

<<网际安全技术构架>>

图书基本信息

书名：<<网际安全技术构架>>

13位ISBN编号：9787121113796

10位ISBN编号：7121113791

出版时间：2010-8

出版时间：南相浩 电子工业出版社 (2010-08出版)

作者：南相浩

页数：248

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## 前言

A report submitted by the US President's Information Technology Advisory Committee (PITAC) in 2005, entitled Cyber Security - A Crisis of Prioritization, marked the arrival of a new era of cyber security (in cyber world or society). If the main task of "information security" is a passive prevention that consists mainly of plugging and patching, the main task of "cyber security" is active management that consists mainly of building trusting system. The core of active management is to establish an authentication system that sets up information security on the basis of certification system. This is so called trusting system. It is a new mission. In the past, since there were no proper evidence-showing and verifying systems, information security can only adopt the principle of "at good will", or based on the presumption that the subject was trustworthy. However, cyber security is totally different. It is established on the basis of "mutual suspicion", not allowing authentication or verification under presumption. Such changes of main task and basic principles first affect basic theory of security. All the security protocols and standards adopting the principle of "good will" in the past shall be reconsidered with "mutual suspicion", for example, communication protocols and standards, trusted computing (including code signing) protocols and standards. This will surely lead to a revolutionary change. At the EU crypt 07 annual meeting, James Hughes (executive chairman of Crypt 04) and Guan Zhi (Ph.D student of Peking University) delivered a presentation on identity-based Combined Public Key (CPK) system. The authoritative experts attending the meeting affirmed that CPK system is novel. Identity-based system represents new development trend of modern cryptosystem, and attracts attention from cryptography community around the world. CPK Cryptosystem has attracted great attention from China's top leaders, and also has received substantial support from the administrations of Guangdong Science and Technology Department and Beijing Municipal Science and Technology Commission. Researchers/Professors Zhou Zhong-yi, Chen Hua-ping, Lü Shu-wang, Zhai Qi-bing, Li Yi-fa and Doctors Tang Wen, Guan Zhi, Chen Yu, Tian Wen-chun, Zheng Xu have involved in this CPK project. Another important progress is that a theory of trust logic is established based on identity authentication, to promote the conventional belief logic to trust logic. The trust logic based on identity authentication is different from the belief logic based on data authentication. The trust logic consisted of identity of entity authentication and body of entity authentication, can conduct "pre-authentication". That is, identity authentication can be conducted before the body event occurs, so as to effectively prevent illegal events from happening. Scaled authentication technology is the core technology to establishing a world of trust. CPK system can solve such international puzzle well. This book systematically introduces solutions in the main fields of trusting system. Such fields include a number of problems which cannot be solved in the past but easily dealt with now, for instance: illegal communication access, illegal software running, seal authentication systems, etc. From examples of application, readers can find that due to the core issue of identity authentication has been solved, a number of difficult problems that was impossible to solve in the past can be easily tackled. Thus, "identity authentication" is the "silver bullet" of cyber security, which will lead to the solution of all other problems. This is the base of a holistic solution of trust system. In the process of researching, Communication expert Sun Yu, Computer expert Qu Yan-wen, IT expert James Hughes and sci&tech information expert Zhao Jan-guo offered useful suggestions. At the beginning of 2009, U.S. government has released some documents related with cyber security. The documents have stressed three points: Addressing system in internet, identity authentication and secure software engineering. The address is the identity of communication. It tells us the Identity Management, including identity definition and identity authentication, will be the basic techniques of future cyber security. How to define identity is an important subject but beyond this book. However, we have enough experience in defining identity in real life such as the mailing address, phone number, bank account number, and so on. This is the reason why we stand for real name system. From the rules of identity definition in real life we may draw an important conclusion: In trusting system, identity must have special meaning and the meaning must be commonly recognized. It is obvious that the in existing IPv4 and IPv6 protocols, the address is defined randomly and only explained by special DNS. It is unfortunate that the protocols go against above mentioned basic rules. This is why Obama

