安全审计系统的自身安全解决方案*)

董振兴 陈 龙 王国胤 董安波
(重庆邮电学院计算机网络安全实验室 重庆400065)

摘 要 随着网络安全问题的日益突出,安全技术与产品也得到了飞速的发展。自身安全问题是网络安全系统的一个研究重点,网络安全产品首要解决的就是自身的安全问题。本文首先提出了一个电子商务的安全审计系统的体系结构,接着分析其可能存在的脆弱点,并给出相应的解决方案来保证它的自身安全,最后在实际开发和测试中验证了该方案的有效性。

关键词 安全审计,自身安全,安全通道

A Solution to the Self-Protection of a Security Audit System

DONG Zhen-Xing CHEN Long WANG Guo-Yin DONG An-Bo
(Lab. of Computer Network Security, Chongqing University of Posts & Telecommunications, Chongqing 400065)

Abstract As the problem of network security is becoming more and more serious, security technologies and products need to be improved quickly. Self-protection is one of the crucial characters of network security systems, and it should be a priority in our consideration. This paper presents a framework for an e-commerce's security audit system, and then analyzes its possible weakness. A self-protection solution for it is developed and implemented. The result shows that it works well.

Keywords Security audit, Self-protection, Safe tunnel

1 引言

黑客及病毒泛滥催生了安全技术与产品的飞速发展,目前已形成防火墙、IDS、防病毒、VPN、PKI/CA 等安全产品体系。伴随着各种安全产品的问世和广泛使用,一个问题越来越突出:安全产品在保护网络系统的安全的同时,它的自身安全如何得到保障呢?

自身安全问题是网络安全系统所必须解决的,如果没有完善的自身防护体系作为保障,即使拥有再强大的功能也无法实现[1]。当前,防火墙、网络防毒软件、入侵检测系统、加密系统等安全设备得到了广泛的使用,它们也首当其冲地成为黑客攻击的目标。以入侵检测系统为例,由于其工作在网络攻防的前线,攻击者一旦成功地侵入网络中的计算机系统,为了掩盖行踪和毁灭作案证据,他们首先要做的就是使检测系统瘫痪或者关闭检测进程。

安全审计是指根据一定的安全策略记录和分析历史操作事件及数据,发现能够改进系统性能和系统安全的一种信息安全保护技术。随着网络的发展,安全审计将显得越来越重要,无论是电子政务、电子商务还是公司内部网络监管,都离不开安全审计,安全审计系统已经成为当前研究和开发的热点。

本文首先提出了一个电子商务的安全审计系统的体系结构,接着分析其可能存在的脆弱点,并给出相应的解决方案来保证它的自身安全,最后在实际开发和测试中验证了该方案的有效性。

2 安全审计系统的体系结构

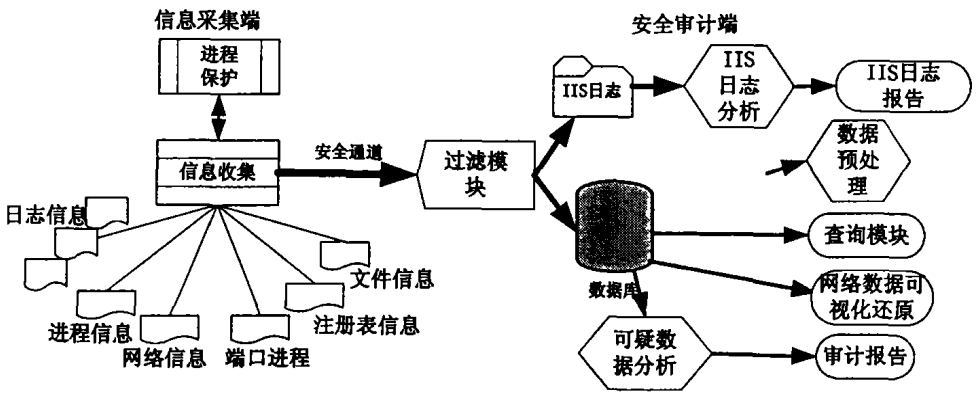

图1 系统体系结构图

*)基金项目:重庆市科技攻关计划项目(No.7220-B-21)、重庆市教委科学技术研究项目(No.020504)。董振兴 硕士研究生,主要研究方向:网络安全;陈 龙 硕士,副教授,主要研究方向:智能信息处理、网络安全;王国胤 博士,教授,博导,主要研究方向:智能信息处理、网络安全;董安波 硕士研究生,主要研究方向:网络安全。

