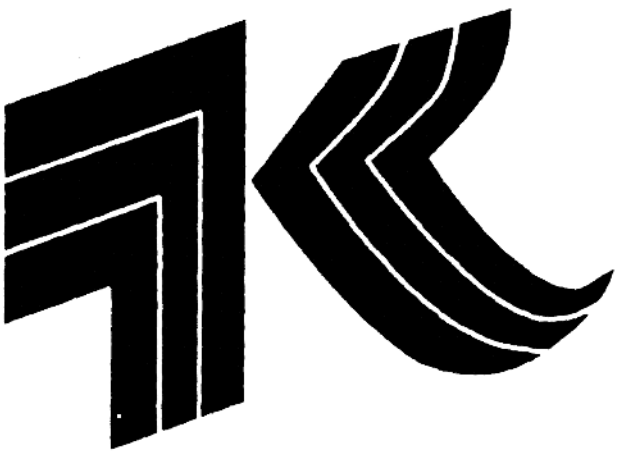
全国高技术重点图书·计算机技术领域

计算机系统安全

The Security of Computer Systems

卢开澄 郭宝安
戴一奇 黄连生 编著

重庆出版社



计算机系统安全

The Security of Computer Systems

THE SECURITY OF COMPUTER SYSTEMS

by Lu Kaicheng Guo Baoan
Dai Yiqi Huang Liansheng

Chongqing Publishing House
Jan. 1999

内 容 提 要

本书重点介绍了计算机系统中的信息安全问题与技术，包括密码技术、数据库安全、操作系统安全、计算机网络安全以及病毒防治和软件保护等技术。本书特别强调现代密码学在计算机系统中的应用，提供了常用的算法和标准，可供计算机、通信与电子系统、信息工程、金融电子化等专业的工程技术人员使用和参考，并可作为大学高年级本科生和研究生的教材使用。

Summary

The problems and techniques of the security for computer systems, Will for example, cryptography, security of database, security of operating system, security of computer network, the protecting techniques against computer virus, the protecting techniques for software, etc. be discussed in this book. We pay attention to the applications of modern cryptology to computer systems specially.

At the end, some source codes are provided for users including computer engineers, electronic engineers and communication engineers etc.

著 者 摘 要

本书著者都是清华大学长期在计算机科学与技术系从事计算机系统安全问题研究的教授。第一作者卢开澄教授，出生于 1930 年，已出版下列图书：

1. 组合数学——算法与分析(两卷本)
2. 图论及其应用(第二版)
3. 组合数学(第二版)
4. 算法与复杂性
5. 计算密码学
6. 计算机算法导引——设计与分析
7. 计算机密码学(第二版)
8. 单目标，多目标，与整数规划

A Brief About the Authors

The authors of this book all are the professors of Tsinghua University, they are engaged in the research for security of computer systems in the Department of Computer Science and Technology in the Tsinghua University for a long time.

Professor Lu Kaicheng, the first author, was born in 1930. He has published the following books:

1. Combinatorial Mathematics(2 Volumes)——Algorithms and Analysis
2. Graph Theory with Its Applications (2nd Edition)
3. Combinatorial Mathematics(2nd Edition)
4. Algorithms and Complexity
5. Computing Cryptography
6. Introduction to Computer Algorithms——Design and Analysis
7. Computer Cryptology(2nd Edition)
8. Single Objective, Multiple Objectives, and Integer Programming

前言

自20世纪90年代以来，计算机在我国乃至全世界得到了迅速普及和发展，计算机网络和系统在全球也得以迅猛发展和延伸，尤其是Internet网络的大力推广。但是，随之而来的计算机安全问题也日益突出，计算机犯罪以及计算机病毒的泛滥严重地威胁着计算机系统，软件被非法拷贝、计算机信息被非法修改、系统授权存在严重缺陷，等等。这些问题已经到了非常严重的地步，各国政府和机构以及一些民间组织和公司正在积极解决这些问题。

众所周知，密码技术一直是各国政府和机要部门非常关心的技术。而且，随着计算机系统的建设，民间用户也开始十分关注他们的计算机系统的安全问题。当前，密码技术已经走向公开，国际上已经颁布了多种加密算法(DES，IDEA等)和数字签名标准(DSA，RSA)，多种安全协议已经在计算机网络系统中得到了使用，密码学可以而且能够为计算机系统的安全发挥更大的作用。

