信息安全技术系列丛书

系统安全与入侵检测

戴英侠　连一峰　王　航　编著

清华大学出版社

(京)新登字158号

内 容 简 介

信息安全是指对整个信息系统的保护和防御,包括对信息的保护、检测、反应和恢复能力等。入侵检测作为信息安全保障中的一个重要环节,它很好地弥补了访问控制、身份认证等传统机制所不能解决的问题,是网络安全中极为重要的一个研究课题。本书重点介绍了入侵检测的方法、响应及攻击的手段。此外,还介绍了如何用数据挖掘的方法分析安全审计数据。最后简单介绍国外在入侵检测方面的有关产品。

书　名:系统安全与入侵检测
作　者:戴英侠　连一峰　王　航　编著
出版者:清华大学出版社(北京清华大学学研大厦,邮编100084)
http://www.tup.tsinghua.edu.cn
印刷者:清华大学印刷厂
发行者:新华书店总店北京发行所
开　本:787×1092 1/16　**印张**:21.25　**字数**:489千字
版　次:2002年3月第1版　2002年3月第1次印刷
书　号:ISBN 7-302-05099-6/TP·2981
印　数:0001~6000
定　价:26.00元

前　言

随着 Internet 的迅猛发展和网络社会的到来，网络将会无所不在地影响社会的政治、经济、文化、军事和社会生活等各方面，网络安全已成为世界各国共同关注的焦点。目前，全球使用 Internet 的用户已经超过了 1 亿。根据 2001 年 7 月份中国互联网络信息中心（CNNIC）的统计材料，我国上网用户已超过 2650 万。与此同时，关于黑客入侵的报道也呈指数增长。黑客的网络攻击与入侵行为，对于国家安全、经济、社会生活造成了极大的威胁。目前，有 120 个国家已经或正在开发网络攻击技术，有些恐怖分子和极端分子甚至可以获得对国防信息系统的控制，严重削弱一个国家对军事力量的部署和维持能力。

现在，我国在 Internet 上开展的各种业务也迅速增加。但是，对于网站的安全保护，无论是思想意识还是相关技术，都有所欠缺。根据 CNNIC 发布的一份报告指出，我国 40% 的网站存在严重的安全漏洞，国内一些著名的门户网站与商务网站曾被黑客攻击过。

为了保障信息安全，除了要进行信息的安全保护，还应该重视提高系统的入侵检测能力、系统的事件反应能力以及系统遭到入侵破坏后的快速恢复能力。它有别于传统的加密、身份认证、访问控制、防火墙、安全路由等安全技术，信息保障强调信息系统整个生命周期的防御和恢复。入侵检测，作为信息安全保障中的一个重要环节，很好地弥补了访问控制、身份认证等传统保护机制所不能解决的问题。关于这方面的研究，国外从 20 世纪 80 年代末就已经开始，近年出现的入侵检测系统（IDS）是一种新型的网络安全技术，能够弥补防火墙的不足，为受保护的网络提供有效的入侵检测及相应的防护手段。

入侵检测是一个全新的、迅速发展的领域，已成为网络安全中极为重要的一个课题。本书重点介绍了入侵检测的方法、响应及攻击的手段；根据作者的研究成果，重点介绍了如何用数据挖掘的方法分析安全审计数据；并对国外在入侵检测方面的产品作了简要介绍，适用于从事入侵检测工作的研究和应用人员。

在本书的写作过程中，除了介绍了大量作者自身的研究内容及成果之外，主要参考了 Rebecca Gurley Bace 所编著的“Intrusion Detection”[1]（该书由美国 Macmillan Technical Publishing 在 1999 年出版）以及其他一些在互联网上公布的研究论文和相关资料，书中恕不一一注明出处。这些资料来源于众多的大学、研究机构、安全团体、安全网站、商业安全公司以及一些研究计算机及网络安全问题的个人。对于他们在推动安全事业发展的过程中所作的工作和努力，在此表示衷心的感谢，其中特别要感谢绿盟的袁仁广、左磊和其他朋友。写作过程中所参考的这些书籍资料，其原文版权属于原作者，特此声明。

本书共分10章，其中第1章由戴英侠编写，第2章由戴英侠、连一峰、王航共同编写，第3、4、6、8章由连一峰编写，第5章由连一峰、王航编写，第7、9章由王航编写，第10章由陈立志编写。此外，许一凡、唐青文和李安为本书作了大量工作，在此表示感谢！

本书得到国家重点基金研究发展规划项目（项目编号：G1999035801）的支持。

作　者

2001年9月12日

第1章

系统安全概要

随着信息网络化的发展，信息安全的概念和实践不断深化、延拓。从二战后军方、政府专享的通信保密，发展到20世纪70年代的数据保护、90年代的信息安全直至当今的信息保障，安全的概念已经不局限于信息的保护，人们需要的是对整个信息系统的保护和防御，包括对信息的保护、检测、反应和恢复能力(PDRR)等。

