21世纪高等学校计算机规划教材

21st Century University Planned Textbooks of Computer Science

计算机网络安全

Computer Network Security

沈鑫剡 编著

- 介绍完整系统的网络安全基础理论
- 突出主流网络安全技术原理和应用
- 提供解决实际网络安全问题的方法

精品系列

人民邮电出版社
POSTS & TELECOM PRESS

校计算机规划教材

ıned Textbooks of Computer Science

计算机网络安全

Computer Network Security

沈鑫剡 编著

精品系列

人民邮电出版社

北京

图书在版编目（CIP）数据

计算机网络安全 / 沈鑫剡编著. -- 北京 : 人民邮电出版社, 2011.3
21世纪高等学校计算机规划教材
ISBN 978-7-115-23874-0

Ⅰ. ①计… Ⅱ. ①沈… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2010)第189693号

内 容 提 要

这是一本既注重于网络安全基础理论，又着眼培养读者解决网络安全问题能力的教材。书中详细讨论了加密算法、报文摘要算法、鉴别协议等网络安全基础理论，病毒实现技术和防御技术，黑客攻击方法和过程，目前主流的网络安全技术（如以太网安全技术、安全路由、信息流管制、VPN、防火墙、入侵防御系统、安全无线局域网等），以及这些安全技术防御黑客攻击的原理和案例，安全网络的设计方法和过程，安全应用层协议及应用等。

本书的最大特点是将计算机网络安全理论、目前主流网络安全技术和安全网络的设计过程有机集成在一起，既能让读者掌握完整、系统的计算机网络安全理论，又能让读者具备运用主流网络安全技术实现安全网络设计的能力。

本书可作为计算机专业本科生、研究生的计算机网络安全教材，也可供从事计算机网络安全工作的工程技术人员参考。

21 世纪高等学校计算机规划教材

计算机网络安全

◆ 编　　著　沈鑫剡
责任编辑　武恩玉

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：21.5　　2011 年 3 月第 1 版
字数：568 千字　　2011 年 3 月北京第 1 次印刷

ISBN 978-7-115-23874-0

定价：36.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

目前计算机网络安全教材百花齐放，各有特色，但总体上可以分成三类。第一类着重讨论加密、鉴别算法及其他安全协议，这一类教材的特点是比较详细地讲述网络安全理论，尤其对各种算法和协议做了深入讨论，但缺乏和当前主流网络安全技术的结合，很难让读者学以致用。第二类主要讨论黑客攻击手段和防御技巧，这一类教材不介绍系统、完整的网络安全理论，有点像黑客攻防大全。第三类是大杂烩，把操作系统安全机制、应用程序安全机制和网络安全机制放在一起讨论，当然，所有内容都是浅尝辄止。这三类教材虽然侧重点不同，但是存在同样的问题：一是不对当前主流网络安全技术进行深入讨论；二是不在具体网络环境下讨论安全网络的设计方法和过程，对许多问题只是空对空地介绍一些基本概念和方法，没有具体结合目前面临的网络安全问题，更没有应用实例。因此，无法培养读者解决网络安全问题的实际能力。

对于一本真正以实现将读者领进计算机网络安全知识殿堂为教学目标的教材必须具备如下几点：（1）必须提供完整、系统的网络安全理论，这样才能让读者理解网络安全技术的实现机制，具有进一步研究网络安全技术的能力；（2）必须深入讨论当前主流网络安全技术，同时，结合网络安全理论讨论这些安全技术的实现原理，让读者知其所以然，也让读者具备用主流网络安全技术解决实际网络安全问题的能力；（3）需要在具体网络环境下讨论运用网络安全技术设计安全网络的方法和过程，给读者提供解决实际网络安全问题的方法和思路，解决读者学以致用的问题。

作为计算机网络安全教材，应该着重讨论和网络有关的安全问题，和操作系统及应用程序有关的安全问题应该在“操作系统”和“算法与程序设计”课程中予以解决，因为离散地讨论一些安全问题会降低该教材的系统性和连贯性，同时，不和整个操作系统结构和程序设计环境结合来讨论操作系统和应用程序安全问题的解决机制，也不利于读者理解、掌握。计算机网络安全教材不可避免地会涉及黑客攻击和防御，但必须从网络总体结构出发，讨论防御黑客攻击的技术，而不是逐个列出攻击手段和防御方法，将教材变成黑客攻防大全，背离了教材着重于基本理论、基本技术和基本方法的宗旨。

