人工免疫机制在木马检测系统中的应用研究

陈雷霆，张 亮

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】指出了当前反病毒软件在检测未知木马方面的不足，介绍了人工免疫系统在反病毒软件自适应性方面的优点，以及人工免疫机制在木马检测方面的可行性；通过对木马新技术的分析，用一个木马模型证明了现在计算机安全体系的不足，提出将木马检测从反病毒软件中迁移到免疫型入侵检测系统中作为子系统，利用其免疫机制来提高木马检测的自适应能力；并同时提出了依据进程的系统资源使用状况来映射进程的系统调用的行为模式，以此建立了基于人工免疫机制的木马检测模型。

关 键 词 网络安全; 人工免疫; 特洛伊木马; 入侵检测

中图分类号 TP393.08 文献标识码 A

Research of Trojan Detection System Based on Artificial Immune

CHEN Lei-ting，ZHANG Liang

(School of Computer Science and Engineering, UEST of China Chengdu 610054)

Abstract This paper points out the deficiency in detecting the unknown Trojan horse of the present anti-virus software at first, introduces the advantage of artificial immune system in self-adaptability aspect, and points out the feasibility of artificial immunity mechanism in Trojan horses detection; Then through an analysis about the new technology of Trojan horses, proves the deficiency of current computer security system with a Trojan horses model, presents the transfer of Trojan horses detection from the anti-virus software to the subsystem of immune IDS, improves the self-adaptive capacity of Trojan horses detection with its immune mechanism; Finally, a behavior mode is put forward, which is mapped from the using situation of process systematic resource to the process systematic call, and by this means, a Trojan horse detection model based on artificial immunity mechanism is set up.

Key words network security; artificial immune; Trojan horse; intrusion detection

特洛伊木马(此后简称木马)作为一种危害极大、难以被检测的攻击工具，通常被反病毒软件作为病毒来处理。反病毒软件的目标侧重于清除病毒，要求采用准确的模式匹配方法来确诊病毒的特征代码，因此，决定反病毒软件自适应能力的发展面临两难境地。此外，木马具有特殊的隐蔽性和反检测性，对木马采用病毒检测的方法，效果往往不佳。近年来，基于人工免疫机制的入侵检测系统(Intrusion Detection System，IDS)研究以其自适应性方面的优越性而成为计算机安全研究的热点，可以考虑将木马检测系统并入到免疫型IDS中，以提高木马(尤其是未知木马)检测的智能水平。

1 免疫型IDS模型

按照检测数据的来源可以将IDS系统分为两类，一类是基于主机的入侵检测系统(Host-Based Intrusion Detection System，HIDS)，其检测数据的来源是主机上操作系统的审计日志；另一类是基于网络的入侵检测

收稿日期：2004－05－13

基金项目：国家863计划项目(2002AA142040)；四川省科技攻关项目(03FG013-008)

作者简介：陈雷霆(1966－)，男，在职博士，副教授，主要从事网络信息安全、网络多媒体方面的研究；张 亮(1975－)，男，硕士，研究生，主要从事网络安全方面的研究.

系统(Network-based Intrusion Detection System，NIDS)，其检测数据的来源是网络上的数据流。文献[1]提出过一个基于免疫的多Agent的NIDS模型，通过流动在网络上的多级Agent的相互协同而实现入侵检测，但缺点是系统负载太大。文献[2，3]提出了一个主从模式的免疫型IDS模型，该模型由两部分构成，通往子网络的两个路由器之间的一台主机构成主IDS，子网络中若干台主机构成从IDS。在主IDS上存储着一个用于生成未成熟检测体的基因库，通过基因重组形成不成熟检测体，再通过基于小生境策略的阴性选择和克隆选择过程产生非自身抗原的成熟检测体，并传送到从IDS。若某个从IDS上的成熟检测体成功检测到了入侵行为，它将成为记忆检测体，其检测信息将反馈给主IDS以实现基因库的进化，生成其克隆并传播到其他的从IDS上，以使每个从IDS都具有针对该入侵行为的检测能力。主IDS和从IDS上都有通信器，相互之间可以传送信息。

通常，HIDS都是分布在网络中的每台主机上，如果与NIDS实现联动，HIDS收集的主机信息可以反馈给NIDS，并协助NIDS更准确地判断网络入侵行为，NIDS收集的网络信息也要反馈给HIDS，以帮助HIDS更准确地分辨主机入侵行为，尤其是蠕虫和木马这些通过网络进行传播和通信的攻击工具。

