

Cyber Security Technical Framework
—Trusting System Based on
Identity Authentication

网际安全技术构架
—基于标识鉴别的可信系统

Nan Xiang - Hao



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>

Cyber Security Technical Framework

—Trusting System Based on Identity Authentication

网际安全技术构架——基于标识鉴别的可信系统

Nan Xiang-hao



電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

Abstract

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.

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有,侵权必究。

图书在版编目(CIP)数据

网际安全技术构架:基于标识鉴别的可信系统:英文/南相浩著. —北京:电子工业出版社, 2010. 8
ISBN 978-7-121-11379-6

I. ①网… II. ①南… III. ①计算机网络-安全技术-英文 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2010)第 136653 号

责任编辑:赵 平

印 刷:北京市天竺颖华印刷厂

装 订:三河市鑫金马印装有限公司

出版发行:电子工业出版社

北京市海淀区万寿路 173 信箱 邮编:100036

开 本:787×980 1/16 印张:16.75 字数:426 千字

印 次:2010 年 9 月第 1 次印刷

印 数:1 500 册 定价:88.00 元

凡所购买电子工业出版社的图书,如有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010) 88254888。

质量投诉请发邮件至 zltz@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线:(010) 88258888。

About the Author

NAN Xiang-hao: Dean, South China Information Security Institute, visiting professor of Information Engineering University and Institute of Computer Science and Technology, Beijing University.

Publications:

1. *Profile to Network Security Technologies*, 2003 (Chinese)
2. *Identity Authentication Based on CPK*, 2005 (Chinese)
3. *CPK Crypto-system and Cyber Security*, 2007 (Chinese)

Forward

Providing trust in the face of anonymity is an impossibility. Since interactions on the Internet can easily be anonymous, it is imperative to find a digital authentication means that is reliable, simple to deploy, and simple to use. A method that will bring trust to the Internet and to the general population is critical. The CPK cryptosystem allows society to enjoy the benefits of eCommerce and individual privacy which is balanced with the social needs.

Anonymity, the ability to perform an act without identifying oneself, is not a new concept, but has been dramatically enhanced because of the Internet. Traditionally, the presence of an offender and a victim in the same location leaves behind physical evidence, and this evidence improves the ability of the police to identify and apprehend an offender. By comparison, the Internet has been shown to be a haven for offenders. Offenders can perform criminal acts at great distances that can transcend national boundaries in near perfect anonymity, making law enforcement dramatically more difficult.

Authentication is the natural defense of anonymity, it forms the foundation for trust by proving identity. Authentication can be used for authorization, privacy, and deterrence.

Authentication for authorization is necessary to access money in the bank or to know that the person who signed the document has the authority to commit for the organization.

Authentication for privacy is necessary to know that a conversation is private between two people. An email to your spouse should not be readable by someone who has attacked the Internet. This form of "direct encryption" has higher levels of trust if there is direct authentication by both parties.

Authentication for deterrence is necessary to be able to know who you interact with. Seeing the license of a car provides some assurance about who you are dealing with if something bad happens, there is a better chance of the police being able to track down the offender.

Cryptographic Authentication attempts to provide this proof of identity from a distance using purely digital means. This is a difficult problem that transcends the mathematics of cryptography and moves into the philosophical issues of trust and the organizational basis of society.

In Whitfield Diffie's and Martin Hellman's 1976 paper "NEW DIRECTIONS IN CRYPTOGRAPHY" the authors introducing the concept of public key cryptography and digital signatures wrote. . .

- Authentication is at the heart of any system involving contracts and billing. Without it, business cannot function. Current electronic authentication systems cannot meet the need for a purely digital, unforgeable, message dependent signature. They provide protection against third party forgeries, but do not protect against disputes between transmitter and receiver.

Since that time, there have been many digital signature schemes proposed and some standardized. In general these are now described as traditional signature schemes that have been implemented as a directed graph of public keys which are signed by a more general key until the point that there is mutual trust.

Traditional digital authentication is tied to the individual. It requires a public key distribution scheme and lacks lawful intercept abilities.

If Alice needs to send an email to Bob, she must first get Bob's public key from a repository, check the revoked key list, and authenticate this key to some root key that she trusts before she can send a message to Bob. This is a significant effort.

If Alice and Bob are conspirators in a crime, their communications cannot be investigated by law enforcement.

