网络安全中的安全审计技术

文/赵 晖

随着计算机技术、通信技术和信息技术的飞速发展，各种各样的网络应用已经越来越广泛地渗透到人类地生活、工作的各个领域。特别是通过Internet，人们可以极为方便地产生、发送、获取和利用信息。Internet在给人们带来巨大便利的同时，也产生了许多意想不到的问题，网络安全就是其中一个突出的问题。

一、网络安全概念

网络安全(Network Security)的通用定义是：网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改和泄露，系统连续、可靠、正常地运行，网络服务不中断。由此可以将计算机网络的安全理解为：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。

网络安全根据其本质的界定，具有以下基本特征：

1. 保密性：保密性是指信息不泄露给非授权的个人、实体和过程，或供其使用的特性。

2. 完整性：完整性是指信息未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不能被破坏、不被插入、不延迟、不乱序和不丢失的特性。对网络信息安全进行攻击其最终的目的就是破坏信息的完整性。

3. 可用性：可用性是指合法用户访问并能按要求顺序使用信息的特性，即保证合法用户在需要时可以访问到信息及相关资源。网络环境下拒绝服务、破坏网络和有关系统的正常运行都属于对可用性的攻击。

4. 可审计性：在信息交流过程后，通信双方不能抵赖曾经做出的行为，也不能否认曾经接收到对方的信息。

5. 可控制性：可控制性是指授权机构对信息的内容及传播具有控制能力的特性，可以控制授权范围内的信息流向以及方式。

二、网络安全模型

网络安全系统并非局限于通信保密、对信息加密功能要求等技术问题，它是涉及到方方面面的一项极其复杂的系统工程。一个完整的网络信息安全系统至少包括以下三类措施，并且三者缺一不可（图1）。

(1) 社会的法律政策，企业的规章制度及网络安全教育。

(2) 技术方面的措施，如防火墙技术、防病毒、信息加密、身份确认、授权。

(3) 审计与管理措施，包括技术措施与社会措施。

实际应用中，主要有实时监控、提供安全策略改变的能力以及对安全系统实施漏洞检查等措施。

该网络信息安全模型中的政策、法律、法规是安全的基石，它是建立安全管理的标准和方法。

增强的用户认证，它是安全系统中属于技术措施的首道防线。用户认证的主要目的是提供访问控制。用户认证方法按其层次的不同可以根据以下三种情况提供认证：

(1) 用户持有的证件，如大门钥匙、门卡等

(2) 用户知道的信息，如密码等

(3) 用户持有的特征，如指纹、声音和视网膜扫描等

授权主要是为特许用户提供合适的访问权限，并监控用户的活动，使其不越权使用。

加密主要满足如下的需求：

(1) 认证：识别用户身份，提供访问许可

(2) 一致性：保证数据不被非法篡改

(3) 隐密性：保证数据不被非法用户查看

(4) 不可抵赖性：使信息接收者无法否认曾经收到的信息

加密是信息安全应用中最早使用的一种行之有效的手段之一，数据通过加密可以保证在存取与传送的过程中不被非法查看、篡改和窃取等。在实际使用中，利用加密技术至少需解决如下问题：

(1) 钥匙的管理，包括数据加密钥匙、私人证书和私密等的保证分发措施

(2) 建立权威的钥匙分发机制

(3) 数据加密传输

(4) 数据存储加密等

在网络信息模型的顶部是审计与监控，这是系统安全的最后一道防线，它包括数据的备份。当系统一旦出现了问题，审计与监控可以提供问题的再现、责任追查和重要数据恢复等保障。网络信息安全模型各部分相辅相成，缺一不可。其中底层是上层保障的基础。

三、安全审计的概念

安全审计(Security Auditing)是指根据一定的安全策略，通过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地方。它的目的是为保证网络系统安全运行，保护数据的保密性、完整性及可用性不受损坏，防止有意或无意的人为错误，防范和发现计算机网络犯罪活动，除采取其他安全措施外，利用审计机制可以有针对性地对网络运行的状况和过程进行记录、跟踪和审查，以从中发现安全问题。此外审计还能为制定网上信息过滤规则提供依据，如发现有害信息的网站后将其加入路由过滤列表，通过信息过滤机制拒绝接收一切来自过滤列表上IP地址的信息，将网上的某些站点产生的信息垃圾拒之门外。

具体作法为：利用技术手段，不间断地将计算机网络上发生的事件记录下来，用事后追查的方法保证系统的安全。采用数据挖掘和数据仓库技术，实现在不同网络环境中终端对终端的监控和管理，在必要时通过多种途径向管理员发出警告或自动采取排错措施，能对历史数据进行分析、处理和追踪。

安全审计系统应该是事前控制人员或设备的访问行为，并能事后获得直接电子证据，防止行为抵赖的系统。审计系统把可疑数据、入侵信息、敏感信息等记录下来，作为取证和跟踪使用。它是信息安全保障系统的重要组成部分。

安全审计的主要功能：记录、跟踪系统运行状况。利用审计工具，监视和记录系统的活动情况，如记录用户登录账户、登录时间、终端以及所访问的文件、存取操作等，并放入系统日志中保存在磁盘上，必要时可打印输出,提供审计报告，使影响系统安全性的存取以及其他非法企图留下线索，以便查出非法操作者；检测各种安全事故。审计工具能检测和判定对系统的攻击，如多次使用错误口令登录系统的尝试，及时提供报警甚至自动处理，使系统安全管理人员能够了解系统的运行情况，及时堵住非法入侵者。审计工具还能识别合法用户的误操作等；保存、维护和管理审计日志。由于审计日志记录了审计、跟踪、检测各种安全事件的结果，是查找、分析网络系统安全事件的客观依据，是重要的系统文档，必须要有可靠的存储和管理机制。