本书内容安排：

第1章主要论述计算机系统安全的有关知识和理论。

第2章主要讲述计算机系统的数据安全，这是本书的重点。主要讲述现代密码技术和数据安全的相关技术，包括数字签名、身份验证、秘密分享、Hash函数等重要的数据安全技术及密码算法(DES，RSA，DSS，等)。

第3章主要讲述计算机系统中的安全协议。本章针对不同的计算机系统的安全要求，讲述各种安全协议的设计技术，包括初级安全协议、中级安全协议和高级安全协议，这些协议多数是以第2章的数据安全技术为基础的。

第4章主要介绍计算机网络安全。主要讲述计算机网络系统中所面临的安全问题，内容包括网络安全策略、网络加密技术、接入控制、用户鉴别、信息流控制和数据完整性等问题，所用技术和协议是以第2章和第3章内容为基础的。

第5章主要讲述操作系统的安全。重点讲述安全的操作系统的设计技术，指出了通用操作系统的安全缺陷，并给出了通用的安全操作系统的设计实例。

第6章主要讲述数据库系统的安全。数据库的安全问题主要包括：数据库所面临的

各种安全问题与对策，数据库中数据的保密性、可靠性和完整性的实现，多级数据库的安全等内容。

第 7 章讲述计算机病毒的编制与防治。

第 8 章讲述软件保护技术，包括软件加密、软件“指纹”制作、软件反跟踪技术及软件破密技术。

本书是在清华大学计算机系理论教研室长期从事计算机安全与密码学研究的基础上编写的。在写作过程中，作者还结合了他们在一些具体的计算机系统的安全设计与实现方面的经验，从实用角度对计算机系统的安全进行了全面介绍。

本书附有密码学主要算法程序的 C 语言源代码，可供读者直接使用。

在本书的编写过程中，得到了重庆出版社的支持和鼓励，作者在此表示衷心感谢。

作　者

1999 年 1 月于清华大学

Preface

Since 90's of 20 century, computers are developed and become popularization rapidly in our country and the whole world, the computers networks and systems are also developed and extended rapidly in the world , especially with the development of the Internet. But accompany with these new development is that the security of computer systems become more serious, the crime of computer and virus threaten the computing systems, software are illegal copied, the information of the computing systems are illegal modified, there exist serious drawback in the authorization systems, etc. These problems are so serious now , such that the governments of many countries, many non – governmental organizations and companies are making great efforts to solve these problems.

It is well known that cryptology is concerned by government and security department for every country. The non – governmental users are concerned their security of their computing systems. Cryptology is become popular today, many encryption algorithms(DES, IDEA etc) and data signature standards(DSA RSA) are published, many security protocols are used in computing systems, it is believed that cryptography can play more important role in computing systems.

The arrangement of the content of the book

The knowledge and theory of computing systems are introduced in Chapter 1.

The data security of computing system is introduced in Chapter 2, this is the main point, which include modern cryptology and data security technology, such as data signature, identity prove, security share, hash function and many encryption algorithm(DES, RSA, DSA, etc).

The secure protocols are introduced in Chapter 3. Designation of secure protocol for different computing systems is proposed, including basic secure protocols, intermediate secure protocols, and advanced secure protocols, these protocols are based on data security in Chapter 2.

The security of computer network is in Chapter 4. Which include the secure problems in networks, such as the secure policy in network, network encryption, access control, users identify, information traffic controlling and datainetegrity. These technology and protocols are based on Chapter 2 and 3.

The secure operating system is in Chapter 5, the main point is designing the secure operating systems. The drawback of the general operating systems is pointed out. The example of the general secure operating system is given in this Chapter.

The secure database is in Chapter 6, which include the security problems and security policy in database, such as the implement of the security, reliability and integrated of data in database, the multi – level secure database is introduced in this Chapter.

Chapter 7 introduces how to write and prevent virus.

Chapter 8 introduces the protection technology of software , include software encryption, the designation of the "finger print" of software, the technology of anti – following tracks of software and the crack of software.

This book is based on the research of the Theory Group of Computer Science and Technology Department of Tsinghua University. With the experience of the authors for designation and implement of the secure computing systems, these secure technology are very useful in real computing systems.

The C source code of the main algorithms is in this book, users can use them directly.

Thanks for the support of Chongqing publishing house to publish this book.

Authors, in Tsinghua University
Jan. 1999

目 录