普通高等教育“十一五”国家级规划教材

高等学校信息安全系列教材

网络安全通信协议

陈性元　杨　艳　任志宇　编著
冯登国　审

高等教育出版社
Higher Education Press

普通高等教育“十一五”国家级规划教材
高等学校信息安全系列教材

网络安全通信协议

陈性元　杨　艳　任志宇　编著
冯登国　审

高等教育出版社
Higher Education Press

内容提要

本书是普通高等教育“十一五”国家级规划教材。本书是作者结合多年来对该课程的教学经验以及从事网络安全理论研究、产品开发及工程实践的体会编写的，从协议原理、安全性分析以及协议应用等方面，较为系统地介绍了 TCP/IP 协议簇各协议层的常用经典网络安全通信协议。

全书共分 6 大部分，共 10 章。第一部分包括第一章和第二章，介绍安全通信协议的基本概念、TCP/IP 协议簇的安全性问题及安全架构。第二部分包括第三章，讨论链路层安全通信协议 PPTP 和 L2TP。第三部分包括第四章，讨论网络层安全通信协议 IPsec 协议。第四部分包括第五章，讨论传输层安全通信协议 SSL 和 TLS。第五部分包括第六、七、八、九章，介绍 PGP、S/MIME、SET、SNMP、S-HTTP 等应用层安全协议。第六部分包括第十章，讨论安全协议的安全性分析方法，并给出 IPsec 协议的分析实例。

本书不仅可作为信息安全、计算机科学与技术、密码学等专业本科高年级信息安全相关的教材，也可作为其他专业本科生和研究生的教学参考书，还可作为从事信息安全研究的工程技术人员的实用工具书。

图书在版编目(CIP)数据

网络安全通信协议/陈性元，杨艳，任志宇编著. —北京：高等教育出版社，2008.3

ISBN 978-7-04-023122-9

Ⅰ.网… Ⅱ.①陈…②杨…③任… Ⅲ.计算机网络-安全技术-通信协议 Ⅳ.TN915.04

中国版本图书馆 CIP 数据核字(2008)第 015170 号

策划编辑	武林晓	**责任编辑**	萧 潇	**封面设计**	于文燕	**责任绘图**	尹 莉
版式设计	张 岚	**责任校对**	王 超	**责任印制**	毛斯璐		

出版发行	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街 4 号	**免费咨询**	800-810-0598
邮政编码	100011	**网 址**	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	北京北苑印刷有限责任公司	**畅想教育**	http://www.widedu.com
开 本	787×1092 1/16	**版 次**	2008 年 3 月第 1 版
印 张	19	**印 次**	2008 年 3 月第 1 次印刷
字 数	420 000	**定 价**	24.00 元

物料号 23122-00

引　言

随着全球信息化进程的不断推进，网络安全问题已经成为信息安全领域探讨和研究的热点问题。在网络和分布计算环境中，通信协议起着至关重要的作用，而网络安全通信协议主要是指实现某种安全目的的通信协议，与密码技术一样，现在已经成为解决网络安全问题的基础和关键。作为计算机专业的学生，学习网络安全通信协议是了解当前计算机发展必不可少的部分，而对于信息安全专业的学生来说，更是必须掌握的基本内容。

目前关于网络安全通信协议的著作，大部分是从密码学的角度来介绍，侧重于协议的分析，缺乏对网络安全通信协议系统全面的介绍。本书作者多年从事网络安全的理论研究及工程实践，从协议原理、安全性分析以及协议应用等方面，较为系统地介绍了 TCP/IP 协议簇的安全架构以及各协议层的常用经典安全通信协议，并进行了相关协议的分析比较。

全书由陈性元主持编写，其中第一、二、四、十章由陈性元编写，第六、七、八、九章由杨艳编写，第三、五章由任志宇编写，由陈性元统稿。

本书的体系结构相对比较灵活，不同层次的协议相对比较独立，而且每一层次介绍了几个安全通信协议，在教学中可以根据不同专业、不同层次的教学大纲要求，选用不同章节，适当取舍后仍能形成连贯、相对完整的教材。书中章节或标题前加星号“*”的内容，可供研究生、从事信息安全研究和开发的工程技术人员学习参考，对于本科生可不作要求。