Identity based encryption provides simpler solutions to these problems. From Adi Shamir's 1984 paper "IDENTITY BASED CRYPTOSYSTEMS AND SIGNATURE SCHEMES" he states:

- In this paper we introduce a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party.

Professor Shamir further states that. . .

- The scheme remains practical even on a nationwide scale with hundreds of key generation centers and millions of users, and it can be the basis for a new type of personal identification card which everyone can electronically sign checks, credit card slips, legal documents, and electronic mail.

One of the values of identity based encryption is the key generating centers can be operated by organizations who can naturally vouch for an individual's identity. For example, an university can vouch for a professor or a student, or a corporation can vouch for an employee.

Identity based encryption also provides a deterrence against the abuse of trust. In practice, a key generated by a corporation has the valuable side effect of allowing policing by that corporation of an individual's use of that key.

The CPK algorithm represents a great step forward in identity based encryption. It creates a

simple to understand, easy to implement, and easy to deploy system that provides all the benefits that these visionaries imagined for public key and identity based cryptosystems.

This book delivers a complete analysis of what Identity, Authentication and Trust mean in a digital age. It shows how CPK can meet the challenges of the internet to make it a safer place.

This book may not result in world peace, but it can provide a roadmap to calm the chaos which exists on the Internet today.

James P. Hughes
Palo Alto, CA, USA

Preface

A report submitted by the US President's Information Technology Advisory Committee (PI-TAC) in 2005, entitled *Cyber Security- A Crisis of Prioritization*, marked the arrival of a new era of cyber security (cyber world). 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 Beijing 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 Qibing, 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-proof". That is, identity authentication can be conducted before the body event occurs, so as to effectively prevent illegal events from happening. Large scale 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 Jian-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 address is defined randomly and only explained by special DNS. in existing IPv4 and IPv6 protocols 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.

Author
In Beijing, Sep. 2009

Contents

Part One Authentication Technique

Chapter 1 Basic Concepts	2
1.1 Physical World and Digital world	2
1.2 A World with Order and without Order	3
1.3 Self-assured Proof and 3rd Party Proof	4
1.4 Certification Chain and Trust Chain	6
1.5 Centralized and Decentralized Management	7
1.6 Physical Signature and Digital Signature	8
Chapter 2 Authentication Logic	11
2.1 Belief Logic	11
2.2 Standard Protocol	12
2.3 Trust Relationship	13
2.3.1 Direct Trust	13
2.3.2 Axiomatic Trust	13
2.3.3 Inference Trust	14
2.4 Trust Logic	15
2.4.1 The Requirement of Trust Logic	15
2.4.2 The Progress in Public Key	16
2.4.3 Entity Authenticity	16
2.4.4 The Characteristics of Trust Logic	18
2.5 CPK Protocol	19
2.5.1 One-way Protocol	19
2.5.2 Two-way Protocol	19
Chapter 3 Identity Authentication	21
3.1 Communication Identity Authentication	21
3.2 Software Identity Authentication	23
3.3 Electronic Tag Authentication	24

3.4	Network Management	24
3.5	Holistic Security	25

Part Two Crypto-systems

Chapter 4	Combined Public Key (CPK)	28
4.1	Introduction	28
4.2	ECC Compounding Feature	28
4.3	Identity-Key	29
4.3.1	Combining Matrix	29
4.3.2	Mapping from Identity to Matrix Coordinates	29
4.3.3	Computation of Identity-Key	30
4.4	Key Compounding	30
4.4.1	The Compounding of Identity-Key and Accompanying-Key(optional)	30
4.4.2	The Compounding of Identity-Key and Separating-Key	30
4.5	CPK Digital Signature	31
4.5.1	Signing with Accompanying-Key(optional)	31
4.5.2	Signing with Separating-Key	31
4.6	CPK Key Exchange	32
4.6.1	Key Exchange with Separating-Key	32
4.6.2	Key Exchange with Accompanying-Key(optional)	32
4.7	Security Analysis	32
Chapter 5	Self-assured and 3rd Party Public Key	35
5.1	New Requirements of the Crypto-System	35
5.2	Development of Crypto-Systems	36
5.3	Digital Signature Mechanism	37
5.3.1	IBC Signature Scheme	37
5.3.2	CPK Signature with Separating-Key	37
5.3.3	CPK Signature with Accompanying-Key	38
5.3.4	PKI Signature Scheme	38
5.3.5	IB-RSA Signature Scheme	39
5.3.6	mRSA Signature Scheme	40
5.3.7	Comparison of Schemes	40
5.4	Key Exchange Scheme	40

