

基于改进贝叶斯算法的信息安全模型

陈福志, 史杏荣

(中国科学技术大学信息网络安全研究中心, 合肥 230027)

摘要: 很多网关系统和入侵检测系统被设计来保护信息系统的安全, 其中一种安全隐患是现有网关系统的不完备性和入侵检测系统的虚警和漏警。该文总结了前人成果, 改进了原有的入侵检测算法, 提出了一个基于改进贝叶斯算法的新模型。该模型提高了入侵检测系统的完备性和准确性, 更有效地保障了信息系统的安全。

关键词: 入侵阻止; 入侵检测; 规则检测; 非规则检测

Information Security Model Based on Improved Bayes Algorithm

CHEN Fuzhi, SHI Xingrong

(Information Network Security Research Center of USTC, Hefei 230027)

Abstract: Although various gateway and intrusion detection system have been designed to protect system security, they work with a hidden trouble on the imperfectness of gateway and the error diagnosis of intrusion detection system. The paper improves the algorithm of intrusion detection system and provides a new security model based on Bayes algorithm. This model improves performance of intrusion detection system and protects the security of information system more effectively.

Key words: Intrusion prevention; Intrusion detection; Rule detection; Ruleless detection

信息技术发展了, 对信息系统及网络基础设施的攻击行为, 也已成为一个越来越严重的问题。在信息安全受到威胁的同时, 网络专家、信息安全专家也在不断提高网络的安全性, 保护信息系统不受侵犯。

在信息网络安全中, 常用的安全模型是阻止(Prevention)和检测(Detection), 但是它们各有利弊。

对于阻止, 传统的方法是建立一个保护域(Protective Shield), 每一个进入系统的人都必须经过身份验证和授权, 同时阻止保护域中的信息向外泄漏。用此方法来实现计算机和网络的安全带来了大量的限制。首先, 它不可能建立一个完全的绝对安全的系统, 其次跟当前的开放趋势是矛盾的。

而入侵检测, 有两种方式: 规则检测和非规则检测^[1]。

规则检测, 又称滥用入侵检测, 它是建立在对过去各种网络入侵方法和系统缺陷的知识积累之上。这样的检测系统具备极高的准确性, 但是, 它的完备性则取决于其数据库的完备程度。

非规则入侵检测又称异常检查, 它是建立在如下的假设基础上: 即任何一个入侵行为都能由于其偏离正常或者所期望的系统和用户的活动规律而被检测出来。描述正常或者合法活动的模型是从通过各种渠道收集到的对过去大量历史活动资料的分析中得到的, 入侵检测器就是把它与当前的活动情况进行对比, 如果发现异常, 则系统发出警告信号, 任何不符合以往活动规律的行为都将被视为入侵行为。因此, 非规则入侵检测系统的完备性很高, 但是它的准确性却难以得到保证, 常常出现虚警和漏警。

Tucker 在 “The Computer Science and Engineering Handbook” 中提出了3种异常检测模式: 操作模式, 平均标准背离模式和事件序列模式。这几种异常检测模式可以在不

需要任何先验知识的基础上检测目标对象, 发现未知的入侵, 但是不是每个对象的行为都是完全标准的, 入侵者也可以慢慢地改变行为来欺骗系统。

本文在总结前人成果的基础上, 改进了贝叶斯算法, 提出了一个新的安全模型。该模型可以检测渐变的入侵行为。并将入侵阻止和入侵检测相结合, 分布检测与中心计算、中心控制相结合, 动态改变检测策略和规则数据库。提高了系统对入侵检测的准确性和完备性。

1 系统模型

新的入侵检测模型框架如图1所示, 主要由以下几个部分组成: 微防火墙, 策略更新, 策略管理和网关防火墙。

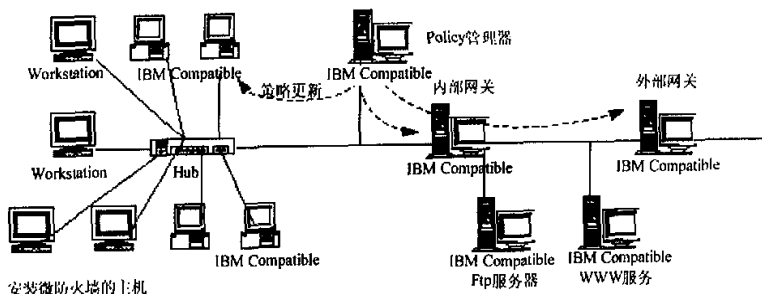


图1 总体模型

图1中, 中心安全策略管理被分到了各个网络主机上执行, 即分布式安全策略。它删除了一些传统网关防火墙的束缚, 采用3级安全控制体系结构。网关防火墙安装在最前端, 作为内部网和Internet的屏障, 在Intranet和Internet的边界对信息包进行过滤。微防火墙安装在每台主机上, 由操作系统内核执行入侵检测和更新策略。策略管理器对整个网络

