WANG LUO AN QUAN BIAN CHENG YU SHI JIAN

网络安全编程与实践

陈卓 阮鸥 沈剑 编著

随书附光盘一张

国防工业出版社
National Defense Industry Press

网络安全编程与实践

陈卓　阮鸥　沈剑　编著

国防工业出版社
·北京·

内容简介

本书首先介绍了网络安全基础概念，然后重点介绍网络安全编程中常用的两种重要的开发包 CryptoAPI、OpenSSL 的编程方法和技巧。本书在基本概念、基本方法讲解后紧跟实例，力求操作步骤清晰易懂，一步一步引导读者掌握网络安全编程方法。

本书理论与实践相结合，实践性强是本书的主要特点，文字通俗易懂，可作为信息安全专业或其他相关专业的教学或参考用书，也可作为从事网络安全研究、软件开发以及网络安全编程爱好者的参考书。

图书在版编目(CIP)数据

网络安全编程与实践/陈卓，阮鸥，沈剑编著．—北京：国防工业出版社，2008.8

ISBN 978-7-118-05755-3

Ⅰ.网… Ⅱ.①陈…②阮…③沈… Ⅲ.计算机网络-安全技术-程序设计 Ⅳ.TP393.0

中国版本图书馆 CIP 数据核字(2008)第 073904 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号　邮政编码 100044)

北京奥鑫印刷厂印刷

新华书店经售

*

开本 787×1092　1/16　**印张**　19¾　**字数**　456 千字

2008 年 8 月第 1 版第 1 次印刷　**印数** 1—4000 册　**定价** 40.00 元(含光盘)

(本书如有印装错误，我社负责调换)

国防书店：(010)68428422　　发行邮购：(010)68414474

发行传真：(010)68411535　　发行业务：(010)68472764

前言

随着网络应用的发展和普及，信息安全的重要性日益突出，信息安全关系到国家的主权，它是国家安全的重要组成部分，构筑面向21世纪的国家信息安全保障体系，无疑具有十分重要的战略意义。

信息安全是一个综合的、交叉的学科领域，涉及数学、信息、通信和计算机等诸多学科的长期知识积累，因此它的理论性很强。同时信息安全也是一个实践性很强的学科，仅仅通过书本，不可能全面深入地掌握信息安全的知识体系，必须理论与实践相结合，其中实践动手能力中比较重要的一个方面就是编程能力的培养，这是作者编写本书的初衷。

在网络安全系统研发中会经常碰到诸如如何对消息进行加密、解密，如何对消息实现数字签名，如何建立一个CA系统等问题。为了解决以上这些实际问题，可以采用一些专用的网络安全开发包，这些网络安全开发包是指用于网络安全研究和开发的一些专业的开发函数库和算法库，它们的主要作用是实现网络安全研究和开发的基本功能，为研究者和开发者进一步研究和开发网络安全服务提供编程接口，使网络开发人员能够忽略一些密码算法的具体过程和网络底层的细节，从而更专注于程序本身具体功能的设计和开发。

网络安全开发包有很多种，功能也大不相同，在现有的多种网络安全开发包中，本书选取的是CryptoAPI和OpenSSL，它们可提供对数据的机密性、完整性、不可否认性以及密钥管理、证书管理等安全服务的编程接口，其特点如下：

(1)CryptoAPI：CryptoAPI是提供开发者在Windows下使用PKI的编程接口。CryptoAPI提供了很多函数，包括编码、解码、加密、解密、消息鉴别、证书管理等功能。

(2)OpenSSL：OpenSSL是用于安全通信的著名开放库，也是一个开放源代码的SSL协议的产品实现，它采用C语言作为开发语言，OpenSSL提供了建立在普通的通信层基础上的加密传输层，这些功能为许多网络应用和服务程序所广泛使用。

OpenSSL的密码算法库是一个强大完整的算法库，它是OpenSSL的基础部分，也是很值得一般密码安全技术人员研究的部分，它实现了目前大部分主流的密码算法和标准，主要包括公开密钥算法、对称加密算法、散列函数算法、X.509数字证书标准、PKCS12、PKCS7等标准。OpenSSL具备的应用程序既能直接使用，也可以方便进行二次开发。

本书内容共分为三篇。

第一篇由第1、2章组成，主要介绍与第二、三篇密切相关的网络安全、密码学的基本概念、基本原理，有一定密码学和网络安全基础的读者可以直接从第二篇开始阅读。

第1章为概述部分，首先介绍了计算机网络安全的定义、面临的主要威胁，网络安全的基本需求：机密性、完整性、可用性、不可否认性等，以及构建网络安全体系结构的主要技术，然后对本书介绍的两种网络安全开发包进行了总体介绍。

