广西科学院学报
Journal of Guangxi Academy of Sciences
2006,22(4):302～305,308
Vol. 22,No. 4 November 2006

一个内网安全监控系统的设计与实现*

Design and Implementation of an Intranet Security Monitoring System

李陶深,严 毅,曾 亮,黄国石,蔡世平,黄顶源
LI Tao-shen, YAN Yi, ZENG Liang, HUANG Guo-shi, CAI Shi-ping, HUANG Ding-yuan

(广西大学计算机与电子信息学院,广西南宁 530004)
(School of Computer, Electronics and Information, Guangxi University, Nanning, Guangxi, 530004, China)

摘要:在 Microsoft Windows NT 系列平台下设计与实现内网安全监控系统。该系统分为监控服务器系统、数据库系统和客户端的响应系统三部分组成,能够重点解决局域网内部系统行为安全和网络行为安全问题,实现网络行为的监视和管理。

关键词:监控系统 内网 数据安全 客户机/服务器
中图法分类号:TP393.07 **文献标识码**:A **文章编号**:1002-7378(2006)04-0302-04

Abstract: On the basis of analysis of the security problems in the intranet, an architecture of the intranet security monitoring system is proposed. The intranet security control techniques in the platform of Microsoft Windows NT series are explained. This system is mainly to solve the problems of LAN internal system behavior security and network behavior security and fulfill the monitoring and control of network behavior.

Key words: monitoring system, intranet, data security, Client/Server

计算机网络的迅速发展,使行业和企业的信息化程度迅速提高,但是因网络应用而出现的隐患和安全问题越来越突出。目前,常用的安全产品主要集中在网络反(防)病毒、防火墙、IDS 和物理隔离网闸等。尽管防火墙和入侵检测技术在防范和抵御来自外部网络的攻击和破坏上担任着重要的角色,但是它们更多地关注来自外部的攻击和破坏,主要实现对网络入侵进行监控和防护,抵御低阶通讯层次的攻击,防止主机及个人电脑的入侵,检测恶意的可执行程序和杜绝网络资源的滥用。防火墙和入侵检测技术对于内部用户攻击和威胁事件以及机构内部信息的保密安全管理几乎起不到作用。

收稿日期:2006-07-17
作者简介:李陶深(1957-),男,广西邕宁人,教授,主要从事网络安全、网络路由、分布式数据库方面的研究。
* 本文得到广西留学回国人员科学基金项目(桂科回 0342001)和广西电子信息应用项目(桂电办 2004-17 号)联合资助。

据美国联邦调查局(FBI)对 484 家公司进行的网络安全专项调查结果显示[1]:85%的安全威胁来自单位内部,其中有 16%来自内部未授权的存取,有 14%来自专利信息被窃取,有 12%来自内部人员的欺骗,只有 5%来自黑客的攻击。这些都使得内网安全问题变得越来越突出。如何更有效地填补以防火墙、入侵检测系统等为代表的网络安全产品对内网安全控制的不足,保证内部网络的安全已经成为一个迫切的、重要的任务。

本文提出一种专门针对内部网络安全管理的体系结构,并设计实现了内网安全监控系统,通过直观有效的安全策略设置,对内网中的各种行为进行监控和管理;并通过完善的日志记录各种敏感行为的痕迹,为管理和审核提供有效途径。

1 内网安全监控系统的设计目标

根据网络安全的特征,结合对内网安全问题的分析,我们将内网安全监控系统的总体设计目标定

位为:通过实施具体的安全防护技术,建立完整的内网信息安全防护体系,采用合适的安全技术和进行制度化的管理,以安全策略、安全资源管理等方式,对内网中的机群进行统一管理,确保在保护区域内构建一个安全控制系统,从多个层次、多个角度,构建内网信息安全保障技术框架。

系统设计的具体目标有:(1)对局域网中的计算机的各种行为实施监控和统一管理,使得保护区域内的信息与网络资源得到统一控制,确保相关资源被合法地使用,保障内网中的信息与网络系统稳定可靠地运行。(2)通过对内网中网络信息流传输进行有效的监督控制,对涉及非法或敏感的操作或行为进行过滤和报警,以达到控制计算机的网络交互行为,防止敏感、机密信息从网络交互过程中泄露的目的。(3)通过对计算机文件系统和各种外设进行监控,掌握和控制远程计算机的资源,监控数据的读写和拷贝、移动等操作,并结合各种外设的特性和合适的加密手段对计算机的重要数据(各种类型的文件等)实施安全保护,防止机密信息被非法访问或者窃取,阻止重要数据从计算机外设途径泄露。(4)通过身份验证、信息加密、进程自我保护、系统文件保护等手段保障监控系统自身的安全。(5)记录敏感的行为痕迹,当出现安全问题需要进行事件回朔分析时,系统能够以日志、数据文件等形式高效地进行事件重现或痕迹描述,提供内网中机群的安全数据审计分析报告。

