内网安全综合审计监管系统的设计与实现

文/赵 晖 严永锋

随着计算机网络的发展，网络安全现状异常严峻，保障网络安全特别是内网安全成为企业和组织日益关注的焦点问题。然而，现有的网络安全技术更多注重的是对外网入侵的防范，对内网行为的监管考虑不周，安全审计监管系统可以对内网的事件进行记录和检查，有效防范和发现内网的违规操作。所以，研究内网安全审计和监管技术具有重要的现实意义。

内网安全审计和监管技术的提出

本文提出了基于系统API(Application Programming Interface，应用程序编程接口，简称API)替换的用户行为审计技术。

在Window的应用程序或用户操作都可以归结为操作系统中对系统API的调用。系统的API是按照动态链接库的方式存放的。

为了对用户的行为进行审计，可以将用户进程中的API函数地址替换为自己定义的API函数，并在自己定义的API函数进行安全检查和记录，就可以实现该进程行为的监控和审计。

因此要监控整个操作系统的操作行为，可以将操作系统的所有用户态的进程的相应API进行替换，那么就可以对整个操作系统上的行为实现监控。

实现这种方案的关键和难点在于API的替换。

我们知道，Windows是一个消息驱动的32位操作系统。在Windows中，所有正在运的进程都有一个独立的2GB的虚拟地址空间，进程之间相互不可见。要在目标程序中运行监控代码就必须将监控代码注入到目标进程。一种常用的方法就是将监控代码编译成一个DLL，再将该DLL注入到目标进程中。

在目标程序中注入监控代码实现监视的方法，常见以下几种方式:

(1) 在目标函数入口写入跳转指令jmp，跳转至监视代码实现监视

(2) 利用API Hook功能，修改EXE和DLL的导入地址表(Import Address Table)，将监控代码中函数入口地址写入导入表中，当EXE或DLL调用其它DLL中API函数时，就可以跳转到监控代码中实现监控。

通过替换系统API方法，我们成功实现了在Windows平台上对用户行为的强制审计，解决了系统实现的一个难题。

1. 系统的总体设计

3.1系统简介

该系统采用的一套B/S结构与C/S结构结合的全新体系结构：在服务端与受控主机客户端之间，采用C/S模式；在服务端和管理用户之间，采用B/S模式。采用这种结构优点在于：信息发布采用B/S结构，保持了瘦客户端的优点；数据交互采用C/S结构，只涉及系统维护、数据更新等，不存在完全采用C/S结构带来的客户端维护工作量大等缺点；对于原有的应用，只需开发用于发布的WWW界面，就可非常容易地升级；将服务器端划分为WEB服务器和WEB应用程序两部分，方便系统维护扩展。

整个系统由安全代理、安全控制中心、管理客户端三部分组成。

3.1.1安全代理

安装在受控计算机上的代理软件，其根据管理员配置的安全策略对用户行为进行监控，当有非法行为发生时，安全代理根据安全策略对用户行为进行控制，同时产生相应的报警事件，以便事后追查、处理。

3.1.2 安全控制中心

该部分由硬件和软件两部分构成，其主要功能是向安全代理下发管理员定义的各种安全策略，接收各个安全代理发送的各种事件信息，同时向管理人员提供各种配置、查询接口，为保证信息传输的安全性，安全控制中心与安全代理、管理客户端的通信，均采用了SSL协议。

3.1.3客户管理端

系统采用的是B/S和C/S相结合的结构,客户管理端就是普通的WEB浏览器。

3.2基本设计概念和处理流程

整个系统采用C/S结构，总体上分为三个大模块，分别为服务器模块，Web模块，客户端模块。

系统管理员通过带有SSL的浏览器通过网络访问Web模块进行用户配置和策略配置，Web模块通知（本地SOAP: Simple Object Access Protocol即简单对象访问协议）服务器模块策略发生改

变，服务器将新的策略发送给客户端模块去执行；系统管理员通过浏览器来对客户端产生的违反安全策略的行为的日志进行审计；通过浏览器获得受控主机的受监管信息。

3.3模块间依赖性描述

(1) 用户管理

系统通过浏览器配置用户，调用JSP模块对系统数据库进行操作；数据库中的数据通过JSP模块读取配置，在浏览器上显示。

(2) 策略配置

系统通过浏览器配置策略，调用JSP模块对系统数据库进行操作；数据库中的数据通过JSP模块读取策略，通知服务器模块重新加载策略，并在浏览器上显示。

(3) 客户端控制

客户端将监控结果定时发送给服务器，服务器在将其发送到数据库，如果服务器连接不上，则将安全日志存在本地待恢复连接后，再发送安全日志。从数据库读取安全策略，通过服务器将其发送给指定客户端，并在浏览器上显示。

4. 总结

安全管理员通过系统管理不同的主机,解决了目前不同的主机需由不同的系统管理员进行管理,管理分散、难度大的问题；系统提供了良好的策略管理界面,强化并简化了安全管理。该系统与防火墙、网络入侵监测系统、网络管理系统等安全管理系统建立有机结合,可以构成一个综合性的安全系统。系统稳定性测试中，各监控模块功能的使用，没有影响受控主机的正常运行；客户端无故障运行时间大于7×24小时（为了保证系统能满足用户连续使用一周时间）；服务端支持的用户数最大达到1000户，无故障运行时间大于30×24小时。

由于本系统涉及的深度、广度都较大,系统设计时间有限,还存在许多不足之处，在系统功能方面还要作进一步的研究和改进，尤其对内网主机的邮件和病毒的审计和监管。以上的问题需逐步深化解决,以使系统更加完善。

（作者单位：陕西理工学院计算机科学与技术系）

相关链接

论网络环境下企业竞争对手识别与情报分析
上市公司网站程序安全需要注意的四个问题
浅论信息技术推动中小企业的发展
基于电子商务的现代物流技术浅析
网络环境下大型建设项目风险
网络调研存在的问题及解决方法
内网安全综合审计监管系统的设计与实现
电子商务环境下传统企业运营模式的转变