信息与通信工程研究生规划教材

网络信息安全理论与技术

Theory and Technology for Network Information Security

蒋 睿 胡爱群 陆哲明 等编著

華中科技大學出版社
http://www.hustp.com

信息与通信工程研究生规划教材

网络信息安全理论与技术

Theory and Technology for
Network Information Security

蒋　睿　胡爱群　陆哲明
宋宇波　秦中元　黄　杰　裴文江　编著

华中科技大学出版社
（中国·武汉）

图书在版编目(CIP)数据

网络信息安全理论与技术/蒋　睿，胡爱群　陆哲明等编著. —武汉：华中科技大学出版社，2007年11月

ISBN 978-7-5609-4287-2

Ⅰ.网…　Ⅱ.①蒋…　②胡…　③陆…　Ⅲ.计算机网络-安全技术-研究生-教材　Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2007)第163007号

网络信息安全理论与技术　　蒋　睿　胡爱群　陆哲明等编著

责任编辑：张志华　　封面设计：潘　群

责任校对：陈　骏　　责任监印：周治超

出版发行：华中科技大学出版社(中国·武汉)

武昌喻家山　邮编：430074　电话：(027)87557437

录　　排：华中科技大学惠友文印中心

印　　刷：湖北新华印务有限公司

开本：850mm×1065mm　1/16　　印张：27.75　　字数：585 000

版次：2007年11月第1版　　印次：2007年11月第1次印刷　　定价：38.80元

ISBN 978-7-5609-4287-2/TP·639

内容提要

什么是信息安全的基础理论一直是困扰学术界的一个问题。除了密码学理论这个方向外，目前关于其他用来解决信息安全问题的技术的基础理论还没有形成共识。本书力求在当前层出不穷的信息安全技术间，阐述并归纳出这些技术赖以支撑的理论基础，并把这些理论分成密码学理论、安全协议理论、模式识别理论、信息隐藏理论以及可信计算理论。

本书分为五个部分。第一部分是关于密码学理论，主要阐述密码学数学基础和常用密码算法理论；第二部分是关于安全协议理论，主要阐述安全协议的形式化分析方法与安全协议的分析、设计理论，同时介绍相应的安全协议；第三部分是关于模式识别理论，主要论述模式分类基础理论，并在此基础上介绍常用的模式识别方法；第四部分是关于信息隐藏理论，主要论述信息的隐藏理论，同时介绍相应的技术应用；第五部分是关于可信计算导论，主要论述可信计算的概念与架构。本书安排的这五个部分内容具有强烈的代表性，既考虑到信息安全知识的覆盖面，又兼顾到先进性和实用性，以信息安全的各个方面最基础、最典型的理论为主要内容，便于教学。各部分按照先介绍基础理论，后讲解应用的方式安排。这是本书不同于目前已有教材的地方。

本书在每一部分后面附有参考文献和适量的有代表性的习题。参考文献方便读者查阅原始文献，习题可以让读者更好地理解书上讲解的内容。

Abstract

It is the problem puzzled the academe all the time for what is the fundamental theory of the information security. Beside the cipher theory, there are many other technologies dealing with the information security. However, the fundamental theories of these technologies are not commonly acknowledged. In this book, we will try our best to expatiate and conclude the fundamental theories, which can support the secure information technologies emerged in endlessly. We classify the theories into five parts, which include the cipher theory, the security protocol theory , the pattern recognition theory, the information hiding theory and the trusted calculation theory.

This book is divided into five parts. The first part is the cipher theory, which mainly expatiatesthe mathematic theory of the cipher and introduce some common cipher algorithm. The second part is the security protocol theory, which mainly expatiates the formal mothed for security protocol and the theory of protocol analysis and design. Also, the corresponding security protocols are introduced in this part. The third part is the pattern recognition theory, which mainly discuss the fundamental theory of pattern classfying and introduce the common method for pattern recognition. The fourth part is the information hiding theory, which mainly discuss the fundamental theory of information hiding and introduce the corresponding applications. The last part is the trusted calculation theory, which mainly introduce the concepts and framework of the trusted calculation. The five parts arranged in this book have strong characters of delegation, they consider not only the coverage of the information security knowledge, but also have the characters of advancement and practicability. It is also convenient for teaching. The difference of this book between the other teaching material is the arrengement method, for which is disscussing the theory first, and introducing the application second.