作者简介: 陈福志(1975—), 男, 硕士生, 研究方向: 信息网络安全; 史杏荣, 教授

收稿日期: 2002-11-16 **E-mail:** cfz@mail.usyc.edu.cn

的安全策略进行分析和配置, 监督节点活动, 联合主机检测各种入侵, 更改入侵数据库, 更改策略, 阻止入侵的蔓延。

2 微防火墙

由于黑客技术的发展, 外部攻击可以很轻易地攻破网关, 对内部网络造成威胁。况且网关防火墙只能保护这个局域网不受外部攻击, 却不能确保它不受内部攻击。因此我们采用微防火墙机制, 它补充了传统网关防火墙的不足之处, 既可防止外部攻击, 又可抵御内部攻击。

图2是微防火墙在节点主机的层结构, 它是分布式入侵检测的主体。每台主机都可以进行入侵检测, 并同策略管理器进行通信。

微防火墙采用规则和非规则检测并行处理, 互不干扰, 动态更新规则库。这样使得入侵检测的准确性和完备性都提高。微防火墙功能结构见图3。

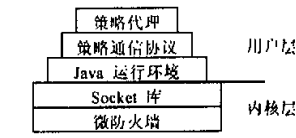


图2 微防火墙的位置

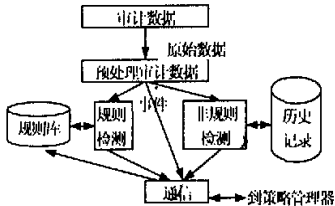


图3 微防火墙功能图

审计数据事件主要包括：文件访问, 系统访问, 资源消耗, 进程创建, 电子邮件, 动态资源使用等。检测的对象包括：用户, 目标系统, 远程主机。将原始数据转换成事件的过程, 就是把每个检测的对象同它们的活动信息联系起来, 统一成检测系统可以识别的格式。

规则检测就是把事件同规则库已知的入侵行为进行匹配, 如果匹配成功, 则同策略管理器进行通信, 更改网关防火墙的策略。如果每个被观测对象的行为都可以用图4中的一条行为曲线来规范它, 则规则检测完全可以胜任入侵检测系统的全部功能。但被观测对象的行为可能是图4中二维空间的任意一条曲线, 显然规则检测对数据库中没有的案例无能为力。如图4, 假设曲线2和曲线4在规则库中, 则用户2被判断为正常者, 用户4被认为是入侵者。对用户1和用户3, 规则检测无能为力, 根据设置的不同, 要么都报警, 要么都不报警。这时非规则检测就会发挥作用。

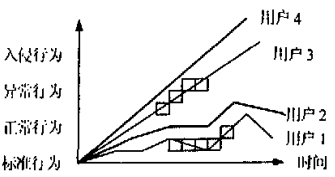


图4 被检测对象行为曲线

非规则检测采用贝叶斯算法, 是对检测对象的异常检

测, 如果发现异常, 则认为是入侵。这种算法提高了检测的完备性。

贝叶斯统计算法把检测对象的行为进行分类, 每个对象所对应的每一个行为都是一个矢量, 就是要把这些矢量进行分类, 分类成正常、一般异常、严重异常、警告等。对于随机变量 X , 必须知道变量 X 对每一个类别的概率分布, 知道了这个概率分布后我们就可以计算向量 x 属于类别 c 的概率

$$P(c|x) = \frac{P(c)p(x|c)}{p(x)}$$

计算出 x 属于各个类的概率, 将 x 归入概率最高的类。其中 $p(c|x)$ 是矢量 x 在类 c 下的条件密度函数, $P(c)$ 是类 c 的先验概率, $p(x)$ 是向量 x 的密度函数。对于连续的概率分布可以用统计的方法获得, 如用 $\hat{P}(c)$ 代替 $P(c)$, 当 $n \rightarrow \infty$ 时,

$$\hat{P}(c) \rightarrow P(c)$$

但是另外一个方面因为这里的概率函数和先验概率都是统计获得, 并且在计算事件的概率通常采用如下的加权法来

获得,
$$P(c) = \frac{\sum_{k=1}^n Wc \cdot 2^{-bk}}{\sum_{k=1}^n 2^{-k}}$$
 其中 Wc 是类 c 的事件, b 是

