# 网络与系统安全实用指南

WANG LUO YU XI TONG AN QUAN SHI YONG ZHI NAN

秦　超　李素科　满成圆　编著
陈　钟　审校

北京航空航天大学出版社
http://www.buaapress.com.cn

# 网络与系统安全实用指南

秦　超　李素科　满成圆　编著

陈　钟　审校

北京航空航天大学出版社

http://www.buaapress.com.cn

## 内容简介

本书以简要介绍网络与系统安全知识为主，针对 Windows NT 和 UNIX 两大主要操作系统，详细介绍了各个系统的安全漏洞、防范措施以及高级安全管理技术等内容。书中提供了详实的使用实例和技术细节。是一本针对网络系统和操作系统安全使用性很强的书籍。通过本书的学习，相信读者能够在实际应用中根据系统需求制定出有效的安全措施实现系统的安全。

本书适合于系统管理员与网络管理员以及对网络与系统感兴趣的计算机安全技术人员。

**图书在版编目(CIP)数据**

网络与系统安全实用指南 /秦超等编著. —北京:北京航空航天大学出版社,2002.10

ISBN 7-81077-089-6

Ⅰ.网… Ⅱ.秦… Ⅲ.① 计算机网络—安全技术—指南②计算机系统—安全技术—指南

Ⅳ.TP393.08-62②TP309-62

中国版本图书馆 CIP 数据核字(2002)第 052426 号

**网络与系统安全实用指南**

秦 超 李素科 满成圆 编著

陈 钟 审校

责任编辑 蔡 喆

*

北京航空航天大学出版社出版发行

北京市海淀区学院路 37 号(100083) 发行部电话:(010)82317024 传真:(010)82328026

http://www.buaapress.com.cn

E-mail:pressell@publica.bj.cninfo.net

北京市云西华都印刷厂印装 各地书店经销

*

开本:787×1092 1/16 印张:26.25 字数:672 千字

2002 年 10 月第 1 版 2002 年 10 月第 1 次印刷 印数:4 000 册

ISBN 7-81077-089-6 定价:39.00 元

# 前　言

随着全球信息化的飞速发展，计算机网络技术已经应用到越来越多的行业领域中，于是出现了众多的新概念、新思想，例如电子商务、电子出版、数字图书馆、电子货币等。然而网络信息技术在给人们带来诸多便利的同时，也留下许多隐患问题，由于病毒、黑客等的攻击破坏，造成了信息泄密和巨大的经济损失。于是信息安全问题逐渐成为关注的焦点。

为了帮助广大 IT 技术人员，特别是网络管理员和安全人员，在掌握基本的信息安全理论知识与实践技术的基础上，能够在实际工作中有效地解决相应的安全问题，我们编写了此书。

本书以简要介绍网络与系统安全知识为主，针对实际威胁安全的因素，给出了具体、有效的解决思路。全书分为三篇。第一篇由第 1—4 章组成，为基础篇，从网络和系统安全的基本概念和理论讲起，介绍了 TCP/IP 协议、密码学基础知识，以及认证和访问控制技术。第二篇由第 5—23 章组成，为基本管理篇，针对 Windows NT 和 UNIX 两大主要操作系统，分析了 Windows NT 的用户和组、文件系统、日志、asp 相关的安全问题；分析了 UNIX 系统上 Telnet、FTP、Web、邮件服务的安全漏洞。第三篇由第 24、25 章组成，为高级系统安全篇，介绍了 Corba、Java 和 DCOM 的安全结构，以及从网络协议层次较为全面地给出每一层可以利用的安全机制。