本教材的特色：

（1）为读者提供完整、系统的网络安全理论；

（2）详细讨论当前主流网络安全技术，并结合网络安全理论讨论这些安全技术的实现原理；

（3）在实际网络环境下给出运用当前主流安全技术设计安全网络的方法和过程；

（4）通过构建防御黑客攻击的网络安全体系，讨论运用网络安全技术全方位防御黑客攻击的方法；

（5）通过综合监控系统和 SSL VPN 这样的技术给出了精致控制网络资源访问过程的方法。

在本书编写过程中，解放军理工大学工程兵工程学院计算机应用教研室的同事俞海英、伍红兵、胡勇强、魏涛和龙瑞对教材内容提出了许多很好的建议和意见，其他同事也给予了很多帮助和鼓励，在此向他们表示衷心的感谢。

作为一本无论在内容组织、叙述方法还是教学目标都和传统计算机网络安全教材有一定区别的新教材，不足之处在所难免，殷切希望使用该教材的老师和学生批评指正，也殷切希望读者能够就教材内容和叙述方式提出宝贵的建议和意见，以便进一步完善教材内容。作者 E-mail 为 shenxinshan@163.com。

作者

2010 年 6 月

目　录

第 1 章 概述

构建安全网络的过程包括了解网络面临的安全问题和引发安全问题的原因，掌握黑客攻击手段，针对性地提出防御黑客攻击的网络安全技术，并将这些网络安全技术有机集成在一起，构成实现安全网络设计目标的网络安全体系。

1.1 网络面临的安全问题

1.1.1 网络结构

网络结构由终端、转发结点和链路组成，终端主要用于完成信息的采集、处理和存储（如图 1.1 所示）。在信息技术领域，信息是一种用二进制表示的数据。链路和转发结点构成端到端通信系统，用于实现两个终端之间的信息传输过程。网络的功能是实现资源共享，允许某个终端共享其他终端的处理器、文件等资源，但这种共享必须受到严格控制，这种控制通过授权实现，因此，更确切地说，网络的功能是保证终端共享已经授权共享的资源。由于人们发明网络的原旨是为了实现相互通信，共享资源，因此，网络的结构不但带有开放性，而且一切都是为方便通信和信息访问而设计的，但发明网络的人根本想像不到 Internet 会在 20 世纪 90 年代如此快速地普及，并与人们的生活紧密相关，人们的大量活动在网上开展，电子银行、网上购物已成为时尚，网络也因此成了攻击目标，开始面临各种各样的安全问题。

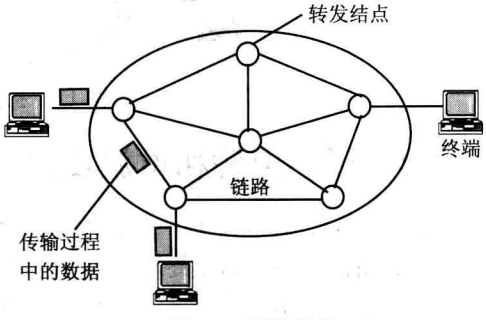

图 1.1 网络结构

1.1.2 非法访问

图 1.1 所示的网络结构首先面临的安全问题是窃取网络中的信息。信息是网络中最重要的资源，信息安全与否已经影响到个人、企业，甚至一个国家的根本利益。网络中主要有存储在终端中的信息和网络传输过程中的信息，因此，针对信息的窃取操作也是以这两类信息为对象展开的。

所谓窃取信息，是指某个用户非法获得没有授权他获得的信息。将这种非法获得信息的过程称为非法访问。非法访问存储在终端中的信息可以通过物理接触终端，将终端中的信息复制到移动媒介中实现，也可以通过网络，用 Telnet、远程桌面系统这样的远程访问工具实现。非法访问

网络传输过程中的信息需要截获或嗅探端到端传输过程中的信息。

图 1.2 所示为用外接集线器窃取信息的例子。集线器具有广播传输特性，从集线器某个端口进入的数据将从所有其他端口广播出去，因此，接在集线器其中一个端口上的信息窃取者可以获得交换机 1 和交换机 2 之间传输的所有数据。图 1.2 中的信息窃取者只能获取两个交换机之间传输的信息，但无法终止信息正常传输过程，这种窃取信息方式称为嗅探。

