

# 基于 P2P 和移动代理的入侵检测系统研究

徐长棣, 刘方爱

(山东师范大学 信息科学与工程学院, 山东 济南 250014)

**摘要:**介绍了现有入侵检测系统在计算机以及网络安全中的意义和现有入侵检测系统的局限性,简述了移动代理和 P2P 技术的优点,提出了一种采用移动代理技术和 P2P 结构的入侵检测系统,避免了当前分布式入侵检测系统存在的单点失效和传输瓶颈问题,提高了系统的自身安全性和各结点的协同检测能力。该系统能够根据环境的变化来进行调整,具有较强的可伸缩性。重点介绍了该系统的结构以及判断入侵的方法。

**关键词:**入侵检测;移动代理;P2P 结构

**中图分类号:**TP393.08

**文献标识码:**A

**文章编号:**1673-629X(2007)01-0164-03

## Research of Intrusion Detection System Based on P2P and Mobile Agents

XU Chang-di, LIU Fang-ai

(College of Information Science and Engineering, Shandong Normal University, Jinan 250014, China)

**Abstract:** Introduces the role of intrusion detection systems in computers and network security and the limits of present intrusion detection systems, outlines the advantages of mobile agents and P2P technology. A novel intrusion detection system based on P2P architecture and mobile agent technology is proposed in this paper. It can avoid the questions of the simple-point invalidation and the transmission bottleneck in the current distributed intrusion detection systems, and enhance the security and collaborative detection capability of the model. The model is scalable and can adjust itself dynamically to adapt to the environmental change. Introduced with emphasis this kind of system structure as well as the judgment invasion method.

**Key words:** intrusion detection; mobile agent; P2P architecture

### 0 引言

随着网络技术和网络规模的不断发展,针对网络和计算机系统的攻击已经屡见不鲜,安全问题已经成为人们关注的焦点。传统的安全防护有防火墙等手段,但防火墙本身容易受到攻击,且对于内部网络出现的问题经常束手无策<sup>[1]</sup>。安全问题已经成为人们关注的焦点。传统的安全防护有防火墙、口令认证、数据加密等手段,但防火墙本身容易受到攻击,特别是对于内部网络出现的问题经常束手无策。根据 CERT 的报告,50% 以上的攻击来自于内部<sup>[2]</sup>。而且,防火墙采用的是一种静态的被动的策略。仅仅采用这些静态防御手段是不能够满足安全需求的,从而引发了入侵检测这一安全领域课题的诞生。

入侵检测(Intrusion Detection)是在 1980 年由 James Anderson 首先提出的<sup>[3]</sup>,是对入侵行为(或企图)的发觉。它是通过对计算机网络或计算机系统中的若干关键点收

集信息并对其进行分析,从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测的软件与硬件的组合便是入侵检测系统(Intrusion Detection System,简称 IDS)<sup>[4]</sup>,它一般包括三个部分:数据的采集、入侵分析检测和响应与恢复。由于它是与网络运行管理系统相结合的,能够有效地监察网络用户的使用行为,不仅能检测网络外部的入侵行为,也能随时监督系统内部的未授权用户行为,从而弥补了传统安全技术的不足<sup>[5]</sup>。

### 1 基于 P2P 入侵检测系统的提出

按照不同的分类标准,传统的 IDS 有多种分类方法。根据检测对象的不同可分为基于主机的入侵检测系统(HIDS, Host-based IDS)和基于网络的入侵检测系统(NIDS, Network-based IDS)<sup>[4]</sup>。HIDS 主要以系统日志、应用程序日志为基础,分析和审计单个主机的网络数据,从中寻找入侵的行为。NIDS 一般在共享式的网络中,通过嗅探、监听所有本网段的数据包,来分析可能的入侵痕迹。

根据检测系统自身体系结构的不同,IDS 可分为:集中式入侵检测系统(Centralized Intrusion Detection System,简称 CIDS)和分布式入侵检测系统(Distributed Intrusion Detection System,简称 DIDS)<sup>[4]</sup>。传统的集中式入侵检测

收稿日期:2006-04-25

基金项目:国家自然科学基金资助项目(60373063)

作者简介:徐长棣(1981-),男,山东菏泽人,硕士研究生,研究方向为网络与信息安全、入侵监测系统;刘方爱,博士生导师,博士,研究方向为网络安全技术、并行/分布式处理、光互连网络路由算法、网络环境下的应用开发技术。