2 特洛伊木马的分析

特洛伊木马常被用作网络系统入侵的重要工具和手段。木马寄生在计算机中，利用用户的疏忽来窃取密码和提升权限，或利用一些操作系统自身的漏洞(如缓冲区溢出等)最终获取管理员权限，修改审计日志，隐藏自己的踪迹，并植入后门。木马用作后门后，采用客户端/服务器端的方式与入侵者进行通信，而成为入侵者扩大攻击范围和隐藏踪迹的跳板，为其他入侵活动提供可能。

现在，对特洛伊木马检测和防御的方法分为两类：一类是通过建立木马特征字典来防范木马，如反病毒软件检查被感染系统和文件是否包含木马特征，NIDS通过包过滤检查网络数据包中是否包含木马特征；另一类是通过对文件或系统的完整性进行检查来防范木马，如利用单向的哈希函数来生成文件或系统的数字签名，HIDS通过对操作系统的审计日志的分析来检测木马。

以上两类方法都属于被动检测方式，对木马的入侵存在着反应迟钝和智能化不足的缺点，尤其是缺乏检测未知木马的自适应能力。目前，对基于计算智能尤其是人工免疫机制的IDS的研究，国内外开展了多项研究，并提出了不少模型。但是，针对木马的检测还没有进行太多的探讨。

3 基于人工免疫机制的木马检测模型

3.1 基本原理

新墨西哥大学的Forrest在反病毒和主机入侵检测研究方面有着较大的影响。文献[4]运用免疫机制来检测程序和受保护数据的异常改动，其实验结果显示，这种方法能够很容易地发现病毒感染引起的数据文件的改变，并且能够检测未知的病毒。文献[5]进一步利用免疫机制进行进程监视，目的是为了检测对主机的入侵活动。根用户(系统管理员)进程的系统调用比其他用户进程更具有潜在危险性，而且在正常情况下，每个根用户进程的系统调用在顺序上有着自己相对稳定的行为。

但是文献[4]和文献[5]的Forrest模型也存在一定不足，由于系统调用的类型种类繁多而且还在不断增加，定义系统调用类型成了一个与自适应要求背道而驰的问题。在Forrest研究的基础上可知，进程的系统调用序列遵循着相对稳定的行为，而不同的系统调用通过对各种系统资源的占有、消耗、放弃、回收也会表现出相对稳定的资源使用行为特征，并且系统资源的类型也是有限的、非常稳定的。根据这一前提，可以将进程以时间为轴的资源使用状况曲线离散化，所得到的进程资源使用状况序列可以有效地表示为计算机系统的“自我”。本文的木马检测模型中仍存在着相对稳定的自体抗原，但自体抗原有着比较明显的新生、演变和凋谢的基因进化过程，这是木马检测模型与其他人工免疫系统不同的地方。

3.2 抗原和抗体的定义

木马检测模型每天跟踪和记录主机上进程的各种系统资源的占用情况(如CPU占用时间、内存占用空间、外部存储器占用时间、IO占用时间、网络占用时间和带宽等)，并以T时间的间隔对其进行采样，建立以一天的时间为长度的资源使用状况曲线的离散序列，最后将它们保存为自体抗原数据段。同时，将木马进程

和木马寄生进程的资源使用状况曲线的离散序列定义为非我抗原，将非我抗原的检测体定义为抗体。由于进程大量存在着对某种功能的反复调用，自体抗原可以通过自我“提纯”减少冗余数据量。为了进一步减少数据量，将采用增量值的方法记录下相邻时间之间的数据量变化值。抗原的结构由不变区和可变区构成，如图1所示。

不变区				可变区
进程名	资源类型	路　径	文件长度	进程的系统资源使用序列

图1　抗原/抗体结构图

不变区包括进程的信息(如进程名、路径、文件长度等)、资源类型等；可变区则是二进制化的系统资源使用状况的离散序列，长度不定。在本文的模型中，将每天得到的数据记录作为一个抗原决定基，假如有M种资源类型，每个自体抗原会有$D\times M$个抗原决定基。检测体(抗体)的结构类似于抗原。经过D天的耐受期后，将得到的所有自体抗原集合成系统的自体抗原基因库。