本书不仅可作为信息安全、计算机科学与技术、密码学等专业本科高年级信息安全相关课程的教材，也可作为其他专业本科生和研究生的教学参考书，还可作为从事信息安全研究的工程技术人员的实用工具书。

国家信息安全重点实验室冯登国教授仔细审阅了全书，并提出了宝贵的意见，在此表示衷心的感谢。本书的编写得到了解放军信息工程大学电子技术学院重点课程建设经费的资助，还得到了解放军信息工程大学电子技术学院信息安全系的大力支持和帮助，得到了吴蓓、祝宁、曹利锋、钱雁斌和张明等同志的帮助，在此一并表示感谢。

由于作者水平有限，加之时间仓促，书中难免存在不妥之处，请读者和同行不吝指正。作者联系方式为 chxy302@ vip. sina. com。

作　者

2007 年 12 月于郑州

目　录

第一部分　绪　论

第一章　安全协议概述 …… 3
1.1　网络安全与安全协议 …… 3
1.1.1　网络安全内涵 …… 3
1.1.2　密码和安全协议 …… 4
1.2　安全协议的概念与分类 …… 4
1.2.1　安全协议的概念 …… 4
1.2.2　安全协议的分类 …… 5
1.3　安全协议的安全性质 …… 6
1.4　安全协议的设计 …… 8
1.4.1　安全协议的缺陷分类 …… 8
1.4.2　安全协议的设计原则 …… 9
习题一 …… 12

第二章　TCP/IP 协议簇的安全架构 … 13
2.1　TCP/IP 协议簇概述 …… 13
2.1.1　TCP/IP 协议簇协议分层 …… 13
2.1.2　TCP/IP 协议簇基本功能保证协议 …… 15
2.1.3　通信协议中帧的复用和分用 …… 18
2.2　TCP/IP 协议簇的安全性分析 … 19
2.2.1　TCP/IP 协议簇协议存在的安全隐患 …… 20
2.2.2　针对 TCP/IP 协议簇协议的典型攻击 …… 24
2.3　TCP/IP 协议簇的安全架构 …… 30
习题二 …… 32

第二部分　链路层安全通信协议

第三章　PPTP 和 L2TP 协议 …… 35
3.1　概述 …… 35
3.2　PPP 协议 …… 35
3.2.1　PPP 协议基本原理 …… 35
3.2.2　PPP 协议中的安全机制 …… 37
3.3　PPTP 协议 …… 39
3.3.1　PPTP 协议综述 …… 39
3.3.2　PPTP 协议工作流程 …… 42
3.3.3　PPTP 分组的封装 …… 43
3.3.4　控制消息的格式和类型 …… 45
3.3.5　控制连接 …… 46
3.3.6　呼叫 …… 52
3.3.7　PPTP 协议中的流量控制 …… 60
3.4　L2TP 协议 …… 61
3.4.1　L2TP 协议综述 …… 61
3.4.2　L2TP 协议工作流程 …… 63
3.4.3　L2TP 协议消息 …… 64
3.4.4　控制连接 …… 72
3.4.5　L2TP 呼叫 …… 74
*3.4.6　L2TP 的有限状态模型 …… 75
3.5　PPTP 协议和 L2TP 协议分析 …… 77
3.5.1　PPTP 协议分析 …… 77
3.5.2　L2TP 协议分析 …… 77
习题三 …… 78