administration took “ identity authentication ” and addressing system as core task of cyber security. The work of cyber security is in progress of developing on its track and has yielded some important results. For example, a new type of network router is designed with real name communication system. The address is the real location that bounded with the sign code, so it can prohibit any unauthorized connection. Meanwhile code signing has been developed rapidly as main part of trust computing. CPK cryptosystem, identity authentication and trust logic is introduced in this book as the basic theory and technology of the trusting system. The construction of trust world needs a joint effort of all nations because we have a common enemy: that is the “ terrorist software ” . I sincerely wish that this book can satisfy the demands of readers, facilitate transition of information security from network security to cyber security.

## <<网际安全技术构架>>

### 内容概要

CPK Cryptosystem changes ordinary elliptic curve public key into an identity-based public key with self-assured property. Self-assured public key can advance the authentication logic from object-authenticating "belief logic" to entity-authenticating "trust logic". Self-assured public key system and trust logic of authentication composes the key technique of cyber security. The construction of trust connecting , computing , transaction , logistics , counter-forgery and network management will be the main contents of the next generation of information security. Readers benefited from this book will be researchers and professors , experts and students , developers and policy makers , and all other who are interested in cyber security.

## <<网际安全技术构架>>

### 作者简介

南相浩，现任北京大学兼职教授和中国民生银行顾问等职务，长期从事密码学、信息安全和信息安全系统研究工作，是中国著名密码学专家。

他是《网络安全技术概论》著作的作者，是《银行行为监管》和《银行行为控制》著作的副主笔。

他是CPK密钥管理算法的提出者。

## 书籍目录

FOREWORD  
CONTENTS  
PART ONE AUTHENTICATION TECHNIQUE  
CHAPTER 1 BASIC CONCEPTS  
1.1 PHYSICAL WORLD AND DIGITAL WORLD  
1.2 A WORLD WITH ORDER AND WITHOUT ORDER  
1.3 SELF-ASSURED PROOF AND 3RD PARTY PROOF  
1.4 CERTIFICATION CHAIN AND TRUST CHAIN  
1.5 CENTRALIZED AND DECENTRALIZED MANAGEMENT  
1.6 PHYSICAL SIGNATURE AND DIGITAL SIGNATURE  
CHAPTER 2 AUTHENTICATION LOGIC  
2.1 BELIEF LOGIC  
2.2 STANDARD PROTOCOL  
2.3 TRUST RELATIONSHIP  
2.3.1 Direct Trust  
2.3.2 Axiomatic Trust  
2.3.3 Inference Trust  
2.4 TRUST LOGIC  
2.4.1 The requirement of Trust Logic  
2.3.2 The Progress in Public Key  
2.4.3 Entity Authenticity  
2.4.4 The Characteristics of Trust Logic  
2.5 CPK PROTOCOL  
2.5.1 One-way Protocol  
2.5.2 Two-way Protocol  
CHAPTER 3 IDENTITY AUTHENTICATION  
3.1 COMMUNICATION IDENTITY AUTHENTICATION  
3.2 SOFTWARE IDENTITY AUTHENTICATION  
3.3 ELECTRONIC TAG AUTHENTICATION  
3.4 NETWORK MANAGEMENT  
3.5 HOLISTIC SECURITY  
PART TWO CRYPTO-SYSTEMS  
CHAPTER 4 COMBINED PUBLIC KEY (CPK)  
4.1 INTRODUCTION  
4.2 ECC COMPOUND THEOREM  
4.3 IDENTITY-KEY  
4.3.1 Combining Matrix  
4.3.2 Mapping from Identity to Matrix Coordinates  
4.3.3 Computation of Identity-Key  
4.4. KEY COMPOUNDING  