系统是在网络的各个网段上放置多个检测器采集当前的网络状态信息,然后由中央控制台集中进行分析和处理。但当有大规模入侵行为时,超过了中央控制器的承受能力,会造成许多事件的遗漏,增加了漏报的概率。而且,网络的时延不能实时地反应当前的网络状态,也可能降低一定的准确性。随着网络系统结构变得日益复杂,广泛采用分布式应用环境、海量存储和高带宽的传输技术,都使得集中式的入侵检测越来越不能满足系统的安全需求。通过将主机检测和网络检测结合起来,并且采用协同的方式,共享整个网络的信息资源,从而出现了分布式入侵检测技术<sup>[6~8]</sup>。当前,分布式入侵检测是入侵检测乃至整个网络安全领域的热点之一。

目前为止,现有的入侵检测系统大多数采用的是难以更改和重新配置的体系结构。在传统的入侵检测系统中,数据收集是通过单一的主机来完成的,并且把收集到的数据发送到单独的分析器上进行数据分析,有些系统虽然采用了分布式的数据收集,但是数据分析也往往是在一个组件中完成的。系统只依靠有限的几个传感器<sup>[9]</sup>(就运算能力来说通常是一个)和唯一的一个事件分析器中来获取,处理和分析网络中的所有数据,从而不可避免地会在检测过程中产生数据丢失和处理瓶颈的问题。近几年来研究者将代理技术引入到入侵检测系统中,通过使用移动代理技术解决了传统IDS中存在的大部分缺点<sup>[10]</sup>。但是这些基于代理的DIDS大都采用的是层次化的结构,当多个底层结点都向高层结点发送分析结果<sup>[5]</sup>时,容易在高层结点处形成处理瓶颈,造成系统丢失数据或者因来不及处理而延迟了对入侵行为的发现,并易成为攻击者的目标<sup>[11,12]</sup>。而协作式模型中各个分析结点具有较大的自主性,不依赖于指定的中心结点,可以减少系统瓶颈,提高系统的容错性。但纯粹的协作式系统也有缺陷,就是各组件相互通信时,可能导致消息量过于庞大。

要解决上述问题,必须有一种比当前的IDS更有效的体系结构。因此,文中将P2P和移动代理引入到入侵检测系统中,提出了一种基于P2P和移动代理的入侵检测系统结构。

## 2 P2P结构入侵检测系统

在文中提出的入侵检测系统中引入了移动代理技术和P2P结构。移动代理是一个独立运行的软件实体,它包括完成所规定功能的代码、数据和状态信息,具有移动性、自主性、反应性、主动性和交互性的特点<sup>[13]</sup>,可以在一定的机制控制下,携带自身代码、数据及其状态信息在网络环境中从一个节点迁移到另一个节点上继续运行。采用P2P(peer-to-peer)结构将各个结点的工作模式设为平等的协作模式,系统的各个部分协同合作,可以不经服务器和其他实体进行直接连接<sup>[14]</sup>,避免了单点失效和数据的传输瓶颈问题<sup>[15]</sup>。