In the end of five parts of the book, there are corresponding references and some typical exercises. The readers can find the references conveniently, and they can understand the contants of the book better through doing exercises.

总　序

随着信息时代的到来，人类已经生活在信息的“海洋”之中，信息和通信已渗入我们生活的各个方面。近年来，我国的电信产业以10%以上的年增长率迅猛发展，“中国制造”的通信产品广泛进入了全球市场。另一方面，信息和通信领域的理论与技术获得了迅速发展，不少技术难题已取得实质性突破，技术进步和产业发展相互推动、相互促进。

产业的发展带来了对人才，特别是高层次专业人才的巨大需求。信息与通信工程是我国工科门类中应用前景广阔、招生量比较大的学科，对我国的现代化建设起着非常重要的作用。其中的通信与信息系统更是近几年硕士研究生报考的热门专业之一。随着硕士研究生的不断扩招，研究生教育成为一个突出的问题。鉴于通信学科的迅猛发展，广大科技工作者和硕士、博士研究生迫切需要学习与掌握信息和通信的现代理论与技术。目前本专业的研究生教材已有一些，其中亦不乏典范之作，但专门针对研究生读者成系列出版的尚为少见。其中的一个原因是各校研究生课程设置自成体系，各校之间不尽相同，这为研究生教材的建设和推广造成了困难。

有鉴于此，来自清华大学等十多所高校、科研单位的教授和专家相约聚首，对通信专业研究生课程体系设置进行探讨，尝试从各校现有的课程体系中提取共同性的知识结构框架，并结合他们多年的教学实践积累，编写一套针对通信专业研究生，兼顾高年级本科生的系列教材，为研究生教育做一点工作。

本系列研究生教材针对性强，知识覆盖较为全面，相信该系列教材的出版将会为读者系统掌握通信科学、信息科学的基础理论与技巧，以及本领域的先进技术方法和现代技术手段提供相对便捷的途径，对培养具有从事通信科学、信息科学以及相关领域的科研与开发和教学工作能力的人才提供有力的手段，对本专业研究生教学起到积极的推动作用。

本系列教材的作者均来自信息和通信学科实力较强的院校，不仅有较为丰富的教学经验，而且在研究方向和地域分布上具有一定的代表性。我有感于他们对教育事业的热忱、对教书育人的执著，遂为之序。

中国工程院院士　李乐民

2007年8月

前　言

近10年来，随着网络技术的普及应用和信息化进程的不断推进，网络信息安全问题日显突出。在信息安全技术的发展过程中，密码学得到了长足的发展，保密通信理论已经成为信息安全的主要技术支撑。然而，网络信息安全的需求远不只是保密通信这个方面，还涉及信息的隐蔽性、完整性、真实性、可控性等多个方面。

在信息的隐蔽性方面，信息隐藏技术已经发展起来，如数字水印技术可以起到保护数字版权的作用。在信息的完整性和真实性方面，信息的摘要技术和数字签名技术已经能够支撑电子政务等应用。

信息的可控性是近几年来发展起来的技术，主要包括信息内容的可检查能力和从信息系统中获取信息的能力，是网络安全监管的重要内容。可信计算技术是近几年的研究热点之一，其目的是为了防止信息系统中的资源被未授权修改。该技术也可以归类到信息的可控性这一分支。它既涉及密码技术，又涉及操作系统技术，是目前被认为最有希望解决病毒攻击等问题的技术方向，因此该技术得到当前国内外信息安全界的高度重视。

当前国内信息安全类教材在上述各个方面的介绍各有侧重。但还没有一本教材全面地讲解信息安全涉及的各种主流技术。另外，由于目前信息安全是一种应用牵引的学科，它主要以解决信息安全应用问题为目标，涉及的技术非常广泛，包括保密通信、入侵检测、协议分析、内容安全、病毒防护等。作者在多年研究以及与同行交流的基础上认为，可以将密码学理论和模式分类理论作为信息安全这门学科的主要基础理论。这一观点供大家讨论。究其原因，信息安全的主要任务是保护信息的安全，其主要工作就是信息的保密性和信息的防窃取。前者的基础是密码学，后者是要进行入侵检测、行为分析、病毒防护等，它的基础理论主要是模式分类。正是基于这点考虑，本书把密码学和模式分类作为网络信息安全的理论基础进行讲解。