1.1 信息安全概述

信息安全可以从理论和工程的两个角度来考虑。一些从事计算机和网络安全的研究人员从理论的观点来研究安全。这些安全专家开发了计算的理论基础，并从这个基础出发来考虑安全问题。他们感兴趣的是通过建造被证明是正确的安全模型，用数学方法描述其安全属性。这些专家为安全领域带来了精确、清晰的论点，这是非常有价值的。

计算机安全领域的另一个派系则以注重实际的、工程的角度来研究安全。这些专家经常对安全问题的起因感兴趣，他们更关心保护操作系统的问题。有人认为，所有从事研究工作的人都必须像理论家那样严密精确，而有人则认为理论家都应该有能力管理操作系统。

这两种方法都有它的合理性。我们采纳两种观点的基本原理，因为两者都能为保护系统提供有价值的东西。

1.1.1 信息安全的内容

信息安全包括以下几方面的内容：

保密性：防止系统内信息的非法泄漏；

完整性：防止系统内软件(程序)与数据被非法删改和破坏；

有效性：要求信息和系统资源可以持续有效，而且授权用户可以随时随地以他所喜欢的格式存取资源。

一个安全的计算机信息系统对这3个目标都支持。换句话说，一个安全的计算机信息系统保护它的信息和计算资源不被未授权访问、篡改和拒绝服务攻击。

1.1.2 工程的定义

工程上谈到一个信息系统是安全的，一个安全计算机系统的实用定义是“一个按预期方式运作的可靠系统”。

对安全的这种直观看法，可以推出与安全相关的基本概念。例如，依赖于一个系统的观点意味着信任这个系统。这个信任是可以计量的吗？如果可以，又怎样来衡量呢？我们是否信任这个系统会按预期的方式运行？谁来决定预期的运行方式？怎样判断系统的实际运行确实与预期的运行方式相匹配？通常指的是该系统受到的损失在可承受的范围之内。

1.2 基本概念

1.2.1 信任

信任(trust)是指对系统的预期运作与实际相符的信心，信任的级别与预期和实际运作关联的信心级别相对应。协同运作的系统元件通过对其他元件充分的信任假设来达到这个目的。在这些假设被证实缺乏根据的情况下，就会存在漏洞，而威胁也经常随之出现。

为信任关联做出评定，相当于划出一个安全的界线，从而限定了相关的安全区域。这个方法在每个结合点对信任关联进行系统的评估，对系统的可信任度作出了更深入的洞察解析。

保护系统的信息安全不可能是绝对的，而是多种约束条件下的折衷选择；对信息防护不应是消极的，它与信息攻击相辅相成。当我们说一个系统是可信的时候，应当有一个边界，以区分内部和外部，边界有物理的和逻辑的边界。无论你将系统的安全界线划到什么位置，都要注意信任所引起的问题。在系统的安全界线内，你必须信任系统管理员和系统用户不会滥用他们的特权，你还必须信任系统放置的物理环境可以保护系统不受物理损害。

对于外界的防范，重心在于对于边界的守卫和对授权的外部人员及程序通过边界后是否超越权限的把握、限制和控制上。就时效而言，内部人员大多在系统边界的内部一侧，当外出时，可通过公共网络对其所连接的内部网络进行授权访问。他们拥有机构所分配的岗位和工作以及在这样的岗位上需要的权限。具有职业道德和职业技能的工作人员，是由人机共同构成的 IT 系统中不可或缺的组成部分。要求内部人员对系统不准有违规、违法的行为。

总之，一个信任系统是指该系统拥有足够的硬件和软件，以保证准许同时进行敏感、分类信息的使用。因而，信任系统被设计成准许军用和智能组织在同一台计算机上放置符合典型级别分类的不同的敏感级别的信息。在早期的研究中，研究者们争论安全审计机制是否可以确定一个信任的系统保险级别。最终，审计机制真正地被包含进《信

任系统评估标准》("橘皮书")里面,在评估信任级别达到 C2 和 C2 以上的系统是必要的。

1.2.2 威胁

一般将威胁(threat)看做是具有足够的技巧和机会的实施者对一个目标系统的脆弱性的觊觎和潜在的危害。几年前,黑客要耗费许多时间,在进行大量的研究之后,才能成功地入侵网络,虽然专家级黑客仍然很多,但国际互联网已步入了一个崭新的时代,只要在任何一个搜索引擎中加入 hacking,password cracking 和 Internet Security 之类的关键字,Internet 的普通用户就可以充分利用免费材料,轻松地查找到关于如何进入他人系统的信息。数以千计的站点都在公布入侵 WINDOWS NT 系统、Web 服务器、UNIX 等系统的方法。这些站点指导人们一步一步地操作。他们还提供入侵系统的工具,以供黑客们使用。这些工具大多具有简单易用的图形界面,使入侵活动自动进行。例如,一个被称为"Crack"的工具,客观存在可能帮助黑客自动猜测 UNIX 系统的密码。还有一个名叫"LOPHTRACK" 的工具,可以破译 WINDOWS NT 的密码。一种叫"SATAN 4"的探测工具专门用于寻找网络上的脆弱系统,并告知黑客们其中的漏洞。