第三部分 网络层安全通信协议

第四章 IPsec 协议簇 …… 83
4.1 概述 …… 83
4.1.1 IPsec 的产生背景 …… 83
4.1.2 IPsec 发展概述 …… 83
4.1.3 IPsec 的设计目标及功能 …… 84
4.1.4 IPsec 的体系结构 …… 84
4.1.5 IPsec 实现方式 …… 85
4.1.6 IPsec 工作模式 …… 86
4.1.7 安全关联 …… 87
4.2 AH 协议 …… 90
4.2.1 设计 AH 的目的 …… 90
4.2.2 AH 头格式 …… 90
4.2.3 AH 操作模式 …… 91
4.2.4 AH 的处理过程 …… 92
4.3 ESP 协议 …… 94
4.3.1 设计 ESP 的目的 …… 94
4.3.2 ESP 包格式 …… 94
4.3.3 ESP 操作模式 …… 95
4.3.4 ESP 的处理过程 …… 96
4.4 IKE 协议 …… 98
4.4.1 IKE 概述 …… 98
4.4.2 阶段 1 交换 …… 100
4.4.3 阶段 2 交换 …… 106
*4.5 IPsec 若干问题 …… 108
4.5.1 IPsec 的更小子集 …… 108
4.5.2 IPsec 与 NAT 的协同 …… 108
4.5.3 IPsec 与 L2TP 的结合 …… 109
4.5.4 IPsec 在支持 VPN 方面的缺陷 …… 110
习题四 …… 111

第四部分 传输层安全通信协议

第五章 SSL 协议和 TLS 协议 …… 115
5.1 概述 …… 115
5.2 SSL 协议规范 …… 116
5.2.1 协议综述 …… 116
5.2.2 握手协议 …… 117
5.2.3 更改密码规格协议 …… 123
5.2.4 警告协议 …… 123
5.2.5 SSL 记录协议 …… 124
5.2.6 SSL 协议中采用的加密和认证算法 …… 126
5.3 TLS 协议规范 …… 127
5.3.1 协议综述 …… 127
5.3.2 TLS 中的改进部分 …… 128
5.4 TLS/SSL 的应用 …… 133
5.4.1 TLS/SSL 与电子商务 …… 133
*5.4.2 利用 TLS/SSL 保证 HTTP 的安全性 …… 134
5.5 安全性分析 …… 138
习题五 …… 141

第五部分 应用层安全通信协议

第六章 电子邮件安全协议 …… 145
6.1 电子邮件安全概述 …… 145
6.1.1 电子邮件的安全需求 …… 145
6.1.2 安全电子邮件标准 …… 145
6.2 电子邮件基本原理 …… 146
6.2.1 电子邮件的传输机制 …… 146
6.2.2 电子邮件中的基本协议及标准 …… 148
6.2.3 MIME …… 150
6.3 PGP …… 156
6.3.1 PGP 概述 …… 156
6.3.2 PGP 提供的安全服务 …… 158

6.3.3 PGP 消息格式及收发过程 …… 163
6.3.4 PGP 的密钥管理 …… 165
6.3.5 PGP/MIME 与 OpenPGP …… 171
6.4 S/MIME …… 176
6.4.1 S/MIME 概述 …… 176
6.4.2 S/MIME 的安全功能 …… 177
6.4.3 S/MIME 的消息 …… 179
*6.4.4 S/MIME 证书的处理 …… 186
*6.4.5 增强的安全服务 …… 186
6.5 PGP 与 S/MIME 的比较 …… 187
6.5.1 实现原理 …… 187
6.5.2 应用前景 …… 188
习题六 …… 189
第七章 SET 协议 …… 190
7.1 电子商务安全概述 …… 190
7.1.1 电子商务概述 …… 190
7.1.2 电子商务的安全需求 …… 191
7.1.3 电子商务安全协议 …… 192
7.2 SET 协议简介 …… 193
7.2.1 SET 概述 …… 193
7.2.2 SET 的安全机制 …… 195
7.2.3 SET 的支付过程 …… 198
7.2.4 SET 的认证 …… 203
7.2.5 SET 的优点与存在问题 …… 207
*7.2.6 SET 的安全性分析 …… 208
7.3 SET 与 SSL 的比较及 SET 的推广前景 …… 211
7.3.1 SET 与 SSL 的比较 …… 211
7.3.2 SET 的推广前景 …… 211
习题七 …… 212
第八章 SNMP 协议 …… 213
8.1 SNMP 概述 …… 213
8.1.1 SNMP 产生及发展 …… 213
8.1.2 SNMP 网络管理模型 …… 215
*8.1.3 SNMP 协议体系 …… 217
8.1.4 SNMP 的安全问题 …… 220
8.2 SNMPv3 …… 222
8.2.1 SNMPv3 体系结构 …… 223
8.2.2 SNMPv3 的消息 …… 227
8.2.3 SNMPv3 的安全机制 …… 229
8.3 SNMPv3 安全性分析与应用情况 …… 236
8.3.1 SNMPv3 安全机制分析 …… 236
8.3.2 SNMPv3 的应用情况 …… 237
习题八 …… 238
第九章 S-HTTP 协议 …… 240
9.1 概述 …… 240
9.2 HTTP 基本原理 …… 241
9.2.1 HTTP 通信方式 …… 241
9.2.2 HTTP 报文结构 …… 242
9.2.3 HTTP 的安全机制 …… 247
9.3 S-HTTP …… 248
9.3.1 S-HTTP 概述 …… 248
9.3.2 S-HTTP 的安全模式 …… 249
9.3.3 S-HTTP 的消息 …… 251
*9.3.4 其他问题 …… 257
9.4 S-HTTP 与 HTTPS 的比较 …… 257
习题九 …… 258

