一种基于免疫系统原理的信息安全系统新模型

于 涵[1], 王 毅[2], 沈昌祥[3]
(1. 解放军信息工程大学, 河南郑州 450004; 2. 哈尔滨工业大学信息对抗技术研究所, 黑龙江哈尔滨 150001;
3. 海军计算技术研究所, 北京 100841)

摘 要: 信息安全系统可以从人体免疫系统的很多特点中得到启发. 在本文利用人体免疫系统机制和信息安全系统之间的可比性设计了一个新的框架模型. 该模型可以实现对重要信息的安全保护. 该框架包含两个平行的信息传输网络: 传统传输网和免疫淋巴网. 传统传输网提供端到端服务, 将重要信息从一个端点传输到另一个端点. 免疫淋巴网提供校验和控制服务, 用来监控和管理传统传输网的行为. 本文还讨论了移动代理的安全性. 本文针对免疫系统特点进行了相应的验证实验. 实验结果表明该模型对于信息安全问题有较好的敌我识别功能.

关键词: 免疫系统; 信息安全; 移动代理
中图分类号: TN911 文献标识码: A 文章编号: 0372-2112 (2006) 12A-2455-03

A New Model of Information Security System Based on Immune System

YU Han[1], WANG Yi[2], SHEN Chang-xiang[3]
(1. *The PLA Information Engineering University, Zhengzhou, Henan 450004, China*; 2. *Institute of Information Countermeasure Technology, Harbin Institute of Technology, Harbin, Heilongjiang 150001, China*; 3. *Computing Technology Institute of China Navy, Beijing 100841, China*)

Abstract: The human immune system has many features for inspirations to information security. We design a framework model using an analogy of human immune mechanism. This model can be used to provide the protection for the safety of important information. The suggested framework consists of two parallel information transmit networks: conventional transmit network (CTN) and immune lymphoid transmit network (ILTN). conventional transmit network provides the end to end services and transmits important information from one end-point to another. Immune lymph transmit network provides authentication and control services that monitor and manage the activities of conventional transmit network. We also discuss a solution to the security of the mobile agent. This paper also accomplished corresponding experiments. The results of the experiment showed that the use of this model is very efficient for the problem of discrimination of the self and norr-self.

Key words: immune system; information security; mobile agents

1 引言

人体免疫系统非常复杂, 它由上亿个细胞组成, 这些细胞并行地防御成千上万的病原体, 使人体免受病原体的入侵. 人体免疫系统检测并消灭病原体对人类的生存至关重要. 如果没有免疫系统, 人可能在几周内就会死亡[1]. 在信息安全领域, 我们可以从免疫系统中得到启发. 人体中免疫系统的作用可以同计算机中的安全系统相类比. 尽管免疫系统和计算机安全系统仍然有很多不同, 但是可类比性在很大程度上可以为改进计算机系统的安全指明了方向.

1974年, 美国诺贝尔奖获得者Jerne提出了免疫网络理论, 引起了世界关注. Farmer、Perelson、Bersini、Varerla等理论免疫学者分别在1986年、1989年和1990年发表了相关论文. 将免疫系统原理应用到计算机安全可以追溯到1994年. Stephanie Forrest和她的研究小组在计算机上建立了一个人工免疫系统[2], 将免疫系统手段用于计算机安全和病毒检测. Kim等[14]在基于免疫学的网络入侵检测系统(IDS)方面进行了研究, 他们比较了生物体免疫系统与IDS的相似性, 证明了免疫系统能够满足IDS的要求. 随着网络的普及, 对计算机系统的安全性研究变得越来越重要, 越来越多的研发人员开始从事这个崭新的研究领域.

从结构上讲免疫系统是多层次的, 可以在多个层次上对病原体进行防御. 免疫系统和血液系统是人体两大液体系统. 尽管免疫系统和血液系统一样在人体全身循环. 但是, 免疫系统在大部分时间并不工作. 免疫系统只有在病原体穿过人体的初级免疫系统后才工作. 所以, 免疫系统可以看作是血液系统的监视器或者控制器[3], 免疫网络与血液循环网彼此独立. 但是现有的人工免疫系统并没有将数据传输网和免疫网络分离开, 这样系统的使用效率会受到很大影响, 同时免疫系统自身的安全性无法得到保证. 本文根据人体多层次免疫防御思想, 试图建立一个信息安全系统模型. 在这个模型中, 其中一个网络就像血液系统一样只将数据从一个端点传送到另外一个端点, 我们称这个网络为传统传输网(Conventional Transmit Network, CTN). 另外一个网络负责监控传统传输网, 我们称之为免疫淋巴网(Immune Lymph Transmit Network, ILTN). 一旦发现有恶意攻击, 免疫淋巴网将处理这些问题, 将发送移动代理来攻克入侵者. 两个网络彼此独立, 保证了系统的效率与可扩展性. 同时, 本文采用基于CA的免疫代理认证方式, 提高了