网络入侵不仅来自于网络外部,也来自于网络内部。对公司不满的员工表现出更大的威胁,并且造成更大的破坏。一个有效的入侵探测方案可以有效地探测到内部或外部入侵。威胁的来源一般为:国外的敌对势力(21%);竞争对手(48%);网络黑客(65%);内部人员(76%)。由此可知,大多数的安全缺口来自于内部,而非外部。其主要原因有:

(1) 内部人员最容易接触敏感信息,他们的行动非常具有针对性,危害的往往是机构中最核心的数据、资源等。

(2) 一般说来,各机构的信息安全保护措施都是"防外不防内",很多公司赖以保障其安全的防火墙对来自内部人员的攻击毫无作用。

(3) 内部人员对一个机构的运作、结构、文化等情况非常熟悉,导致他们在行动时不易被发觉,事后也难以被发现。

内部人员的威胁至少与下面的角色有关,随着角色的改变,风险的程度也随之改变:

- 授权用户
- CERT 人员
- 网络管理员
- 系统维护人员
- 系统管理员
- 建筑物维护人员
- 信息安全官员
- 建筑物安全人员

准确定义"内部人员"确实相当困难。人们有时形容内部人员就像变色龙,可依据不同身份和所处的环境而改变。一般说来,"内部人员"的范畴除了固定人员以外,还包括

非全时人员、临时人员、外出人员、以前的内部人员和系统开发者等等。针对内部人员的威胁,还可进行以下分析:

(1) 内部人员的意图是什么? 其行为可能包括日常的错误,由此引起系统削弱或隐私信息的无意泄露,但更严重的是怀有恶意企图的内部人员的行为。

(2) 内部人员可以是个体的人,也可以是软件、固件或硬件。例如,恶意的代码是内部人员进行威胁的普遍方式,而且很拙劣。

(3) 内部人员界定多宽,给定每个类型什么样的可信程度,如何清晰地描绘机器可读的可信级别,这些因素成为各种系统进程中识别可信程度的基础。

1.2.3 系统的脆弱性

脆弱性(vulnerability)来源于系统的安全漏洞。由于人类对自然规律的认识及其应用能力的局限性,目前提供社会应用的电子信息系统,客观上还存在许多不完善的地方,还有各种各样的脆弱性的表现。例如,已提供全球广泛使用的 Windows 操作系统就存在很多安全漏洞(技术上称之为 Bug)。有着久远发展历史并已广泛应用的 UNIX,也未免于患,其安全漏洞也不少。

安全漏洞不仅可能存在于软件程序中,在芯片中也可能存在。法新社 1997 年 11 月曾经报道 Intel 公司发言人汤姆·沃尔德落普的如下评述:"我们已经确认奔腾和具有多媒体扩展(MMX)技术的奔腾处理器芯片存在一处新的缺陷"。他证实,如果当操作者享有进入系统的特权,并能向处理器发出一项特殊指令时,该缺陷会使系统死机,这就使得不怀好意的黑客可能利用这一缺陷,导致使用这种芯片的个人计算机和网络陷于瘫痪。据估计,过去 3 年中 80% 的个人计算机(大约两亿台)使用着这些芯片。

关于系统脆弱性的报道,在风险公告和计算机应急响应小组(CERT)的公告中大量出现。不仅是原来没有设置信息安全防线的设备不可能提供安全保障,即便是后来开发应用的所谓安全计算机操作系统、数据库、信息网络、防火墙等,在不同环节上,人们仍然可以找到不少的问题。而这些问题的出现,并不是技术工作者有意的破坏,而是系统脆弱性的客观存在。其中主要表现为如下几个方面:

(1) 软件的 Bug

服务器守护程序、应用程序、操作系统以及协议栈等软件的 Bug 经常是入侵者利用的对象,主要反映在程序编制过程没有考虑到对特殊输入的处理。这些程序引起的脆弱性有:

- 缓冲区溢出

缓冲区溢出是拒绝服务攻击中最可能出现的一种。例如,程序员一般不会想到用户账号可能有几百个字节,但一旦有人这样做了,就导致难以估计的错误。通过仔细研究源代码,就可以利用缓冲区溢出后的系统处理得到超级用户权限。

