<<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

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 Cript 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, L ü 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.

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.

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

FOREWORDCONTENTSPART ONEAUTHENTICATION TECHNIQUECHAPTER 1BASIC CONCEPTS1.1 PHYSICAL WORLD AND DIGITAL WORLD1.2 A WORLD WITH ORDER AND WITHOUT ORDER1.3 SELF-ASSURED PROOF AND 3RD PARTY PROOF1.4 CERTIFICATION CHAIN AND TRUST CHAIN1.5 CENTRALIZED AND DECENTRALIZED MANAGEMENT1.6 PHYSICAL SIGNATURE AND DIGITAL SIGNATURECHAPTER 2AUTHENTICATION LOGIC2.1 BELIEF LOGIC2.2 STANDARD PROTOCOL2.3 TRUST RELATIONSHIP2.3.1 Direct Trust2.3.2 Axiomatic Trust2.3.3 Inference Trust2.4 TRUST LOGIC2.4.1 The requirement of Trust Logic2.3.2 The Progress in Public Key2.4.3 Entity Authenticity2.4.4 The Characteristics of Trust Logic2.5 CPK PROTOCOL2.5.1 One-way Protocol2.5.2 Two-way ProtocolCHAPTER 3IDENTITY AUTHENTICATION3.1 COMMUNICATION IDENTITY AUTHENTICATION3.2 SOFTWARE IDENTITY AUTHENTICATION3.3 ELECTRONIC TAG AUTHENTICATION3.4 NETWORK MANAGEMENT3.5 HOLISTIC SECURITYPART TWOCRYPTO-SYSTEMSCHAPTER 4COMBINED PUBLIC KEY (CPK)4.1 INTRODUCTION4.2 ECC COMPOUND THEOREM4.3 IDENTITY-KEY4.3.1 Combining Matrix4.3.2 Mapping from Identity to Matrix Coordinates4.3.3 Computation of Identity-Key4.4. KEY COMPOUNDING4.4.1 The Compounding of Identity-Key and Accompanying-Key4.4.2 The Compounding of Identity-Key and Separating-key4.5 CPK DIGITAL SIGNATURE4.5.1 Signing with Accompanying-Key4.5.2 Signing with Separating-key4.6 CPK KEY EXCHANGE4.6.1 Key Exchange with Separating-key4.6.2 Key Exchange with Accompanying-Key4.7 CONCLUSIONCHAPTER 5SELF-ASSURED AND 3RD PARTY PUBLIC KEY5.1 NEW REQUIREMENTS OF THE CRYPTO-SYSTEM5.2 DEVELOPMENT OF CRYPTO-SYSTEMS5.3 DIGITAL SIGNATURE MECHANISM5.3.1 IBC Signature Scheme5.3.2 CPK Signature with Separating-key5.3.3 CPK Signature with Accompanying-Key5.3.4 PKI Signature Scheme5.3.5 IB-RSA Signature Scheme5.3.6 mRSA Signature Scheme5.3.7 Comparison of Schemes5.4 KEY