LOIS

信息安全国家重点实验室

信息安全丛书

Security Protocol
Theory and Method

安全协议
理论与方法

范 红　冯登国 编著

科学出版社
www.sciencep.com

信息安全国家重点实验室信息安全丛书

安全协议理论与方法

范　红　冯登国　编著

国家重点基础研究发展规划资助项目(项目编号:G1999035802)
国家杰出青年科学基金资助项目(项目编号:60273027,60025205)

科学出版社

北　京

内 容 简 介

本书是《信息安全国家重点实验室信息安全丛书》之一。书中系统地介绍了当前计算机网络安全协议的理论和方法，主要内容包括安全协议的基本概念、缺陷以及可能受到的攻击类型，基于推理结构性方法，基于攻击结构性方法，基于证明结构性方法，安全协议分析的形式化接口，安全协议设计的形式化方法，Kerberos 协议，IPSec 协议，SSL 协议，X.509 以及 SET 协议。

本书可作为高等院校计算机、通信、信息安全等专业的教学参考书，也可供从事相关专业的教学、科研和工程技术人员参考。

图书在版编目(CIP)数据

安全协议理论与方法/范红，冯登国编著. —北京：科学出版社，2003
(信息安全国家重点实验室信息安全丛书/冯登国主编)
ISBN 7-03-012277-1

Ⅰ.安… Ⅱ.①范…②冯… Ⅲ.计算机网络-安全-通信协议
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2003)第 086891 号

策划编辑：鞠丽娜/责任编辑：韩 洁
责任印制：吕春珉/封面设计：王 浩

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com

新蕾印刷厂 印刷
科学出版社发行 各地新华书店经销

*

2003 年 10 月第 一 版 开本：B5 (720×1000)
2003 年 10 月第一次印刷 印张：27 1/2
印数：1—5 000 字数：532 000

定价：42.00 元

(如有印装质量问题，我社负责调换〈路通〉)

《信息安全国家重点实验室信息安全丛书》编委会

序　言

人类的进步得益于科学研究的突破、生产力的发展和社会的进步。

计算机、通信、半导体科学技术的突破，形成了巨大的新型生产力。数字化的生存方式席卷全球。农业革命、工业革命、信息革命成为人类历史生产力发展的三座丰碑。古老的中华大地，也正在以信息化带动工业化的国策下焕发着青春。电子政务、电子商务等各种信息化应用之花，如雨后春笋，在华夏沃土上竞相开放，炎黄子孙们，在经历了几百年的苦难历程后，在国家崛起中又迎来了一个运用勤劳和智慧富国强民的新契机。

科学规律的掌握，非一朝一夕之功。治水、训火、利用核能都曾经经历了多么漫长的时日。不掌握好科学技术造福人类的一面，就会不经意地释放出它危害人类的一面。

生产力的发展，为社会创造出许多新的使用价值。但是，工具的不完善，会限制这些使用价值的真正发挥。信息化工具也和农业革命、工业革命中人们曾创造的许多工具一样，由于人类认识真理和实践真理的客观局限性，存在许多不完善的地方，从而形成信息系统的漏洞，造成系统的脆弱性，在人们驾御技能不足的情况下，损害着人们自身的利益。

世界未到大同时，社会上和国际间存在着竞争、斗争、战争和犯罪。传统社会存在的不文明、暴力，在信息空间也同样存在。在这个空间频频发生的有些人利用系统存在的脆弱性，运用其"暴智"来散布计算机病毒，制造拒绝服务的事端，甚至侵入他人的系统，盗窃资源、资产，以达到其贪婪的目的。人类运用智慧开拓的信息疆土正在被这些暴行蚕食破坏着。

随着信息化的发展，信息安全成为全社会的需求，信息安全保障成为国际社会关注的焦点。因为信息安全不但关系国家的政治安全、经济安全、军事安全、社会稳定，也关系到社会中每一个人的数字化生存的质量。

信息革命给人类带来的高效率和高效益是否真正实现，取决于信息安全是否得以保障。什么是信息安全？怎样才能保障信息安全？这些问题都是严肃的科学和技术问题。面对人机结合，非线性、智能化的复杂信息巨系统，我们还有许多科学技术问题需要认真的研究。我们不能在研究尚处肤浅的时候，就盲目乐观地向世人宣称，我们拥有了全面的解决方案；我们也不能因为面对各种麻烦，就灰头鼠脸，自暴自弃，我们需要的是具有革命的乐观主义精神，坚忍不拔的奋勇攀登科学技术高峰的坚定信念。