该内网安全监控系统是在 Microsoft WindowsNT 系列各个平台下开发实现,可对内部网络系统的失密、泄密管理,阻止内网主机通过在线方式、离线方式和数据拷贝转移等方式泄漏敏感信息,实现对网内计算机进行合理、有效的信息安全管理,最大限度地保障信息网络内部信息的安全。

2 内网安全监控系统的总体架构

内网安全监控系统采用多对一的 Client/Server (C/S)架构,系统总体结构如图 1 所示。监控服务器程序运行在管理员操作的服务器上,监控客户端程序运行在内网中的各台主机上。监控服务器对监控客户端进行控制,通过对监控客户端进行身份验证,向监控客户端发送命令、设置策略等方法,规定监控客户端的工作方式。监控客户端还有一个离线保护的策略库,当与监控服务器断开连接的时候可以使用离线保护策略对各个主机进行安全防护。

为了在较复杂的网络环境下适应远程管理的需要,达到通过远程计算机管理监控服务器工作的目的,系统预留了可以扩展的远程管理系统接口。

当前系统需要对分散的桌面系统进行统一管理,并且需要有效地控制各种资源的使用,对系统进行监控和防护,并且可随着管理的需要进行策略变更,灵活地控制机群的各种行为。所以有必要在受控的机器上运行一个后台的程序,用于接受管理员的各种命令和策略设置。为提高 C/S 模式的安全性,在受控端后台运行的程序需要做好自我防护,以抵御外部的破坏和攻击,防止被意外删除和终止。监控客户端作为一个不可见的后台监控程序,采用监控事件通知和被动响应管理服务器命令的方式,可大

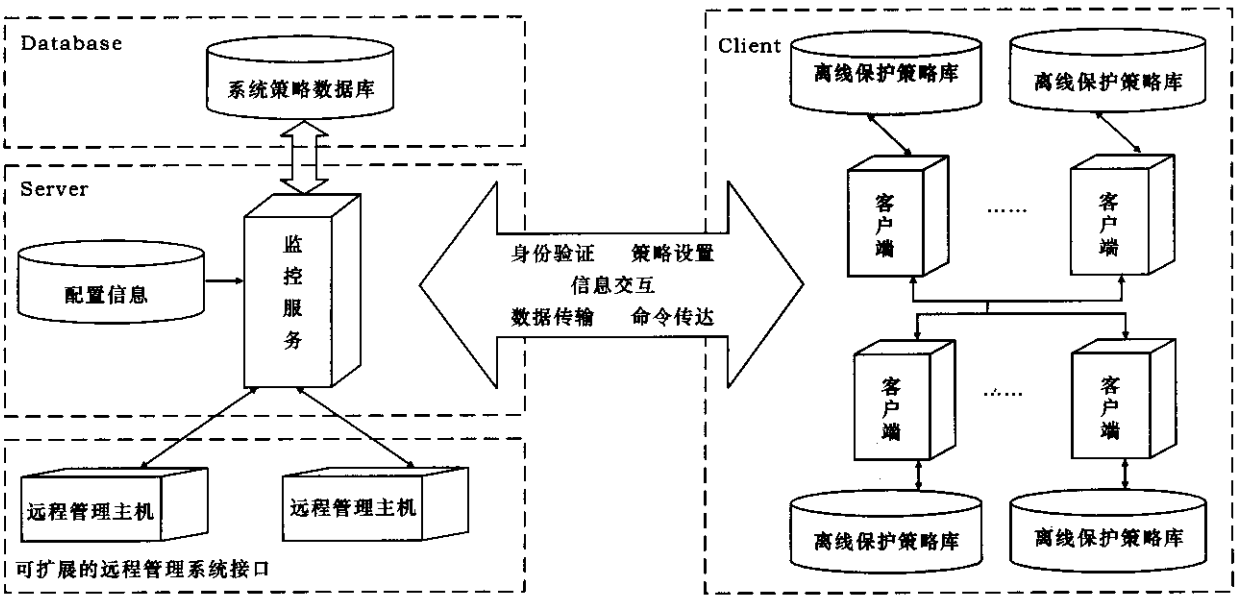

图 1 内网安全监控系统结构

大减少系统资源和网络带宽的占用。

内网中分散的桌面系统是安全管理最大的障碍,系统采用C/S的方式对内网的机群进行集中统一管理,由管理员操作服务器,通过设置安全策略的方式,将策略传达到内网中的客户端,客户端根据策略进行响应,监控并保障受控端(内网机群)的安全,保证内网的资源被合法地使用,防止分散的桌面系统失去控制而引发安全问题。

