An Object-immunity-based Intrusion Detection System for the Internet Banking System

基于对象免疫的入侵检测系统及其在网上银行的应用

胡 翔 华建兴 （上海交通大学计算机科学与工程系 200000）

摘要：本文采用对象免疫的思想，提出一个入侵检测系统的构建方法，着重探讨对象免疫入侵检测的机理、实现方法以及系统模型，并介绍了对象免疫入侵检测在网上银行的应用。

关键词：对象免疫 入侵检测 网络安全

1 引言

入侵检测技术是一种积极主动的安全防护技术，在网络系统受到危害之前拦截和响应入侵，提供对内部、外部攻击和系统误操作的实时保护[1]。目前，网络入侵检测的分析手段可分为模式匹配以及统计分析。

模式匹配通过探测器收集网络上的数据信息，与模式数据库中的入侵行为相比较，若两者匹配则认为是入侵行为，否则作为正常的网络通信。其原理是攻击或入侵总能表示成模式或特征形式，检测准确率和效率非常高，处理过程中不需要大量计算，占用系统资源较少。然而，与病毒防火墙类似的不足是需要不断更新模式库，对未知的入侵手段毫无办法[2]。

统计分析亦称为异常检测，通过将正常的网络的流量、网络延时以及不同应用的网络特性（如时段性）统计分析后作为参照值，若收集到的信息在参照值范围之外，则认为有入侵行为。它能够检测到未知的入侵行为，但误报、漏报率较高，且不适应网络环境突然变化。

现在的越来越多的入侵检测系统兼有模式匹配以及统计分析功能。然而，目前统计分析手段在系统变化适应性上的缺陷以及误报漏报率过高，使其实用性大大降低。本文提出一种以对象免疫思想构建的入侵检测系统，实现面向对象的保护。

2 对象免疫入侵检测的原理与实现方法

计算机系统始终是一个自由的、开放式的却是存在安全缺陷的系统，自然的免疫系统为计算机安全系统提供了有益的启发。免疫系统的特性，如分布性、多样性、任意性、适应性、层次性、动态性等等则为计算机免疫系统提出了多样的体系架构。

2.1 免疫系统原理

人体免疫功能一般包括：免疫防御、免疫稳定、免疫监视。所谓免疫防御功能，是指当人体受到病原微生物侵袭时，体内白细胞就会对此种外来致病物质加以识别，并产生一种特殊抗体，有效清除微生物，维护人体健康。产生的这种抗体，通常称为免疫力。在机体淋巴细胞组织内可存在千百种抗体形成细胞（即B细胞），每一种抗体形成细胞只识别相应的抗原决定簇（antigenic determinant），当受抗原刺激后可增殖分化为一种细胞群[6]。免疫过程包括：

(1) 免疫细胞对抗原分子的识别过程

(2)免疫细胞的活化和分化过程

(3) 效应细胞和效应分子排异作用。

对象免疫入侵检测利用免疫防御功能的原理，对外来物质（网络数据）加以识别，如是非法数据（类比抗原决定簇）则产生抗体主动拦截，免疫对象受到有效保护[3]。对象免疫系统具有免疫系统共有的特点，它是一个动态系统，不断有新的抗原产生，也不断有相对应的抗体生成，从而抵御入侵。

