第33卷 第24期 计 算 机 工 程 2007年12月
Vol.33 No.24 Computer Engineering December 2007
·安全技术· 文章编号：1000—3428(2007)24—0172—03 文献标识码：A 中图分类号：TP393

基于 Agents 的层次型网络安全监控系统

王新昌，刘育楠
（解放军信息工程大学电子技术学院，郑州 450004）

摘 要：针对现有的集中式网络监控系统存在的不足，设计并实现一种网络安全监控系统，系统采用层次结构，将监控功能分散到各个受控终端的监控Agent上，减轻监控服务器的工作负荷和对网络带宽的需求，实现对网络实时安全监控。对监控Agent的设计与系统实现进行了分析讨论。应用表明，系统具有良好的灵活性和可扩展性。

关键词：网络安全监控；层次结构；代理

Hierarchical Network Security Monitor System Based on Agents

WANG Xin-chang, LIU Yu-nan
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】This paper points out the deficiencies of the existed centralized network monitor system, a network security monitor system is designed and implemented. This system takes hierarchical structure and distributes monitor functions to monitor agents located in terminals so as to lighten the load of monitor server and network and realize real-time security monitor of network. The design of monitor agents and the implementation of the system are discussed. Applications show that the system is flexible and extendable.

【Key words】network security monitor; hierarchical structure; agent

传统的网络监控大多为集中方式(如基于SNMP的网络管理)，采取定期轮询或监听各类Agent节点的Trap信息等方式来实现[1]。随着网络规模的扩大、流量的增加、服务种类和数目的增多，集中式体系结构的缺陷越来越明显，主要表现为：容易造成丢包的现象，系统的可扩展性差，对网络带宽的要求高，中心管理部分易成为系统瓶颈等[2]。为弥补网络监控的不足，本文提出了一种基于Agent的层次型网络安全监控系统，并进行了设计与实现。

1 系统设计

考虑系统的灵活性和可扩展性，整个系统采用监控控制台/监控服务器/监控代理 3 层结构，并细分为监控应用层、监控业务层、系统管理层、系统服务层、数据预处理层、安全通信层、数据采集层以及监控 Agent 层 8 个层次。系统层次结构模型与实际系统部署的对应关系如图 1 所示。

根据层次结构模型，各个层次的功能为：

(1)监控应用层。为监控管理员提供应用界面，负责将监控管理员的管理、设置和操作转化为一系列指令，通过安全传输协议传达给监控服务器。

(2)监控业务层。提供一系列安全监控业务，包括状态监控、应用监控、外设监控、用户行为监控以及网络行为监控等。

(3)系统管理层。提供系统的管理维护，包括日志管理、用户管理和监控策略配置等。

(4)系统服务层。提供安全监控所需要的通用系统服务，包括监控 Agent 调度、数据处理、统计分析以及报警等，同时提供监控数据库用于日志数据的存储。

(5)数据预处理层。对监控日志和终端日志数据进行预处理；

(6)安全通信层。通过安全通信协议为系统提供安全通信服务。

(7)数据采集层。采集监控日志、终端日志等监控数据。

(8)监控 Agent 层。运行监控 Agent，实际执行各项监控业务。

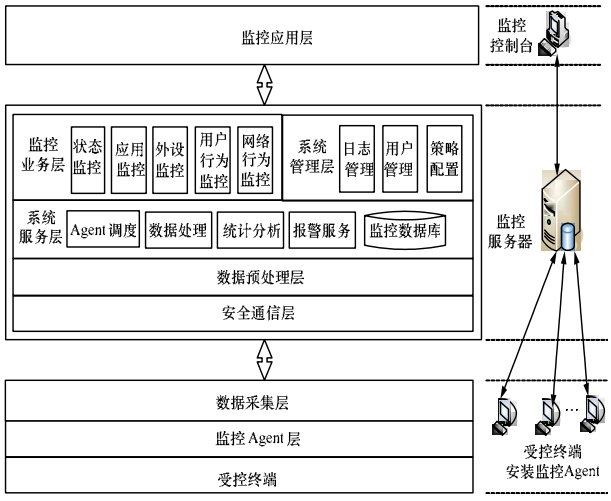

图 1 系统层次结构模型与实际部署的对应关系

系统的工作原理可以描述为：监控管理员通过监控控制台进行各项监控设置和操作；监控控制台将监控管理员的设置和操作转化为一系列指令和策略传达给监控服务器；监控服务器通过安全通信协议启动终端上的监控 Agent 实现对网络内所有受控终端进行监控；监控 Agent 根据策略和指令进行监控任务的实际执行；监控执行过程中，监控 Agent 一方