第2章介绍了和本书密切相关的一些密码学基本概念，包括密码算法的分类，几种有代表性的对称密码算法和非对称密码算法的实现原理、数据的鉴别技术、数字签名和身份认证技术、网络安全协议等。

第二篇由第3、4章组成，介绍了CryptoAPI实用网络安全编程方法和技巧。

第3章对CryptoAPI的体系结构进行了总体上的介绍，并介绍了CryptoAPI的编译环境设置，为了让读者对CryptoAPI有一个直观、初步的认识，本章给出了一个采用CryptoAPI实现消息加密、解密的完整程序，并对该程序结构以及所使用的主要函数进行了说明。

第4章在CryptoAPI的密钥管理、数据编码/解码、数据的加密和解密、数字签名和验证、证书和证书库管理几个方面详细介绍了CryptoAPI提供安全服务的编程实现方法。

第三篇由第5、6、7三章组成，介绍OpenSSL的编程与应用。

第5章首先介绍了OpenSSL的基本结构和功能，然后介绍了OpenSSL编译安装的步骤，最后介绍了OpenSSL应用程序提供的基本指令的基本格式和使用方法。

第6章主要介绍采用OpenSSL的高层算法封装EVP函数实现安全服务的编程方法。首先总体上介绍了OpenSSL的高层算法封装EVP函数的几种主要类型，然后按以下五个方面：对称算法、公钥算法、哈希摘要算法、消息鉴别码MAC算法、数字签名和验证算法，分别介绍了其编程实现的方法，每个方面都详细介绍了相关的数据结构、相关函数的功能、参数、使用方法，并对给出的程序实例进行了详细说明。

第7章介绍了采用OpenSSL实现SSL/TSL协议和PKI相关功能的编程实现方法。首先介绍采用OpenSSL的BIO连接库建立一个简单的服务器和客户端的编程实现，然后在此基础上，介绍了一个加入了SSL握手的服务器和客户端连接实例。7.2介绍了采用OpenSSL的相关函数实现服务器和客户端的双向认证。7.3介绍了如何使用OpenSSL库对PKI的相关标准进行编程实现，以此为基础就可以建立一个完善的PKI系统。7.4介绍了OpenSSL提供的高层I/O接口BIO库的编程方法，并介绍了Engine机制的原理、数据结构，并给出了一个Engine实例。

每章内容后都附有本章小结、习题，帮助读者掌握基本概念和关键技术，使读者能学以致用，尽快进入实用状态。

本书所有程序都在VC6.0环境中编译运行通过，部分程序代码由于篇幅限制只给出了主要源代码，所有程序源代码可参见本书所附光盘。

本书可以满足两部分读者的需求：一方面可作为信息安全专业或其他相关专业的教材或教学参考书；另一方面可作为从事信息安全领域的软件开发人员的参考书。

本书第一篇由陈卓编写；第二篇由阮鸥编写；第三篇由沈剑编写，陈卓负责全书的内容组织和统稿工作。

在本书的出版过程中，得到了北京邮电大学周亚建博士的大力帮助。此外，湖北工业大学的研究生严敬川、陈刚在本书的编写工作上也给予作者很大的帮助，谨在此一并表示衷心感谢。