编　者

2002 年 10 月

# 目　录

## 第一篇　基础篇



## 第二篇　管理篇

**第 18 章　Web 服务器的安全**



**第 19 章　邮件服务的安全问题**



**第 20 章　UNIX(Linux)防火墙**



**第 21 章　UNIX 系统的常见网络攻击及其对策**



**第 22 章　入侵检测**

## 第三篇 高级系统安全篇

# 第一篇　基础篇

## 第1章　计算机安全概述

### 1.1　计算机安全简介

计算机安全事业始于20世纪60年代末期。当时，计算机系统的脆弱性在美国已日益为政府和私营部门的一些机构所认识。由于当时计算机的速度和性能较落后，使用的范围也不广，再加上美国政府把它当作敏感问题而加以控制，使有关计算机安全的研究一直局限在比较小的范围内。进入20世纪80年代后，计算机的性能得到了成百上千倍的提高，应用的范围也在不断扩大，计算机已遍及世界各个角落。人们还利用通信网络把孤立的单机系统连接起来，相互通信和共享资源。

今天，随着计算机技术、网络技术和联网规模的快速发展，人们已经进入了网络时代。地域、文化、时间和背景的差距已经不再那么重要，世界上所有的东西几乎都是触手可及的。这使人类体验到了计算机和网络的无穷魅力，充分享受到高科技带来的无穷乐趣。

但是，计算机信息有共享和易于扩散等特性，它在处理、存储、传输和使用上有着严重的脆弱性，很容易被遗漏、丢失、干扰和滥用，甚至被篡改、泄露、窃取、冒充和破坏，还有可能受到计算机病毒的感染，所以随之而来并日益严峻的问题是计算机信息的网络安全问题。

计算机安全包括3个方面：物理安全、逻辑安全和网络安全。物理安全指系统设备及相关设施受到物理保护，避免破坏、丢失等。逻辑安全包括信息完整性、保密性和可用性。

开放性的信息网络带来了开放性的技术，使得网络系统的安全问题变得更加重要。特别是进入2000年以来，网络黑客频频无端攻击国际互联网，包括雅虎、亚马逊、美国有线电视新闻网等在内的美国8家著名网站先后受到不明黑客发起的“阻断服务”袭击，造成了超过12亿美元的经济损失。中国内地多个网站也曾遭到网络黑客的猛烈攻击。网络安全问题刻不容缓地摆在我们面前。

当今网络技术和应用的快速发展，对计算机系统安全提出了更新、更高的要求：

1. 保密性(Confidentiality)

保密性指保证计算机及网络系统的硬件、软件和数据只能为合法用户所使用。由于无法保证是否有非法用户截取网络上的数据，必须采用保密技术来确保数据的保密性。数据加密技术就是用来实现此目标的。

2. 完整性(Integrity)

完整性指维护信息的一致性，防止非法用户对系统数据的篡改。可以采用数据加密和校

验技术实现此目标。

3. 可用性(Availability)

可用性是面向用户的安全要求,指合法用户根据需要可以随时访问系统资源。

4. 身份认证(Authentication)

身份认证指对网络用户进行验证,证实其身份与其所声称的身份是否一致。身份认证既可以建立在基于第三方可靠的权威认证服务基础上,也可以采用较简单的个人对个人的身份认证技术,确保数据来源和目的的可靠性。简单认证的依据可以是用户账号和密码,或者主机地址等,复杂的认证需要有认证协议,与其它安全机制结合使用。

5. 不可否认性(Non—repudiation)

不可否认性是针对通信各方信息真实同一的安全要求,指参与网络通讯过程的各方(用户、实体或者进程)无法否认其过去的参与活动。

6. 授权和访问控制(Access Control)

授权和访问控制规定了用户对数据的访问能力,包括什么用户有权访问、对数据拥有什么操作权力等等。

上述安全特性和技术之间并不是孤立的,它们常常相互结合地使用来完成更强大、更安全的功能;例如,身份认证和授权、存取控制的综合运用可以确保数据的保密性,不可否认技术与认证技术结合可以防止非授权用户对敏感数据的访问。