第六部分 安全协议安全性分析

第十章 安全协议安全性分析 …… 261
10.1 概述 …… 261
10.1.1 安全协议的安全性与安全性分析 …… 261
10.1.2 安全协议安全性分析的基本方法 …… 261
10.2 形式化分析 …… 262
10.2.1 形式化分析前提 …… 262
10.2.2 形式化分析基本方法 …… 263
10.2.3 BAN 逻辑及 BAN 类逻辑 …… 264

*10.2.4 SADL …… 269
10.3 IPsec 协议簇安全性分析实例 …… 274
10.3.1 IPsec 协议簇安全性分析的目的与意义 …… 275
10.3.2 AH 协议和 ESP 协议的安全性分析 …… 276
10.3.3 IKE 协议安全性分析 …… 281
10.3.4 IPsec 安全性分析小结 …… 291
习题十 …… 291
参考文献 …… 292

第一部分　绪　　论

网络安全通信协议属于安全协议，主要是将密码技术应用到网络通信中，以实现某种安全功能。与密码技术一样，网络安全通信协议已经成为解决网络安全问题的基础和关键。第一章讨论安全协议在网络安全中的重要性及安全协议的概念、分类、安全性质及安全缺陷等。第二章首先讨论 TCP/IP 存在的安全隐患及面临的攻击，描述 TCP/IP 协议簇的安全架构，并简单介绍各层提供的安全通信协议的特点，本书各章的内容也是按照各安全通信协议在 TCP/IP 中的不同层次来进行安排的。

第一章　安全协议概述

1.1　网络安全与安全协议

1.1.1　网络安全内涵

随着计算机网络的开放性、共享性和互连程度的增强，特别是现代网络技术和 Internet 的飞速发展，以及全球信息化、网络化进程的不断推进，在 Internet 及其他网络上运行的应用和提供的服务越来越多，所以网络的安全问题也变得越来越突出。网络安全问题已成为关乎国家安全、军队存亡、战争胜败的重要问题。

网络安全，其实质就是指网络信息系统的安全，网络安全问题是现代信息安全所要研究和解决的主要问题，也是近几年信息安全领域探讨和研究的热点问题。随着计算机网络的发展，网络安全的概念也在不断发展。

在大型计算机主宰的时代，科学计算是最为主要的应用实例。网络连接的目的是共享计算资源，其远程终端和本地主机的连接属于“机器－机器”类型的通信。当时人们需要保护的是设在专用机房内的主机以及数据的安全属性，因此这个时期的信息安全是面向单机、面向数据的。

20 世纪 80 年代，随着个人计算机、局域网的出现和发展，以及数据库技术的推广应用，网络应用的目的开始由资源共享走向信息共享，信息系统的体系结构以客户－服务器（client/server）结构为主，网络通信属于“人－机器”的通信类型，这时的安全需求是需要提供对系统用户身份的认证、授权与访问控制。另外，当时的通信协议依据功能和过程的分工划分，成为层次形式的协议，传输层协议至少具有连接管理、差错控制和流量控制等协议机制，保证数据的准确和顺序，因此，对网络的安全保护开始着手从协议考虑，因此，这个时期的信息安全是面向协议、面向用户的。