在向读者们热情推荐本书的同时，我们也深深感到计算机网络安全的理论、技术以及应用可谓博大精深，网络安全新技术如雨后春笋般层出不穷。

书中如有错误和疏漏，敬请各位同仁批评指正，并提出宝贵意见。

作者

目 录

第一篇

第1章 概述 …… 1

1.1 引言 …… 1

1.1.1 计算机网络面临的主要威胁 …… 1

1.1.2 计算机网络安全的基本需求 …… 3

1.1.3 主要的网络安全技术 …… 3

1.2 网络安全编程简介 …… 5

1.2.1 借助开发工具实现网络安全编程 …… 5

1.2.2 几种常见网络安全开发包 …… 5

1.2.3 如何使用网络安全开发包 …… 6

本章小结 …… 7

复习思考题 …… 7

第2章 网络安全基础 …… 8

2.1 密码学基本概念 …… 8

2.1.1 密码学的历史与发展 …… 8

2.1.2 密码体制的构成 …… 9

2.1.3 密码体制的分类 …… 9

2.2 对称密码体制 …… 10

2.2.1 DES …… 10

2.2.2 其他几种对称分组算法 …… 13

2.2.3 分组算法的工作模式 …… 15

2.2.4 序列算法 …… 17

2.2.5 对称密码的局限性 …… 18

2.3 公钥密码体制 …… 18

2.3.1 公钥密码体制基本概念 …… 18

2.3.2 RSA 算法 …… 20

2.3.3 Diffie－Hellman 交换 …… 20

2.3.4 对称密码体制与公钥密码体制的比较 …… 21

2.4 密钥管理 …… 22

2.4.1 密钥的种类与层次式结构 …… 22

2.4.2 密钥的生成与分发 …… 23
2.5 消息的鉴别与数字签名 …… 24
2.5.1 哈希函数 …… 24
2.5.2 消息鉴别的原理 …… 26
2.5.3 数字签名 …… 26
2.6 证书与 PKI …… 28
2.6.1 数字证书 …… 28
2.6.2 CA 认证中心 …… 30
2.6.3 公共密钥基础设施 PKI …… 32
2.7 网络安全协议 …… 34
2.7.1 网络安全协议概述 …… 34
2.7.2 SSL 简介 …… 35
本章小结 …… 36
复习思考题 …… 36

第 二 篇

第 3 章 CryptoAPI 概述 …… 37
3.1 CryptoAPI 简介 …… 37
3.1.1 微软加密服务体系 …… 37
3.1.2 CryptoAPI 体系架构 …… 39
3.1.3 CryptoAPI 基本功能 …… 39
3.2 CryptoAPI 编程 …… 41
3.2.1 Crypto API 编译环境设置 …… 41
3.2.2 例子程序 …… 43
本章小结 …… 54
复习思考题 …… 54
第 4 章 CryptoAPI 安全服务的编程实现 …… 55
4.1 CryptoAPI 编程基础 …… 55
4.1.1 CryptoAPI 密钥管理 …… 55
4.1.2 CryptoAPI 编码与解码 …… 65
4.2 CryptoAPI 数据加解密 …… 78
4.2.1 加解密操作流程 …… 78
4.2.2 文件加密 …… 78
4.2.3 文件解密 …… 86
4.2.4 数字信封打包及拆解 …… 90
4.3 CryptoAPI 数字签名 …… 101
4.3.1 CryptoAPI 数字签名流程 …… 101

4.3.2 哈希与数字签名 …… 102
4.3.3 利用数字证书进行签名与验证 …… 109
4.3.4 数字签名与消息加密 …… 117
4.4 CryptoAPI 证书与证书库 …… 127
4.4.1 CryptoAPI 证书与证书库概述 …… 127
4.4.2 应用工具 makecert 介绍 …… 130
4.4.3 CryptoAPI 证书库管理 …… 132
4.4.4 CryptoAPI 证书管理 …… 152
本章小结 …… 163
复习思考题 …… 164

第 三 篇

第 5 章 OpenSSL 概述与基本指令 …… 165
5.1 OpenSSL 概述 …… 165
5.1.1 OpenSSL 基本结构和功能 …… 165
5.1.2 OpenSSL 的编译安装 …… 168
5.1.3 在 VC++6.0 下使用 OpenSSL 库的环境设置 …… 173
5.2 OpenSSL 基本指令介绍 …… 175
5.2.1 对称加密算法指令 enc …… 176
5.2.2 非对称加密指令 …… 177
5.2.3 信息摘要和数字签名指令 …… 179
5.2.4 证书和 CA 指令 …… 180
5.3 OpenSSL 基本指令的应用 …… 182
5.3.1 创建 CA …… 183
5.3.2 计算文件摘要 …… 186
5.3.3 加密算法运算速度表 …… 187
本章小结 …… 188
复习思考题 …… 188
第 6 章 OpenSSL EVP 编程 …… 189
6.1 对称算法以及 Base64 编码编程 …… 189
6.1.1 主要数据结构和函数说明 …… 189
6.1.2 程序举例 …… 197
6.2 公钥算法编程 …… 202
6.2.1 相关函数说明 …… 202
6.2.2 程序举例 …… 204
6.3 哈希摘要算法编程 …… 207
6.3.1 相关函数说明 …… 207