- 特殊字符组合

这类问题主要出现在 CGI 程序中。例如,用户键入"| mail < /etc/passwd"这样一条命令,系统就会截取管道符"|"并调用"mail"程序将 passwd 文件发到用户信箱中。

- 竞争条件

由于操作系统的多任务性，当两个程序同时访问同一段数据时就可能产生错误。例如，A 与 B 程序同时对文件 F 进行读写操作，A 首先将 F 的内容读进内存，当 A 还未来得及完成文件修改保存操作，B 对 F 进行了读写保存的完整操作，待 A 完成保存操作后，B 对 F 的修改已不复存在。

（2）系统配置不当

- 缺省配置

操作系统的默认配置往往照顾用户的友好性，但容易使用的同时也意味着容易受到攻击。

- 系统管理员失职

由于操作系统的复杂性，没有经过严格培训的系统管理员很难做到万无一失。

- 系统后门

为了在调试程序时方便，或使用时方便，往往留有一些默认口令或非正常进入系统的方法。这些后门一旦被发现，便成为严重的安全漏洞。

- 信任关系

相互有信任委托关系的主机很容易遭到攻击。

（3）脆弱性口令

大部分人的口令由自己或家人的名字组成，或加上简单数字（例如门牌号、生日等），或与账号相同。攻击者可以通过猜测口令或在拿到口令文件后，利用口令计算程序、口令字典进行蛮力攻击。

（4）信息泄漏

入侵者常用的方法之一就是窃听。在广播式的局域网上，将网卡配置成“混杂”模式（miscellaneous），就可以监听到网络上的所有数据包。如果在服务器上安装窃听软件（sniffer），就可以拿到远程用户的账号和口令。

（5）设计缺陷

- 协议缺陷

最典型的就是 TCP/IP 协议，在协议设计时并没有考虑安全因素。虽然现在已经充分意识到这一点，但由于 TCP/IP 已经广泛使用，因此，无法被完全替代。例如 ICMP，IP spoofing，SYN floods 等攻击就是利用了协议的缺陷。

- 操作系统缺陷

虽然操作系统在设计时考虑了很多安全因素，但也不可避免地存在一些缺陷。例如，Windows NT 中的用户权限在启动时由系统注册表获得，这样就可以导致许多安全漏洞。

1.2.4 安全策略

网络的安全策略（security policy）是计划的需求，在现实社会安全中有时是一个神奇的概念，最初的安全定义是指建立一个理想的系统，安全地实现这些计划。或者说安全策略将安全的抽象概念映射到真实世界中。在最初定义安全的时候，我们指出它基于一些

想法,即由什么构成一个系统的预期行为。安全策略将这些预期用文字记载下来。安全策略有两个定义,(1) 正式的安全策略,通常由一个数学模型所构成,这个数学模型收集了系统所有可能的状态和操作,并伴随着状态操作存在的可能时间和方式的约束。政府的可信系统(government's trusted systems initiative)把系统安全策略定义为系统安全功能部件执行的规则集。编写安全策略、正式而明确地定义哪些行为是不允许的是一项困难的工作。(2) 管理上的安全策略,它概述了安全目标并提交管理资源以达到目标。除此之外,还分配责任、划分职务、确定管理和安全控制。最后,这个策略构架起到保护信息和计算资产的程序的作用,并予以实行。值得注意的是策略始终是一致的,程序更详细一些,但很少更改。而在实行时就具有动态性了,它反映了系统当时的特征细节。

在某个安全区域内使用与安全相关的活动的一套规则。这些规则是由此安全区域中所设立的一个安全权力机构制定的,并由安全控制机构描述。实施的安全策略主要由安全策略目标、机构安全策略和系统安全策略这 3 个不同方面来描述。所谓安全策略目标,是指某个机构对所要保护的特定资源必须要达到的目的所进行的描述。其目的是保护系统信息的完整性、有效性、保密性及可用性。机构安全策略是一套法律、规则及实际操作方法,用于规范某个机构如何管理、保护和分配资源以达到安全策略的既定目标。系统安全策略是指为支持此机构的安全策略要求,如何将特定的信息技术系统付诸工程实现的方法。

1.3 已有的安全组件

1.3.1 访问控制

访问控制(access control)防止对资源的未授权使用,包括防止以未授权方式使用某一资源。访问控制需采取两种措施:一种是识别与确证访问系统的用户,即身份认证;另一种是决定该用户对某一系统资源可进行何种类型的访问(读、写、运行等等)。为了使计算机系统更安全,需要两种不同类型的访问控制:自主访问控制(discretionary access control,简称 DAC)与强制访问控制(mandatory access control,简称 MAC)。自主访问控制是一种最普通的访问控制手段。在自主访问控制下,用户可以按自己的意愿对系统参数作适当的修改以决定哪个用户可以访问他们的文件。一个用户(或一段用户程序或一个进程)可以有选择地与其他用户共享他的文件。强制访问控制是用户与文件都有一个固定的安全属性。系统利用安全属性来决定一个用户是否可以访问某个文件。安全属性是强制性的,它是由安全管理员或操作系统根据限定的规则分配的,用户或用户的程序不能修改安全属性。如果系统认为具有某一安全属性的用户不适于访问某个文件,那么任何人(包括文件的拥有者)都无法使该用户具有访问文件的能力。