20 世纪 90 年代，随着互联网的普及和发展，高性能多媒体计算机和基于光纤传输的高速网络把网络应用带入一个飞速发展的新阶段。在传统的资源共享和信息共享的基础上，出现了面向知识共享的新型网络应用，“人－人”的通信是其最为显著的特征，其中具有代表性的就是协同计算、网络会议系统和网络即时通信。不可否认性、可服务性以及基于内容的个人隐私、网络环境的知识产权保护等面向用户的安全需求，在知识共享时期变得更加突出；随着信息化进程的不断推进，系统的可生存、可恢复、可再生等高可用性要求和可控性要求越来越迫切，因此，这个时期的信息安全为面向数据、面向用户的安全属性赋予了新的内涵，同时更加强调面向系统的安

全属性。

所以,可以从面向数据、面向用户和面向系统等方面理解信息安全。

- 面向数据的安全概念:保护信息的机密性、完整性、可用性和可控性。
- 面向用户的安全概念:实现对实体的认证、授权、访问控制、不可否认性和可服务性以及基于内容的个人隐私、知识产权保护等。
- 面向系统的安全概念:保证信息系统的可用性、可控性、可恢复性、可再生性、可生存性。

面向数据与面向用户网络安全概念的结合就是网络安全体系结构中的安全服务,而这些安全服务又要依靠加密、数字签名、访问控制、数据完整性、安全审计、灾难恢复、病毒防护、防黑客入侵等安全机制和措施加以实现。从历史的、人网大系统的概念出发,现代的信息安全涉及个人权益、企业生存、金融风险防范、社会稳定和国家的安全。它是物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全以及公共、国家信息安全的总和。

1.1.2 密码和安全协议

网络安全研究的对象是计算机网络,计算机网络以通信为手段来达到资源共享的目的,而只有依靠协议才能实现通信。因此,在网络环境和分布计算环境中,通信协议起着至关重要的作用。

安全协议又称为密码协议、安全通信协议,是实现信息安全交换和某种安全目的的通信协议。用于计算机网络的安全协议又称为网络安全通信协议,是网络安全体系结构中的核心问题之一。它是将密码技术应用于网络安全系统的纽带,是确保网络信息系统安全的关键。

安全协议是否存在安全漏洞即是否完备成为它能否提供网络安全保障的关键,安全协议的安全性不仅依赖于所采用的密码算法强度,而且与算法的应用环境(通信行为的规则和格式)密切相关。一个不安全的安全协议可以使入侵者不用攻破密码而得到信息或产生假冒。

因此,"密码和安全协议是网络安全的核心"已成为网络及信息安全界的共识。研究网络安全通信协议及其完备性是网络安全这个问题的关键所在。采用各种技术手段或方法设计安全协议并分析其安全性已是人们研究的重要课题之一。

1.2 安全协议的概念与分类

1.2.1 安全协议的概念

首先来考察一下协议、通信协议、安全协议的概念。

1. 协议

所谓协议,是指两个或两个以上参与者为完成某项特定的任务而采取的一系列步骤。它有

3 个要点:一是至少两个以上参与者;二是目的明确;三是按照约定的规则有序地执行一系列步骤。

2. 通信协议

所谓通信协议,是指通信各方关于通信如何进行所达成的一致性规则,即由参与通信的各方按确定的步骤做出一系列的通信动作完成的。换句话说,通信协议是定义通信实体之间交换信息的格式及意义的一组规则。

3. 安全协议

所谓安全协议,是指通过信息的安全交换来实现某种安全目的所共同约定的逻辑操作规则。换句话说,安全协议是指通过信息的安全交换来实现某种安全目的的协议。简单地说,安全协议就是指实现某种安全目的的通信协议,所以又称为安全通信协议。由于安全协议通常要用到密码技术,所以又称为密码协议。

4. 网络安全通信协议

网络安全通信协议属于安全协议,是指在计算机网络中使用的具有安全性功能的通信协议,也就是说,通过正确地使用密码技术和访问控制技术来解决网络中信息的安全交换问题。

根据安全协议的概念,安全协议除了具有协议和通信协议的基本特点外,还应包含以下基本要素:

① 保证信息交换的安全,目的是完成某种安全任务。安全协议就是为了完成某种安全任务而必须保证进行的信息交换(通信)的安全。

② 使用密码技术。密码技术是安全协议保证通信安全所采用的核心技术,例如信息交换的机密性、完整性、不可否认性等均要依赖密码技术。

③ 具有严密的共同约定的逻辑交换规则。保证信息安全交换除了采用密码技术以外,逻辑交换规则是否严密,即协议的安全交换过程是否严密都十分重要,安全协议的分析往往是针对这一部分而进行的。

④ 使用访问控制等安全机制。必要时还应使用访问控制等安全机制,IPsec 协议簇在进行安全通信时就特别强调这一点。事实上,在其他安全协议中,当解密失败或完整性检验无法通过时,通常都会丢弃(discard)报文,这就是最基本的访问控制。

1.2.2　安全协议的分类

对于安全协议进行严格的分类是件很难的事情,从不同的角度出发,就会有不同的分类方法。目前普遍认为按照安全协议的功能分类较为合理,将安全协议分为密钥建立协议、认证建立协议以及认证的密钥建立协议等 3 类。一些文献对这一分类方法提出了改进意见,建议分为身份认证协议、密钥建立协议、非否认协议等 3 类。

根据安全协议的功能分类无疑较为合理,也容易被人们所接受。但上述分类中没有考虑信息安全交换,所以,笔者认为可以将安全协议进行如下分类。

(1) 认证协议

主要实现认证功能,包括消息认证、数据源认证和实体认证(身份认证)。

(2) 密钥管理协议

主要实现建立共享密钥的功能。可以通过密钥分配来建立共享密钥,这也是目前密钥管理的主要方法,也可以通过密钥交换来共享密钥,如 IKE。包括密钥分配、密钥交换等密钥管理协议。

(3) 不可否认协议

主要通过协议的执行,达到不可否认的目的。包括发方不可否认协议、收方不可否认协议、数字签名协议等。

(4) 信息安全交换协议

实现信息的安全交换功能。例如 IPsec 协议簇除了 Internet 密钥交换协议(The Internet key exchange,IKE)和 Internet 安全关联与密钥管理协议(Internet security association and key management protocol,ISAKMP)外,认证头(authentication header,AH)和封装安全载荷协议(encapsulation security payload protocol,ESP)就是典型的信息安全交换协议。

说明:信息安全交换过程中当然离不开密钥管理和数据源认证,但密钥管理协议和认证协议并不能代替信息安全交换协议。

1.3 安全协议的安全性质

安全协议的主要目的是保证通信中数据的机密性及完整性,同时还要保证通信主体身份的识别与认证,以及提供不可否认性等安全性质。安全协议的目标就是保证这些安全性质在协议执行完毕时能够得以实现,或者换言之,评估一个安全协议是否安全的方法就是检查其所欲达到的安全性质是否遭到攻击者的破坏。

一般通过协议消息的传递来达成通信主体身份的识别与认证,并在此基础上为下一步的秘密通信分配所使用的会话密钥,因此,对通信主体双方身份的认证是基础,是前提,而且在认证的过程中,对关键信息的秘密性及完整性的要求也是十分必要的。另外,作为与认证协议不同的另一类协议——电子商务协议,由于其自身的特点,也有一些特殊的性质要求。简单地说,安全协议的目标就是保证这些安全性质在协议执行完毕时能够得以实现。

1. 认证性

认证是最重要的安全性质之一,所有其他安全性质的实现都依赖于此性质的实现。认证是分布式系统中的主体进行身份识别的过程。认证可以对抗假冒攻击的危险,认证可以用来确保身份,并可用于获取对某人或者某物的信任。在协议中,当某一成员(声称者)提交一个主体身份并声称它是那个主体时,需要运用认证以确认其身份,或者声称者需拿出证明其真实身份的证据,这个过程称为认证的过程。在协议的实体认证中可以是单向的也可以是双向的。安全协议