6.3.2 程序举例 …… 209
6.4 消息鉴别码 MAC 算法编程 …… 210
6.4.1 函数说明 …… 211
6.4.2 程序举例 …… 213
6.5 摘要签名和验证算法编程 …… 216
6.5.1 相关函数说明 …… 216
6.5.2 程序举例 …… 218
本章小结 …… 222
复习思考题 …… 222
第 7 章 OpenSSL 应用与高级编程 …… 224
7.1 SSL/TSL 编程 …… 224
7.1.1 一个基本的服务器 …… 224
7.1.2 一个基本的客户端 …… 229
7.1.3 服务器和客户端证书的生成 …… 231
7.1.4 有 SSL“握手”的服务器 …… 232
7.1.5 有 SSL“握手”的客户端 …… 237
7.2 双向认证的 SSL 连接 …… 240
7.2.1 双向认证的 SSL 服务器 …… 240
7.2.2 双向认证的 SSL 客户端 …… 246
7.3 PKI 编程 …… 249
7.3.1 PKI 编程概述 …… 249
7.3.2 X.509 标准的编程实现 …… 251
7.3.3 PKCS#7 标准的编程实现 …… 268
7.3.4 PKCS#12 标准的编程实现 …… 277
7.4 OpenSSL 高级编程 …… 284
7.4.1 BIO 库 …… 284
7.4.2 OpenSSL 的 Engine 机制 …… 297
本章小结 …… 306
复习思考题 …… 306
参考文献 …… 308

第一篇

第1章 概 述

1.1 引言

1.1.1 计算机网络面临的主要威胁

当你遨游在 Internet 浩瀚无际的信息海洋时，就会发现计算机只有同网络相连，才是名副其实的计算机，从一定意义上讲，“网络就是计算机”，“计算机就是网络”，两者密不可分。随着计算机网络的飞速发展，这一关于计算机的现代理念已经越来越得到人们的认可。因此，要给计算机网络安全下定义，首先要了解计算机安全的概念。

国际标准化组织(ISO)将计算机安全定义为：“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。”

综合上述计算机安全的定义以及计算机和网络的密切关系，可以给计算机网络安全作如下定义：“保护计算机网络系统中的硬件、软件及其数据不受偶然或者恶意原因而遭到破坏、更改、泄露，保障系统连续可靠地正常运行，网络服务不中断。”

计算机网络如此容易受到侵害，由于主要存在两个方面的问题：一方面，资源共享是计算机网络的重要特点，这对于无数的计算机用户无疑是天大的好事，否则，网络也不会受到人们的如此青睐。但也正是因为共享，却被一些别有用心者钻了空子，使得网络信息及网络设备的安全容易受到种种不同程度的威胁；另一方面，从网络协议结构设计看，如今使用最广泛的网络协议是 TCP/IP 协议，它最初的主要设计目标是互联、互通、共享，而不是安全。实践证明，该协议中已被发现有许多安全漏洞和隐患，这是因为研制者在设计初并没有过多考虑网络的安全性能。因此，计算机技术包括网络技术，虽然已经从过去的研究阶段进入了商品实用阶段，但是它的技术基础却是不安全的，有其脆弱的一面，这是不可否认的客观事实。

知己知彼，百战不殆。下面通过计算机网络上用户的通信来考察一下计算机网络面临的主要威胁。

(1) 截获：当发送方通过网络与接收方通信时，如果不采取任何保密措施，那么其他人就有可能截获并偷听到他们的通信内容，如图 1-1 所示。

(2)篡改：未授权方不仅获得了访问而且篡改了内容。随着信息技术的发展，信息处理与计算能力得到了极大的提高，敌人对保密通信体制的攻击，除了原来的截获—破译外，在很多场合，特别是在实时性要求不太高的情况下，对手可采用在信道中间插入一个

图 1-1　消息被截获

非法设备，对原来的信息进行诸如删除、添加、修改等活动。例如，发送方 A 给接收方 B 发如下消息："我是 A，请立即给我汇款 1 万元"，报文在转发的过程中，被 C 篡改成"我是 A，请立即给 C 汇款 10 万元"；或者 C 将 A 发送给 B 的"请原地待命"改成"请马上撤退"，都会给 A、B 之间带来无法挽回的损失，如图 1-2 所示。