## 1.2 网络安全体系

有效数据所存储或流通的设备或线路,都是网络安全要考虑的范畴,除了防火墙和登录口令,我们还需要考虑很多事情。

在考虑网络安全问题的过程中,主要应该考虑以下 5 个方面的问题:网络是否安全,操作系统是否安全,用户是否安全,应用程序是否安全,以及数据是否安全。

目前,这个 5 层次的网络系统安全体系理论已得到了国际网络安全界的广泛承认和支持,并已将这一安全体系理论应用在各自的产品之中。下面将逐一对每一层的安全问题做出简单的阐述和分析。

### 1.2.1 网络层的安全性(Network Integrity)

网络层的安全性问题核心在于网络是否受到控制,即:是不是任何一个 IP 地址来源的用户都能够进入网络。如果将整个网络比作一幢办公大楼的话,对于网络层的安全考虑就如同为大楼设置守门人一样。守门人会仔细察看每一位来访者,一旦发现危险的来访者,便会将其拒之门外。

通过网络通道对网络系统进行访问的时候,每一个用户都会拥有一个独立的 IP 地址。这一 IP 地址能够大致表明用户的来源所在地和来源系统。目标网站通过对来源 IP 进行分析,便能够初步判断来自这一 IP 的数据是否安全,是否会对本网络系统造成危害,以及来自这一 IP 的用户是否有权使用本网络的数据。一旦发现某些数据来自于不可信任的 IP 地址,系统便会自动将这些数据阻挡在系统之外。并且大多数系统能够自动记录那些曾经造成过危害的 IP 地址,使得它们的数据将无法第二次造成危害。

### 1.2.2 系统的安全性(System Integrity)

在系统安全性问题中,主要考虑两个问题:一是病毒对于网络的威胁,二是黑客对于网络的破坏和侵入。

病毒的主要传播途径已由过去的软盘、光盘等存储介质变成了网络。多数病毒不仅能够直接感染网络上的计算机,也能够将自身在网络上进行复制。同时,电子邮件、文件传输(FTP)以及网络页面中的恶意 Java 小程序和 ActiveX 控件,甚至文档文件都能够携带对网络和系统有破坏作用的病毒。这些病毒在网络上进行传播和破坏的途径和手段多种多样,使得网络环境中的防病毒工作也变得更加复杂,网络防病毒工具必须能够针对网络中各个可能的病毒入口进行防护。

一般的系统,如 Windows NT,UNIX,甚至拨号服务器、路由器等,都包含最基本的用户账号以及登录口令的安全机制。在系统连接到 Internet 后,一般的做法是在 Internet 和企业内部网的连接处放置一套防火墙系统。这样做可以给系统一定的安全保密能力。

目前已经有足够多的黑客资源提供各种破解、拦截、猜测密码的工具。传统的密码保护显得微不足道。实际上密码本身也会有泄露。种种因素,使得密码成为一个必要但是已不再真正安全的工具。

对于网络黑客而言,他们的主要目的在于窃取数据和非法修改系统。其手段之一是窃取合法用户的口令,在合法身份的掩护下进行非法操作。其手段之二是利用网络操作系统的某些合法但不为系统管理员和合法用户所熟知的操作指令。例如在 Unix 系统的缺省安装过程中,会自动安装大多数系统指令,据统计,其中大概有约 300 个指令是大多数合法用户根本不会使用的,但这些指令往往会被黑客所利用。

要弥补这些漏洞,就需要使用专门的系统风险评估工具帮助系统管理员找出哪些指令是不应该安装的,哪些指令是应该缩小其用户使用权限的。在完成了这些工作之后,操作系统自身的安全性问题将在一定程度上得到保障。

### 1.2.3 用户的安全性(User Integrity)

对于用户的安全性,所要考虑的问题是:是否只有那些真正被授权的用户才能够使用系统中的资源和数据。

首先要做的是对用户进行分组管理。这种分组管理应该是针对安全性问题而考虑的分组,也就是说,应该根据不同的安全级别将用户分为若干等级,每一等级的用户只能访问与其等级相对应的系统资源和数据。其次应该考虑的是强有力的身份认证,其目的是确保用户的密码不会被他人猜测到。