2.2 系统模型

系统模型中强调一个动态循环的过程，首先系

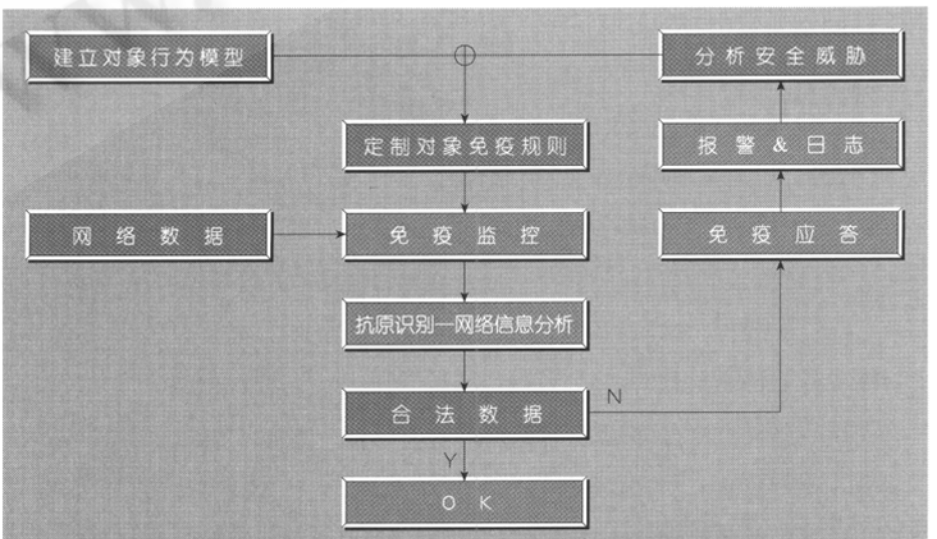

图1 系统模型

统管理员通过分析网络面临的现实威胁，针对特定对象行为模型制订对象免疫规则，而后免疫系统通过网络数据镜像监控网上信息，根据免疫规则进行抗原识别，分析网络数据是否合法，如识别为非法则启动免疫应答程序，网络管理员根据报警记录重新分析网络安全威胁，完善对象免疫规则，并可根据报警和日志信息调整防火墙规则，循环中达到动态免疫。对象免疫核心是围绕对象行为模型定制免疫规则，免疫实现则是通过免疫检测和免疫响应。

2.3 对象免疫系统实现方法

首先必须明确被保护对象，并建立对象行为模型。每一个受保护对象均有其特定行为模型，如对象只提供特定服务，只接受特定主机请求等等，根据行为模型定制相应的免疫规则。被保护对象可以是一台对外服务主机或是一个关键应用服务网段。如作为主机，对象行为模型要素包括主机MAC地址、IP地址、服务端口、应用属性、客户属性等等；如作为应用服务网段，对象行为模型要素包括网段中合法主机MAC地址、IP地址、通信协议、访问行为等等。将对象行为模型各种要素之间的合法组合作为检测依据，有任何违反对象行为模型，通过免疫应答实时响应。

其次针对不同类型非法访问采取不同的响应机制。对于面向连接的协议如非法TCP连接直接阻断；而面向非连接的协议如非法UDP数据则报警，及时通知系统管理员；如发现其他未知协议如系统自有的非标准协议，也通过报警通知系统管理员。

最后系统管理员检查系统报警和日志，如果属系统正常数据，可在安全规则中确认其合法性，如属非法数据，需及时调整防火墙规则、完善对象安全规则，并可跟踪入侵行为。

3 对象免疫入侵检测系统的特点

从美国FBI统计表明对于黑客进攻系统而造成损失的有超过80%是内部人员攻击和系统管理员失误造成的，即80%的损失是从内部网发生的。因此，对象保护不仅仅是由防火墙来完成，对象免疫系统能够弥补对象自身或因误操作而产生的漏洞，从而在同一网络中完成对特定对象的保护。

3.1 对象性

本系统强调特定对象的保护，根据对象独有的行为模式定制的安全规则，弥补对象固有缺陷，如对象自身安全漏洞以及安全策略的错误配置[4]，包括开放额外服务、被植入后门程序等等。

3.2 适应性

人体免疫系统能够适应不同的环境变化，与此类似，对象免疫入侵检测系统在不同操作系统的网络环境中同样能发挥作用。网络层以及传输层的对象免疫具有操作系统无关性，Unix、AIX、WinNT等操作系统在网络层以及传输层协议一致性保证对象免疫适应各种开放式网络环境。

3.3 可扩展性

采用对象免疫思想构建入侵检测系统具有检测方法可扩展性。2.3节提出了检测对象行为模型各要素的组合，而检测手段可以是任何行之有效的方法，系统功能可充分扩展。

3.4 排异性

对象免疫系统对被保护对象的违规行为以及其他对象的一切行为均视为非法，并作出应答。如被保护对象自身属性的改变，或者被保护网段中增加了新主机，对于免疫系统来说都属于需要被清除的"异物"。如同免疫系统中存在过敏反应，在入侵检测系统中也不可避免存在误警。对于误警问题，本系统将报警信息及时反馈给系统管理员，如确认为合法数据可在免疫规则中确定其合法性。