的认证的实现是基于密码的，即如果声称者知道某一秘密，则验证者相信声称者所声称的身份。具体有以下几种方法。

① 声称者使用仅为声称者和验证者知道的密钥封装的一个消息，如果验证者能够成功地解密消息或验证封装是正确的，则声称者的身份得到证明。

② 声称者使用其私钥对消息签名，验证者使用声称者的公钥验证签名，如正确，则声称者的身份得到证明。

③ 声称者通过可信第三方来证明自己。

上述几种方法往往被综合使用以建立可靠的认证系统。在上述方法中所传递的消息中都应包含不可重复值以抵抗重放攻击。

2. 机密性

机密性的目的是保护协议消息不被泄露给非授权拥有此消息的人，即使是攻击者观测到了消息的格式，它也无法从中得到消息的内容或提炼出有用的消息。保证协议消息机密性最直接的办法是对消息进行加密。加密使得消息由明文变为密文，并且任何人在不拥有密钥的情况下是不能解密消息的。加密的体制分为对称加密体制和非对称加密体制，前者的密钥管理更为简单，后者的效率更高。在同一类密码体制中，不同的密码算法有不同的强度和代价。在安全协议中，一般不考虑具体的密码算法的执行细节，但在实际应用中这往往又可能造成协议机密性的缺陷。

3. 完整性

完整性的目的是保护协议消息不被非法篡改、删除和替代。最常用的方法是封装和签名，即用加密的办法或者散列函数产生一个明文的摘要附在传送的消息上，作为验证消息完整性的依据，称为完整性校验值(ICV)。一个关键性的问题是，通信双方必须实现达成有关算法的选择等诸项共识。如果被保护的消息存在一定的冗余，加密消息的冗余能保证消息的完整性效果。因为如果一个攻击者不知道加密密钥而修改了密文的一部分，则会导致在解密的过程中产生不正确的结果。

4. 不可否认性

不可否认性是电子商务安全协议的一个重要的性质。其目的在于通过通信主体提供对方参与协议交换的证据来保证其合法利益不受侵害，即协议主体必须对自己的合法行为负责，而不能也无法事后否认。电子交易通信过程的各个环节都必须是不可否认的，即交易一旦达成，发送方不能否认他发送的信息，接收方则不能否认他所收到的信息。不可否认协议的主体的目的在于收集证据，以便事后能够向可信仲裁证明对方主体的确发送或接收了消息。证据一般是以签名消息的形式出现的，从而将消息与消息的发送者进行了绑定。在认证和密钥分配协议中，主体双方的目标是一致的，如共享一个良好的会话密钥等。而在不可否认协议中，主体的目标各不相同，因而协议要考虑诚实主体通信之间可能存在的恶意攻击者。要达成不可否认这一目标，协议必须具有两个特点：证据的正确性和交易的公平性。

1.4 安全协议的设计

1.4.1 安全协议的缺陷分类

尽管协议设计者尽可能在协议设计时回避可能出现的人为错误,但是安全协议在实际应用时仍会出现各种类型的缺陷。产生缺陷的原因是十分复杂的,很难有一种通用的分类方法将安全协议的安全缺陷进行分类。大致来看,安全协议的缺陷从来源上可区分为两类:一类是由于设计时的不规范引发的,另一类是在具体执行时产生的。但是这样的分类太过笼统了,于是,S. Gritzalis 和 D. Spinellis 根据安全协议缺陷产生的原因和相应的攻击方法对安全协议进行了分类,共分为以下 6 类。

(1) 基本协议缺陷

基本协议缺陷是由于在安全协议的设计中没有或很少防范攻击者而引发的协议缺陷。例如,对加密的消息签名,由于签名者并不一定知道被加密的消息内容,而且签名者的公钥是公开的,从而可使攻击者通过用他自己的签名替换原来的签名来伪装成发送者。

(2) 并行会话缺陷

协议对并行会话攻击缺乏防范,从而导致攻击者通过交换适当的协议消息能够获得所需要的信息。包括并行会话单角色缺陷、并行会话多角色缺陷等。

(3) 口令/密钥猜测缺陷

这类缺陷产生的原因是用户往往从一些常用的词中选择其口令,从而导致攻击者能够进行口令猜测攻击;或者选取了不安全的伪随机数生成算法构造密钥,使攻击者能够恢复该密钥。口令猜测攻击可分为可检测的口令在线猜测攻击、不可检测的口令在线猜测攻击和可离线的口令猜测攻击 3 类。