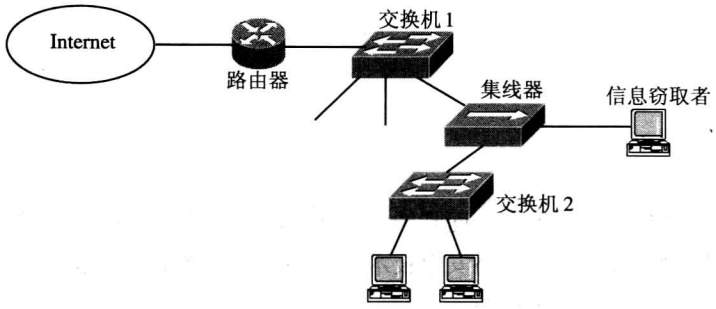

图 1.2　用集线器窃取信息的例子

1.1.3　非法篡改

非法篡改信息是指某个用户改变没有授权他改变的信息，如删除终端中的某个重要文件，改变终端中某个用户的访问权限，改变经过网络传输的信息。图 1.3 中，篡改者中途拦截源终端传输给目的终端的信息，改变其内容后，再发往目的终端。拦截或截获将终止信息正常传输过程，因此，源终端发送的、被篡改者拦截的信息无法通过正常传输路径到达目的终端。

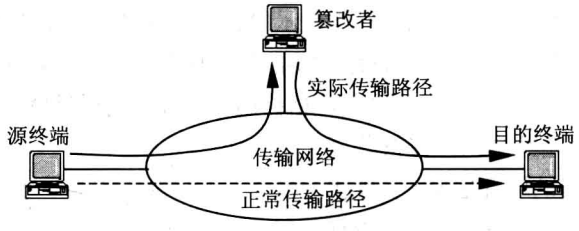

图 1.3　拦截并篡改信息内容

1.1.4　冒名顶替和重放攻击

如图 1.4 所示，终端 B 是一台服务器，授权终端 A 进行管理，因此，终端 B 接收到管理消息时，确认管理消息的发送端是终端 A 时才执行管理消息包含的命令，发送端鉴别过程通常就是一个检查封装管理消息的 IP 分组的源 IP 地址的过程。终端 C 为了让终端 B 执行有利于它的命令，冒充终端 A 与终端 B 通信，即用终端 A 的 IP 地址作为封装终端 C 发送的管理消息的 IP 分组的源 IP 地址。

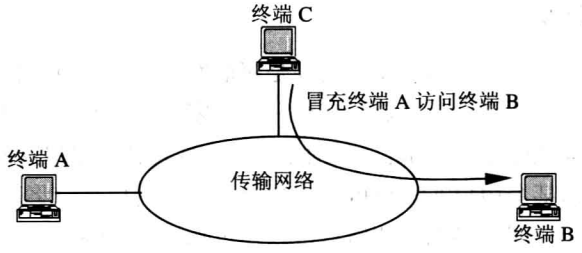

图 1.4　冒名顶替过程

图 1.3 中，篡改者截获源终端发送给目的终端的信息后，复制一份，然后不加修改地转发给目的终端，经过一段时间后，篡改者可以再次转发原先复制的信息，使目的终端重复接收源终端发送的信息，这种攻击方式称为重放攻击。如果该信息包含源终端要求目的终端完成某次交易的命令，如购买一定数量物品的指令，重放攻击将导致目的终端重复进行多次交易。

1.1.5　伪造重要网站

黑客通过 DNS 欺骗将某个重要网站的域名解析成黑客终端的 IP 地址，当用户用该重要网站的域名访问网站时，实际进入了黑客伪造的 Web 页面，用户登录时输入的私密信息（如用户名和口令、银行账号和密码）被黑客截获，黑客可以利用这些私密信息实施破坏活动。

1.1.6　抵赖曾经发送或接收过信息

随着电子商务的开展，大量商务活动通过网络进行，如果用户 A 通过网络发送要求经纪人 B 完成某次交易的信息，但随后后悔，用户 A 可以否认曾经向经纪人 B 发送过要求完成该次交易的信息。同样，经纪人 B 为了自身利益也可以否认曾经接收过用户 A 要求完成该次交易的信息。

1.1.7　拒绝服务攻击

拒绝服务（Denial of Service，DoS）攻击就是用某种方法耗尽网络设备、链路或服务器资源，使其不能正常提供服务的一种攻击手法。目前常见的拒绝服务攻击主要有利用操作系统或应用程序漏洞使服务器崩溃；通过发送大量垃圾信息浪费链路带宽，使正常信息因为阻塞而被丢弃。