本书的读者对象主要是信息安全学科的研究生，通过对本书的学习使他们能够充分了解信息安全的理论、技术范畴及今后的研究方向。同时，本书可作为信息学科高年级本科生关于信息安全专业的基础教材，为进一步从事信息安全技术的研究和工作奠定基础。书中的信息隐藏、安全协议、模式识别三个章节可以作为博士研究生的学习内容。

本书编写分工如下。第一部分是关于密码学理论，主要由宋宇波博士撰写；第二部分是关于安全协议理论，主要由蒋睿博士撰写；第三部分是关于模式分类理论，主要由秦中元博士撰写；第四部分是关于信息隐藏理论，主要由陆哲明教授撰写；第五

部分是关于可信计算导论，主要由黄杰副教授撰写。全书由胡爱群教授统稿和修订。裴文江教授参与了本书部分章节的起草和审稿工作。

由于信息安全学科起步较晚，内容覆盖面很宽，本书难以覆盖所有的知识点。虽然每一个部分的撰写人都是在该方向上具有专业特长的科研人员，有一定的教学经验，但也难免存在疏漏甚至错误之处，恳请读者批评指正，并欢迎与我们联系，以便今后修订时提高本书的质量。对读者提出的宝贵建议，我们深表感谢！

编　者

2007 年 8 月

目　录

第一部分　密码学

引　言

什么是密码学？简单地说，它是关于消息保密的研究的科学。它既是一门科学，也是一门非常古老的艺术，某些学者认为密码学出现在发明书写的时候。如今，密码学随着计算机的广泛应用得到快速发展。纵观其发展历史，可以分为三个阶段：从古代到1949年前称为第一阶段，这时的密码学只是一门艺术而非科学；从1949年到1976年称为第二阶段，1949年香农的一篇名为《Communication Theory of Secrecy Systems》的论文开创了密码学的科学时代，在这篇论文中，香农创建了基于信息论的密码系统数学模型，从理论上证明密钥数目至少要和可能的消息数目一样多时，才能实现完全保密(perfect security)；从1976年至今称为第三阶段，1976年W. Diffie和M. E. Hellman在发表的《New Directions in Cryptography》论文中首次提出了公钥密码学，将密码学带入快速发展阶段。

各个研究领域都有自己的语言，使用特定的术语以方便理解待研究的对象。术语密码学(cryptology)由James Howell于1645年提出，该词来源于希腊词根"cryptos"和"logos"，意为有隐藏含义的单词。密码学分为密码编码学(cryptography)和密码分析学(cryptanalysis)两个分支。密码编码学由英国人Thomas Browne于1658年发明，graphy来源于希腊词根"graphein"，意为书写。密码编码学即是关于秘密书写的研究的科学。从事密码编码学研究的人称为密码编译专家(cryptographer)。原始的消息称为明文(plaintext)，被伪装的消息则称为密文(ciphertext)。最终封装并被发送的消息称为密码(cryptogram)。将明文转换为密文的过程称为加密(encrypt)或是译成密码(encipher)。而将密文转换为明文的相反过程称为解密(decrypt)或是解译(decipher)。密码分析学则与密码编码学相对立，它是关于用数学方法进行密码破解的研究的科学。analysis来源希腊词根"analyein"，意为解开。从事密码分析的人称为密码分析专家(cryptanalyst)。

进行加密和解密的数学函数称为密码算法(algorithm)或密码(cipher)。它通常包含两个函数：一个用于加密，另一个用于解密。古代密码算法的保密性是基于算法细节的保密，显然这并不安全。现代密码算法函数中引入称为密钥(key)的参数，密钥值的范围即为密钥空间(keyspace)，该参数只有通信双方秘密拥有。荷兰人Kerchoffs在1883年提出了密码算法设计的一个重要原则："算法的秘密必须全部隐藏在密钥中"。即算法的安全性是基于密钥的安全性而非算法本身的安全性。假设