EXCHANGE SCHEME5.4.1 IBE Key Exchange5.4.2 CPK Key Exchange5.4.3 Other Key Exchange Schemes5.4.4 Performance Comparison5.5 DISCUSSION ON TRUST ROOTCHAPTER 6BYTES ENCRYPTION6.1 TECHNICAL BACKGROUND6.2 CODING STRUCTURE6.2.1 Transposition Table (disk)6.2.2 Substitution Table (subst)6.3 8-BIT OPERATION6.3.1 Assumptions6.3.2 Key Derivation6.3.3 Combination of Data and Keys6.3.4 Left Shift Accumulation6.3.5 Transposition Conversion6.3.6 Single Substitution Conversion6.3.7 Re-combination of Data and Keys6.3.8 Right Shift Accumulation6.3.9 Re-transposition6.4 7-BIT OPERATION6.4.1 Given Conditions6.4.2 Key Derivation6.4.3 Combination of Data and Key6.4.4 Left Shift Accumulation6.4.5 Transposition Conversion6.4.6 Single Substitution Conversion6.4.7 Re-combination of Data and Key6.4.8 Right Shift Accumulation6.4.9 Re-composition6.5 SAFETY EVALUATION6.5.1 Key Granularity6.5.2 Confusion and Diffusion6.5.3 Multiple-level Product ConversionPART THREECPK SYSTEMCHAPTER 7CPK KEY MANAGEMENT7.1 CPK KEY DISTRIBUTION7.1.1 Authentication Network7.1.2 Communication Key7.1.3 Classification of Keys7.2 CPK SIGNATURE7.2.1 Digital Signature and Verification7.2.2 Signature Format7.3 CPK KEY EXCHANGE7.4 CPK DATA ENCRYPTION7.5 KEY PROTECTION7.5.1 Password Verification7.5.2 Password ChangeCHAPTER 8CPK-CHIP DESIGN8.1 BACKGROUND8.2 MAIN TECHNOLOGY8.3 CHIP STRUCTURE8.4 MAIN FUNCTIONS8.4.1 Digital Signature8.4.2 Data EncryptionCHAPTER 9CPK ID-CARD9.1 BACKGROUND9.2 ID-CARD STRUCTURE9.2.1 The Part of Main Body9.2.2 The Part of Variables9.3 ID-CARD DATA FORMAT9.4 ID-CARD MANAGEMENT9.4.1 Administrative Organization9.4.2 Application for ID-Card9.4.3 Registration Department9.4.4 Production Department9.4.5 Issuing DepartmentPART FOURTRUST COMPUTINGCHAPTER 10SOFTWAREID AUTHENTICATION10.1 TECHNICAL BACKGROUND10.2 MAIN TECHNOLOGY10.3 SIGNING MODULE10.4 VERIFYING MODULE10.5 THE FEATURE OF CODE SIGNINGCHAPTER 11CODE SIGNING OF WINDOWS11.1 INTRODUCTION11.2 PE FILE11.3 MINI-FILTER11.3.1 NT I/O Subsystem11.3.2 File Filter Driving11.3.3 Minifilter11.4 CODE AUTHENTICATION OF WINDOWS11.4.1 The System Framework11.4.2 Characteristics Collecting11.5