3.3　免疫应答模型

免疫应答模型如图2所示。检测体(抗体)的产生，是在阴性选择器中通过小生境策略算法生成抗体序列数据，然后与不变区构成不成熟的检测体。根据阴性选择原理，检测体在经过自体耐受后，被释放到检测空间中执行检测任务。在检测到非己抗原后，该抗体执行克隆选择，克隆出的抗体通过几轮阴性选择和克隆选择后得到成熟的检测体集合。

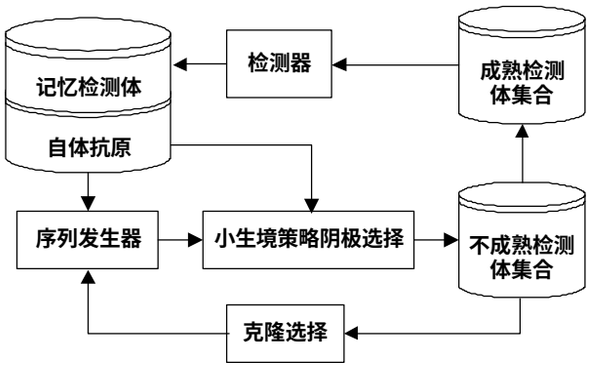

图2　免疫应答模型

检测算法可以采用所属IDS的算法，比如连续r位匹配算法。该算法描述为，当连续匹配的位数大于等于r值时，两个序列匹配，否则不匹配。在产生算法设计中，利用连续r位的匹配规则，可实现以较小的检测器集合检测到较大范围的“非我”行为。同时，可对多种资源的检测结果进行综合，以得出最全面的评价结果，减小误报的概率。定义N为资源类型数量，P_i为某种资源的检测匹配度，A_i为某种资源的加权值，从而得到以下的匹配度的评价公式 $P_r=\sum_{i=1}^{N}A_iP_i$，在该匹配度P_r超过某一阈值Q_r后，检测模块向管理模块发出警告，由管理模块运用预定义的反应策略进行处理。如果检测模块没有及时收到回复，系统则通过通信模块和其他主机上的NIDS和木马检测HIDS进行通信，由它们加强对来自本系统的信息进行严密监视。在等待一段时间Tn以后，汇集来自其他HIDS和NIDS的反馈信息，对匹配度的评价公式修改为 $P=P_r+\sum_{j=1}^{M}B_jP_j$，式中，$M$为其余HIDS和NIDS的数量，$B_j$为采信度，$P_j$为其他主机上的NIDS和木马检测HIDS得出的匹配度评价值。在该匹配度P超过某一阈值Q后，系统再次向管理模块发出警告，并写入安全日志。在得到管理模块的审查确认以后，该检测体将被录入记忆检测体集合中。

3.4　基因库的进化

在本文的木马检测模型中，抗体具有进化机制，自体抗原也经历着缓慢的进化过程。首先，在系统资源监视器中产生新的自体抗原，通过特征“提纯”，清除数据序列中冗余特征序列段。“提纯”算法可以将数据序列分成几个子序列，将相同的数据片段进行合并，清除冗余的数据；然后，“提纯”的自体抗原和基因库中的自体抗原进行比较，如果类似则被抛弃，反之则进一步筛选。

本文利用 $r^2=\left(\sum_{i=1}^{N}(X_i-\bar{X})(Y_i-\bar{Y})\right)^2\Big/\sum_{i=1}^{N}(X_i-\bar{X})^2\sum_{i=1}^{N}(Y_i-\bar{Y})^2$ 的相关系数公式来计算自体抗原之间的相关性。相关系数产生一个(0, 1)的数，该数关系到两个输入序列的相似性，其定义为X，$Y\in\{0, 1, \cdots, 255\}^N$，$N=L/8$，$L$为序列长度。筛选步骤如下：首先合并基因库中的自体抗原和当前的自体抗原候选集合；然后计算所有自体抗原的数据段之间的相关性，可以得到一对相关性最大的自体抗原；继续选择两者各自相关性集合的最大值进行比较；依次类推，最终筛选出被淘汰的自体抗原。自体抗原进化模型如图3所示。