4.4.1 The Compounding of Identity-Key and Accompanying-Key  
4.4.2 The Compounding of Identity-Key and Separating-key  
4.5 CPK DIGITAL SIGNATURE  
4.5.1 Signing with Accompanying-Key  
4.5.2 Signing with Separating-key  
4.6 CPK KEY EXCHANGE  
4.6.1 Key Exchange with Separating-key  
4.6.2 Key Exchange with Accompanying-Key  
4.7 CONCLUSION  
CHAPTER 5 SELF-ASSURED AND 3RD PARTY PUBLIC KEY  
5.1 NEW REQUIREMENTS OF THE CRYPTO-SYSTEM  
5.2 DEVELOPMENT OF CRYPTO-SYSTEMS  
5.3 DIGITAL SIGNATURE MECHANISM  
5.3.1 IBC Signature Scheme  
5.3.2 CPK Signature with Separating-key  
5.3.3 CPK Signature with Accompanying-Key  
5.3.4 PKI Signature Scheme  
5.3.5 IB-RSA Signature Scheme  
5.3.6 mRSA Signature Scheme  
5.3.7 Comparison of Schemes  
5.4 KEY EXCHANGE SCHEME  
5.4.1 IBE Key Exchange  
5.4.2 CPK Key Exchange  
5.4.3 Other Key Exchange Schemes  
5.4.4 Performance Comparison  
5.5 DISCUSSION ON TRUST ROOT  
CHAPTER 6 BYTES ENCRYPTION  
6.1 TECHNICAL BACKGROUND  
6.2 CODING STRUCTURE  
6.2.1 Transposition Table (disk)  
6.2.2 Substitution Table (subst)  
6.3 8-BIT OPERATION  
6.3.1 Assumptions  
6.3.2 Key Derivation  
6.3.3 Combination of Data and Keys  
6.3.4 Left Shift Accumulation  
6.3.5 Transposition Conversion  
6.3.6 Single Substitution Conversion  
6.3.7 Re-combination of Data and Keys  
6.3.8 Right Shift Accumulation  
6.3.9 Re-transposition  
6.4 7-BIT OPERATION  
6.4.1 Given Conditions  
6.4.2 Key Derivation  
6.4.3 Combination of Data and Key  
6.4.4 Left Shift Accumulation  
6.4.5 Transposition Conversion  
6.4.6 Single Substitution Conversion  
6.4.7 Re-combination of Data and Key  
6.4.8 Right Shift Accumulation  
6.4.9 Re-composition  
6.5 SAFETY EVALUATION  
6.5.1 Key Granularity  
6.5.2 Confusion and Diffusion  
6.5.3 Multiple-level Product Conversion  
PART THREE CPK SYSTEM  
CHAPTER 7 CPK KEY MANAGEMENT  
7.1 CPK KEY DISTRIBUTION  
7.1.1 Authentication Network  
7.1.2 Communication Key  
7.1.3 Classification of Keys  
7.2 CPK SIGNATURE  
7.2.1 Digital Signature and Verification  
7.2.2 Signature Format  
7.3 CPK KEY EXCHANGE  
7.4 CPK DATA ENCRYPTION  
7.5 KEY PROTECTION  
7.5.1 Password Verification  
7.5.2 Password Change  
CHAPTER 8 CPK-CHIP DESIGN  
8.1 BACKGROUND  
8.2 MAIN TECHNOLOGY  
8.3 CHIP STRUCTURE  
8.4 MAIN FUNCTIONS  
8.4.1 Digital Signature  
8.4.2 Data Encryption  
CHAPTER 9 CPK ID-CARD  
9.1 BACKGROUND  
9.2 ID-CARD STRUCTURE  
9.2.1 The Part of Main Body  
9.2.2 The Part of Variables  
9.3 ID-CARD DATA FORMAT  
9.4 ID-CARD MANAGEMENT  
9.4.1 Administrative Organization  
9.4.2 Application for ID-Card  
9.4.3 Registration Department  
9.4.4 Production Department  
9.4.5 Issuing Department  
PART FOUR TRUST COMPUTING  
CHAPTER 10 SOFTWARE ID AUTHENTICATION  
10.1 TECHNICAL BACKGROUND  
10.2 MAIN TECHNOLOGY  
10.3 SIGNING MODULE  
10.4 VERIFYING MODULE  
10.5 THE FEATURE OF CODE SIGNING  
CHAPTER 11 CODE SIGNING OF WINDOWS  
11.1 INTRODUCTION  
11.2 PE FILE  
11.3 MINI-FILTER  
11.3.1 NT I/O Subsystem  
11.3.2 File Filter Driving  
11.3.3 Minifilter  
11.4 CODE AUTHENTICATION OF WINDOWS  
11.4.1 The System Framework  
11.4.2 Characteristics Collecting  
11.5