1.3.2 鉴别与认证

在可信的计算机信息系统初始运作时,首先要求用户标识自己的身份,并使用保护机

制(如口令、证书等)来鉴别用户的身份;阻止非授权用户访问用户身份鉴别数据。通过为用户提供惟一标识,计算机可信信息系统能够使用户对自己的行为负责。计算机可信信息系统还具备将身份标识与该用户所有可审计行为相关联的能力。

具体地说,鉴别与认证(identification and authentication)机制可以根据对你的要求分为3个类别:你了解什么、你有什么和你是什么。每个类别都包括系统向用户索要的"机密"以及只有用户和系统知道的这个"机密"信息。如果用户提供的"机密"与系统所保存的信息相符合,系统就证实用户的身份并允许用户对系统的访问。

"你了解什么"是传统的I&A机制的基础。在这些系统中,login和password用来鉴别和验证用户。不幸的是,这个方法被证明是多种攻击的漏洞,如密码破译和特洛伊木马。这些攻击导致密码暴露在攻击者眼前。这项验证技术正逐渐被更强健的防御系统单独通过机密的零知识(zero-knowledge)技术所取代。

基于"你有什么"的验证系统包括基于令牌的系统,如向用户提供的智能卡、密钥或特殊的磁盘等。大多数令牌都使用机密机制和物理的不可改机制,以防止攻击者伪造和欺骗。

基于"你是什么"的验证系统,包括生物测定学配置、使用声音、指纹和视网膜来鉴定和验证用户身份等。有些系统使用混合方法,例如,有些商务智能卡令牌也包括了指纹扫描。

基本的"询问-响应"验证过程有时不仅仅在开始的系统访问处使用,还可以在入侵检测中作为判断可疑行为是来自入侵者还是合法用户的手段。

1.3.3 加密

信息的保密性是信息安全的一个重要方面。早期的信息安全机制只有加密,通过执行多种功能来保护信息,可以有效地隐蔽数据文件和所传输的内容,消除未授权者监视的可能性,还可以检测到数据的意外更改或有意的篡改,加密还可以为文档的作者提供验证。保密的目的是防止敌手破译信息系统中的机密信息,加密是实现信息保密性的一种重要手段。所谓数据加密就是使用数学方法来重新组织数据,使得除了合法的接收者外,任何其他人要想恢复原先的"消息"(将原先的消息称作"明文")或读懂变化后的"消息"(将变化后的消息称作"密文")是非常困难的。将密文变换成明文的过程称作解密。可用一个数据加密系统实现上述过程,我们用图1.1来描述该系统。

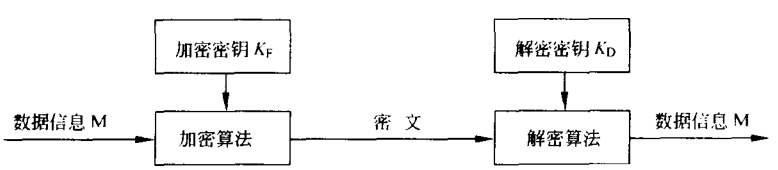

图1.1 密码系统示意图

加密技术是保障信息安全的核心技术,它可以在计算机和网络通信中用来解决身份鉴别、访问控制以及信息的保密性、完整性、不可否认性。若在互连、互通、互操作意义下

应用密码技术，就必须拥有行业自主的系列密码算法（包括序列密码、分组密码、公开密钥密码、HASH 函数等）、保证安全性的应用协议、安全应用密码的密钥管理系统以及与系统平台的安全无缝结合。

1.3.4 现有产品

当前流行的安全产品很多，如防火墙、VPN、CA 及扫描器等，我们有选择地加以介绍。

1.3.4.1 防火墙

防火墙（firewalls）出现得很早，最初可能是作为路由器的一个附加功能来实现的。路由器在处理网络数据包路由的同时，根据预先设定的过滤规则检查这些数据包是否满足“通行条件”，符合条件的就通过，否则拒绝通行。随着形势的发展和需求的进一步提出，专门的防火墙软、硬件陆续出现，功能也不断完善和加强。尽管现在大家普遍认为仅有防火墙的保护网络并非很安全，但相信至少在相当长的时间内它在网络安全方面的地位是不容置疑的。