3.5 准确性

某些入侵检测系统可以很容易与防火墙结合，当发现有攻击行为时，过滤掉所有来自攻击者的IP的数据。但是，不恰当的反应容易带来新的问题，一个典型例子便是：攻击者假冒大量不同IP进行模拟攻击，而入侵检测系统自动配置防火墙

表1 对象行为模型

Host Name	MAC	IP Address	Port Number	Permit Source Address
Web Server	M1	N2.31	a,b,c	Any
Application Server	M2	N1.21	d	N2.31,N1.22
CA Server	M3	N1.22	e	N1.23
CA Admin	M4	N1.23	None	None

表2 N1网段对象免疫示例规则

Source Address	Des Address	Protocol	Port Number	Action Mode
N2.31	N1.21	TCP	d	permit
N1.22	N1.21	TCP	d	permit
N1.23	N1.22	TCP	e	permit
..*.*	*.*.*.*	TCP	*	Reset&Alarm&Log
..*.*	*.*.*.*	*	*	Alarm&Log

表3 N2网段对象免疫示例规则

Source Address	Des Address	Protocol	Port Number	Action Mode
..*.*	N2.31	TCP	a	permit
..*.*	N2.31	TCP	b	permit
..*.*	N2.31	TCP	c	permit
N2.31	N1.21	TCP	d	permit
..*.*	*.*.*.*	TCP	*	Reset&Alarm&Log
..*.*	*.*.*.*	*	*	Alarm&Log

将这些实际上并没有进行任何攻击的地址都过滤掉，于是形成了新的拒绝访问攻击 (DOS)[5]。而基于对象免疫的入侵检测系统可弥补统计分析误报和漏报的不足，针对每个对象采用不同的免疫策略，对系统的结合度较高，从而提高对象免疫入侵检测系统报警准确率。

4 在网上银行的应用

采用对象免疫的思想构建的入侵检测系统在网上银行应用示例如下。

4.1 网上银行拓扑简图

图2作为简化的网上银行拓扑，局域网交换机将网络中所有网络通信镜像到入侵检测设备上，图中有N1、N2两个网段，均有入侵检测设备接入。

4.2 网上银行潜在的网络安全隐患

网上银行安全要求非常高，在系统设计时安全措施非常全面细致而且复杂。然而，安全问题不是静态的。随着应用需求的不断增加，系统不可避免需要重新配置，原有安全设计可能显得不足，重新配置系统也会造成系统新的漏洞。针对对象变化或新增对象，基于对象免疫的入侵检测系统将定制相应的安全规则，从而不断适应新的环境。

4.3 对象免疫入侵检测的实现

以下是利用对象免疫思想实现入侵检测的一种方法，在网络层、传输层及应用层 (结合模式识别) 实现对象免疫，从而保障对象安全。

"表1" 是简化的网上银行对象在网络层和传输层的行为模型，明确被保护对象可分为两类：对象主机、对象网段。对象主机包括CA Admin、CA Server、Application Server、Web Server；被保护网段 (C类地址) 包括N1、N2。并得到被保护对象属性：CA Admin只可访问CA Server TCP port e，Application Server的TCP port d只能被CA Server以及Web Server访问，Web Server TCP port a、b、c对外提供服务。

网上银行入侵检测系统为每个对象主机定制相应规则，将对象行为模型各种要素之间进行合法组合，包括MAC地址捆绑、"表2"、"表3" 对象行为模型规则实施等等。对象免疫规则被看作主机对象以及网段对象的抗体，一旦有针对主机对象的非法访问或网段对象上有非法访问 (包括模式匹配中检测到的非法行为)，免疫系统立即应答，然后向控制台报警并记录日志。它不仅防止外部黑客入侵，而且可以防止内部人员误操作所造成的系统安全漏洞。网上银行经常受到来自Internet的漏洞扫描，对象免疫系统也能够立即阻断扫描行为，从源头上阻止入侵行为，而且通过日志以及报警，系统管理员可以及时发现系统细微变化，迅速响应。