基金项目：国家“863”计划基金资助项目
作者简介：王新昌(1975－)，男，讲师、硕士，主研方向：网络与信息安全；刘育楠，副教授、硕士
收稿日期：2007-01-28 **E-mail：**wxchtbb@163.com

面记录监控结果形成监控日志，另一方面对终端系统信息进行采集，形成终端日志，并将日志数据通过安全通信协议发送到监控服务器，最后由监控服务器进行数据预处理后提交到监控数据库。在系统运行过程中，系统定期或按照系统监控管理员要求对监控日志、终端日志和系统自身日志进行各项查询、审计、统计分析等工作。

2 监控 Agent 设计

2.1 监控 Agent 的类型

监控 Agent 运行于网络上的受控终端，主要负责监控业务的实际执行。对应监控服务器中的状态监控、应用监控、外设监控、用户行为监控和网络行为监控业务，分别设置相应的监控 Agent。监控 Agent 的类型如图 2 所示。

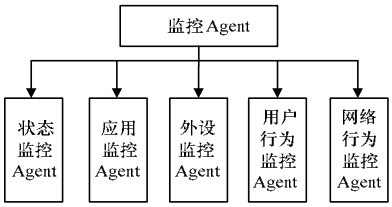

图 2 监控 Agent 的类型

(1)状态监控 Agent。实现对网络终端用户信息、系统信息、系统进程、系统服务、设备信息、用户和组以及文件操作等状态信息的监视和记录。

(2)应用监控 Agent。对网络终端中的进程和服务进行监控。通过对网络终端进程和服务信息的实时采集，并根据监控策略采用白名单和黑名单两种方式控制网络终端中的进程和服务。

(3)外设监控 Agent。根据相应安全策略对受控终端的 USB 端口、串行端口、并行端口、打印端口等外设接口以及 USB 盘、软驱、光驱、调制解调器等外部设备实施存取控制。

(4)用户行为监控 Agent。对网络及终端用户的行为进行监控，包括登录、文件操作、磁盘操作、程序卸载与安装等。

(5)网络行为监控 Agent。实现对网络及终端用户的网络使用和访问等行为进行监控，放行符合安全策略的网络行为，禁止违反安全策略的网络行为。

监控 Agent 采用智能代理技术实现，可以根据监控业务的调整进行灵活的增加、删除和修改。

2.2 监控 Agent 的功能模块

监控 Agent 的功能模块框图如图 3 所示。

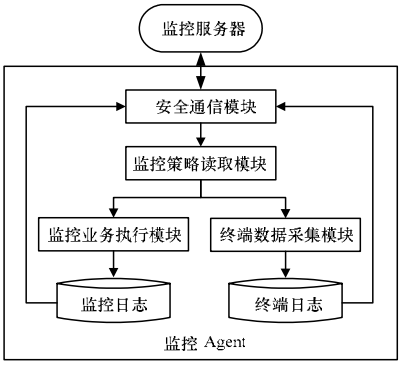

图 3 监控 Agent 的功能模块

监控 Agent 的工作过程为：

(1)监控 Agent 通过安全通信模块读取监控服务器传来的监控策略和操作指令。

(2)监控 Agent 根据监控策略和操作指令执行监控业务，并记录监控结果形成监控日志。

(3)监控 Agent 通过终端数据采集模块对终端系统信息进行采集，形成终端日志。

(4)监控 Agent 将监控日志数据和终端日志数据通过安全通信模块发送到给监控服务器。

3 系统实现

3.1 监控 Agent 的实现

利用Agent机制来实现网络安全监控的前提是开发或者选择提供Agent基础功能的平台。目前已经有较多的Agent平台可供选择，并且提供了成熟的开发环境。本文选择Zeus多代理设计开发平台(Zeus agent building toolkit)。Zeus是英国电信实验室智能代理研究小组综合现有的代理技术规范，研究开发出的用于快速开发协作式多代理系统的设计开发平台。Zeus系统严格遵循FIPA97 规范，系统的Java源程序全部公开以方便用户研究与扩展[3-4]。

本文在 Zeus 平台的基础上扩展了 Zeus 的能力，添加了一定的约束,构建起网络安全监控系统的框架。系统利用 Zeus 的 NameServer，Facilitator 等公共代理(Utility Agents)提供的代理名字与功能解析服务，从而实现了 Agent 的网络分布。同时为了实现平台无关性，系统采用 Java 作为开发语言，开发工具为 JDK1.42。