C/S的工作方式应用于内网安全管理显得比较灵活,它允许客户端系统更大限度地附着到远端系统,与服务器端之间也可以灵活地进行通信,客户端可以访问服务器上的资源,灵活地把信息(特别是处理比较大的数据)反馈给服务器。当处于离线状态(即和管理员运行的服务器程序断开连接)时,可使用内置的安全策略,或者使用最近一次由管理员指定的策略对本机进行离线防护,保证受控的机器在与管理服务器脱机的状态下仍然得到控制和保护。

3 内网安全监控系统设计

内网安全监控系统分为监控服务器系统、数据库系统和客户端的响应系统三部分组成。

3.1 监控服务器系统(控制台)

可在任意一台内网计算机上运行监控系统控制台程序,已获得授权的系统管理员可通过控制台对所有的客户端进行监控,包括:查看修改所有策略规则、查看所有监控日志、对单一客户端进行实时监控。监控服务器系统主要分为以下功能模块。

3.1.1 策略规则

每一个监视控制项都有3类策略规则,即全局策略规则、组策略规则、单机策略规则,它们的优先级是:全局策略<组策略<单机策略,管理员可以进行多种设置。对策略的任何改动,控制台将会通知受影响的客户端立即更新策略规则。在策略无改动的情况下,管理员也可以强制客户端更新策略规则。

3.1.2 监控日志

监控日志模块的功能是浏览某客户端的各个监控日志,并提供强大的搜索功能。内网安全监控系统通过以日志形式记录计算机终端用户的操作,为规范计算机终端用户的行为提供依据;同时,通过日志进行安全审计和事后追查是安全防范的有效手段,记录日志能够对企图进行数据破坏的行为起到威慑作用,并为安全审计提供有力的依据。

不同的行为产生不同性质的日志信息,内网安全监控系统根据行为分类存储日志信息,方便用户对日志信息进行的操作,及时备份和删除客户端的日志信息。包括:(1)删除全部客户端日志信息;(2)删除选定客户端日志信息;(3)查询客户端的日志信息;(4)查看特定时间的日志信息;(5)查看全部日志信息。

3.1.3 实时监控

控制台直接连接某一客户端,令其进入实时监控模式。处于实时监控模式的客户端,监视所产生的日志不再写入本地数据库,而是直接写入系统中心数据库,控制台相应监控窗口定时刷新以取得该客户端的最新日志。

为了便于用户对内网安全监控系统进行管理操作,将提供默认的监控配置和用户自定义配置两种配置方式,便于不熟悉和熟悉本系统配置的用户配置本系统的监控策略。默认监控配置是在用户不熟悉相关控制策略配置的情况下,默认监控配置能够提供足够的安全监控需求,为不同安全级别选择不同的默认监控策略。自定义监控配置是在用户熟悉各种监控策略配置的情况下,用户可选择自定义监控策略,修改默认监控策略或者自定义全新的控制策略等,满足不同安全监控需求。

3.1.4 计算机运行管理

任意一个客户端的安装,均需要得到授权方可成为监控系统的一员,防止非法人员通过安装一个客户端后,在客户端这个面具后面进行非法活动。所有联网的计算机,如果发现没有安装客户端、或者客户端不正常工作(比如不产生应有的监控日志、控制台无法对其进行实时监控),均视为内网非法用户,应发出警报通知各控制台并记录。

内网安全监控系统将提供以下具体管理行为,用于对内部网络中的本地计算机进行资源管理。

3.1.4.1 监控系统进程 提供远程停止Windows操作系统中活动进程的功能;提供基于策略的系统进程远程管理功能。

3.1.4.2 管理用户和组 提供远程管理Windows操作系统中用户和组的功能。

3.1.4.3 卸载已安装程序 提供远程卸载Windows操作系统中已安装应用程序的功能。

3.1.4.4 监控系统服务 提供远程管理Windows操作系统中已安装的服务以及驱动的功能:远程启动/暂停/停止/继续服务,远程配置服务启动方式,远程修改服务属性。