在大型的应用系统之中,有时会存在多重的登录体系。用户如需进入最高层的应用,往往需要多次输入多个不同的密码。如果管理不严,多重密码的存在也会造成安全问题上的漏洞。所以在某些先进的登录系统中,用户只需要输入一个密码,系统就能够自动识别用户的安全级别,从而使用户进入不同的应用层次。这种单一登录体系能够比多重登录体系提供更高的系统安全性。

### 1.2.4 应用程序的安全性(Application Integrity)

在这一层中需要考虑的问题是:是否只有合法的用户才能够对特定的数据进行合法的操作。

其中涉及两个方面的问题:一是应用程序对数据的合法权限,二是应用程序对用户的合法权限。例如在公司内部,上级部门的应用程序应该能够存取下级部门的数据,而下级部门的应用程序一般应该不允许存取上级部门的数据。同级部门的应用程序的存取权限也应有所限制,同一部门不同业务的应用程序也应该不允许访问对方的数据。这样可以避免数据的意外损坏,也是从安全方面的考虑。

### 1.2.5 数据的安全性(Application Confidentiality)

在系统信息安全领域,安全保护的根本对象应当是那些存储在磁盘系统上的有效数据,设置防火墙、使用密码、数据加密等做法都是有效的手段。有效数据存储的任何设备、系统,数据流通的任何线路、连接都是网络安全所要考虑到的,网络安全应当是一个系统的、长期的问题。

对于数据的安全性所要考虑的问题是:机密数据是否还处于机密状态。

在数据的保存过程中,机密的数据即使处于安全的空间,也要对其进行加密处理,以保证即使数据失窃,偷盗者(如网络黑客)也读不懂其中的内容。这是一种比较被动的安全手段,但往往能够收到最好的效果。还有就是将如何贯彻实施系统内部的安全策略,如何检测非法入侵,如何做到一体化的安全管理。

上述的五层安全体系并非孤立分散,它们相互作用相辅相成。简而言之,针对安全问题所涉及的领域;信息安全问题要从下面的问题去考虑:

◇ 如何提高系统自身的安全性;
◇ 如何建立并实施安全策略;
◇ 如何跟踪和限制超级用户的特权活动;
◇ 如何建立安全问题报警系统;
◇ 如何从攻击者的角度去考虑系统的安全性;
◇ 如何设置系统边界的安全;
◇ 如何设置安全堡垒;
◇ 如何检查边界安全性;
◇ 如何保护用户终端数据和传输状态的数据的安全。

## 1.3 网络安全的结构层次

### 1.3.1 物理安全

1. 自然灾害(如雷电、地震、火灾等),物理损坏(如硬盘损坏、设备使用寿命到期等),设备故障(如停电、电磁干扰等),意外事故。解决方案:防护措施,安全制度,数据备份等。

2. 电磁泄漏,信息泄漏,干扰他人,受他人干扰,乘机而入(如进入安全进程后半途离开),

痕迹泄露(如口令密钥等保管不善)。解决方案:辐射防护,屏幕口令,隐藏销毁等。

3. 操作失误(如删除文件,格式化硬盘,线路拆除等),意外疏漏。解决方案:状态检测,报警确认,应急恢复等。

4. 计算机系统机房环境的安全的特点是可控性强,一旦被破坏损失也大。解决方案:加强机房管理,运行管理,安全组织和人事管理。

### 1.3.2 安全控制

1. 微机操作系统的安全控制。如用户开机键入的口令(某些微机主板有"万能口令"),对文件读写、存取的控制(如 UNIX 系统的文件属性控制机制)。主要用于保护存储在硬盘上的信息和数据。