在文中提出的基于P2P结构的入侵检测系统结构

中,网络中的每个结点都是一个完整的入侵检测系统,它们之间是完全对等的。在这种结构下,每一个结点都会有若干个结点和它连接是最近的,称这些结点为这个结点的邻居结点。

如图1所示,结点A有邻居结点B和C,结点B有邻居结点A,C和D,结点C有邻居结点A,B和D,结点D有邻居结点B,C和E,结点E有邻居结点D。

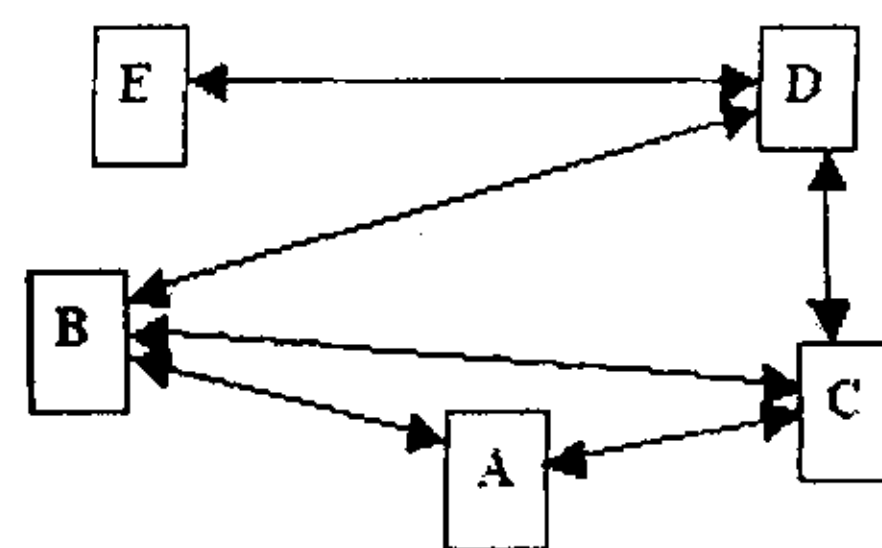


图1 邻居结点示意图

每个结点上的系统主要由三个部分组成:核心信息部分、检测部分和移动代理部分。每一个结点都存储有和它相邻的结点的核心信息,比如关键数据文件的校验和、文件结构、一些访问控制文件的信息。移动代理根据检测需要也分为多种,它们在各个结点上运行并且把运行结果报告给检测部分。当一个结点收到可疑的入侵信息后,它立即把这个信息发送给它的邻居结点,然后由这些邻居结点判断这一结点发来的信息是否值得信任。如果这些邻居结点中大多数能够确认前一结点发送来的信息是值得信任的,那么这些邻居结点就继续向它们各自的邻居结点发送这个入侵信息,否则,它们认为这个结点是可信任的,不再继续向它们的邻居结点发送这个信息。

在这种结构中,每个结点上建立一个记录异常信息的日志数据库,用来存放已经确认的异常事件。如果探测到有新的异常事件发生,就立即与受攻击结点本身的日志数据库中的记录相比较,如果这个结点的日志数据库中没有这个记录,就等待它的邻居结点来判断这个事件是不是一个攻击行为,如果是就把这个事件记录到这个日志中,并且把这个攻击信息发送给网络中的其他结点;如果发现已经有了这个记录就不再向邻居结点发送信息,结点自身采取措施阻止这个事件,这样可以减少一部分的网络流量。

在图1的结构中,对于结点A,它存储有自身的核心信息,而且还有邻居结点B,C中的一些信息,如文件校验和、文件大小等信息。从A发出一个专门检测校验和的检测代理负责定期地检测B中文件的校验和并返回给A,和A中存储的值进行比较看是否匹配。如果发现B中文件校验和与A中先前存储的校验和不匹配,则认为B中的文件可能被修改,于是从结点A再发出一个检测文件大小代理,来比较B中现有文件的大小和A中的数据是否一致,如果不一致,则认为B是危险的,A中B的信誉值降低。接着A把这个信誉值发送给它的邻居结点B和C。结点C经过数字认证确认由A发来的信息是可信的才接受这个信息,然后C同样向B发送一个代理,把代理返回的值和自身存储的值相比较,如果也是不匹配,那么这个信誉值再次降低,并把降低后的信誉值发送到结点



D, 结点 D 重复 C 的操作, 最后由 D 把这个信誉值再发送给 A。如果发现大多数的结点都认为 B 中的文件信息已经被改变, A 就做出判断: B 受到了入侵, 并把这个事件更新到日志数据库中, 然后把这个信息发送给其他结点, 其他结点的日志数据库也做出相应的更新。

### 3 结论及进一步的工作

文中提出了一种基于 P2P 结构的入侵检测系统, 并引入了移动代理, 各个代理之间互相独立又相互协作, 而且可以根据实际要求添加或者减少部分代理, 而且网络中的结点也可以按照要求增加或者减少, 在分布式入侵检测系统的基础上能够进一步降低网络流量提高检测效率。下一步的工作是进一步完善这种结构, 实现这种入侵检测系统。