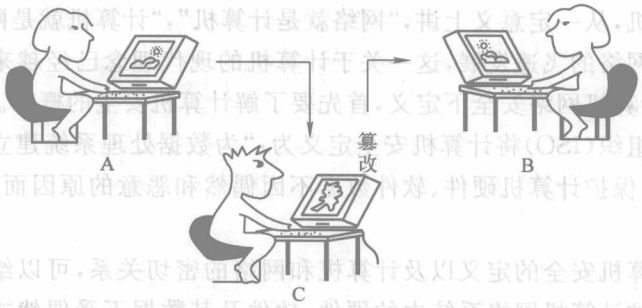

图 1-2　消息被篡改

(3)抵赖：这是通信双方之间可能发生的安全隐患，例如 A 否认自己曾经给 B 发出过的报文(如签发的支票)。在电子商务系统中特别需要提供抗抵赖服务。

(4)黑客攻击：拒绝服务、缓冲区溢出、木马是黑客攻击的常用形式，例如，拒绝服务 DoS(Denial of Service)是一种破坏性的攻击方式，旨在使目的主机陷入停顿或无意义的繁忙，从而使合法用户无法正常使用资源，造成网络效率降低甚至瘫痪。如 Ping 风暴是一种常用的 DoS 攻击方法，只要多人约定在某个时刻同时对目标主机使用 Ping 程序，就可能逐渐耗尽目标主机的网络带宽和处理能力，造成网络效率急剧降低或瘫痪。

目标探测和扫描一般是黑客攻击的第一步，目标探测是用自动和人工的方法获得与目标网络相关的物理和逻辑参数以明确攻击的目标，扫描是对计算机系统或网络进行扫描检测，找出隐含的安全隐患和漏洞，然后攻击者就可利用口令破解、木马、拒绝服务、缓冲区溢出等具体的攻击形式发起攻击。

(5) 病毒危害：计算机病毒也是计算机网络面临的主要威胁之一。所谓病毒(Viruses)是指一段可执行的程序代码，通过对其他程序进行修改，可以"感染"这些程序，使它们含有该病毒程序的一个复制，有的病毒还具备引发损坏和植入攻击的能力。由于网络的设计目标是资源共享，所以网络是计算机病毒滋生的理想家园，随着 Internet 的发展，大大地加速了病毒的传播速度。

1.1.2 计算机网络安全的基本需求

面对计算机网络面临的威胁，人们对计算机网络中的数据安全提出了以下安全需求：

(1)数据的机密性。首先人们意识到的是信息保密。在传统信息环境中，普通人通过邮政系统发送信件，为了个人隐私还要装上信封。可是到了使用数字化信息的今天，以明文的形成在网上传来传去，连个“信封”都没有，我们发的电子邮件都是“明信片”，那还有什么秘密可言，因此，就提出了信息安全中数据机密性的需求。

数据机密性是指数据不被未授权者获取，机密性可以保护被传输的数据免受如图 1-1 所示的截获攻击。

(2)数据的完整性。针对在网络环境中如何防止信息被黑客篡改或者说信息被移花接木后怎样才可以被察觉，人们提出了网络中数据完整性的需求。

数据的完整性是指保证真实的数据从发送方到达接收方。在经过网络传输后的数据，必须与传输前的内容与形式完全一样，其目的就是保证信息系统上的数据处于一种完整和未受损的状态，数据在传输的过程不会被有意或无意的事件所改变、破坏和丢失。系统需要一种方法来确认数据在此过程中没有被改变。

(3)数据的可用性。数据的可用性是授权者可以随时使用信息的服务特性，即攻击者不能占用资源而阻碍授权者的工作。由于互联网是开放性网络，需要时就可以得到所需要的数据，这是网络设计和发展的基本目标，因此数据的可用性要求系统当用户需要时能够存取所需要的数据，或者说能够得到系统提供的服务。前面介绍的拒绝服务、网络环境下拒绝服务、缓冲区溢出、病毒等都属于对数据可用性的攻击。

(4)不可抵赖和不可否认。是指用户不能抵赖自己曾做出的行为，也不能否认曾经接到对方的信息，这在网络交易系统如电子商务中十分重要。

1.1.3 主要的网络安全技术

(1)网络安全的基石——密码技术。构建网络安全的体系结构离不开密码技术，没有密码技术的支撑，网络安全无从谈起。密码理论是网络安全的重要基石，是保护网络信息安全的核心与关键技术，随着通信和计算机技术发展起来的现代密码学，不仅在解决信息的机密性，而且在解决信息的完整性、可用性和抗抵赖性方面发挥着不可替代的作用。本书在第 2 章将介绍密码学中的加密、鉴别和数字签名等基本理论。

数据加密可以用来实现数据的机密性，使得加密后的数据能够保证在传输、使用和转换过程中不被第三方非法获取。数据经过加密变换后，将明文转换成密文，只有经过授权的合法用户，使用与发送方共享的密钥通过解密算法才能将密文还原成明文。反之，未经授权的用户因不掌握密钥，无法获得原文的信息。数据加密可以说是许多安全措施的基本保证。