四、安全审计系统结构

安全审计系统(Security Auditing System)由审计中心、审计控制台和审计Agent组成，如图2所示:

审计中心使整个审计系统的数据进行集中存储和管理，并使用应急响应的专用软件，它基于数据库平台，采用数据库方式进行审计数据管理和系统控制，并在无人看守的情况下长期运行。审计控制台是提供给管理员用于对审计数据进行查阅，对审计系统进行规则设置，实现报警功能的界面软件。可以有多个审计控制台软件同时运行。审计Agent是直接同被审计网络和系统连接的部件，不同的审计Agent完成不同的功能。审计Agent将报警数据和需要记录的数据自动保送到审计中心，并由审计中心进行统一的调度管理。

五、安全审计系统的模型

根据通用入侵检测框架 (Common Intrusion Detection Framework,CIDF)的模型，作者认为安全审计系统由事件产生器(Event generators)、事件分析器(Event analyzers)、响应单元(Response units)、事件数据库(Event databases)组成，组件结构如图3所示。

其中，事件是需要分析的数据统称，它可以是网络中的数据包，也可以是从系统日志等其他途径得到的信息等等。事件产生器的目的是从整个计算环境中获得事件，并向系统的其他部分提供此事件。事件分析器的作用是分析得到的数据，并产生分析结果。响应单元则是对分析结果作出反应的功能单元，它可以作出切断连接、改变文件属性等强烈反应，也可以只是简单的报警。事件数据库是存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。

在日常使用中，也经常以数据采集部分、分析部分和控制台部分来分别代替事件产生器、事件分析器和响应单元这些术语。

六、安全审计系统的分类

按照不同的依据标准，安全审计系统有多种分类方式。

根据审计的目标系统，安全审计系统主要分为两种:基于网络的审计和基于主机的审计。前者包括对网络信息内容和协议的分析;后者包括对系统资源，如打印机、Modem、系统文件、注册表文件等的使用进行事前控制和事后取证，形成重要的日志文件。

根据安全审计系统的部署方式，可以分为集中式和分布式两种形式。

根据系统的响应方式，可以分为主动式和被动式两种。主动式对审计出的结果进行主动响应，包括

强制违法用户退出系统，关闭相关服务等等;被动式只是对审计出的异常进行报警。

七、内网安全审计技术的现状及发展

在电子政务网或企业网中，某些文件非常重要，具有一定级别的人才能观看，观看后要形成观看记录；文件不能被随意拷贝、删除，且必须对该文件的访问或试图访问进行严密监控并形成日志，日志中清楚地记录来自哪台设备的哪个用户已经或试图读取这些文件，以便事后取证。安全审计系统中的文件保护功能很好地实现了这项需求。

另外，某些组织严格限制任何终端设备通过拨号接入互联网，以防泄密。但是，仅仅通过行政管理手段很难监控，而安全审计系统中的拨号和网络审计，不仅能预防并制止随意拨号，还能清楚地显示，哪台终端的哪个用户在哪个时段试图访问或成功访问了哪个网站，它们事后想抵赖都不行。这一技术功能很好地解决了以前关于拨号上网监管不利的问题。其他还有许多功能，如进程监控、文件监控，这些都是企业或电子政务网中所需要的。

一个网络要保护起来分三个阶段：事前、事中和事后。事前就是把网络已经潜在的安全问题或者是潜在的弱点、隐患发现出来并弥补，这类产品用得比较多的就是扫描系统。事中是对正在运行的系统防止黑客攻击，用得最多、最普遍、最成熟的是防火墙和入侵检测技术。而事后的取证，就必须用到审计系统[11]。如果说防火墙是一道保护网络的重要关卡，那么网络安全审计则是一支在网络内部值勤的网上巡警。网络安全审计能够帮助对网络进行动态实时监控，可通过寻找入侵和违规行为，记录网络上发生的一切，为用户提供取证手段。网络安全审计不但能够监视和控制来自外部的入侵，还能够监视来自内部人员的违规和破坏行动，它是评判一个系统是否真正安全的重要尺度。从这个定义来看，IDS实际是一种审计机制，但它并不全面，安全审计还包括事前的预防。

目前，安全审计分为网络审计和主机审计。前者包括对网络信息内容和协议的分析；后者包括对系统资源，如打印机、Modem、系统文件、注册表文件等使用进行事前控制和事后取证，形成重要的日志文件。未来，我们还会研究对应用系统的审计，如对各类数据库系统进行审计，这也是审计系统的技术发展之路（作者单位：陕西理工学院计算机科学与技术系）

相关链接

基于JSP的WEB电子购物车实现研究
电子商务绩效评价应用研究
网络安全中的安全审计技术
浅析教育网站安全解决方案
成本会计软件发展的艰辛之路
企业实施ERP的现状、问题及对策
EVA指标在企业财务管理中运用价值的探讨
浅议电子商务环境下物流业解决方案及其发展趋势

地址：北京市朝阳区关东店甲1号106室 邮编：100020 电话/传真：（010）65015547/ 65015546

制作单位：集团经济研究网络中心