现代的防火墙不但要能够安全地向外界提供网络服务，比如 WWW，FTP，E-mail 等，同时需要一个制定整个系统内部统一安全策略的管理界面（中心），而且对于系统内部不同部分之间也要能够进行必要的隔离和监控。同时，防火墙要能够与系统中其他一些安全部件相互配合，例如，CA 认证中心、LDAP 目录服务器、额外的认证服务机制（RADIUS，TACACS/TACACS +/SecuID）等。还有一点不能忽视的就是防火墙的可扩展性，要留有足够的拓展空间才能适应将来迅速发展和变化的安全需求。

总之，防火墙是一种古老而又有着很大发挥余地的网络安全构件，在未来相当长的时间内仍然会发挥相当重要的作用。

作为近年来新兴的保护计算机网络安全的技术性措施，防火墙是一种隔离控制技术，在某个机构的网络和不安全的网络之间设置障碍，阻止对信息资源的非法访问，也可以使用防火墙阻止专利信息从公司的网络上被非法输出。换言之，防火墙是一道门槛，控制进、出两个方向的通信。通过限制与网络或某一特定区域的通信，以达到防止非法用户侵犯 Internet 和公用网络的目的。防火墙是一种被动防卫技术，由于它假设了网络的边界和服务，对内部的非法访问难以有效地控制。因此，防火墙适合于相对独立的、与外部网络互连途径有限、网络服务种类相对集中的单一网络，如我们所常见的企业专用网。

实现防火墙的主要技术有数据包过滤、应用网关和代理服务等。

- 包过滤（packet filter）技术是在网络层中对数据包实施有选择的通过，依据系统内事先设定的过滤逻辑，检查数据流中每个数据包之后，根据数据包的源地址、目的地址、所用的 TCP 端口与 TCP 链路状态等因素来确定是否允许数据包通过。

包过滤技术作为防火墙的应用有 3 类：① 路由设备在完成路由选择的数据转发之外，同时进行包过滤，这是目前较常用的方式；② 在工作站上使用软件进行包过滤，但是

价格较贵;③ 在一种称为屏蔽路由器的路由设备上启动包过滤功能。近来有些厂商,如3Com,开始通过软件实现对非法数据包的登录和报告,但是启动这种功能对路由器的性能影响较大。

- 应用网关(application gateway)技术是建立在网络应用层上的协议过滤. 它针对特别的网络应用服务协议即数据过滤协议,对数据包进行分析并形成相关的报告。应用网关对某些易于登录和控制所有输出输入的通信的环境给予严格的控制,以防止有价值的程序和数据被窃取。在实际工作中,应用网关一般由专用工作站系统来完成。
- 代理服务(proxy server)是设置在 Internet 防火墙网关的专用应用级代码。这种代理服务准许网络管理员允许或拒绝特定的应用程序或一个应用的特定功能。包过滤技术和应用网关是通过特定的逻辑判断来决定是否允许特定的数据包通过,一旦判断条件满足,防火墙内部网络的结构和运行状态便"暴露"在外来用户面前,这就引入了代理服务的概念,即防火墙内、外计算机系统应用层的"链接"由两个终止于代理服务的"链接"来实现,这样就成功地实现了防火墙内、外计算机系统的隔离。同时,代理服务还可用于实施较强的数据流监控、过滤、记录和报告等功能。代理服务技术主要通过专用计算机硬件(如工作站)来承担。

结合上述几种防火墙技术的优点,可以产生通用、高效和安全的防火墙。若将应用网关技术和包过滤技术结合起来,将保证应用层的安全性、统一支持处理所有协议、审计和预警等,其运转对于用户和建立系统都是透明的,并且包括了面向所有的图形用户接口、便于配置和管理。

1.3.4.2 VPN

VPN 是英文 Virtual Private Networking 的缩写,中文一般译作虚拟专用网,或虚拟子网。简单地说,一个 VPN 就是利用基于公共基础设施建设起来的公开网络(如 Internet)的数据传输能力,借助相关安全技术和手段实现的,能够提供安全、可靠、可控的保密数据通信的一条安全通道。因为是在公共网络上搭建起来的、逻辑上属于自己的专用安全通道,所以加上了虚拟(Virtual)一词。在当今复杂的网络计算环境中,传统的 VPN 所涵盖的范围已经被极大地拓宽,人们现在所提到的 VPN 已经不再简单地专指加密和认证。一个完整的 VPN 解决方案应该包括以下 3 个方面的考虑:

- 安全性:包括访问控制、利用认证和加密技术保证安全有效的网络连接、使用者的身份识别、数据的保密性和完整性等。
- 流量控制:包括带宽控制、确保 QoS(服务质量)、VPN 的可靠性和高效性等。
- 可操作性和可管理性:包括基于安全策略的集中式管理能力(可以是本地或者远程的管理方式),确保与整个公司的总的安全管理策略相配合,同时、VPN 的实现方式要求具有良好的可扩展性(scalability)等。