5 总结

利用对象免疫思想构建的入侵检测系统，其核心是围绕对象行为模型的免疫规则。本文介绍了对象免疫在数据链路层、网络层、传输层的实现机制，对象免疫的最终目标是将对象行为模型的免疫规则覆盖网络各协议层，使每个对象受到针对性的保护，从而最大限度地减少内部人员误操作所造成的损失，并杜绝从外部和内部网对受保护对象的非法访问，有效地保障关键应用安全运行。

参考文献

1 Somayaji, A., Hofmeyr, S. and Forrest, S.,1997, Principles of a Computer Immune System, In Proceeding of New Security Paradigms Workshop, Langdale, Cumbria, Pages 75-82。

2 Richard A. Kemmerer, NSTAT: A Model-based Real-time Network Intrusion Detection System, Tech. Report TRCS97-18, University of California, Santa Barbara, 1997。

3 Allen, et.al., "State of the Practice of Intrusion Detection Technologies", Technical Report , CMU/SEI-99-TR-028, ESC-99-028, January 2000。

4 Lindqvist, Ulf, On the Fundamentals of Analysis and Detection of Computer Misuse, PhD dissertation, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, 1999。

5 Schuba, Christoph, Ivan V. Krsul, and Markus G. Kuhn, Analysis of a Denial of Service Attack on TCP, COAST Laboratory, CS Dept. Purdue University, 1997。

6 龙振洲等，医学免疫学，第二版，人民卫生出版社，1999。

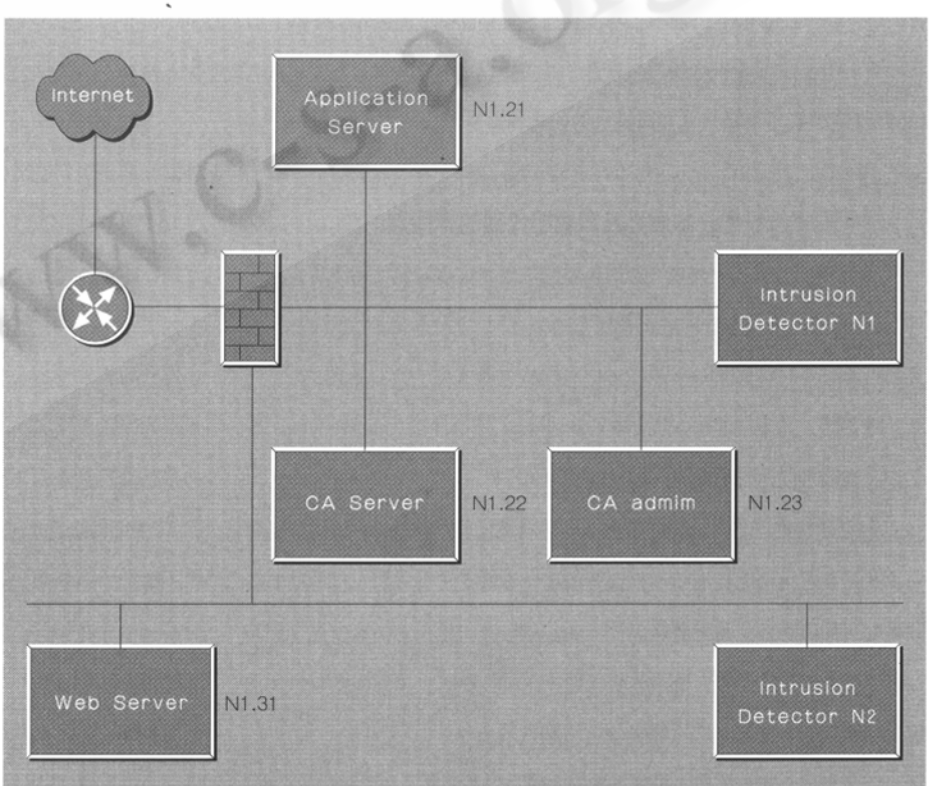

图 2 网上银行拓扑简图