3.2 监控数据采集与分析的实现

网络安全监控系统的监控数据包括监控日志、网络终端日志、网络安全监控系统自身日志 3 部分。

(1)监控数据采集。监控数据采集包括监控日志数据采集、网络终端日志数据采集和网络安全监控系统自身日志。监控 Agent 在执行监控业务的同时，记录监控过程和监控结果，形成监控日志；监控 Agent 的终端数据采集模块负责采集网络终端的系统日志；网络安全监控系统自身日志主要包括网络安全监控配置信息及用户操作日志，由监控控制台进行记录，形成日志并存储到本地日志数据库。这些监控数据由安全通信模块在安全通信信道的保护下，统一传送到监控服务器。

(2)监控数据的预处理。监控服务器接收到监控数据后，由于网络数据流量很大，不利于对数据的分析，因此服务器首先对监控进行数据预处理，去除监控数据中重复和无关的数据，生成供下一步分析的目标数据源并存入监控数据库。接下来即可以充分利用数据库的优点，进行监控信息的查询与综合分析。

(3)监控数据的综合分析。在监控数据中，监控日志记录了监控Agent对受控终端的监控过程和结果,终端日志则记录了受控终端的系统事件、系统进程、系统服务等信息，对于检测和发现对受控终端的入侵以及受控终端中资源和权限滥用具有重要作用，系统对监控日志和受控终端日志进行了详细而综合的分析,以全面监视和保障网络中各个终端的安全，分析方法采用基于特征的统计分析方法[5]。网络安全监控系统自身日志的分析主要用来为其他日志分析提供参考。

综合分析完成后，由安全监控报告生成模块负责把监控数据的分析结果汇总成详细的安全监控报告，并以文本文件或网页的形式输出。

3.3 层间安全通信的实现

系统采用层次结构，需要保证监控代理与监控服务器、监控控制台与监控服务器之间通信的安全。系统通过对 SNMPv3 协议进行编程扩展来保证层间通信的安全。系统定

义的监控服务器与监控 Agent 之间通信的数据格式如图 4 所示。

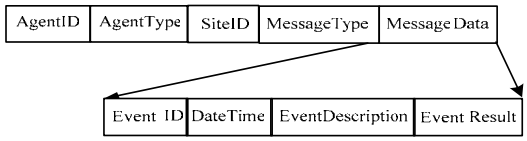

图 4　层间通信数据格式

其中，AgentID 为代理标识；AgentType 为 Agent 类型；SiteID 为产生事件的终端的唯一标识；MessageType 为信息类型；MessageData 为信息数据内容；EventID 表示由系统定义的事件 ID；DateTime 表示事件发生时间；EventDescription 表示对事件的描述；EventResult 则表示对事件的监控处理结果。

4　系统应用分析

对系统进行了测试和使用，应用表明系统具有以下特点：

(1)有效性。通过模拟测试以及在实际工作环境下测试，系统能够准确记录和反映非法主机登录、非法网络访问、对终端中的资源和权限的滥用，以及网络中的其他安全事件。

(2)易扩展性。系统的功能、使用范围易于扩展，对于新的监控功能或者新的网段，只需添加新的监控 Agent 即可。而且系统采用了层次结构，系统结构本身也可以进行方便、灵活的扩展。

(3)可靠性。系统采用层次结构和分布式监控 Agent，减轻了监控服务器的工作负荷，降低了对网络带宽的需求，提高了系统及网络的可靠性。

(4)自身安全性。系统采用经过自定义扩展的 SNMPv3 协议实现安全通信，解决了通信和数据传输的安全问题。

5　结束语

本文设计并实现的网络安全监控系统采用了层次结构，将安全监控、数据采集等功能分散到各个受控终端的监控 Agent上，减轻了监控服务器的工作压力，克服了在流量极大的情况下容易造成丢包，对网络带宽的要求高、中心管理部分易成为系统瓶颈等缺点[6]。与传统网络监控系统相比，具有更大的灵活性和可扩展性，具有良好的性能和实用价值。

参考文献

[1] 邓　瑛, 常国岑, 王晓辉. 网络安全监控与审计系统的设计与实现[J]. 计算机工程, 2002, 28(14): 195-198.

[2] 张　承, 蒋东兴, 刘启新, 等. 浅析网络监控系统对网络性能的影响[J]. 小型微型计算机系统, 2002, 23(9): l059-l062.

[3] Boudaoud K, Labiod H, Boutaba R, et al. Network Security Management with Intelligent Agents[C]//Proc. of Network Operations and Management Symposium. Honolulu, HI, USA: [s. n.], 2000: 579-592.