目前，网络安全问题已经成为电子商务、电子政务发展的一大阻力，传统的技术手段如防火墙、安全路由器、身份认证系统等已经不能满足日益变化的网络安全需求了。对此，我们提出了一种安全解决方案，即电子商务的安全审计系统[2]，其体系结构如图1所示。

安全审计系统由两个主要模块组成：信息采集和安全审计。在结构图中，安全通道左边是信息采集模块，工作在网络服务器上，而安全审计模块则安装在另一台单独的主机（与网络隔离）上，由安全通道连接到信息采集端。

3 系统可能存在的脆弱点

电子商务系统服务器由于提供商业交易服务的缘故，成为了黑客经常攻击的主要目标。而用来记录电子商务应用和犯罪证据的安全审计系统，更会成为入侵者的重点攻击对象，受多方面的威胁。

审计系统工作在这种环境下，根据其体系结构，可能会有如图2所示的五个脆弱点。

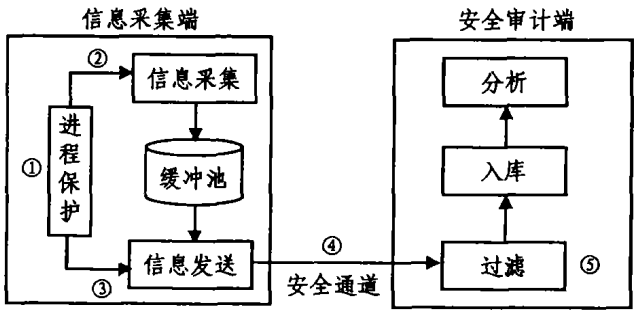

图2 脆弱点分布

这五个脆弱点分别是：信息采集端的进程保护脆弱点、信息采集脆弱点、信息发送脆弱点、数据传输脆弱点和安全审计端的数据过滤脆弱点。

（1）进程保护脆弱点。攻击者可能破坏进程保护模块，使其崩溃，导致信息采集和发送模块失去保护；

（2）信息采集脆弱点。攻击者可能进行大规模扫描和“洪水”攻击，导致采集模块超负荷工作而产生异常。另外，攻击者也可能攻击进程本身，杀掉信息采集进程；

（3）信息发送脆弱点。攻击者可能通过恶意程序关闭发送模块。除此之外，还存在发送过程中数据被篡改的可能；

（4）数据传输脆弱点。攻击者一旦获得控制主机的权限，即可以发现通道的入口，从而发送恶意数据、堵塞或者截断通道；

（5）数据过滤脆弱点。攻击者控制传输通道后，就可能对数据过滤模块的正常运行产生影响。当大量、高频率的恶意数据到达时，数据过滤模块会因系统资源的大量耗用而降低效率，从而导致大量有用数据的丢失。

针对以上几个脆弱点，下面将分别采取措施予以避免或消除。

4 解决方案

4.1 信息采集端

信息采集模块的核心功能由两个进程实现：信息采集进程和信息发送进程。若没有相应的保护机制，普通的进程很容易被其它进程关闭或中止，采集和发送进程也是如此。

目前，有多种保护进程的方法，如：兄弟进程，即同时生成两个进程，互相监视，若有一个退出，则马上启动对方；注册系统服务进程，由于其系统级别达到 System 级，一般的用户无法关闭；远程线程技术，将自身插入到系统进程的内存空间，效果同注册服务进程；还有驱动级的进程等。这些方法的特点可以分为两类，一是提升进程的用户级别，使其它进程无法访问；二是牺牲系统资源，以产生一个进程副本来保证进程始终在系统中运行。以上两类方法都存在不足之处，前者无法保证没有级别更高的恶意程序，后者是进程和其副本有同时被关闭的可能。除此之外，这些方法只是被动防守，在有些强力攻击下，这些进程也不能幸免于难。