以上 3 点是一个完整的 VPN 所必须具备的基本因素。现代 VPN 已不是仅仅采用认证和加密手段在公网上建立起一条保密逻辑信道而是更强调灵活性和可扩展性。因为对于现代企业集团来说,不但要保证集团内部数据通信的安全和畅通,而且也需要和自己的

战略合作伙伴、产品和原料的分销商、供应商以及自己的客户之间保持畅通、高效、安全的联系渠道。在采用 VPN 这种先进安全技术的同时，怎样使其能够很好地融合到企业原有的安全和管理机构中也是在系统实施前必须慎重考虑的问题。今后如果还要建设其他相关的安全设施，例如 CA 认证中心等，以发展自己的电子商务业务，那么所采用的技术就要求能够适应形势和业务发展的需要。

1.3.4.3 扫描器

扫描器(scanner)是一种自动检测远程或本地主机安全性弱点的程序，通过使用扫描器，你可以发现远程服务器的各种 TCP 端口的分配、它们提供的服务以及它们的软件版本，直观或间接地了解到远程主机所存在的安全问题。扫描器通过选通远程 TCP/IP 不同的端口服务，并记录目标给予的回答，可以搜集到很多关于目标主机的各种有用的信息。例如，是否能用匿名登录访问 FTP 服务，是否有可写的 FTP 目录，是否能用 Telnet 以及 HTTPD 是用 Root 还是普通用户在运行等。

对于一个功能较完备的扫描器，它能对操作系统与服务程序所存在的各种系统漏洞和 Bug 进行检测。为了实现该项功能，需要检查各个系统配置文件，例如：

/etc/passwd	口令文件
/etc/hosts	主机列表文件
/etc/networks	网络列表文件
/etc/protocols	协议列表文件
/etc/services	服务列表文件
/etc/hosts. equiv	主机信任列表文件

比较成熟的扫描器，如 SATAN，Nessus，ISS 等，都能对这些配置文件进行细致的检测，并给出完整的报告和建议。

扫描器并不是一个直接的攻击网络漏洞的程序，它仅能帮助发现目标机的某些内在弱点。一个好的扫描器能对它得到的资料进行分析，帮助查找目标主机的漏洞。但它不会提供进入一个系统的详细步骤。

扫描器应该有 3 项功能：发现一个主机或网络的能力；一旦发现一台主机，具有发现什么服务正运行在这台主机上的能力；通过测试这些服务，发现漏洞的能力。

1.4 安全问题的产生

当安全问题产生的时候，存在的问题数量是庞大的，但绝大多数问题的起因可以归到 3 类中：设计/开发、管理和信任。

1.4.1 系统设计及开发

第一类问题由在系统设计和开发过程中产生的错误、缺陷和遗漏组成。这些问题导致软件漏洞和硬件漏洞。例如，为了防止密钥泄露，可以将其注入智能卡。而研究者发

现,通过改变电压和时钟周期的方法,可以提取卡中的密钥,其结果造成密钥泄密。另一个经典的例子是系统软件 race conditions 问题。Race conditions 问题是这样引起的:在检查一个数值的合法性和实际使用它之间有个时间间隔。在这个时间间隔内,攻击者可以使用一个非法的数值来替代它,以欺骗软件常规程序执行非标准的操作。还有另一个被许多 UNIX 攻击方法利用的漏洞。通过命令行来运行的特权程序所传递的参数检查失败,就会被攻击者调用这些程序,提供可引起输入缓冲区溢出的参数,然后攻破程序获得特权 shell。

健全的工程测试、严格标准的程序和质量保证过程可以防止很多这种类型问题的发生。

1.4.2 系统管理(包括安全意识)

第二个导致安全问题的区域在于管理系统区域。这些问题包括系统配置本身和用来提供保护的安全系统的配置存在的问题。其中一个例子就是为系统文件设置不适当的特权属性(如让 UNIX 密码文件为所有人提供可读可写权限)。另外,也存在系统管理员或用户关闭、撤销安全机制所引起的问题。在一些大机构中经常出现这样的问题:有职员在内部系统——桌面 PC 机上安装了未授权的 modem,由于 modem 提供了一个通往机构内部网的通道,攻击者就可以绕过防火墙的检测。

1.4.3 信任关系

最常见的问题可能是来自与信任有关的过分乐观的天真假设。许多这种类型的问题都是因为开发环境与运作环境之间无法预知的差异而引起的。比如,UNIX 原来是在大学环境里由程序员开发出来的。在那里,信息共享是起码的标准,威胁级别是很低的。随着时间的推移,出现了商业装置的 UNIX,威胁模型就不一样了。在这种情况下,信任假设并没有推广到原来开发场所之上的环境。事实上,有些是同时属于设计和开发的问题。系统的设计者和实现者相信系统会在一个可靠的环境中以可靠的方式使用。设计者相信顾客会以特定的方式来使用系统,而顾客则相信产品会像供应商允诺的那样运行。在大量的系统中,用户相信系统的每个部件会以预期的方式运作。这种信任也可以扩展到系统的人工部分,用户相信有人在以能胜任的持续的方式管理着系统。