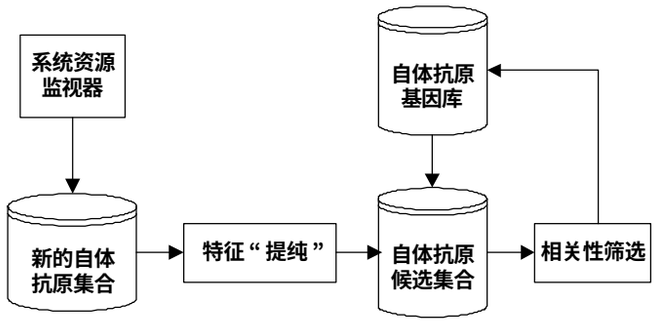

图3 自体抗原进化模型

3.5 特殊的安全策略

拥有根用户(系统管理员)权限的木马对HIDS及木马检测系统本身也有着巨大的威胁，因此本文的模型需要特殊的安全策略。

1) 自我保护机制。本文的木马模型引入数字签名技术对程序和关键数据进行保护，采用启动多个监视进程只激活其中一个的策略，一旦其中一个进程被木马删除，其他的进程可以激活和恢复被删除进程。2) 分布式数据存储。本文采用分布式的数据存储方法，将数据的副本传送给其他的HIDS，保存在其他的主机上。

3.6 木马模型的总体设计

基于人工免疫机制的木马检测系统设计了一个管理模块，分别由管理控制、通信接口、安全日志和人机交互四个子模块组成。在管理模块的控制下，检测器执行检测并经过管理控制模块审查提交记忆检测体；管理控制模块根据需要访问基因库，与其他HIDS交换基因信息，把对检测数据的分析结果和入侵检测的警告信息保存到安全日志中，同时和其他HIDS和NIDS交换日志，以实现分布式数据存储。而所有的外部通信都由通信接口模块负责。人机交互模块是与管理员进行交互的接口，它包含一个安全策略子模块，其中定义了一些默认的安全策略，当管理员不在的时候指导管理控制模块处理相应的事务。

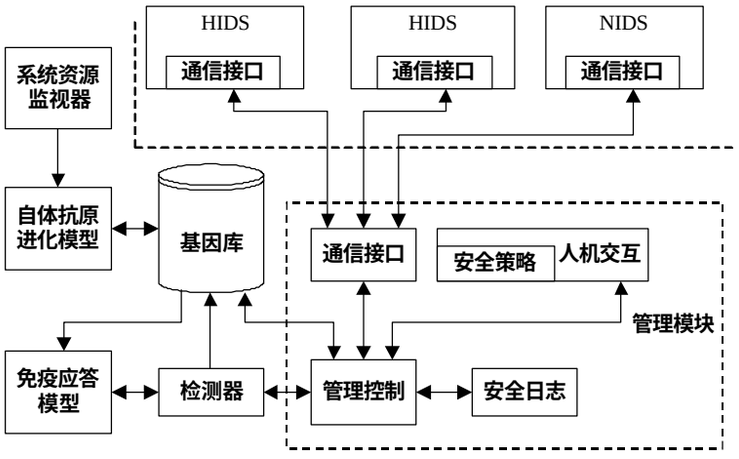

图4 基于人工免疫机制的木马检测系统模型

4 结 束 语

基于人工免疫机制的木马检测系统是基于主机的检测模型，而且提出了自体抗原的进化问题，无疑会增加主机的负担，因此，如何提高自体抗原的进化算法和其它免疫算法的效率，如何确定模型中定义的耐受时间、采样间隔、激活阈值等，是下一步重点研究的内容。如何与IDS实现良好的联动，如何防御和清除木马、恢复被感染的系统也有待进一步探索和研究。

参 考 文 献

[1] Dasgupta D. Immunity-based intrusion detection system: a general framework [C]. Proceedings of the 22nd National Information Systems Security Conference, NIST Publishers, Crystal City, 1999

[2] Kim J, Bentley P. The artificial immune model for network intrusion detection[C]. 7th European Conference on Intelligent Techniques and Soft Computing. Aachen, Germany, 1999. 13-19

[3] Kim J, Bentley P. Negative selection and niching by an artificial immune system for network intrusion detection[C]. GECCO’99, Orlando, Florida, 1999

[4] Forrest S, Perelson A, Allen L, et al. Self-nonself discrimination in a computer[C].In: Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, 1994, 202-212

[5] Forrest S, Hofmeyr S, Somayaji A, et al. A sense of self for unix processes[C]. Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, 1996. 120-128

编 辑 熊思亮