调节参数。从公式可以看出, 随着时间的向前推移, 以前的事件对统计概率的影响越来越小。每次的检测都是一次坐标轴的移动, 由于只跟当前事件的前 n 个事件比较, 当前的行为只要在图5所示的方框内, 都认为是合法的。因此用户1和用户3都将被认为是合法者。这是因为用户4利用了检测系统的学习原理, 从而渐变它的入侵过程, 使得入侵检测系统无法检测到它的入侵。

因此我们令 $f(Wc)$ 为 c 类事件的随时间的函数, 取其梯度作为渐变过程的衡量标准。

$$T(c) = \sum_{k=1}^n f'_k(Wc)$$
 从公式

可以看出, 它衡量了被检测对象的行为是在规定范围内波动, 还是一直在偏离正常行为。它所使用的是绝对坐标, 而不是原来Bayes算法的相对坐标(图5)。所以当 $T(c)$ 超过阈值的时候就可以认为是愚弄安全系统学习过程的渐变入侵, 在图6中, 改进的Bayes算法可以检测出用户1、2合法, 而用户3、4进行了入侵行为。改进的Bayes算法同规则检测一起, 使得入侵检测更加准确完备。

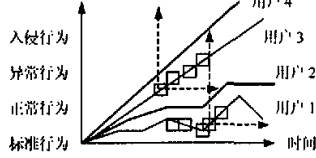


图5 原来的Bayes检测

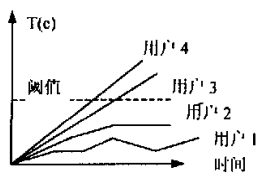


图6 改进的Bayes检测

微防火墙还集成了身份验证、接入控制、加密等功能。它的策略管理只能由策略管理器统一管理分配,就是主机的root用户也无法改变策略。微防火墙在个人主机上实现接入控制,这样在Intranet内可以不用IPSec,获得性能的提高。另外在个人主机上实现接入控制,也不用再限制网络的拓扑结构。这种系统更健壮,具有兼容性和扩展性。

3 策略更新

动态安全要求频繁的策略更新,主要包括在微防火墙、管理器和网关防火墙上的规则库的改变和非规则检测参数的改变。一个基本的目的是执行紧急使命功能。Kai Hwang等检查了E-mail, RPC, SNMP等进行策略更新,发现它们都不适合。最后选定了3种较好的策略更新机制:移动代理, CORBA中间层和RMI中间层。这3种策略更新机制都达到了动态安全。我们从执行速度、可扩展性、安全性和健壮性几个方面对这3种策略更新进行了比较,发现RMI具有最好的性能,所以选用基于Java的RMI包来广播策略更新。

RMI是基于Java对象的分布式计算模型,它是Java的RPC机制。它的一个好处就是语言独立的,因此RMI可以让用户自由添加Java功能,并且能够进行无缝连接。RMI使用登记管理器来协调通信,图7给出了使用RMI来进行策略更新的过程。

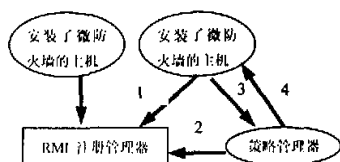


图7 策略更新过程

RMI策略更新机制有3个组成部分:远程方法,通信接口和RMI注册管理器。远程方法提供微防火墙策略更新的接口;通信接口提供远程方法同RMI注册管理器的接口以及主机同策略管理器之间的通信协议;RMI注册管理器对各个主机注册进行身份验证和授权,维护每个主机的数据库,包括接口参数、威胁事件、历史事件等。

RMI进行策略更新分成4步。首先节点主机向RMI注册管理器登记它们的远程方法,这必须经过验证和授权。然后策略管理器可以向RMI管理器数据库请求主机的威胁数据。第3步,RMI管理器向策略管理器返回主机的威胁事件。第4步,策略管理器在处理事件后用约定的通信协议广播它的策略更新,并使得它的3级安全策略具有一致性。

