"软件人"技术与入侵检测系统结合,利用其优势互补设计基于群体"软件人"的智能入侵防御系统;2)针对群体"软件人"的检测分析算法及自身的安全进行更深入地研究,使入侵防御系统的智能化程度、检测性能、可操作和维护性将有大幅度提升。相信随着研究的深入,基于群体"软件人"的智能入侵防御系统会得到不断地完善,它的应用也将更为广泛。

参 考 文 献

[1] Snapp S R, Brentano J, Dias G V, et al. DIDS (Distributed Intrusion Detection System)-Motivation, Architecture, and An Early Prototype// Proc. of the 14th National Computer Security Conf. Vol 10. Washington, 1991:167-176

[2] White G B, Fisch E A, Pooch U W. Cooperating Security Managers: A Peer-based Intrusion Detection System. IEEE Network, 1996, 10(1):20-23

[3] Asaka M, Taguchi A, Goto S. The Implementation of IDA: An Intrusion Detection Agent System// Proc. of the 11th FIRST Conf. 1999. Brisbane, 1999

[4] 褚永刚. 大规模分布式入侵检测系统关键技术研究. 博士学位论文. 北京:北京邮电大学, 2005:65-72

[5] 曾广平,涂序彦. 软件人[A]// 中国人工智能学会第 10 届全国学术年会论文集[C]. 北京:北京邮电大学出版社, 2003:677-682

[6] Tu X Y, Zeng G P, Tang T. HADS: Humanized Autonomous Decentralized Systems [A]// Proc. of the International Symposium on Autonomous Decentralized Systems (ISADS'2005) [C]. 2005:593-598

[7] Lu Q L, Zeng G P, Tu X Y. SoftMan and Agent [A]// Proc. of the International Conference on Networking, Sensing and Control (ICNSC'2005) [C]. Tucson, AZ, USA, March 2005

[8] Zaki M, Sobh T S. Attack Abstraction Using a Multiagent System for Intrusion Detection [J]. Journal of Intelligent & Fuzzy Systems, 2005,16:141-150

[9] Dasgupta D, Gonzalez F, Yallapu K, et al. CIDS: An Agent-based Intrusion Detection System [J]. Computers & Security, 2005,24:387-398

[10] Dasgupta D, Rodriguez J, Balachandran S. Mining Security Events in a Distributed Agent Society [A]// Proc. of the Conference on Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security, part of SPIE Defense and Security Symposium-2006 [C]. Orlando, Florida, April 2006

[11] Azzedine B, Renato B M, Kathia R L, et al. An Agent-based and Biological Inspired Real-time Intrusion Detection and Security Model for Computer Network Operations [J]. Computer Communications, 2007,1:1-14

[12] Zeng G P, Tu X Y, Zhang S M. Study on the Organization Models of SoftMan Group [A] // Proc. of the International Conference on Networking, Sensing and Control (ICNSC'2005) [C]. 2005