1.2　网络攻击手段举例

1.2.1　病毒

病毒是一种具有自复制能力并会对系统造成巨大破坏的恶意代码，它首先隐藏在某个实用程序中，隐藏过程或是由实用程序设计者完成，或是由病毒感染该实用程序的过程完成。当某个计算机下载该实用程序并运行它时，将运行隐藏在其中的恶意代码，即病毒，病毒将感染其他文件，尤其是可执行文件，并接管一些系统常驻软件，如鼠标中断处理程序。如果病毒接管了鼠标中断处理程序，当鼠标操作激发该中断处理程序时，将首先激发病毒程序，病毒程序可以再次感染其他文件，并视情况执行破坏操作，如清除所有硬盘中的文件。当感染了病毒的实用程序被其他计算机复制并执行时，病毒将蔓延到该计算机。

对于单台计算机，病毒传播主要通过相互复制实用程序完成，对于接入网络的计算机，从服务器下载软件、下载主页、接收电子邮件等操作都有可能感染病毒。接入网络的计算机一旦感染病毒，安全将不复存在，存储在计算机中的信息将随时有可能被破坏，机密信息将随时外泄，非授权用户随时有可能通过远程桌面这样的工具对计算机进行非法访问。

1.2.2　非法截获信息

1．ARP 欺骗

图 1.5 所示的网络结构中，黑客终端分配的 IP 地址为 IP C，网卡的 MAC（Medium Access

Control，媒体接入控制）地址为 MAC C，而终端 A 分配的 IP 地址为 IP A，网卡的 MAC 地址为 MAC A，正常情况下，路由器 ARP 缓冲区中应该将 IP A 和 MAC A 绑定在一起，当路由器需要转发目的 IP 地址为 IP A 的 IP 分组时，或者通过 ARP（Address Resolution Protocol，地址解析协议）解析出 IP A 对应的 MAC 地址（如果 ARP 缓冲区中没有 IP A 对应的 MAC 地址），或者直接从 ARP 缓冲区中检索出 IP A 对应的 MAC 地址 MAC A，将 IP 分组封装在以 MAC R 为源 MAC 地址，MAC A 为目的 MAC 地址的 MAC 帧中，然后，通过连接路由器和终端 A 的以太网将该 MAC 帧传输给终端 A。当黑客终端希望通过 ARP 欺骗来截获发送给终端 A 的 IP 分组时，它首先广播一个 ARP 请求帧，请求帧中将终端 A 的 IP 地址 IP A 和自己的 MAC 地址 MAC C 绑定在一起，路由器接收到该 ARP 请求后，在 ARP 缓冲区中将 IP A 和 MAC C 绑定在一起，当路由器需要转发目的 IP 地址为 IP A 的 IP 分组时，将该 IP 分组封装在以 MAC R 为源 MAC 地址，MAC C 为目的 MAC 地址的 MAC 帧中，这样，连接路由器和终端的以太网将该 MAC 帧传输给黑客终端，而不是终端 A，黑客终端成功拦截了原本发送给终端 A 的 IP 分组。为了更稳妥地拦截发送给终端 A 的 IP 分组，黑客终端通常在实施拦截前，通过攻击瘫痪掉终端 A。

