第 7 章　网络安全

随着计算机网络的发展，网络中的安全问题也日趋严重。当网络的用户来自社会各个阶层与部门时，大量在网络中存储和传输的数据就需要保护。由于计算机网络安全是另一门专业学科，所以本章只对计算机网络安全问题的基本内容进行初步的介绍。

本章最重要的内容是：

(1) 计算机网络面临的安全性威胁和计算机网络安全的主要问题。

(2) 对称密钥密码体制和公钥密码体制的特点。

(3) 鉴别、报文鉴别码、数字签名、证书、证书链的概念。

(4) 网络层安全协议 IPsec 协议族和运输层安全协议 TLS 的要点。

(5) 应用层电子邮件的安全措施。

(6) 系统安全：防火墙与入侵检测。

7.1　网络安全问题概述

本节讨论计算机网络面临的安全性威胁、安全的内容和一般的数据加密模型。

7.1.1　计算机网络面临的安全性威胁

计算机网络的通信面临两大类威胁，即**被动攻击**和**主动攻击**（如图 7-1 所示）。

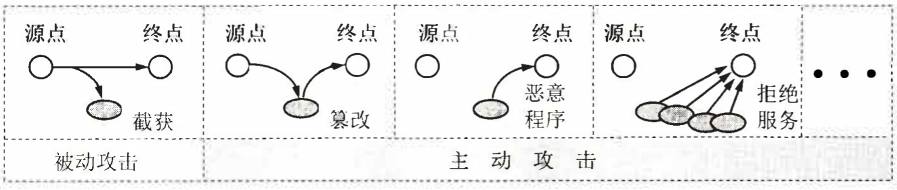

图 7-1　对网络的被动攻击和主动攻击

被动攻击是指攻击者从网络上窃听他人的通信内容。通常把这类攻击称为**截获**。在被动攻击中，攻击者只是观察和分析某一个**协议数据单元** PDU（这里使用 PDU 这一名词是考虑到所涉及的可能是不同的层次）而不干扰信息流。即使这些数据对攻击者来说是不易理解的，他也可通过观察 PDU 的协议控制信息部分，了解正在通信的协议实体的地址和身份，研究 PDU 的长度和传输的频度，从而了解所交换的数据的某种性质。这种被动攻击又称为**流量分析**(traffic analysis)。在战争时期，通过分析某处出现大量异常的通信量，往往可以发现敌方指挥所的位置。

主动攻击有如下几种最常见的方式。

(1) **篡改**　攻击者故意篡改网络上传送的报文。这里也包括彻底中断传送的报文，甚至是把完全伪造的报文传送给接收方。这种攻击方式有时也称为更改报文流。

(2) **恶意程序**　恶意程序(rogue program)种类繁多，对网络安全威胁较大的主要有以下几种：