3.1.4.5 在线监测与远程控制计算机 监测计算机的开机、关机、上网、下网、网络连接、身份认证、文

件操作等行为,捕获其当前用户信息等。

3.1.4.6 远程控制用户行为 可以设置键盘是否锁定、鼠标是否锁定、光驱是否锁定、软驱是否锁定、是否锁定注册表、是否隐藏桌面、是否屏蔽热键、是否关闭任务栏、是否隐藏开始按钮等。

3.1.4.7 远程管理共享资源 可查看共享文件夹列表,并可设置共享的开放与禁止。

3.1.4.8 可远程操作计算机 远程控制计算机的重启、关机、注销、锁定、睡眠、屏保等。

3.2 数据库系统

内网安全监控系统数据库分为控制台数据库和本地数据库。

3.2.1 控制台数据库

控制台数据库包括系统中心数据库、策略数据库和日志数据库。系统中心数据库安装在独立的数据库服务器上,使用 MSSQL;策略数据库和日志数据库分别部署到两台不同的服务器上,以减轻压力。

策略数据库存储各种策略规则。控制台可直接查看修改策略规则,作为控制台控制客户端的第一依据(另一个依据就是:在实时监控的时候控制台直接向客户端发送指令,该指令只在客户端当前进程内有效);客户端主动获取策略规则。

日志数据库存储各种客户端提交的日志,供控制台查看。

3.2.2 本地数据库

本地数据库包括策略数据库和日志数据库。其中:(1)策略数据库用于保存客户端配置、专用策略规则。客户端启动时或收到策略指令时,均会从系统中心数据库读取与本机相关的策略规则,并覆盖本地策略,然后再从本地提取策略来进行监控控制。(2)日志数据库临时存储各监视模块产生的日志。每隔一段时间,客户端检查本地是否有未提交给中心数据库的日志,如有,则提交给系统中心数据库,本地日志删除。

3.3 客户端的响应系统

客户端的响应系统主要根据策略规则执行相应的监视和控制功能,它主要提供以下功能。

3.3.1 内部网络安全管理

3.3.1.1 IP 地址访问控制 计算机的网络访问主要依靠 IP 地址,通常情况下,内部网络中任意两台计算机之间都可以通过 IP 地址访问,这给内部网络安全带来了很大隐患:第一,内部员工有可能通过 IP 地址访问其他计算机,获取不适当的资料;第二,一旦内部网络遭受外部网络黑客入侵时,黑客很有可能利用被入侵的计算机通过 IP 地址访问其他未被入侵的本地计算机。为了消除以上存在的隐患,内网安全监控系统将提供 IP 地址访问控制功能,使计算机对本地网络的访问限定在安全范围之内。功能包括限定能够访问的 IP 地址和限定不能访问的 IP 地址。

3.3.1.2 端口访问控制 计算机的网络通信归根结底是通过网络端口进行的,端口也正是计算机安全中最薄弱的地方,各种入侵者或者黑客软件往往都会利用端口漏洞对计算机系统进行攻击。内网安全监控系统提供端口访问控制功能,为网络安全管理员进行安全管理提供一条有效途径。功能主要包括限定开放或不开放的端口。

3.3.2 数据信息安全保护

数据信息安全的特征包括 3 个方面:数据完整性、数据机密性、数据操作的不可抵赖性[2]。存储媒介携带、网络传输以及文档打印是信息泄漏的主要途径。内网安全监控系统通过禁止移动存储媒介携带、禁止网络传输、禁止打印等手段阻止数据信息的不适当传播,保证数据信息的机密性。另外,对数据信息的操作行为进行日志记录,为安全审计提供依据,保证数据操作的不可抵赖性。具体实现如下:

3.3.2.1 存储设备控制 存储媒介携带是信息泄漏的主要途径之一,各种可移动存储媒介的使用都可能造成信息泄漏[3]。为防止这一途径造成的信息泄漏,系统要能够禁用通过外部设备接口(IEEE1394/ USB/PCMCIA)连接到本地计算机的物理存储设备:包括已连接的设备和将要连接的设备。

3.3.2.2 网络传输控制 网络传输是信息泄漏的另一主要途径,通过邮件的发送、FTP 传输和 HTTP 传输都可能造成信息泄漏[3]。为防止这一途径造成的信息泄漏,本系统应能够禁止邮件发送、FTP 和 HTTP 传输。这些功能可通过封锁特定的网络通讯端口实现。但由于邮件发送、FTP 和 HTTP 又是计算机应用中不可避免的应用功能,当不得不使用邮件发送、FTP 和 HTTP 传输时,将通过记录邮件发送日志、FTP 和 HTTP 传输日志为安全审计提供可审查的信息。