收稿日期: 2006-04-13; 修回日期: 2006-11-25
基金项目: 国家863计划(No. 2005AA733120)

免疫系统自身的安全性.

本文的组织结构如下:第二部分概要介绍免疫系统.第三部分指出基于免疫系统原理的新型信息安全模型框架.第四部分是结论和后续的工作展望.

2 免疫系统概述

人体免疫系统是一个抵抗外部侵袭的完美攻防体系,它为人体各项机理的正常工作提供了保障.人体免疫系统由特殊的细胞、组织、器官组成,它通过产生免疫应答来实现对外部物质和病原体的有效控制[4].

人体免疫系统有两大主要问题:识别和探测入侵者或病原体,有效消灭和杀死有害入侵者.传统观点认为免疫系统的主要功能是识别"自我"和"非我".最近,一些科学家认为免疫系统的主要功能是为了保持人体的动态平衡.这两种观点强调了免疫系统的两个不同的功能.不论这两种观点哪个更正确,有一点可以达成共识的是,免疫系统的主要功能是保护人体的安全.从这个角度出发,本文将建立一个安全模型来保护信息传输系统的安全.

最重要的人体免疫系统是淋巴系统,它和血液系统一起构成人体最重要的两个液体系统.血液系统将血液从心脏流向动脉,然后流向毛细血管,最后通过静脉返回到心脏.淋巴系统淋巴液流经淋巴血管和淋巴器官.这两个系统在人体中相互交融,保证了人体正常的生理功能.在免疫系统中,脾、胸腺、阑尾和骨髓等淋巴器官产生大量的细胞,这些细胞称为白细胞.有两种基本的白细胞:噬菌细胞和淋巴细胞.噬菌细胞用来吞噬入侵的病原体或者细菌;淋巴细胞用来识别特殊的病原体并进行记忆,保证再次遭受相同病原体攻击时能迅速进行应答.淋巴细胞分布式存在于全身,而且可以独立地消灭外来抗原.最重要的两种淋巴细胞是 B 型淋巴细胞和 T 型淋巴细胞.淋巴细胞在其表面携带抗原受体.每个淋巴细胞可以有多个相同的受体.这些受体对一个特定的抗原特异.识别过程发生在淋巴细胞的受体绑定了病原体的抗原决定基.绑定的强度取决于亲和力.抗体只呈递一种单独类型的受体,而抗原可能呈递很多抗原决定基.这意味着一个抗原可以被多个不同的抗体识别.

3 新的模型框架

人体免疫系统保护人体免受病原体的侵袭.类似地,一个信息安全系统可以保护计算机免受入侵.我们可以用免疫系统的解决方式来处理信息安全系统所面临的问题[5].我们希望建立一个动态的网络模型来防止网络入侵.

特别地,人体免疫系统识别和消灭像病菌这样的病原体但不能损害组成我们身体的细胞或组织.同样地,一个理想的安全系统应该能够监测和防止异常和未授权的计算机行为,而不会影响计算机系统的正常应用[6].

新型的信息安全模型的主要框架如图 1 所示.这个框架包含两个并行的信息传输网络:传统传输网和免疫淋巴网.建立两个传输网络的思想源于人体免疫系统.在第二部分已经提过,淋巴系统和血液系统是人体的两个主要的液体系统,他们共同工作来保证人体的安全.传统传输系统提供端到端的服务,将重要信息从一个端点传输到另一个端点.而免疫淋巴网提供校验和控制服务,用来监控和管理传统传输网的行为.

这两个网络在端点处连接在一起.端点可能是一台计算机、网络通信设备或者是其他工作在传输网络上的实体.端点可以类比为免疫系统的淋巴结.

