<<密码协议>>

图书基本信息

书名：<<密码协议>>

13位ISBN编号：9787040362503

10位ISBN编号：7040362503

出版时间：2012-11

出版时间：高等教育出版社

作者：董玲，陈克非　著

页数：344

字数：430000

<<密码协议>>

前言

网络通信协议是计算机节点之间为了通信而对需要交换消息的格式、规则的描述和规定。
密码协议，又称安全协议，是一类特殊的通信协议，它通过一些密码学的手段来达到某种特殊的安全性目标。

网络通信协议通常具有层次结构，每一层协议进行相应的操作以逐步完成通信的全过程。
通常，安全机制根据需要可以被嵌入到不同的协议层中。
例如，众所周知的传输层安全协议TLS就是在TCP协议之上附加的协议，以实现特定的安全服务功能。
事实上，密码协议广泛用于密钥建立、实体认证、消息认证、安全传输数据、不可抵赖等方面。
由于通信过程不能保证实时与同步，一些密码协议并不如设计者所期望的安全，经典的例子如Needham-Schroeder公钥认证协议，从协议公布到安全漏洞被发现历经了17年。

本书的着眼点是密码协议安全性分析，首先引入可信任新鲜性的概念，在此基础上提出了协议安全性分析的新鲜性原则以及一种基于新鲜性原则的有效、易用、新颖的协议安全性分析方法——信任多集形式化方法。
所做的这一切，试图要回答下面的问题：　　·协议的安全性（计算上安全，或实际的安全）究竟意味什么？

·协议的安全性是否可以通过工程的方法检验？

·如何使安全性的验证简单易行并能自动实现？

本书可作为通信协议安全性研究人员、学生以及工程技术人员的参考书。
书中列举了大量密码协议分析的实例，可帮助读者理解、掌握相关概念和方法。
这些内容对从事密码协议研究的专业人员，特别对密码协议设计和分析的工程师都将有所启发。
本书提出的基于可信任新鲜性的安全性分析方法在实际应用中更加易于操作，分析过程也更为有效，即使是一个没有密码学专业背景的工程师也能很快掌握。

本书分为中、英文两个版本，分别在海内外发行。
在写作过程中得到许多专家、同行和朋友的鼓励、支持与帮助，这成为我们完成本书的动力。
为此，首先要感谢蔡吉人院士和裴定一教授，他们在得知本书的写作计划时给予了热情的鼓励，并向“国家科学技术学术著作出版基金”作了推荐；特别要感谢来学嘉教授，他对本书的前期工作给出了不少有益的建议；我们还要感谢上海交通大学密码与信息安全实验室的龙宇博士以及博士生王亮亮、硕士生程正杰、本科生傅婧、罗施博等人，他们为本书分担了不少从英文版到中文版的翻译、校对等工作。
最后，我们要感谢高等教育出版社的编辑陈红英女士，正是她的鼓动与建议才使我们下决心写作本书，在长达两年多的时间里，我们保持着很好的沟通与相互理解，她为本书付出了许多辛勤劳动。

<<密码协议>>

内容概要

《信息安全系列丛书·密码协议：基于可信任新鲜性的安全性分析》主要介绍如何利用系统工程思想和可信任新鲜性的方法，分析和设计密码协议。
作者基于可信任的新鲜性标识符概念，提出了一个新颖的新鲜性原则。
该原则指出了一种有效的、易用的密码协议安全性分析方法。
使用这种分析方法，可以有效检验协议在实际应用中能否满足安全需求。
此外，书中给出大量的分析实例，详细图解了如何基于概率定义安全性，如何将安全指标定量化，如何针对具体的协议寻找漏洞，如何自动实现协议漏洞的查找，等等。

作者简介

董玲，网络系统建设和信息安全领域高级工程师，上海交通大学密码与信息安全实验宰兼职教授，研究兴趣是信息安全和应用密码学，特别是实际应用的密码通信协议和密码系统的安全性分析。

陈克非，上海交通大学计算机科学与工程系教授，长期从事密码与信息安全理论研究，主要研究兴趣是序列密码、可证明安全、密码协议分析、数据安全。
近年来承担多项国家自然利学基令、国家高技术发展计划（863计划）项目，发表学术论文150多篇，编辑出版学术著作7部。

<<密码协议>>

书籍目录

<<密码协议>>

版权说明