CONCLUSION  
 CHAPTER 12 CODE SIGNING OF LINUX  
 12.1 GENERAL DESCRIPTION  
 12.2 ELF FILE  
 12.3 LINUX SECURITY MODULE (LSM) FRAMEWORK  
 12.4 IMPLEMENTATION  
 PART FIVE TRUST CONNECTING  
 CHAPTER 13 PHONE TRUST CONNECTING  
 13.1 MAIN TECHNOLOGIES  
 13.2 CONNECTING PROCEDURE  
 13.3 DATA ENCRYPTION  
 13.4 DATA DECRYPTION  
 CHAPTER 14 SOCKET LAYER TRUST CONNECTING  
 14.1 LAYERS OF COMMUNICATION  
 14.2 SECURE SOCKET LAYER (SSL)  
 14.3 TRUSTED SOCKET LAYER (TSL)  
 14.4 TSL WORKING PRINCIPLE  
 14.5 TSL ADDRESS AUTHENTICATION  
 14.6 COMPARISON  
 CHAPTER 15 ROUTER TRUST CONNECTING  
 15.1 PRINCIPLE OF ROUTER  
 15.2 REQUIREMENTS OF TRUSTED CONNECTION  
 15.3 FUNDAMENTAL TECHNOLOGY  
 15.4 ORIGIN ADDRESS AUTHENTICATION  
 15.5 ENCRYPTION FUNCTION  
 15.5.1 Encryption Process  
 15.5.2 Decryption Process  
 15.6 REQUIREMENT OF HEADER FORMAT  
 15.7 TRUSTED COMPUTING ENVIRONMENT  
 15.7.1 Evidence of Software Code  
 15.7.2 Authentication of Software Code  
 PART SIX TRUST E-COMMERCE  
 CHAPTER 16 E-BANK AUTHENTICATION  
 16.1 BACKGROUND  
 16.2 COUNTER BUSINESS  
 16.3 BUSINESS LAYER  
 16.4 BASIC TECHNOLOGY  
 16.5 BUSINESS AT ATM  
 16.6 COMMUNICATION BETWEEN ATM AND PORTAL  
 16.7 THE ADVANTAGES  
 CHAPTER 17 E-BILL AUTHENTICATION  
 17.1 BILL AUTHENTICATION NETWORK  
 17.2 MAIN TECHNOLOGIES  
 17.3 APPLICATION FOR BILLS  
 17.4 CIRCULATION OF BILLS  
 17.5 VERIFICATION OF CHECK  
 PART SEVEN TRUST LOGISTICS  
 CHAPTER 18 E-TAG AUTHENTICATION  
 18.1 BACKGROUND  
 18.2 MAIN TECHNOLOGY  
 18.3 EMBODIMENT ( )  
 18.4 EMBODIMENT ( )  
 CHAPTER 19 THE DESIGN OF MYWALLET  
 19.1 TWO KINDS OF AUTHENTICATION CONCEPT  
 19.2 SYSTEM CONFIGURATION  
 19.3 TAG STRUCTURE  
 19.3.1 Structure of Data Region  
 19.3.2 Structure of Control Region  
 19.4 TAG DATA GENERATION AND AUTHENTICATION  
 19.4.1 KMC  
 19.4.2 Enterprise  
 19.4.3 Writer and Reader  
 19.5 PROTOCOL DESIGN  
 19.6 CONCLUSION  
 PART EIGHT FILE & NETWORK MANAGEMENT  
 CHAPTER 20 E-MAIL AUTHENTICATION  
 20.1 MAIN TECHNOLOGIES  
 20.2 SENDING PROCESS  
 20.3 RECEIVING PROCESS  
 CHAPTER 21 DATA STORAGE AUTHENTICATION  
 21.1 SECURITY REQUIREMENTS  
 21.2 BASIC TECHNOLOGY  