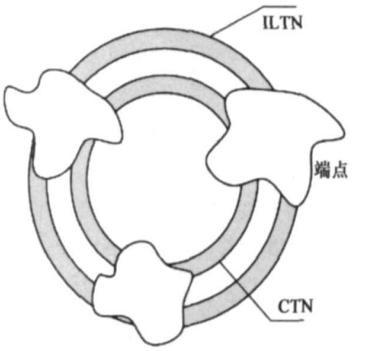

图 1 新型的信息安全模型框架

保证信息系统的安全不是一次或者静态的处理过程.相反地,应该是一个动态的、反复的过程[7].另外,人体免疫系统的自治性、分布式和多层结构特点提示我们可以利用 agent 技术实现信息安全系统的设计.

Agent 在某种情况下讲是无人管理的,它完全由自己来控制.从结构上说,agent 是一组传感器、决策器和激励器的组合.从行为上看,agent 是内部空间到外部空间的映射[8].当 agent 收到一项任务,它可以自己来实现这个独立的工作,也可以将这个任务分成多个子任务,然后从一系列候选的 agent 中选择更合适的 agent 来执行这个子任务.

在我们的信息安全系统模型中,我们定义三个 agent:监控 agent、管理 agent 和执行 agent.在这个框架中,不同的 agent 可能相互协作.他们可能在传统传输网和免疫淋巴网中穿行.这个过程由图 2 所示.

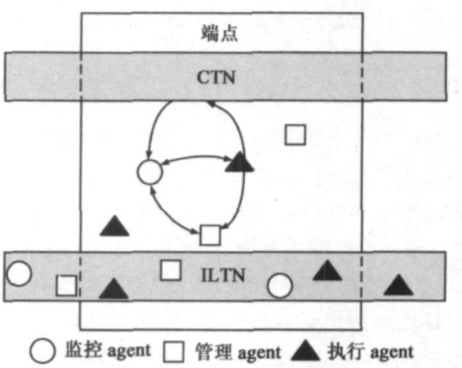

图 2 新模型中的三种 agent

不同类型的 agent 的功能是独特的,但是不同类型的 agent 可以在一起相互协作.监控 agent 在各个端点之间巡游,并且检查无效或者未授权的进程.它通过产生字符串来进行模式匹配[9].监控 agent 的作用和 B 型淋巴细胞的功能非常相像[10].当和外部的网络连接上以后,就会产生监控 agent 来监视端点的输入.而且当一个新的进程被检测出是外部进程时,监控 agent 就会产生并监视该进程.

管理 agent 用于控制连接的状态.比如,连接所用的协议和端口号,数据包的编号等.管理 agent 可以用于在多个 agent 之间携带消息并进行协商.它还可以控制执行 agent 对非授权进程采取行动.这和人体免疫系统淋巴腺体分泌 T 型淋巴细

胞来刺激 B 型淋巴细胞消灭病原体的功能非常相似.

执行 agent 根据安全状况来执行特定的工作. 比如, 当一个未授权的入侵被监控 agent 检测出来以后, 执行 agent 将切断整个连接并关闭端点. 然后, 执行 agent 将记录该过程并将入侵信息传送到信息系统的中心数据库. 执行 agent 还会对一些可能出现的安全漏洞进行适当的补救.

Agent 增加了通信任务的灵活性, 但是灵活性是在增加易受攻击为代价的. 在这个模型中, 我们同样考虑了 agent 的安全性问题[11]. 根据抗原决定基的原理, 我们得到数字抗原决定基的概念[12]. 每个 agent 可以利用公钥密码术来进行数字签名. 这样就能够有效区分出独特的 agent. 根据这种思想, 将为进行通信的每个 agent 产生一个证书. 我们还可以利用 CA 技术解决颁发证书的问题[13]. CA 可以控制签发和撤销证书. 出于安全考虑, CA 可以建立在信息系统中心, 可以建立多层次的可信任的模型. 因此, agent 可以互相监控并检测到恶意的 agent. CA 可以撤销颁发给该恶意 agent 的证书, 从而保证了信息安全系统的安全性.

4 实验结果

为了验证本模型的有效性, 本文选用 http://iris.cs.uml.edu:8080/ 中使用的标准自我和非我数据库. 该数据可以通过 Sniffer 等网络抓包工具获得的. 主要表示在网络入侵情况下, 如 IP 欺骗攻击情况下的数据. 测试主要针对通信类型、源端口、目的端口、协议类型等信息来确定攻击者的信息. 实验结果表明免疫应答时间随着负载包大小的增加逐渐增加.