2. 网络接口模块的安全控制。在网络环境下对来自其他机器的网络通信进程进行安全控制。主要包括身份认证,客户权限设置与判别,审计日志等。

3. 网络互联设备的安全控制。对整个子网内的所有主机的传输信息和运行状态进行安全监测和控制。主要通过网管软件或路由器配置实现。

### 1.3.3 安全服务

对等实体认证服务,访问控制服务,数据保密服务,数据完整性服务,数据源点认证服务,禁止否认服务等,都属于安全服务。

### 1.3.4 安全机制

加密机制,数字签名机制,访问控制机制,数据完整性机制,认证机制,信息流填充机制,路由控制机制,公证机制等,都是安全机制。

## 1.4 网络安全的要素

下面就根据上面讲过的五层安全体系以及网络安全的结构层次讨论网络安全的要素。

### 1.4.1 网络的安全

1. 防火墙系统

企业内部网的第一道防线是进出 Internet 的关口。没有这道防线,对 Internet 打开的门和对公司内部打开的门一样。防火墙在企业网的内外之间设置了一道有效的屏障,保护网络边界并防止黑客入侵。防火墙作为一个单一的关口,能检查、审核和认证所有进入网络的数据交换。任何可疑的活动,都会根据设置的规则发出报警。

目前,市场上有三种基本类型的防火墙:路由器、静态包过滤系统和应用层代理防火墙,每种提供不同程度的安全性和适应性。(有关防火墙的内容,会在后面的章节进行详细地讨论。)

值得注意的是,防火墙仅仅是一个网络的隔离设备,它对很多安全问题仍会束手无策:

◇ 来自系统内部的威胁

◇ 保护存储于笔记本电脑上的重要数据

◇ 保护通过 Internet 的数据

◇ 已穿过防火墙的攻击

其中，尤其对来自系统内部或已穿过防火墙的攻击束手无策。一个黑客说："有些系统真好，穿过了防火墙，里面就是天堂。"实际上，由于防火墙本身的漏洞，以及其升级换代速度远跟不上黑客攻击技术和工具能力的提高，使得它无法阻隔所有的攻击和穿透。

2. 边界安全漏洞检查

类似网络系统内部的安全检查，在建立边界防火墙后，从其外部模仿攻击者对系统进行攻击，检查安全漏洞。

3. 边界入侵检测和报警

在防火墙的外部安装报警系统，监视各种攻击行为并采取相应的措施。

4. 安全私有网络

当 Internet 作为一种有效的手段来扩大公司的网络的时候，怎样建立一个安全的私有网络，保护各个站点之间的通讯呢？一个解决办法就是在通迅连接上采用 VPN。

VPN 是虚拟专用网，它集合了数字加密验证和授权来保护经过 Internet 的信息的技术。在远程用户和公司网络之间建立一个安全管道：

◇ 封装和加密数据包

◇ 对网络上访问公司资源的用户进行授权、验证和加密

在传输前，数据被加密和封装来保护它避免被截获，通过加密这些数据包，信息不能够被查、修改或截取。另外，即使被截取，也不能提供任何有用的信息，它使用强大的工业标准加密算法，确保数据在 Internet、WAN 或者客户网络上传输时不能被截取和破解。

使用 VPN 技术可以安全地在不可信任的 Internet 网络上传输信息。

### 1.4.2 网络内部系统以及服务器的安全

现在的网络包括各种各样的系统和平台，如 UNIX、Netware、Windows NT 等系统和手提电脑、PC 机、小型机和大型机等平台。成功的企业越来越多地依赖于各种迅速增长的网络应用。然而，这种复杂的网络已经开始面临来自不同系统信息安全的挑战，我们关心的不仅仅是能否有充足的网络连接到 Internet 上，或者有多少潜在的信息提供给外界，而在于我们的系统是否安全。

假如我们定义的安全标准是完全不允许非法访问，但实际上，即使花费巨大，仍然无法实现 100%的安全。换句话说，计算机环境安全的基本策略是在安全性能和安全支出上取得平衡，同时保证信息传递的完整性、可用性和保密性。