3.3.2.3 打印控制 信息泄漏的另一途径是数据信息文件的打印。数据的信息量通常是很大的,除了存储设备携带和网络传输,数据信息打印后携带出

(下转第 308 页)

3 系统的主要优势

凭借ZigBee技术的种种优点，将ZigBee技术引入RFID中，使得基于ZigBee技术的无线射频识别系统有了明显的改良，其主要优势在于：(1)长距离的识别不需要进行方向配置，提高系统灵活性；(2)成本低、时延小、技术相对简单、存储容量大，在用电管理上，通过睡眠唤醒功能上的改进，使其功耗大大降低；(3)由于现在ZigBee芯片集成的功能越来越多，其本身可扩展性高，促使整个系统的可扩展性也随之提高；(4)ZigBee技术在通信时采用CSMA\CA机制，保证了数据信息的可靠性；(5)ZigBee技术提供CRC数据包完整性校验，使用了AES－128的加密算法，并采用基于直序列展频技术的接取方式，确保整个传输阶段的安全性，提高了抗干扰特性和保密性[4]。

4 结束语

目前RFID技术的难点还是远距离识别和识别的准确抗干扰性，只有更全面地解决RFID技术的种种问题，才能使得RFID的应用范围更广泛。基于ZigBee技术的无线射频识别系统能很好地解决其中一些主要难点，为RFID技术注入新的强大的活力。本文在充分考虑RFID系统的现有状况和深入分析技术难题的前提下，将ZigBee技术与RFID技术相结合，构建一套基于ZigBee技术的无线射频识别系统。ZigBee技术和RFID技术还在不断的发展，随着技术的不断更新，其结合后的优势将更为突出，将更好地改善我们的生活。

参考文献：

[1] 李锦涛，郭俊波，罗海勇，等. 射频识别(RFID)技术及其应用[C]. 信息技术快报，2004：11.
[2] 王权平，王莉. ZigBee技术及其应用[C]. 现代电信科技，2004.
[3] MC13192 Reference Manual：Rev 1. 3[EB/OL]. [2005-04]. http://www. freescale. com/files/rf _ if/doc/ref _ manual/.
[4] IEEE STD 802. 15. 4：Wireless medium access control (MAC) and physical layer (PHY) specifications for Low-rate wireless personal area networks (LR-WPANS)[M]. New York：Institute of electrical and electronic engineers，Inc，2003.
[5] 蒋泰，蒋利. 基于ZigBee技术的低成本无线数传系统的实现[J]. 广西大学学报，2005，30(4)：332-336.

(责任编辑：邓大玉)

(上接第305页)

去也会造成信息泄漏。为尽量避免不适当的数据信息打印，可以对打印功能实行相应的控制。实现打印控制功能有两个途径：(1)将打印机与本地计算机的逻辑连接停用；(2)禁止调用操作系统打印功能。

3.3.2.4 获取数据信息操作的日志 除了数据信息泄漏之外，数据信息的篡改和销毁也会使企业或单位的利益遭受损害，而数据信息的篡改和销毁归根结底大部分都是对数据信息存储文件的操作。对数据文件的操作是不可避免的，除了相应的备份和操作权限的限制以外，对数据文件的破坏性操作的追查，能避免对数据文件的再次破坏。本系统将对有可能对数据文件造成破坏或者信息泄漏的操作行为，包括文件的打开、删除、复制、剪切、移动、另存为等，以日志形式记录，从而为对数据泄漏和数据信息的破坏性操作的追查提供依据。

4 结束语

本文在现有的计算机网络安全体系的基础上提出了一个内部网络安全保障的解决方案。本文的重点是研究和实现Windows2000/XP/2003系统操作平台的设备访问监视和控制。所设计实现的内网安全监控系统由安全策略设置、安全资源管理、操作行为跟踪等主要系统组成部件，可监控内网系统网络资源使用和主机数据访问情况，抵御来自于内、外网的恶意访问和攻击行为，阻止机密、重要的信息通过网络等途径泄露，防止或监视重要数据被非法查看、拷贝、移动或者删除，并以日志、数据文件等方式提供安全问题审计分析报告，从而对内部网络中计算机资源的使用进行有效的监督和控制。

参考文献：

[1] 李涛. 网络安全概论[M]. 北京：电子工业出版社，2004.
[2] 沈昌祥. 信息安全工程导论[M]. 北京：电子工业出版社，2003.
[3] 谭思亮，求是科技. 监听与隐藏——网络侦听揭密与数据保护技术[M]. 北京：人民邮电出版社，2002.

(责任编辑：韦廷宗)