为保护采集和发送进程，我们采取的方法由如下几个步骤组成：

步骤1：进行系统脆弱性扫描，关掉不必要的服务和进程；同时给出升级系统的建议；

步骤2：启动异常进程的检测模块，用来检测和清除当前操作系统里不正常或者多余的进程；

步骤3：启动信息采集模块；

步骤4：启动信息发送模块，该模块具有监测发送成功与否的功能；

步骤5：启动用来记录采集模块运行情况的日志记录模块；

步骤6：启动进程保护模块，即在操作系统的服务进程中插入远程线程，用来保障信息采集和发送进程的持续运行。

通过步骤1和2，可以降低信息采集模块被外部中止的可能性。步骤4发送数据时，将数据进行封装（一种简单的方法是前1个字节代表信息的类型，接下来的4个字节存放数据包的大小，跟着是若干字节的校验码，最后才是数据块）。这样，一旦数据被篡改，监测机制马上可以发现。步骤5可以用来审计信息采集模块的工作情况。步骤6则通过远程线程技术来达到守护信息采集和发送模块正常工作的功能。由于它本身寄居在操作系统的服务进程空间里，对外完全透明，因而不存在被摧毁的可能。在这种工作方式下，脆弱点1、2和3得到了强化。

4.2 数据传输通道

在信息采集端，数据采集和数据发送是分离的，这样做的好处是使模块功能单一化，工作时互不干扰。它们共享一个缓冲区（缓冲区对外部进程屏蔽），采集进程得到数据并写入缓冲区，发送进程从缓冲区读出数据，打包后放入传输通道。这样，数据能否被正确地传送到安全审计端就由三个因素决定：发送进程写入的数据正确与否、通道稳定性和可靠性的程度。

本安全传输通道采用双通道方式，一个通道作为主要通道进行大部分的数据传输，另一个隐藏起来作为辅助通道，当主通道无法正常工作时作为后备启用。在仿真系统实现中，我们分别以网卡和并行口作为主、辅通道，并行口的驱动采用专门设计的软件，增加了系统的稳健性。安全通道的结构如图3所示。

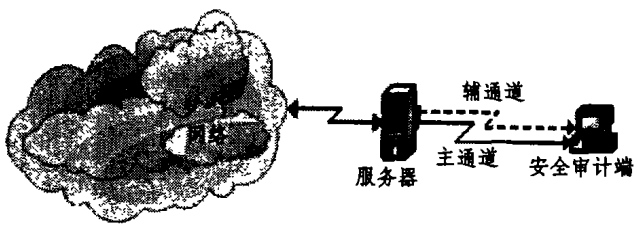

图3 安全通道的构成

安全通道的工作方式决定了通道在数据传输过程中是稳定的和可靠的。图4描述了它的工作原理。

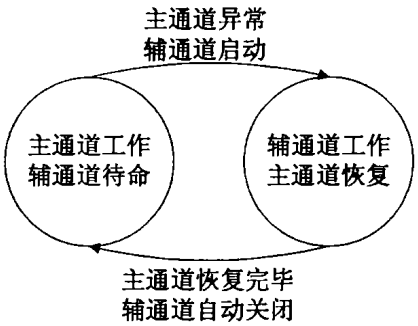

图4 通道的工作原理

在第3节中，通道的脆弱点在于被阻塞、恶意使用或中断，由于这种双通道的设计，通道被阻塞和中断的情况已不存在，而对于通道的恶意使用，还是会造成大量错误数据流入到安全审计端。考虑到对服务器的性能影响，我们将处理错误数据的工作放到安全审计端进行。下面是安全审计端采取的相应措施：

(1)在安全审计端启动接收过滤模块；

(2)监测网络固定端口的数据流，若连续发现有 n(n 不大于5)次数据格式不符合约定，自动中断主通道，启用辅通道；

(3)启用辅通道传输 m(m 不大于3)秒，重新启用主通道，关闭辅通道。

这些措施可以有效减少恶意数据带来的危害。由于通道具有根据环境自行调整的功能，除非硬件故障，通道都可以确保数据的正常传输。这样，第3节中描述的脆弱点得到了保护。

4.3 安全审计端

安全审计端的脆弱点具体表现在数据过滤模块上。在前面的描述中，安全审计端通过网线(主通道)连接到服务器，由于使用 TCP/IP 协议进行数据传输，若不采取适当的措施，安全审计端存在被攻击者控制的危险。

实际系统中，我们采取的措施是，只保留一个端口用来进行数据的接收，将其它所有服务端口关闭或禁止访问，从而限定外界的连接只能通过与过滤模块交互来进行，而过滤模块对不符合约定格式的数据包采取抛弃策略。这个实现过程比较简单，这里不再详细描述。

5 审计系统自身安全性的测试

审计系统的自身安全性测试主要包含两个方面：一方面是系统的健壮性，即程序本身在各种网络环境下是否都能正常工作；另一方面是数据传输的安全性，即程序各个模块之间的通信是否可靠。