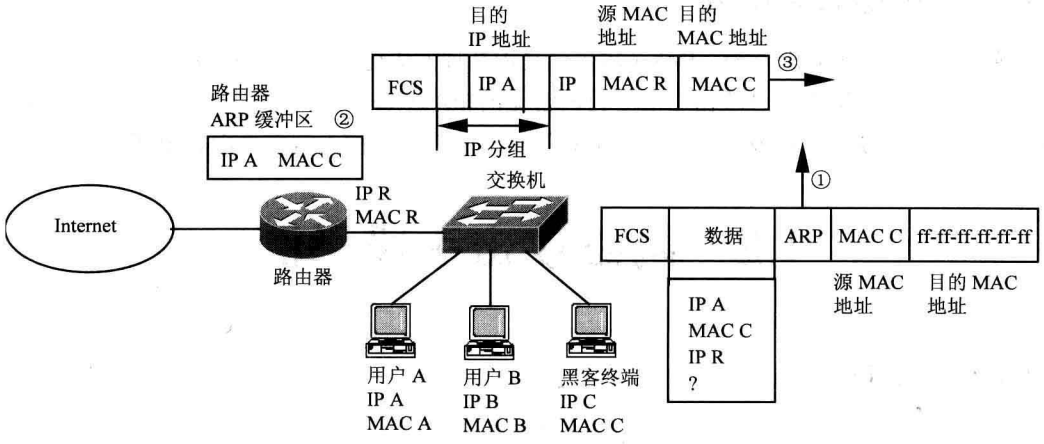

图 1.5　ARP 欺骗过程

2．伪造路由信息

针对图 1.6 所示的网络拓扑结构，路由器 R1 通过路由协议生成的正确路由表如图中路由器 R1 正确路由表所示，这种情况下，终端 A 发送给终端 B 的 IP 分组，将沿着终端 A→路由器 R1→路由器 R2→路由器 R3→终端 B 的传输路径到达终端 B。如果某个黑客终端想截获连接在 LAN 1 上终端发送给连接在 LAN 4 上终端的 IP 分组，通过接入 LAN 2 中的黑客终端发送一个以黑客终端 IP 地址为源地址、组播地址 224.0.0.9 为目的地址的路由消息，该路由消息伪造了一项黑客终端直接和 LAN 4 连接的路由项，和黑客终端连接在同一网络（LAN 2）的路由器 R1 和 R2 均接收到该路由消息，对于路由器 R1 而言，由于伪造路由项给出的到达 LAN 4 的距离最短，将通往 LAN 4 传输路径的下一跳路由器改为黑客终端，如图中路由器 R1 错误路由表所示，并导致路由器 R1 将所有连接在 LAN 1 上终端发送给连接在 LAN 4 上终端的 IP 分组错误地转发给黑客终端。图中终端 A 发送给终端 B 的 IP 分组，经过路由器 R1 用错误的路由表转发后，不是转发给正确传输路径上的下一跳路由器 R2，而是直接转发给黑客终端。

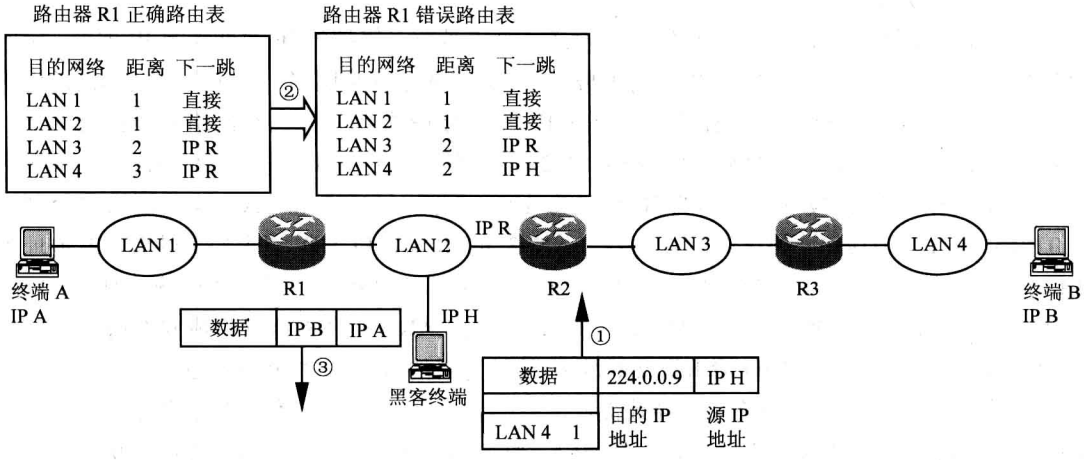

图 1.6　伪造路由过程

1.2.3　拒绝服务攻击

拒绝服务攻击就是用某种方法耗尽网络设备、链路或服务器资源，使其不能正常提供服务的一种攻击手段。SYN 泛洪攻击是一种通过耗尽服务器资源，使服务器不能正常提供服务的攻击手段；Smurf 攻击是一种通过耗尽网络带宽，使被攻击终端不能和其他终端正常通信的攻击手段。