人是有能力认识真理的，今天对信息安全的认识，就经历了一个从保密到保护，又发展到保障的趋近真理的发展过程。因为信息安全的问题不仅仅是因为技术原因引起的，它涉及到人、社会和技术，因此，仅仅靠技术是不能有效地实施信息安全保障的。从社会学的观点来看，只有依靠有信息安全觉悟和技能的人及科学有效的管理来实施综合的技术保障手段，才能取得良好的效果。

为了推动我国信息化发展的进程，信息安全国家重点实验室组织编写了《信息安全国家重点实验室信息安全丛书》。在本丛书的编写过程中，我们既注重学术水平，又注意其实用价值。本丛书从信息安全保障体系，操作系统安全，数据库安全，网络安全，无线网络安全，网络攻击，密码技术，PKI 技术，信息隐藏，安全协议，安全事件应急响应，量子密码通信等多个角度，分析和总结信息安全的科学问题以及信息安全保障的理论与技术，因此，这套丛书有较大的适用范围。我们将努力把国内外信息安全的最新研究成果写进书中，以使一些读者阅读本丛书后在理论、方法、技术上有新的启发和收获，从而切实解决工作中的实际问题。

本丛书的组织方式是开放式的，今后将根据学科发展陆续组织出版信息安全领域的优秀图书。

信息安全只能是相对而言，它是动态发展的。任何人都不能宣称自己终极了对信息安全的认识。让我们一起努力，不断地深化自己的研究，借鉴国外先进的科学技术，结合国情，与时俱进地推出信息安全保障的新理论、新办法和新手段，用我们的智慧保卫我们的信息疆土，使我们的信息家园尽量祥和安宁。

限于作者的水平，本丛书难免存在不足之处，敬请读者批评指正。

《信息安全国家重点实验室信息安全丛书》编委会

2003 年 7 月

前　言

网络安全是目前人们关注的一个热点。在一个分布式的互联网网络环境中，人们通过安全协议来具体实现安全共享网络资源的需求。已有的安全协议往往被证实并不如它们的设计者所期望的那样安全，复杂的网络环境使得攻击者可利用安全协议自身的缺陷来实施各种各样的攻击，从而达到破坏网络安全的目的，因此，安全协议的安全性成为网络安全的关键。安全性的达成需从两方面着手，一是安全协议的安全性是否满足形式化的分析，二是对安全协议进行形式化的设计。本书对现在国内外最新的安全协议形式化分析与设计方法进行了比较详细的论述，建立了完整而系统的安全协议研究理论，并介绍了当前的最为实用的几个安全协议，包括 Kerberos 协议、IPSec 协议、SSL 协议、X.509 以及 SET 协议的实现方法。

全书共 12 章。第 1 章介绍了安全协议所涉及的一些基础密码学知识，包括密码体制、数学签名、Hash 函数、密钥管理与分配以及公钥证书和基础设施。第 2 章主要介绍了安全协议的概念、缺陷与可能受到的攻击类型、认证协议及其所受攻击实例，以及安全协议形式化分析的研究现状与面临的新问题。第 3 章到第 6 章介绍了现有的一些安全协议形式化分析方法，包括基于推理结构性方法，基于攻击结构性方法，基于证明结构性方法，以及安全协议分析的形式化接口，第 7 章介绍了安全协议设计的形式化方法。第 8 章到第 12 章介绍了五个安全协议的实现方法和工作原理，包括 Kerberos 协议、IPSec 协议、SSL 协议、X.509 以及 SET 协议。

本书是作者在长期从事理论研究和科研实践的基础上编写的，我们汲取了大量国内外现有文献的精华，对内容做了精心的安排以适应不同层次和不同专业的读者的需求。书的最后附有相关的参考文献，提供了与本书有关的资料，供有兴趣的读者参考。