1. 建立并实施网络安全策略

针对系统安全管理的复杂性，安全问题重要的解决办法是建立一套完整可行的安全策略，统一管理和实施这些策略。在以下章节中，将就安全策略进行详细的介绍。

2. 网络安全漏洞检查

一个网络系统的安全漏洞就是它保护最弱的那部分。不管其他部分如何保险，一旦此漏洞被利用，就会给网络带来灾难。如何找到这个漏洞并加以保护，是系统管理员的使命之一。

系统管理员面对服务器、用户和网络设备，需要阅读大量审核文件，进行大量的日常维护和指导工作，不可能把全部精力放在安全防范上。黑客则正好相反，可以把全部精力放在入侵目标上，试着发现目标的各种安全漏洞。

如果能模拟黑客的行为，搜寻系统的安全漏洞，并加以保护和改进，黑客的可乘之机就会越来越少。而事实上，大多数管理员缺乏跟踪黑客行踪，查找安全漏洞的专业技能。网络安全检测软件就是这种功能的软件系统。它可以帮助系统管理员在合适的时间查找整个网络的安全漏洞，并给出详细的报告和解决办法。

3. 入侵检测以及报警

表示有入侵行为发生的现象有以下几种。

(1) 登录失败：如果用户在登录过程中输入了错误的口令，就会引起登录失败，根据用户尝试登录的时间与次数，可以初步判定是常规失误还是蓄意入侵。

(2) FTP 日志：如果在 FTP 日志中发现了未知的 IP 地址，表示入侵者曾试图进行连接。

只要管理员经常登录到每台服务器上阅读、审核跟踪信息，绝大多数非法闯入能够被察觉，没有被察觉的多半是由于管理员没有相关的知识或充足的时间。不过，除非可以猜测入侵者的心理动机，否则多数情况下对入侵者的跟踪是无效的。

管理员不可能把大量的时间花在系统正常运行时产生的审核跟踪资料上，但这样往往会遗漏关键的提示信息。解决上述两个问题的方法是采用好的过滤器警报系统。

### 1.4.3 网络的用户安全

基于 Web 浏览器和服务器计算给了用户集中管理信息和服务的能力，同时又提出了相应的安全访问控制要求。一个问题就是：怎样才能使我们的合作伙伴、供应商和客户有选择性的访问呢？

1. 双因素的增强型认证机制

VPN 产品一定要提供一种用户验证方法。传统的验证依靠静态的或可重新使用的口令，这些口令很容易被黑客得到，而且经常回存到信笺中，写到策略或者电子钱包中。强大的双因素验证提供了更高一级的远程访问安全性，同时并没有增加用户的负担，不需要附加的口令或 login 过程。当出现提示后，用户只需输入个人识别码 PIN，进行透明的用户和网络间的验证，数据交换只一次，而且用户的 PIN 不会在网络上传输，即使这个信息交换被任何黑客技术截取，也是无法访问的。

通常的授权机制有时会因为被绕过而起不到作用，双因素的验证方法可以大大提高安全性，用户的 PIN 仅仅激活安全的远程访问，而且对用户来说是透明的。

验证不仅用来确定一个个体，而且决定他有权访问哪些资源。例如你的远程和移动雇员有权访问财务、竞争对手和产品信息；而你的合作伙伴只有权访问合作项目的信息，不能访问财务和竞争对手的信息；你的客户则可以访问基于 Web 的信息，而不能访问公司的详细信息。每一个用户需要分配一个不同的安全类别：远程、移动或外部用户。

2. 远程访问控制

远程用户分布在各个分站点，但要求有同公司一样的安全级别。这就意味着他们也需要防火墙，需要用一个探测工具检查网络或安装一个防入侵工具，防火墙之间还要用 VPN 连接起来。所以应该寻找一种防火墙产品，既支持 VPN，又支持多个远程防火墙，可以通过总公司进行集中管理，远程防火墙也应该具备同样的功能，提供最大的灵活性、安全性和经济性。