当信任被打破的时候会发生什么呢?这种情况通常意味着安全问题的产生。很多情况下,其他人看来问题很明显,惟独对问题负责的人却看不到。当然也有人在监视系统的运作时注意到了异常的系统行为。

1.5 安全的相对性和协作性

信息安全是信息空间中的斗争,不受国界的限制,分不出前线和后方。信息安全是高技术、高知识、高智能和高智商的争战。信息安全是基础设施、知识、技术、管理、法律、法

规等综合起来的系统工程。保证信息安全是一种动态过程，这里不存在充分条件，也不可能一劳永逸。保护信息安全不可能是绝对的，而是多种约束条件下的折衷选择。信息防护不应是消极的，它与信息攻击相辅相成。

信息安全并不是某一个人、一个单位可以实现的，它需要整个社会的支持，要求不同团体的协作，形成统一的法律、法规、协议和标准等，以便建立信息空间中的信赖性。很重要的一点是，当人类的许多关系正从物理空间转移到信息空间之际，每个人都需要按规定签署他自己的身份识别号码和证书，以便建立对你的信任关系及正常的网络次序。当然，还应有信息空间中的仲裁机构来解决网络上的纠纷，这样才能使我们既能保证信息安全，又能符合信息化社会发展的需要。

从另一方面来讲，维护一个系统的安全需要各种各样的措施和产品（如防火墙，IDS，VPN，CA 认证中心等），这就需要有些部门及公司联合起来才能实现。

1.6 小结

本章主要论及信息安全的基本概念、系统的脆弱性和所受到的威胁，阐述了系统的访问控制、鉴别、认证以及加密等安全防护机制，介绍了相关的安全产品，扫描器、防火墙安全、VPN 等。

第2章

入侵检测简介

2.1 传统安全模型的局限性

从一开始，人们就企图先构筑某种安全的系统模型，然后想方设法地去实现。著名的Bell-Lapadula安全操作系统模型虽已被广泛接受，但完整性模型（如Biba，Clark-Wilson、Lipner模型）还没有引起足够重视，可靠性模型则更不用说。另外，这些理论模型本身也未必是绝对安全的。继而，人们制定了一系列的安全法则和评测标准，用来构筑一个相对稳固的安全系统。从美国国防部推动的可信计算机系统评价准则（TCSEC）到西欧四国（英、德、法、荷）联合推动的信息技术安全评价准则（ITSEC），发展到六国七方（美（NIST、NSA）加、英、德、法、荷）联合推动的信息技术通用安全评价准则（CC）阶段。虽然这些准则在很大程度上给人们提供了安全保护的策略，如这些准则的前两个都以访问控制机制作为主要安全策略。TCSEC将侧重点放在了系统的保密性方面，ITSEC从保密性、完整性、可用性3个方面提出了要求。CC则进一步考虑了综合应用可信计算机技术和密码技术，从更多的方面实施安全策略。但“安全”永远只能是一个理论上的和相对的概念，仍然有一些不安全的因素没有考虑到。

有诸多的原因导致构筑一个安全系统的困难：首先，系统软件、操作系统正变得越来越复杂，使得软件设计者在设计时无法预料程序运行时的系统状态，更无法精确地预测在不同系统状态下会发生什么结果，所以，系统往往存在漏洞。另外，随着联网需求的日益增长，要将来自系统外部的服务请求完全隔离是不可能的。再者，组成计算机网络的某些关键技术也并非安全，如广泛应用的TCP/IP协议本身就有许多不完善之处。从根本上讲，绝对安全的计算机是根本不存在的，绝对安全的网络也是不存在的。即使再安全的系统，也可能有各种各样的漏洞，如今令计算机界“谈虎色变”的黑客们正是利用了这些漏洞对网络进行攻击。

无论是安全模型，还是系统安全等级评估标准，人们主要是从身份认证和访问控制这两个方面来保证系统的安全性。但是，传统的身份认证技术，包括Kerberos技术，并不能抵制脆弱性口令、字典攻击、特洛伊木马、网络窥探器以及电磁辐射等攻击手段。对于访问控制，入侵者也可以利用脆弱性程序或系统漏洞绕过访问控制，或者提升用户权限，或者非法读写文件等。网络防火墙虽然为网络服务提供了较好的身份认证和访问控制技术，但是防火墙并不能阻挡所有的入侵行为，最常见的有test.cgi和phf攻击。