作者

2003 年 5 月

目　录

第1章 引 论

1.1 密码体制

1.1.1 基本原理

密码体制是认证协议的基础。假设我们有一个消息P(P通常为明文或数据项),密码算法的作用是将P转换为不为网络监视者所知的消息形式,这一过程称为加密。P的不可识别形式称为密文,记为C。意定的接收者希望从密文C中恢复出明文P,这一过程称为解密。加密与解密过程如图1.1所示。

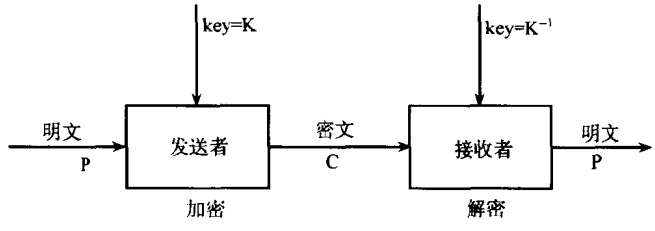

图1.1 加密与解密

一般而言所使用的加解密算法是公开的。加解密操作的使用受限于对所涉及的密钥的访问的适当约束。

1.1.2 对称密钥密码体制

在对称密码体制中,加密密钥K和解密密钥K^{-1}通过公开技术可很容易地相互获得。一对主体用密钥K对消息加密之后发送给对方或解密从对方处接收的秘密消息。持有密钥的一方可以生成任意明文对应的密文,以及阅读任何密文。为保证通信的安全,通信双方将保守此密钥的秘密性。

1.1.3 公钥密码体制

目前关于数字签名的研究主要集中在基于公钥密码体制的数字签名的研究上。公钥密码体制的观点是由Diffie和Hellman在1976年首次提出的,它使密码学发生了一场变革。1977年由Rivest,Shamir和Adleman提出了第一个比较完善

的公钥密码算法，这就是著名的 RSA 算法，从那时起，人们基于不同的计算问题，给出了大量的公钥密码算法。

公开密钥加密的基本思想是：每个用户拥有两个密钥，一个是公开密钥 pk，它类似于电话本上的号码，对任何其他用户都公开；另一个是私有密钥 sk，仅为自己拥有。加密算法 E 和解密算法 D 都是公开的。虽然 sk 是由 pk 决定的，但却不能根据 pk 计算出 sk。

公开密钥加密体制的安全性依赖于一种特殊的数学函数——单向陷门函数，其性质为：从一个方向求值容易，但逆向计算却很困难。公开密钥算法的特点为：

1）用加密密钥 pk 对明文 X 加密后，用解密密钥 sk 解密即可恢复出明文，即 Dsk(Epk(x))=X；另外，加密和解密的计算可以对调，即 Epk(Dsk(x))=X。

2）加密密钥不能用来解密，即 Dpk(Epk(x))≠X。

3）在计算机上可以容易地产生成对的 pk 和 sk。

4）从已知的 pk 推导出 sk 是“计算上是不可能的”。

公钥算法往往基于解决某些问题的计算困难性上，RSA 算法的安全性是基于分解大整数的困难性。如果密码分析者能从用户的公钥 n 在多项式时间内计算出 p 和 q，那么 RSA 算法将是不安全的，这也引发了人们对因子分解这一古老的数论问题的兴趣并取得了一些可喜的进展。目前，最有实用价值的因子分解算法有二次筛法、数域筛法、椭圆曲线算法等。

1.2　数字签名

美国国家安全局与国家标准局通力合作，于 1991 年提出了美国数字签名体制 DSS 及其算法 DSA。数字签名类似于手写签名，具有不可仿造性和不可否认性。随着计算机网络技术的发展，数字签名技术也在不断发展，并得到广泛应用。

1.2.1　数字签名(Digital Signature)技术

一个数字签名方案至少应满足以下三个条件：

1）签名者事后不能否认自己的签名。

2）接收者能验证签名，而任何其他人都不能伪造签名。

3）当双方关于签名的真伪发生争执时，第三方能解决双方之间发生的争执。

根据数字签名标准 DSS(Digital Signature Standard)，数字签名的步骤一般有以下几步：

1）发送方用一个 Hash 函数对消息进行处理，形成一个固定长度的信息摘要(如采用 SHA-1 或 MD5 算法)。

2）发送方将自己的私人密钥 sk 和消息摘要进行 DSA 算法计算，产生数字签