1．SYN 泛洪攻击

如图 1.7 所示，黑客终端伪造多个本不存在的 IP 地址，请求和 Web 服务器建立 TCP 连接，服务器在接收到 SYN=1 的建立 TCP 连接请求后，为请求建立的 TCP 连接分配资源，并发送 SYN=1、ACK=1 的确认响应。但由于黑客终端是用伪造的 IP 地址发起的 TCP 连接建立过程，服务器发送的确认响应不可能到达真正的网络终端，因此，也无法接收到来自客户端的确认报文，该 TCP 连接处于未完成状态，分配的资源被闲置。当这种未完成的 TCP 连接耗尽服务器的资源时，就无法对正常的建立 TCP 连接请求作出响应，Web 服务器的服务功能被抑制。正常终端如果接收到 SYN=1、ACK=1 的确认响应，且自己并没有发送过对应的建立 TCP 连接请求，就向服务器发送 RST=1 的复位报文，使服务器可以立即释放为该 TCP 连接分配的资源，因此，黑客终端用伪造的、网络中本不存在的 IP 地址发起 TCP 连接建立过程是成功实施 SYN 泛洪攻击的关键。

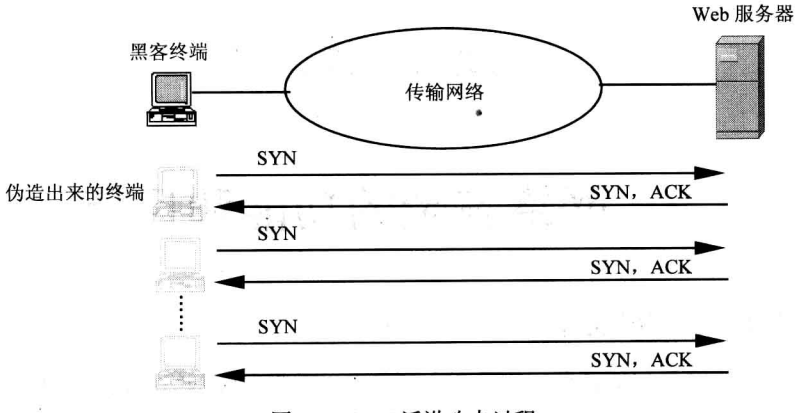

图 1.7　SYN 泛洪攻击过程

2．Smurf 攻击

Smurf 攻击过程如图 1.8 所示，黑客终端发送一个以被攻击终端的 IP 地址为源 IP 地址，定向广播地址为目的 IP 地址的 ICMP ECHO 请求报文，定向广播地址是网络号为某个特定网络的网络号，主机号全 1 的 IP 地址，以这种地址为目的 IP 地址的 IP 分组将发送给网络号所指定网络中的全部终端，假定 LAN 1 的网络号为 192.1.1.0/24，黑客终端的 IP 地址为 192.1.1.1，LAN 2 的网络号为 192.1.2.0/24，被攻击终端的 IP 地址为 192.1.2.1，LAN 3 和 LAN 4 的网络号分别为 10.1.0.0/16 和 10.2.0.0/16，黑客终端发送给 LAN 3 的 ICMP ECHO 请求报文的源 IP 地址为 192.1.2.1，目的 IP 地址为 10.1.255.255。这样的 IP 分组在 LAN 3 中以广播方式传输，到达 LAN 3 中的所有终端。由于接收到 ICMP ECHO 请求报文，因此 LAN 3 中所有终端生成并发送以自身 IP 地址为源 IP 地址，ICMP ECHO 请求报文的源 IP 地址为目的 IP 地址的 ICMP ECHO 响应报文，这些 IP 分组一起发送给被攻击终端，导致被攻击终端和 LAN 3 之间的数据传输通路发生拥塞，使其他网络中的终端无法和被攻击终端正常通信。黑客终端能够阻塞掉被攻击终端连接网络的链路的主要原因是利用了目标网络的放大作用，由于定向广播地址的接收方是特定网络中的所有终端，因此，黑客终端发送的单个 ICMP ECHO 请求报文将引发特定网络中的所有终端向被攻击终端发送 ICMP ECHO 响应报文，如果该特定网络中有 100 个终端，那么黑客终端发送的攻击报文就被放大了 100 倍。如图 1.8 所示，在 LAN 3 和 LAN 4 分别连接 3 个终端的情况下，黑客终端发送的 2 个 ICMP ECHO 请求报文导致被攻击终端接收到 6 个 ICMP ECHO 响应报文。