[4] Turck F, Vanhastel, SBackx P. Design of Generic Architecture for Service Management and Monitoring of Service Level Agreements Through Distributed Intelligent Agents[C]//Proc. of Intelligent Network Workshop. Boston, MA, USA: [s. n.], 2001: 50-57.

[5] 温　研, 王怀民, 胡华平. 分布式网络行为监控系统的研究与实现[J]. 计算机工程与科学, 2005, 27(10): 13-15.

[6] 王旭仁, 毕学尧, 许　榕, 等. 实时网络安全监控系统的设计和实现[J]. 计算机工程, 2005, 31(4): 209-211.

(上接第 171 页)

$$\sum_{i=1}^{n}(h_iK_i+R_i)+K_B\,?=sp+(m'+(T)_x)T$$

或 $(T)_x(hK_A+R+K_B)?=sp+m'T$ 后，原始签名者 A_i 不能否认将代理签名权委托给了 B，代理签名者 B 也不能否认对消息进行了签名，因为完成委托与代理签名协议过程的前提是掌握相应私钥及协议中产生的随机数。

(4)代理签名权撤消灵活

当原始签名人想撤消代理签名者 B_i 的代理签名权时，他可以通过媒体公开宣布原有委托信息(R_i , f_i)不再有效，注销代理签名密钥 f'。

(5)算法简洁、高效

方案充分发挥了 HCC 密钥短、安全性高的优势，在 64-bit 处理器的计算机上，该方案的运算可以用单个计算机的字去处理，避免了多精度整数运算，大大降低了存储和运算的系统开销。

需要特别指出的是，签名者 B 每次签名时必须更换随机产生的秘密参数 v，否则攻击者根据 s 与 m' 值的变化，从签名式(1)~式(3)可得：

$$\begin{cases}s=(T)_x(hk_A+u+k_B)-m'v(\mathrm{mod}\,l)\\ s'=(T)_x(hk_A+u+k_B)-m''v(\mathrm{mod}\,l)\end{cases}$$

$$\Rightarrow v=(s'-s)(m'-m'')^{-1}(\mathrm{mod}\,l)$$

$$k_B=(s+m'v)(T)^{-1}{}_x-hk_A-u(\mathrm{mod}\ l)$$

同理在多重代理签名中，由式(5) ~式(7)可得

$$\begin{cases}s=k_B+\sum_{i=1}^{n}(h_ik_i+u_i)-(m'+(T)_x)v(\mathrm{mod}\,l)\\ s'=k_B+\sum_{i=1}^{n}(h_ik_i+u_i)-(m''+(T)_x)v(\mathrm{mod}\,l)\end{cases}$$

$$\Rightarrow v=(s'-s)(m'-m'')^{-1}(\mathrm{mod}\,l)$$

$$k_B=s-\sum_{i=1}^{n}(h_ik_i+u_i)+(m'+(T)_x)v(\mathrm{mod}\,l)$$

如不更换随机数，协议过程越多私钥就越不安全，当协议次数大于一定次数时，就完全能够攻破私钥，破坏整个签名系统。

4　结束语

随着电子商务与电子政务的不断发展，代理授权协议越来越多地体现出了其应用价值，但是现有代理签名协议存在着密钥量大，运算复杂，软硬件实现时系统开销大、安全性差等缺陷。本文研究了如何充分发挥超椭圆曲线密码密钥长度短、效率高、安全强度大的优势，设计面向工程应用的代理授权方案。本文提出的基于超椭圆曲线密码的混合代理签名方案体现了低通信消耗与低系统开销的设计原则，特别适合当前电子商务与电子政务等网络业务需要快速交互反应的发展趋势，有广阔的应用前景。

参考文献

[1] 周宣武, 杨晓元. 网络中基于椭圆曲线密码的密钥管理方案[J]. 计算机工程, 2004, 30(11): 89-91.

[2] Avanzi R M. Aspects of Hyper-elliptic Curves over Large Prime Fields in Software Implementations[C]//Proc. of International Association for Cryptology Research. New York: Spring-Verlag, 2004: 148-162.

[3] Abe M, Ohkubo M, Suzuki K. 1 out of n Signature from a Variety of Keys[C]//Proc. of Advances in Cryptology-ASIACRYPT'02. New York: Spring-Verlag, 2002: 415-423.

[4] 杨义先, 孙　伟. 现代密码新理论[M]. 北京: 科学出版社, 1999.

[5] Wollinger T, Guajardo J. Hyper Elliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves[C]//Proc. of CHES'03. New York: Spring-Verlag, 2003: 351-365.