4 策略管理

策略管理器负责配置策略、更新策略、协调Intranet的两级保护。在图1中,指定微防火墙级别为3,策略管理器级别为2,网关防火墙级别为1。对于来自Internet和Intranet的攻击,对每个级别,定义两个不同的策略规则集, S_i 表示对外部的策略集, T_i 表示对内部的策略集。这些规则集应该满足下面的关系: $S_3 \subset S_2 \subset S_1$; $T_3 \supset T_2 \supset T_1$ 。从策略规则集关系可以看出网关防火墙的主要任务是防止外部攻击,微防火墙的主要任务是防止内部攻击。

图8描述了基于RMI的入侵检测系统的安全管理框架结

构核心,主体包括微防火墙和策略管理器。在各个主机上的微防火墙检测异常事件,处理异常事件。并把事件和入侵警告报告给管理器。管理器通过入侵检测控制器监测微防火墙。策略管理器处理入侵警告和事件。发现入侵的时候,经过决策系统自动更新安全策略,并激活所有的节点响应。

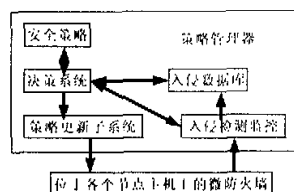


图8 策略管理

入侵检测监控器是建立在RMI注册管理器上的,减少系统中非法和恶意远程方法的接入。决策系统要配合3个方面作出决策:(1)管理者的宏观安全策略;(2)某个微防火墙的入侵警告;(3)综合各个微防火墙对每个观测对象的事件记录的再分析。它体现了分布式和中心式两种模式,分布策略提高了检测的效率,中心分析提高了检测的准确性。

当策略管理器通过决策系统作出决策后,就通过策略更新子系统广播策略更新。因为在策略更新的过程中有RMI注册管理器参与验证和授权,可以防止攻击者伪装成策略管理器广播更新策略。策略管理器同时动态配置网关防火墙的安全策略,防止DoS攻击、IP欺骗、探测、扫描、非授权外部接入等。

5 结束语

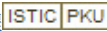
本文在改进的Bayes算法的基础上系统地描述了一个完整的入侵检测模型。模型中的微防火墙实现了分布式的入侵检测,提高了系统性能,缩短了反应时间。改进的贝叶斯算法防止了入侵者欺骗检测系统学习的过程。中心分析提高了系统准确性。采用RMI的策略更新,使得策略更新既快且准,认证授权机制防止入侵者的伪装欺骗。

将来的研究要提高微防火墙的结构,减少网络主机的软件攻击,使得网内主机移动到网外仍然具有网内的使用特征和安全性。入侵检测要向无线网、异种网和宽带网发展。策略更新实现多播也需要进一步研究。在宽带网中,采用多播协议来进行更新可以提供更大的可扩展性、安全性和更小的兼容性问题。

参考文献

- 1 黄允聪,严望佳编著.网络安全基础.北京:清华大学出版社,1999-06
- 2 Helman P, Liepins G. Foundations of Intrusion Detection. Computer Security Foundations Workshop V, 1992
- 3 Hwang K, Gangadharan M. Micro-firewalls for Dynamic Network Security with Distributed Intrusion Detection. Network Computing and Applications, 2001
- 4 Buschkes R, Kesdogan D. How to Increase Security in Mobile Networks by Anomaly Detection. Computer Security Applications Conference, 1998
- 5 唐正军.黑客入侵防护系统源代码分析.北京:机械工业出版社,2002

基于改进贝叶斯算法的信息安全模型

作者: 陈福志, 史杏荣
作者单位: 中国科学技术大学信息网络安全研究中心, 合肥, 230027
刊名: 计算机工程 
英文刊名: COMPUTER ENGINEERING
年, 卷(期): 2003, 29 (20)
被引用次数: 2次

参考文献(5条)

1. 黄允聪;严望佳 网络安全基础 1999
2. Helman P;Liepins G Foundations of Intrusion Detection 1992
3. Hwang K;Gangadharan M Micro-firewalls for Dynamic Network Security with Distributed Intrusion Detection 2001
4. Buschkes R;Kesdogan D How to Increase Security in Mobile Networks by Anomaly Detection 1998
5. 唐正军 黑客入侵防护系统源代码分析 2002

引证文献(2条)

1. 唐淑珍 基于贝叶斯的入侵检测[期刊论文]-软件导刊 2010(4)
2. 王泽东, 刘宇, 朱随江, 刘宝旭, 潘林 采用行为分析的单机木马防护系统设计与实现[期刊论文]-计算机工程与应用 2011(11)

本文链接: http://d.wanfangdata.com.cn/Periodical_jsjgc200320047.aspx