3. 移动用户访问控制

客户端的 VPN 软件运行在用户的笔记本电脑中，而服务器端的 VPN 软件可以集成在防

火墙中或者防火墙后的边界网关内，二者都有优点和不足。依靠防火墙的 VPN 软件能保证防火墙到 VPN 客户端的连通性，大多数 VPN 通过集中的防火墙控制台进行管理。而独立于防火墙的 VPN 软件可以提供优越的集中式网络管理，而又不影响它的性能。

### 1.4.4 Internet 和 Extranet 上的数据安全

Internet 因其经济、有效而成为一种颇具吸引力的商业工具，但它是一种公共网络，没有足够的安全性。在 Internet 上通信，如果没有正确的安全方面的技术支持是非常危险的，E-mail、文件和口令很容易被不同探测器或者黑客工具截获。事实上，很多黑客工具在 Internet 上又是免费提供的。那么，应该如何保护网络上的用户的敏感数据呢？

1. 安全的远程 Web 访问

公司发展基于 Web 的应用，把它作为一种方便的发布信息和访问公司服务的手段。它可以提供有价值的公司信息，因此会被频繁地访问。因此，内部的 Web 服务器也成为黑客攻击的目标。因此需要控制和管理“谁允许访问”和“哪些内容允许访问”。

对于现今的 Web 技术的局限性，提供安全集中式的基于 Web 信息的访问控制是对它的一种挑战。Web 浏览器和 Web 服务器是一种有利的通信方式，很多新近开发的 Web 技术如 Cookies 没有安全性和伸缩性设计，多数服务器需要独立的验证和管理。新的 Web 技术可以提供更多的安全管理：

◇ 伸缩性：访问控制系统与 Web 应用结构是相互独立的，提供了简单易用的集中式的管理界面。它使 Web 开发者可以再利用 Web 应用来扩展他们的需求，不需要重新设计控制系统和管理员再培训。

◇ 单一授权：安全访问控制不仅需要包括一个集中化的服务器检验用户和用户目录，而且也包括了管理 tickets 的机制。Ticket 携带用户的授权信息，用户只需要一个标准的 Web 浏览器，不必进一步的验证。通讯是在 Internet 上进行的，所以安全管理员必须加密所有的授权信息。初始化授权和 ticketing 后，用户才能进入 Web 站点，访问他们允许访问的内容。由于 tickets 是把用户信息存放在浏览器中，访问控制系统必须处理两件事：第一，它必须防止黑客利用 sniffing 获得 ticket，防止修改 ticket 获得访问权限；第二，它必须确定管理员给 tickets 定义的生存周期。利用单一标识可以防止用户名和口令被黑客获取，避免用户在一个不安全的地方存储复杂以及难于记忆的口令。进一步说，使用只有一次有效的口令也会大大减少用户名和口令被黑客获取的危险性。

◇ 集中安全管理：采用集中控制的方法能给管理员和用户带来方便，它可提供图形用户界面来选择授权方法、设置和管理用户访问。另外，因为多数公司为每一个 Web server 设有独立的 Web master 和 content 管理员，访问控制应用也允许独立的 content 管理员应用访问保护来定义目录和内容。这对于动态的 Web 访问和优先级设定是非常重要的。

◇ 互操作性：选择 Web 安全访问工具的同时，也要求它支持多平台，既可以支持 Windows NT，又可以支持 UNIX。当 Web 站点越来越成熟的时候，新的服务和流量也会随之增加，这就需要一个适应新增长的解决方法。传统的方法不能适应跨平台的环境，它们依靠 Web 服务器，SSL 加密和应用程序等，会降低 Web 的应用和实用性。因此，选择一种与现有平台和安全结构无缝集成的 Web 安全技术是非常重要的。