表 1　负载包大小对应的免疫应答时间

负载包大小	免疫应答时间
1k	0.0120s
4k	0.0197s
16k	0.0543s
64k	0.1051s
256k	0.3346s
1M	0.6004s
2M	1.0301s
4M	1.3522s

表 2　攻击次数对应的免疫应答时间

攻击次数	免疫应答时间
1	2.3522s
2	1.0197s
3	0.0243s
4	0.0102s
5	0.0061s
10	0.0004s

本文还测试了及在第一次遭受攻击和在多次遭受相同攻击情况下的反应时间. 实验结果如表 2 所示. 实验结果表明在多次遭受攻击的情况下, 该系统能够进行迅速的免疫应答.

5 结论

本文提出了一个基于人体免疫系统的新模型. 在这个模型中, 我们吸收了免疫系统的多个值得借鉴的基本原理, 根据这些基本原理建立一个安全有效的智能信息系统. 我们利用 agent 技术提供动态、可扩展的检测方式. 本文还讨论了 agent 的安全性问题. 今后的工作集中如何在执行过程中改变或修复 agent, 从而建立更为复杂和完整的信息安全框架. 另外, 建立一个标准的 agent 通信安全协议将是解决信息安全系统的更有效的方案.

参考文献:

[1] Male D. Immunology-An Illustrated Outline[M]. New York: Gower Medical Publishing Ltd, 1986.

[2] Hofmeyr S A, Forrest S. Architecture for an artificial immune system[J]. Evolutionary Computation. 2000, 7(1): 45- 68.

[3] Forrest S, Hhfmeyr S A, Somayaji A. Computer immunology[J]. Communications of the ACM. 1997, 40(10): 88- 96.

[4] Alberts B. Molecular Biology of the Cell[M]. New York: Garland Science, Taylor & Francis Group, 2002.

[5] Boukerche A, Notare M S M A. Conception, Analysis and Development of a Security Management System for Telecommunication Networks[D]. Brazil: Federal University of Santa Catarina, 2000.

[6] Timmis J I. Artificial Immune Systems: A Novel Data Analysis Technique Inspired by the Immune Network Theory [D]. Aberystwyth: University of Wales, 2000.

[7] Harmer P, Williams P, Gunsch G, Lamont G. An artificial immune system architecture for computer security applications[J]. IEEE Transactions on Evolutionary Computation, 2002, 6(3): 252- 279.

[8] Harmer P. A Distributed Agent Architecture for a Computer Virus Immune System[D]. US: Air Force Inst. Technology, Wright Patterson AFB, OH, 2000.

[9] Dasgupta D, Dasgupta D. Artificial Immune Systems and Their Applications[M]. Heidelberg, Germany: Springer Verlag, 1999.

[10] Dasgupta D, Nino F. A comparison of negative and positive selection algorithms in novel pattern detection[A]. Proc IEEE Int Conf on Systems, Man and Cybernetics[C]. Nashville, 2000. 125- 130.

[11] Gray R S. Agent Tcl: A flexible and secure mobile-agent system[A]. Proc. 1996 Tcl/Tk Wksp[C]. Milano, Italy: Springer Press, 1996. 9- 23.

[12] Gary M, Johannes P R, Anoop S. ANSWER: network monitoring using object-oriented rules[A]. Proceedings of the Tenth Conference on Innovative Applications of Artificial Intelligence [C]. Madison, Wisconsin: AAAI Press, 1998. 1087- 1093.

[13] Housley R. RFC 2459, Internet X.509 Public key Infrastructure Certificate and CRL Profile[S]. 1999. 12- 26.

[14] Kim J, Bentley P. The human immune system and network intrusion detection[A]. 7th European Congress on Intelligent Techniques and Soft Computing (EUFTT'99) [C]. Aachen, Germany: Verlag Mainz, 1999. 13- 19.

作者简介:

于 涵　男, 1974 年 8 月出生于江苏盐城, 现为解放军信息工程大学博士研究生. 研究方向为信息安全.

王 毅　男, 1982 年 8 月出生于黑龙江省哈尔滨市. 2005 年毕业于哈尔滨工业大学自动化测试与控制系. 现为哈尔滨工业大学硕士研究生.

沈昌祥　男, 1940 年 8 月生, 中国工程院院士, 博士生导师, 海军计算技术研究所研究员. 研究领域: 信息安全.