对于数据的完整性，可以采用鉴别技术来实现，鉴别技术也是密码学的主要应用领域之一。为了防止数据在传输过程中被非法篡改、删除、产生，只需在通信介质两端进行密码学鉴别。鉴别技术就像明查秋毫的大法官，通过对鉴别算法产生的消息鉴别码的比对，立刻就能发现接收到的数据是否被作过手脚，常用的鉴别算法有 MD5、SHA 等。

对于通信中的抵赖行为，在密码学中可以采用“数字签名”来解决。数字签名的目的

是使发送方把签了名的消息发送给接收方以后，便不能否认其签名的消息；而接收方能够验证发送方的签名，但不能伪造。数字签名的作用类似于传统的手写签名，一旦双方就消息的内容和消息的来源发生了争执，应能向仲裁者提供出有效的证据，证明是一方抵赖还是另一方诬告。

除此以外，密码学的应用还涉及身份认证，空调管理等多个方面。

(2)网络安全协议。通过前面的介绍可知采用密码技术可以提供数据的机密性、完整性、抗抵赖等安全服务，那么这些安全服务如何在网络中系统地实施呢？OSI 参考模型是用 7 层概念功能层的方法来描述网络的结构，但因特网体系结构 TCP/IP 只用了 4 层，TCP/IP 本身并没有考虑网络的安全问题，于是人们提出了若干网络安全协议试图在 TCP/IP 的各个层面上来解决其安全问题，比如 SSL(Secure Socket Layer)、IPSec、SET 协议等，用户在具体安全方案的实施中，可以根据实际的安全需求很方便地在操作系统和路由器中进行安全协议的配置，网络安全协议其实很大程度上是密码学在网络中的实际应用。

(3)防火墙技术。防火墙是插在内部网与不安全的外部网络之间的一个隔离层，它通过建立受控的连接来形成一道安全的屏障，它隔离内部网与外部网，使内部网有选择地与外部网进行信息交换，阻止外界对内部资源的非法访问。防火墙增强了内部网络的安全性，用户可以安全地使用网络，更好地利用网络的资源。比较常用的防火墙有：包过滤防火墙、代理服务器(也叫应用级网关)、电路级网关、规则检测防火墙等。

防火墙也有自身的限制，这些缺陷包括：

①定义数据包过滤器会比较复杂，并且随着过滤器数目的增加，路由器的吞吐量会下降，因此防火墙可能会是潜在的瓶颈。

②防火墙无法阻止某些可以绕过防火墙的攻击。

③防火墙无法阻止来自内部的威胁。

因此，防火墙不能解决所有的安全问题，防火墙只是整个安全策略的一部分。

(4)入侵检测。入侵检测是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力(包括安全审计、监视、进攻识别和响应)，提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，了解网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

(5)网络病毒防护。面对病毒的猖獗，需要建立起有效的技术措施，能从病毒传染的各种可能途径入手，不受病毒种类和变形的限制，能够防、杀结合，甚至能够安全运行受病毒感染的程序，保证网络系统的有效、正常运行。

(6)PKI。PKI 是 Public Key Infrastructure 的缩写，即“公开密钥基础设施”，是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。

完整的 PKI 系统必须具有权威认证机关(CA)、数字证书库、密钥备份及恢复系统、证书作废系统、应用接口等基本构成部分，构建 PKI 也将围绕着这五大系统来着手构建。PKI 技术可运用于众多领域，其中包括：虚拟专用网络(VPN)、安全电子邮件、Web 交互

安全及倍受瞩目的电子商务安全领域，基于网络环境下数据加密/签名的应用将越来越广泛，PKI作为技术基础可以很好地实现通行于网络的统一标准的身份认证，其中既包含有线网络，也涵盖了无线通信领域。可以预见，PKI的应用前景将无比广阔。

(7)虚拟专用网(VPN)技术。虚拟专用网是一种在公用网络中实现专用网络功能的技术。在VPN中，任意两个节点之间的连接并无专用网所需的物理链路，而是利用公众网的资源动态组成。这种公众网可以是ATM、帧中继网、IP网，从而形成逻辑上的专用网络。目前，因特网已成为全球最大的网络基础设施，几乎延伸到世界的各个角落，于是基于因特网的VPN技术越来越受到广泛关注。

1.2 网络安全编程简介

1.2.1 借助开发工具实现网络安全编程

网络安全本身理论性和实践性都很强，掌握了网络安全相关基本概念、基本原理后可以运用到实际的工程中，在实际应用中，需要针对实际应用环境开发一些特定应用程序以提供相应的安全服务，而这时掌握一些实用的网络安全编程工具就显得犹为重要。