CONCLUSIONCHAPTER 12CODE SIIGNING OF LINUX12.1 GENERAL DESCRIPTION12.2 ELF FILE12.3 LINUX SECURITY MODULE (LSM) FRAMEWORK12.4 IMPLEMENTATIONPART FIVETRUST CONNECTINGCHAPTER 13PHONE TRUST CONNECTING13.1 MAIN TECHNOLOGIES13.2 CONNECTING PROCEDURE13.3 DATA ENCRYPTION13.4 DATA DECRYPTIONCHAPTER 14SOCKET LAYER TRUST CONNECTING14.1 LAYERS OF COMMUNICATION14.2 SECURE SOCKET LAYER (SSL)14.3 TRUSTED SOCKET LAYER (TSL)14.4 TSL WORKING PRINCIPLE14.5 TSL ADDRESS AUTHENTICATION14.6 COMPARISONCHAPTER 15ROUTER TRUST CONNECTING15.1 PRINCIPLE OF ROUTER15.2 REQUIREMENTS OF TRUSTED CONNECTION15.3 FUNDAMENTAL TECHNOLOGY15.4 ORIGIN ADDRESS AUTHENTICATION15.5 ENCRYPTION FUNCTION15.5.1 Encryption Process15.5.2 Decryption Process15.6 REQUIREMENT OF HEADER FORMAT15.7 TRUSTED COMPUTING ENVIRONMENT15.7.1 Evidence of Software Code15.7.2 Authentication of Software CodePART SIXTRUST E-COMMERCECHAPTER 16E-BANK AUTHENTICATION16.1 BACKGROUND16.2 COUNTER BUSINESS16.3 BUSINESS LAYER16.4 BASIC TECHNOLOGY16.5 BUSINESS AT ATM16.6 COMMUNICATION BETWEEN ATM AND PORTAL16.7 THE ADVANTAGESCHAPTER 17E-BILL AUTHENTICATION17.1 BILL AUTHENTICATION NETWORK17.2 MAIN TECHNOLOGIES17.3 APPLICATION FOR BILLS17.4 CIRCULATION OF BILLS17.5 VERIFICATION OF CHECKPART SEVENTRUST LOGISTICSCHAPTER 18E-TAG AUTHENTICATION18.1 BACKGROUND18.2 MAIN TECHNOLOGY18.3 EMBODIMENT（Ⅰ）18.4 EMBODIMENT（Ⅱ）CHAPTER 19THE DESIGN OF MYWALLET19.1 TWO KINDS OF AUTHENTICATION CONCEPT19.2 SYSTEM CONFIGURATION19.3 TAG STRUCTURE19.3.1 Structure of Data Region19.3.2 Structure of Control Region19.4 TAG DATA GENERATION AND AUTHENTICATION19.4.1 KMC19.4.2 Enterprise19.4.3 Writer and Reader19.5 PROTOCOL DESIGN19.6 CONCLUSIONPART EIGHTFILE & NETWORK MANAGEMENTCHAPTER 20E-MAIL AUTHENTICATION20.1 MAIN TECHNOLOGIES20.2 SENDING PROCESS20.3 RECEIVING PROCESSCHAPTER 21DATA STORAGE AUTHENTICATION21.1 SECURITY REQUIREMENTS21.2 BASIC TECHNOLOGY21.3 FILE UPLOADING PROTOCOL21.4 FILE DOWNLOADING PROTOCOL21.5 DATA STORING21.5.1 Establishment of Key File21.5.2 Storage of Key File21.5.3 Documental Database Encryption21.5.4 Relational Database EncryptionCHAPTER 22SECURE FILE BOX22.1 BACKGROUND22.2 SYSTEM FRAMEWORK22.3 FEATURES OF THE SYSTEM22.4 SYSTEM IMPLEMENTATIONCHAPTER 23E-SEAL OF CLASSIFICATION23.1 BACKGROUND TECHNOLOGY23.2 MAIN TECHNOLOGIES23.3 WORKING FLOW23.4 EMBODIMENT23.5 EXPLANATIONCHAPTER 24WATER-WALL FOR INTRANET24.1 BACKGROUND24.2 WORKING PRINCIPLES24.3 THE DIAGRAM OF INTRANET WATER-WALL24.4 WATER-WALL FOR INDIVIDUAL PC24.5 GUARDING POLICYCHAPTER 25DIGITAL RIGHT AUTHENTICATION25.1 TECHNICAL BACKGROUND25.2 MAIN TECHNOLOGIES25.3 MANUFACTURER'S DIGITAL RIGHT25.4 ENTERPRISE'S RIGHT OF OPERATION25.5 CLIENT'S RIGHT OF USAGEREFERENCESAPPENDICESAPPENDIX AWALK OUT OF MYSTERIOUS“ BLACK CHAMBER ”APPENDIX BIDENTITY AUTHENTICATION OPENING A NEW LAND FOR INFORMATION SECURITYAPPENDIX CSEARCHING FOR SAFE“ SILVER BULLET ”APPENDIX D“ ELECTRONIC ID CARD ” ATTRACTS INTERNATIONAL ATTENTIONAPPENDIX ECPK SYSTEM GOES TO THE WORLDAPPENDIX FIDENTITY 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 acertificate that uses private key variables as the main authentication parameters. CA certificate is is-sued by a third party, and is a certificate that uses public key variables as the main authenticationparameters. ID-card is issued by the authority, it can authorize. CA certificate is issued by a thirdparty,it generally cannot authorize. CA certificate needs to operate online,while ID-card can be op-erated off-line and can directly be used to authenticate identity, to establish relatively reliable trustrelationship. CA certificate of PKI indirectly establish a relatively loose trust relationship with third-party proof.

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。

版权说明