当前网络攻击方法主要有四大类：刺探与扫描、恶意程序、拒绝服务、监听。结合一些工具，我们使用多种方法进行测试，具体如下：

(1)从外部扫描和攻击服务器；

(2)在服务器上种植木马，尝试关闭信息采集和发送进程；

(3)提升木马的用户级别至 System 级，再次尝试关闭信息采集和发送进程；

(4)发送大量数据包进行通道稳健性测试；

(5)审计系统运行中断开网络物理连接，测试通道的自动切换等；

(6)使用 Sniffer 工具进行网络监听。

整个攻击测试过程持续两个多小时，扫描频率为500次/秒，结果如下：

首先扫描探测获得服务器的用户密码，在此基础上，得到服务器的控制权；种植木马后，查找信息采集和发送进程，尝试关闭这两个进程，操作失败；提升木马用户级别至 System 级，关闭信息采集和发送进程成功，但信息采集和发送进程自动重启；通过主通道往审计端发送大量数据包，主通道时断时续，说明通道自动在主辅通道间切换，具有很好的防"洪水"攻击的能力；审计系统运行中物理断开主通道，数据依然能够正常发送到安全审计端；Sniffer 在攻击发起端进行监听，得不到任何审计系统传输的数据。

从实验结果上看，我们使用的解决方案使审计系统具有了很好的健壮性和安全性，同时也具有一定的隐蔽性(辅通道)，有效地解决了审计系统的自身安全问题。

上述攻击测试中，我们比较容易地获得了服务器系统的控制权，这是因为为了测试审计系统在没有防火墙的保护下是否可以正常地工作，网络服务器上没有安装其它的安全防护产品。

网络安全只是一个相对的概念，不可能有绝对的安全，本安全审计系统也是如此。为进一步加强安全审计系统的安全，我们建议实行"多层次防护"策略[3]，在安全审计端和网络服务器上安装网络防火墙和病毒防火墙。

所谓"多层次防护"，就是应用和实施一个基于多层次安全系统的全面信息安全策略，在各个层次上部署相关的网络安全产品，增加攻击者侵入所花费的时间、成本和所需要的资源，从而有效地降低被攻击的危险，达到安全防护的目标。结合网络防火墙和病毒防火墙，审计系统的自身安全性也将会得到更大程度的提高。

结论 电子商务系统的安全问题是个日益严重的问题，由此产生的网络犯罪所造成的危害也越来越大。安全审计系统作为一种有效的信息安全保护工具，应用将会越来越广，其作用也会受到更多的重视，而其自身的安全保障性能，将会严重影响到系统的可信度。因此，研究安全审计系统，很重要的一点就是解决系统自身的安全问题。本文所提出的自身安全问题解决方案，在实际开发和测试中取得了很好的效果，对于其它类似系统的开发，也是一个借鉴和启发。

参 考 文 献

1 胡昌振. IDS 的自防护原则与技术途径. 北京理工大学信息安全与对抗技术研究中心. http://www.china-infosec.org.cn/teaching/index.php?id=6390&page=6390
2 董安波，陈龙，等. 电子商务安全审计系统的设计与实现. 计算机工程与应用，已录用，待发表
3 海默. 多层防护构筑网络安全. http://www.edu.cn/20011204/3012783.shtml
4 Yeung D-Y, Ding Yuxin. Host-based intrusion detection using dynamic and static behavioral models. Pattern Recognition, 2003, 36:229～343
5 Lindqvist U, Jonsson E. How to Systematically Classify Computer Security Intrusions. In: proc. of the 1997 IEEE Symposium on Security & Privacy, 1997. 154～163
6 Fyodor. The Art of Scanning. Phrack Vol. 51. http://www.phrack.com
7 CFI Software Company. Log-based intrusion-detection and analysis in Windows 2000/NT. http://www.windowsecurity.com
8 岳兵，傅红娟，等. 完善入侵检测系统审计信息的方法. 计算机学报，2002(6)：772～777
9 黄锦，李家滨. 基于防火墙日志信息的入侵检测研究. 计算机工程，2001(9)：115～117
10 许霆，袁萌，等. 网络监控审计系统的设计与实现. 计算机工程与应用，2002. 149～153
11 (美)Anonymous，等. 最高安全机密. 机械工业出版社，2002
12 (美)Stallings W. 网络安全要素——应用与标准. 人民邮电出版社，2000