什么是网络安全开发包呢？网络安全开发包是指用于网络安全研究和开发的一些专业编程接口或开发包，它的主要作用是提供用于网络安全研究和开发的基本功能的实现，为研究者和开发者进一步研究和开发网络安全提供编程接口，为网络安全服务的实现提供方便。

一般一种网络安全开发包是针对特定的网络安全服务而开发的，它可以提供某一种或多种网络安全服务。网络安全开发包都经过很多网络安全研究和开发者的长期研究而成，通过不断测试和使用而逐渐成熟，并在实际的应用中得到推广。

某些网络安全开发包基本上已经实现了某个特定网络安全服务的基本框架和基本功能，然后开发者可以在这个已经构造好的基本框架下进行进一步的开发，这样就为开发者节省了时间和精力，为进一步开发功能更强大的系统提供方便。

1.2.2 几种常见网络安全开发包

网络安全开发包的种类很多，其实现的功能也千差万别，下面介绍一些常见的网络安全开发包：

(1)CryptoAPI：CryptoAPI是提供开发者在Windows下使用PKI的编程接口。CryptoAPI提供了很多函数，包括编码、解码、加密、解密、哈希计算、证书管理等功能。CryptoAPI在安全通信中应用十分广泛。

(2)OpenSSL：OpenSSL是用于安全通信著名的开放库，也是一个开放源代码SSL协议的产品实现，它采用C语言作为开发语言，OpenSSL提供了建立在普通通信层基础上的加密传输层，这些功能为许多网络应用和服务程序所广泛使用。

它的密码算法库是一个强大完整的密码算法库，它是OpenSSL的基础部分，也是很值得一般密码安全技术人员研究的部分，它实现了目前大部分主流的密码算法和标准。主要包括公开密钥算法、对称加密算法、散列函数算法、X.509数字证书标准、PKCS12、

PKCS7 等标准。OpenSSL 具备的应用程序，既能直接使用，也可以方便进行二次开发。

以上这两种网络安全开发包的运用是本书的介绍重点，它们主要提供保证数据的机密性、完整性、不可否认性以及身份鉴别的功能。

除了上面介绍的，在实际应用中还会使用到以下的网络安全开发包：

(1)Crypto++：Crypto++是采用标准 C++编写而成，也是一个自由软件，Crypto++实现了多种公开密钥算法、对称加密算法、数字签名算法、信息摘要算法以及其它相关的算法等。Crypto++于 1995 年 6 月发布了 1.0 版本，目前最新的版本是 Crypto++™ Library 5.5，可以适应各种常用的操作系统和编译平台，更多信息可参考网站 http://www.cryptopp.com。

(2)Cryptix：如果从事 Java 开发程序，还可以选择 Cryptix，它是 Sun 公司发布的采用 Java 语言的关于 Java Cryptography Extension (JCE)的开放源码的 API 实现。

(3)网络数据包捕获开发包 Libpcap 和 WinPCap：网络数据包捕获开发包 Libpcap 是一个专门用来捕获网络数据的编程接口，它提供了以下的各项功能：捕获原始数据包，包括在共享网络上各主机发送和接收数据包；在数据包发往应用程序之前，按照自定义的规则将某些特殊的数据包过滤掉；在网络上发送原始的数据包；收集网络通信过程中的统计信息。由于网络数据包捕获功能是很多安全系统都要实现的功能，所以 Libpcap 可应用到网络嗅探器、网络协议分析、网络入侵检测、安全扫描等网络安全系统中。

WinPCap (windows packet capture)是 Libpcap 在 windows 平台下的版本。

(4)网络入侵检测开发包 Libnids：Libnids(Library Network Intrusion Detection System)是一个用于网络入侵检测系统设计的专业开发包，提供了一个网络入侵检测系统的基本框架和基本功能，可以快速实现网络入侵检测的基本功能。

1.2.3 如何使用网络安全开发包

网络安全开发包归根结底是一些函数库，它们采用了一些特定的数据结构，提供了编程接口。使用网络安全开发包就是要掌握怎样使用这些数据结构和函数。总的说来，借助网络安全开发包进行网络安全软件与系统开发，应从以下几方面入手：