(4) 陈旧消息缺陷

陈旧(stale)消息缺陷是指协议设计中对消息的新鲜性没有充分考虑,从而使攻击者能够进行消息重放攻击,包括消息源的攻击、消息目的的攻击等。根据消息的来源与去向,陈旧消息攻击可分为消息来源攻击和消息目的地攻击。

(5) 内部协议缺陷

协议的可达性存在问题,协议的参与者中至少有一方不能完成所有必需的动作而导致的缺陷。

(6) 密码系统缺陷

协议中使用的密码算法和密码协议导致协议不能完全满足所要求的机密性、认证等需求而产生的缺陷。

这种缺陷的分类方法是比较合理、全面的,因为它囊括了安全协议缺陷来源的 3 个主要方

面:安全协议本身的缺陷;协议需要依赖实施机制所产生的缺陷;协议具体实施时产生的缺陷。基本协议缺陷和并行会话缺陷属于协议本身的缺陷,即在假设协议所用到的密码算法及密码技术均是安全的前提下,协议仍旧存在的缺陷。口令/密钥猜测缺陷和陈旧消息缺陷属于协议需要依赖实施机制所产生的缺陷,因为这些缺陷的产生很大一部分都是依赖于实施采用的机制,也就是说,如果可以改善这些机制,那么就有可能避免这些缺陷。内部协议缺陷和密码系统缺陷属于具体实施时产生的缺陷,即在具体实施过程中会出错或者受到攻击。

1.4.2　安全协议的设计原则

安全协议的安全性,意味着非法用户不可能从协议中获得比协议自身所体现的更多的有用的信息,但是现有的许多协议在设计上普遍存在着某些安全缺陷,那么如何设计安全协议才能满足协议的安全性、有效性、完整性和公平性的要求呢? 这就需要在设计协议时遵守一些原则,下面则是根据上述对安全协议的缺陷分类而归纳的 6 类共 10 条设计原则。

1. 避免基本协议缺陷产生的原则

基本协议缺陷的产生通常是因为协议设计的时候没有遵循清晰性原则所造成的,这里所说的清晰性包括消息的清晰性和运行环境的清晰性。要保证消息的保密性、认证性、完整性和不可否认性,就需要尽量避免基本协议缺陷。

(1) 保证消息清晰性的原则

原则 1:每条消息应该是独立完整的。

这条原则说明每条消息都应该能够准确地表达出它所想表达的含义,一条消息的解释应完全由其内容来决定,而不必借助于上下文来推断。协议消息或者采用标准的形式化语言加以描述,或者采用非形式化的自然语言描述。例如,一个认证服务器 s 要发送一条消息,内容为:“在接收到位模式 P 之后,s 就给 A 发送一个密钥 K,用来给 A 和 B 之间进行通信”。当接收者接收到此消息之后,不需要上下文就可以清楚知道此消息的内容,而且也清楚知道此消息的发送者与接收者。如果消息未能与通信双方主体进行正确绑定,或者消息内容并未完全反映设计者的意图,需要借助于上下文来分析,就会使攻击者可利用此消息来替换本协议其他轮次中的消息,还可能进行角色冒充攻击。

原则 2:加密的部分从文字形式上是可区分的。

也就是说,安全协议中所用到的加密项从文字上就可以区分,那么当一个主体接收到一个加密项就知道这个加密项属于哪条消息,是消息的哪一部分。例如,某协议消息 1 中包含一个加密项 $\{A,N_a\}K_{ab}$,其中,此加密项使用 A 和 B 的会话密钥 K_{ab} 进行加密,N_a 是 A 产生的随机数,在消息 2 中包括 $\{B,N_b\}K_{ab}$,那么这两条消息在文字上十分相似,有可能在协议的并发运行中引发攻击。所以在消息 2 中把 $\{B,N_b\}K_{ab}$ 改成 $\{N_b,B\}K_{ab}$,可以使接收者知道此加密项是来自消息 2,可以避免某些攻击。

原则 3:如果一个参与者的标识对于某条消息的内容是重要的,那么最好在消息中明确地包