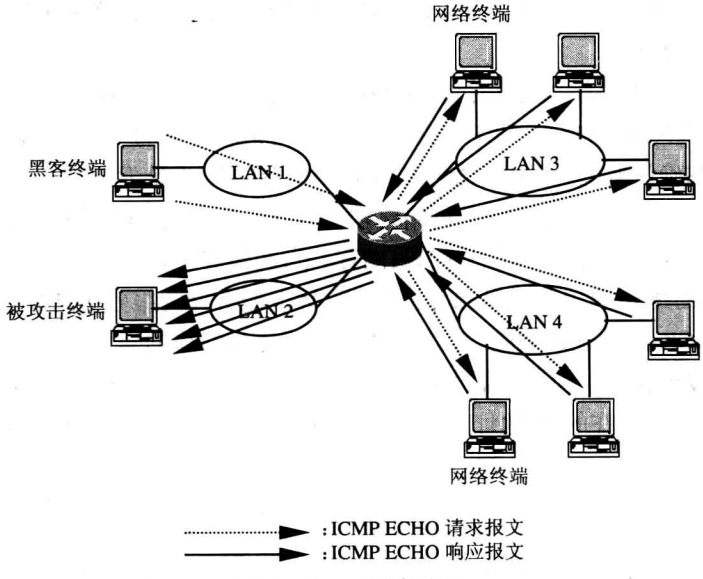

图 1.8　Smurf 攻击过程

1.3　网络安全的功能和目标

1.3.1　网络安全的功能

网络安全是信息安全的组成部分。信息安全顾名思义就是保障网络中信息的安全。网络中的信息由存储在终端中的信息和传输过程中的信息组成，因此，信息安全必须保障存储在终端中的信息

的安全和传输过程中的信息的安全，由计算机安全保障存储在终端中的信息的安全，由网络安全保障传输过程中的信息的安全。随着互联网的普及和发展，网络已经成为病毒的主要传播途径，黑客也常常通过网络远距离窃取存储在某个计算机中的信息，如此，网络安全除了保障传输过程中的信息的安全外，还须包括阻断病毒传播和黑客非法访问途径的功能。因此，网络安全可以定义为是所有用于保障传输过程中的信息的安全、阻断病毒传播和黑客非法访问途径、应对各种各样网络攻击手段的机制和技术的集合。显然，网络安全不应包括操作系统和应用程序的安全机制和技术。

1.3.2　网络安全的目标

网络安全目标是实现信息的可用性、保密性、完整性、不可抵赖性和可控制性。

1．可用性

可用性是信息被授权实体访问并按需使用的特性。通俗地讲，就是做到有权使用信息的人任何时候都能使用已经被授权使用的信息，信息系统无论在何种情况下都要保障这种服务；而无权使用信息的人，任何时候都不能访问到没有被授权使用的信息。

2．保密性

保密性是防止信息泄露给非授权个人或实体，只为授权用户使用的特性。通俗地讲，信息只能让有权看到的人看到，无权看到信息的人，无论在何时，用何种手段都无法看到信息。

3．完整性

完整性是信息未经授权不能改变的特性。通俗地讲，当信息在计算机存储和网络传输过程中，非授权用户无论何时，用何种手段都不能删除、篡改、伪造信息。

4．不可抵赖性

不可抵赖性是信息交互过程中，所有参与者不能否认曾经完成的操作或承诺的特性，这种特性体现在两个方面，一是参与者开始参与信息交互时，必须对其真实性进行鉴别；二是信息交互过程中必须能够保留下使其无法否认曾经完成的操作或许下的承诺的证据。

5．可控制性

可控制性是对信息的传播及内容具有控制能力的特性。通俗地讲，就是可以控制用户的信息流向，对信息内容进行审查，对出现的安全问题提供调查和追踪手段。

1.4　网络安全机制

1.4.1　加密

信息存储和传输过程中，存在被非法访问、嗅探和截获的可能，为了保障信息的保密性，最好的办法是对信息进行加密，加密是指用加密算法（E）和密钥（K1）对明文（P）进行运算，使其成为无法正常识别的密文（Y）的过程，如图 1.9 所示。而解密是加密的逆过程，是指用解密算法（D）和密钥（K2）对密文（Y）进行运算，重新得到明文（P）的过程。

$$Y=E_{K1}(P) \tag{1.1}$$

$$P=D_{K2}(Y) \tag{1.2}$$

$$D_{K2}(E_{K1}(P))=P \tag{1.3}$$

式（1.1）是加密公式，式（1.2）是解密公式，式（1.3）是还原明文过程。如果加密密钥 K1= 解密密钥 K2，称加密解密算法为对称密钥算法，如果加密密钥 K1 ≠ 解密密钥 K2，称加密解密算