(1)掌握网络安全的基本概念、基本原理。要着手进行网络安全编程，应首先对网络安全相关概念和原理进行全面的了解，如密码学基本知识，具体包括对称密码算法、公钥密码算法、鉴别技术和数字签名的原理与应用，此外，还包括黑客攻击与防御、网络安全协议、防火墙、入侵检测技术等网络安全技术，正因为如此，在本书的第 2 章针对以上部分内容进行了简要的讲解。

(2)掌握网络安全开发包的数据结构。每种网络安全开发包都使用了很多数据结构，这些数据结构在编程中都要使用到，它们是信息的载体。特别是一些典型的数据结构，他们基本上描述了开发工具的一些核心内容，掌握它们对于理解和掌握网络安全开发包是非常重要的。

(3)网络安全开发包的输出函数。网络安全开发包的输出函数是一个提供给用户的编程接口，它是开发者直接打交道的对象，也是开发者最终要掌握的对象。使用网络安全开发包归根结底是调用网络安全开发包提供的输出函数，所以掌握输出函数是最重要的，也是了解网络安全开发包的目的所在。要掌握网络开发工具的输出函数，必须从函数的返回值、函数的参数描述和函数的功能这三方面了解。

本章小结

本章对网络安全进行了总体介绍。首先介绍了网络安全问题的由来、网络面临的主要威胁，针对这些安全威胁提出了网络安全的基本需求，然后介绍了目前现有的一些主要的网络安全技术。

在网络安全编程方面介绍了当前几种常用的网络安全开发包，以及运用这些网络安全开发包的基本方法。

复习思考题

1. 简述网络安全问题的由来。
2. 如何提供数据的机密性、完整性？
3. 简述密码学与网络安全的关系。
4. 有哪些常用的网络安全开发包？要运用这些网络安全开发包应从哪几方面入手？

第2章　网络安全基础

2.1　密码学基本概念

2.1.1　密码学的历史与发展

在战争期间，如果通信联络人员被敌方俘虏，密件中的情报如果泄露出去后果将不堪设想，这使人们自然而然产生了“秘密书写”的念头，我们可以将不愿意被无关的第三方所知道的内容用某种方法变换一下，使变换后的内容仅仅被有关人员所理解，而在其他人眼里，这些东西则好像杂乱无章的“天书”一般。早在4000多年前，古埃及人就在墓志铭中使用过类似象形文字的奇妙符号，这是史载最早的密码形式。公元前约50年，罗马皇帝朱利叶斯·凯撒(Julius Casesar)发明了一种用于战时秘密通信的方法，后来被称为“凯撒”密码。

千百年来，人们运用自己的智慧创造出形形色色编写密码的方法，由于军事、外交、情报等方面的需要，不断刺激密码学的发展。密码编写得好与坏，有时会产生重大的、甚至决定性的影响。例如，第二次世界大战期间，英国情报部门在波兰人的帮助下，于1940年破译了德国自认为可靠的Enigma(图2-1)三转轮密码机密码系统，使德方遭受重大损失。当时，一大批优秀的密码专家和学者都卷入了密码学的研究工作，这些努力后来证明对战争的进程均产生了重大的影响，也极大地促进了密码学的发展。

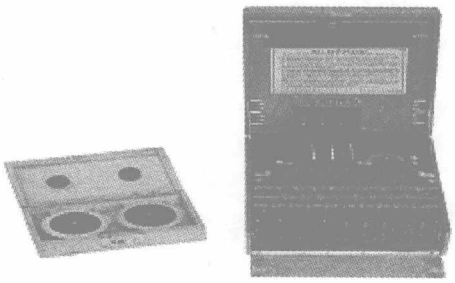

图2-1　Enigma密码机

早期的密码多数应用于军事、外交、情报等敏感的领域。因为其本质决定了它不同于一般的科学。由于国家利益等安全因素，密码学的研究往往不能够公开，至少不能完全公开，所以，公开发表的有关文献和资料总是不能反映出当时密码学发展的真正水平。但是，自20世纪70年代以来，在计算机网络技术迅速发展的大背景下，公开发表的密码学研究成果急剧增加，密码学研究的这种“秘密”本质发生了重大变化。

历史的车轮滚滚向前，密码学紧跟科学技术前进的步伐，经历了如下发展历程：从密码学初级形式的手工阶段，经过中级形式的机械阶段，发展到今天高级形式的电子与计算机阶段。计算机的出现大大促进了密码学的变革，正如德国学者T. Beth所说：“突然，现代密码学从半军事化的角落里解脱出来，一跃成为通信科学领域中的中心研究课题。”

由于商业应用和大量计算机网络通信的需要，民间对数据保护、数据传输的安全性，