#### 参考文献:

- [1] 张超, 霍红卫. 入侵检测系统概述[J]. 计算机工程与应用, 2004(3): 116-119.
- [2] 王洪涛, 何欣. 网络入侵检测概述[J]. 网络安全技术与应用, 2002(5): 13-16.
- [3] Anderson J P. Computer Security Threat Monitoring and surveillance[R]. [s.l.]: James P Anderson Co., 1980.
- [4] 唐正军, 李建华. 入侵检测技术[M]. 北京: 清华大学出版社, 2004.
- [5] Zaki M, Sobh T S. Attack abstraction using a multi-agent system for intrusion detection[J]. Journal of Intelligent & Fuzzy Systems, 2005, 16: 141-150.
- [6] Staniford-Chen S, Tung B, Schnackenberg D. The common intrusion detection framework(CIDF)[C]//The 1st Information Survivability Workshop. Orlando, FL, USA: [s.n.], 1998.
- [7] Staniford-Chen S, Cheung S, Crawford R, et al. GrIDS - A graph based intrusion detection system for large networks[C]//The 19th National Information Systems Security Conference (NISSC). Baltimore, MD, USA: [s.n.], 1996: 361-370.
- [8] Maniyan B J S, Garcia-Fernandez J O, Lsacoff D, et al. Architecture for intrusion detection using autonomous agents[R/OL]. COAST Laboratory, Purdue University, COAST Tech Rep: 9805, 1998. <http://www.cerias.purdue.edu/homes/aafid/docs/tr9805.pdf>.
- [9] Porras P A, Neumann P G. EMERALD: Event monitoring enabling responses to anomalous live disturbances[C]//The 20th National Information Systems Security Conf(NISSC). Baltimore, MD, USA: [s.n.], 1997: 353-365.
- [10] 徐峰, 宋如顺. 基于 P2P 多代理数据融合入侵检测模型研究[J]. 计算机工程与应用, 2004(17): 159-161.
- [11] Bace R, Mell P. Intrusion Detection Systems[EB/OL]. 2001. [http://linuxsecurity.org/resource\\_files/intrusion\\_detection/sp800-31.pdf](http://linuxsecurity.org/resource_files/intrusion_detection/sp800-31.pdf).
- [12] Kruegel C, Toth T. Distributed Pattern Detection for Intrusion Detection[EB/OL]. 2002-04. [http://www.infosys.tuwien.ac.at/Staff/tt/publications/Distributed\\_Pattern\\_Detection\\_for\\_Intrusion\\_Detection.pdf](http://www.infosys.tuwien.ac.at/Staff/tt/publications/Distributed_Pattern_Detection_for_Intrusion_Detection.pdf).
- [13] 张云勇, 刘锦德. 移动代理技术[M]. 北京: 清华大学出版社, 2003.
- [14] 陈建华, 黄道颖. 计算机对等网络 P2P 技术[J]. 计算机工程与应用, 2003(33): 162-164.
- [15] Peer-to-Peer Working Group. Taxonomy of Peer-to-Peer Architecture[EB/OL]. 2001. <http://batalion.ucsd.edu/ggf/P2P-Taxonomy-v095.pdf>.

(上接第 163 页)

复杂度可以与某些多项式时间算法的时间复杂度相媲美了。

### 3.3 算法还可用于攻击整数 MH 背包密码

整数 MH 背包密码允许明文序列  $x_1, \dots, x_n$  取大于 1 的整数, 即  $x_i \in [0, k], k > 1$ 。若公钥序列为  $a_1, \dots, a_n$ , 密文为  $M$ , 则上述算法破解出明文序列的步骤如下:

先构造新序列  $a_1, 2a_1, \dots, ka_1, a_2, 2a_2, \dots, ka_2, \dots, a_n, \dots, ka_n$ , 记为序列  $a_i'$ ; 然后将序列  $a_i'$  作为公钥序列和密文  $M$  代入上述算法中计算, 所得的结果记为序列  $x_1', \dots, x_{kn}'$ , 对于序列中的每一个  $x_j' = 1$ , 计算  $t = \lceil j/k \rceil, s = j - (t-1) * k$ , 其中  $\lceil \cdot \rceil$  是向上取整号,  $/$  是除法运算, 则令  $x_t = s$ ; 最后令序列  $x_1, \dots, x_n$  中没有赋值的为 0, 则所求得的序列  $x_1, \dots, x_n$  就是明文信息。

### 4 总结

文中研究了 MH 背包密码的攻击算法, 提出了利用动态规划思想攻击 MH 背包密码的基本算法及其改进算法。这两个算法能够克服以前算法中存在的缺点, 具有计

算复杂度低、简单、易于实现、对于大部分多次循环高密度 MH 背包密码也有有效的优点。并且, 这两种算法既适用于二进制 MH 背包密码, 也适用于整数 MH 背包密码。在算法所耗费的时间和空间上, 改进算法做了很大的改进, 使算法的性能有了进一步的提高。

#### 参考文献:

- [1] Garrett P. 密码学导引[M]. 北京: 机械工业出版社, 2003.
- [2] 陈志平, 徐宗本. 计算机数学——计算复杂性理论与 NPC, NP 难问题的求解[M]. 北京: 科学出版社, 2001.
- [3] 樊丰, 林东. 网络信息安全 & PGP 加密[M]. 北京: 清华大学出版社, 1999.
- [4] Lagarias J C, Odlyzko A M. Solving Low-Density Subset Sum Problems[J]. Journal of the Association for Computing Machinery, 1985, 32(1): 229-246.
- [5] 卢开澄. 计算机密码学——计算机网络中的数据保密与安全[M]. 北京: 清华大学出版社, 1999.