法为不对称密钥算法。由于加密和解密运算都是改变信息内容的过程，只是改变过程互逆，因此，两者可以互换，即 $E_{K1}(D_{K2}(P)) = D_{K2}(E_{K1}(P)) = P$。

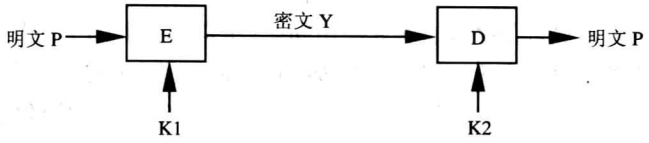

图 1.9　加密解密过程

除非同时获悉密钥 K2 和解密算法，否则，即使获得密文，也无法解读密文包含的内容，即无法还原密文对应的明文。

1.4.2　身份鉴别

电子商务中，时常需要验证信息发送者的身份，鉴别就是验证发送者身份的过程，因此，为了实现鉴别，发送者发送的信息中需要包含用于确认其身份的内容，简单的鉴别通过检测封装信息的 IP 分组的源 IP 地址实现，由于存在源 IP 地址欺骗攻击，这种检测方法已经无法鉴别发送者身份，常见的鉴别机制是给发送者分配一个密钥 K，该密钥 K 只有发送者和鉴别发送者身份的鉴别者知道，当发送者给鉴别者发送信息 P 时，发送给鉴别者的是 $P \| E_K(P)$，‖ 表示串接操作符，用于将两串信息合并在一起，如“123456”‖“ABCD”=“123456ABCD”，E 是对称密钥算法中的加密算法。鉴别者用加密算法 E 对应的解密算法 D 和密钥 K 对附在信息 P 后面的密文进行解密，如果解密结果等于信息 P（$D_K(E_K(P)) = P$），就表示发送者拥有密钥 K，发送者身份得到确认。

1.4.3　完整性检测

为了防止信息传输过程中被篡改，接收端需要能够检测出信息是否被篡改的机制，这种机制称为完整性检测机制。在构成传输信息的帧结构（如 MAC 帧）时，通常附加检错码，检错码 C 是需要传输的信息 P 的一种函数，即 C=F(P)（F 是某种函数），当 P 发生改变时，C 随之发生改变，好的检错码一是要求长度固定，和信息 P 长度无关，且为了减少开销，长度尽可能小；二是能够检测出信息 P 的任意改变，即只要 $P' \neq P$，$F(P') \neq F(P)$。事实上，这两个要求是相悖的，因此，好的检错码只是在两者之间取得较好的平衡。发送端发送的消息是 $P \| C$（$C = F(P)$），如果传输过程中 P 改变为 P′，但 C 没有改变，接收端根据 $F(P') \neq C$ 确定 P 或者 C 在传输过程中发生改变，这就是检错码的检错原理。单纯用检错码是无法检测出信息是否被篡改的，因为，篡改者将 P 改变为 P′的同时，可以将 C 改变为 C′，且使 $C' = F(P')$。保证接收端能够检测出被篡改的信息的前提是使篡改者无法同时改变信息 P 和检错码 C，为了做到这一点，发送端发送的消息是 $P \| E_K(C)$（C=F(P)，密钥 K 只有发送端和接收端知道），这样，接收端检测信息是否被篡改的过程如下：根据接收到的信息重新计算检错码，然后将重新计算的检错码和对密文解密运算后的结果比较，如果两者相等，表示信息没有被篡改，如果两者不相等，表示信息已经被篡改，由于篡改者无法知道密钥 K，因此，篡改者只能改变信息 P，无法重新根据改变后的信息 P′，计算 $E_K(C')$（$C' = F(P')$），导致接收端能够检测出被篡改的信息。当然，这种检测机制必须保证篡改者无法根据 P，产生 P′，且使 $P \neq P'$，但 $F(P) = F(P')$，否则，篡改者如果将信息 P 改变为 P′，那么接收端是无法检测出这种改变的。简单的检错码算法很难做到这一点，因此，需要提出一种新的算法 F，根据目前的计算能力能够保证：对于任何长度的 P，无法得出 P′，$P \neq P'$，但 $F(P) = F(P')$。这种不同于检错码