 21.3 FILE UPLOADING PROTOCOL  
 21.4 FILE DOWNLOADING PROTOCOL  
 21.5 DATA STORING  
 21.5.1 Establishment of Key File  
 21.5.2 Storage of Key File  
 21.5.3 Documental Database Encryption  
 21.5.4 Relational Database Encryption  
 CHAPTER 22 SECURE FILE BOX  
 22.1 BACKGROUND  
 22.2 SYSTEM FRAMEWORK  
 22.3 FEATURES OF THE SYSTEM  
 22.4 SYSTEM IMPLEMENTATION  
 CHAPTER 23 E-SEAL OF CLASSIFICATION  
 23.1 BACKGROUND TECHNOLOGY  
 23.2 MAIN TECHNOLOGIES  
 23.3 WORKING FLOW  
 23.4 EMBODIMENT  
 23.5 EXPLANATION  
 CHAPTER 24 WATER-WALL FOR INTRANET  
 24.1 BACKGROUND  
 24.2 WORKING PRINCIPLES  
 24.3 THE DIAGRAM OF INTRANET WATER-WALL  
 24.4 WATER-WALL FOR INDIVIDUAL PC  
 24.5 GUARDING POLICY  
 CHAPTER 25 DIGITAL RIGHT AUTHENTICATION  
 25.1 TECHNICAL BACKGROUND  
 25.2 MAIN TECHNOLOGIES  
 25.3 MANUFACTURER'S DIGITAL RIGHT  
 25.4 ENTERPRISE'S RIGHT OF OPERATION  
 25.5 CLIENT'S RIGHT OF USAGE  
 REFERENCES  
 APPENDICES  
 APPENDIX A WALK OUT OF MYSTERIOUS "BLACK CHAMBER"  
 APPENDIX B IDENTITY AUTHENTICATION OPENING A NEW LAND FOR INFORMATION SECURITY  
 APPENDIX C SEARCHING FOR SAFE "SILVER BULLET"  
 APPENDIX D "ELECTRONIC ID CARD" ATTRACTS INTERNATIONAL ATTENTION  
 APPENDIX E CPK SYSTEM GOES TO THE WORLD  
 APPENDIX F IDENTITY AUTHENTICATION BASED ON CPK SYSTEM

章节摘录

插图：ID-card and CA certificate are different in nature. ID-card is issued by the authority, and is a certificate that uses private key variables as the main authentication parameters. CA certificate is issued by a third party, and is a certificate that uses public key variables as the main authentication parameters. ID-card is issued by the authority, it can authorize. CA certificate is issued by a third party, it generally cannot authorize. CA certificate needs to operate online, while ID-card can be operated off-line and can directly be used to authenticate identity, to establish relatively reliable trust relationship. CA certificate of PKI indirectly establish a relatively loose trust relationship with third-party proof.



## <<网际安全技术构架>>

### 编辑推荐

《网际安全技术构架:基于标识鉴别的可信系统(英文版)》：网际安全技术构架——基于标识鉴别的可信系统。

<<网际安全技术构架>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>