5.4.1	IBE Key Exchange	41
5.4.2	CPK Key Exchange	41
5.4.3	Other Key Exchange Schemes	42
5.4.4	Performance Comparison	43
5.5	Discussion on Trust Root	44
Chapter 6	Bytes Encryption	45
6.1	Technical Background	45
6.2	Coding Structure	47
6.2.1	Transposition Table (disk)	47
6.2.2	Substitution Table (subst)	48
6.2.3	Key Structure	49
6.2.4	Operation Flowchart	51
6.3	8-bit Operation	51
6.3.1	Assumptions	51
6.3.2	Key Derivation	52
6.3.3	Combination of Data and Keys	52
6.3.4	Left Shift Accumulation	53
6.3.5	Transposition Conversion	54
6.3.6	Single Substitution Conversion	54
6.3.7	Re-combination of Data and Keys	55
6.3.8	Right Shift Accumulation	55
6.3.9	Re-transposition	56
6.4	7-bit Operation	56
6.4.1	Given Conditions	56
6.4.2	Key Derivation	57
6.4.3	Combination of Data and Key	58
6.4.4	Left Shift Accumulation	58
6.4.5	Transposition Conversion	59
6.4.6	Single Substitution Conversion	60
6.4.7	Re-combination of Data and Key	60
6.4.8	Right Shift Accumulation	61
6.4.9	Re-composition	61
6.5	Security Evaluation	62

6.5.1	Key Granularity	62
6.5.2	Confusion and Diffusion	63
6.5.3	Multiple-level Product Conversion	63

Part Three CPK System

Chapter 7	CPK Key Management	66
7.1	CPK Key Distribution	66
7.1.1	Authentication Network	66
7.1.2	Communication Key	67
7.1.3	Classification of Keys	67
7.2	CPK Signature	68
7.2.1	Digital Signature and Verification	68
7.2.2	Signature Format	68
7.3	CPK Key Exchange	69
7.4	CPK Data Encryption	70
7.5	Key Protection	70
7.5.1	Password Verification	70
7.5.2	Password Change	71
Chapter 8	CPK-chip Design	72
8.1	Background	72
8.2	Main Technology	72
8.3	Chip Structure	74
8.4	Main Functions	77
8.4.1	Digital Signature	77
8.4.2	Data Encryption	78
Chapter 9	CPK ID-card	80
9.1	Background	80
9.2	ID-card Structure	81
9.2.1	The Part of Main Body	82
9.2.2	The Part of Variables	82
9.3	ID-card Data Format	83
9.4	ID-card Management	85
9.4.1	Administrative Organization	85

9.4.2	Application for ID-card	86
9.4.3	Registration Department	87
9.4.4	Production Department	88
9.4.5	Issuing Department	90

Part Four Trust Computing

Chapter 10	SoftwareID Authentication	92
10.1	Technical Background	92
10.2	Main Technology	93
10.3	Signing Module	94
10.4	Verifying Module	95
10.5	The Feature of Code Signing	97
Chapter 11	Code Signing of Windows	98
11.1	Introduction	98
11.2	PE File	98
11.3	Mini-filter	99
11.3.1	NT I/O Subsystem	99
11.3.2	File Filter Driving	100
11.3.3	Mini-filter	101
11.4	Code Authentication of Windows	102
11.4.1	The System Framework	102
11.4.2	Characteristics Collecting	102
11.5	Conclusion	102
Chapter 12	Code Signing of Linux	103
12.1	General Description	103
12.2	ELF File	103
12.3	Linux Security Module (LSM) Framework	104
12.4	Implementation	105

Part Five Trust Connecting

Chapter 13	Phone Trust Connecting	108
13.1	Main Technologies	108
13.2	Connecting Procedure	109

13.3	Data Encryption	110
13.4	Data Decryption	111
Chapter 14	Socket Layer Trust Connecting	112
14.1	Layers of Communication	112
14.2	Secure Socket Layer (SSL)	113
14.3	Trusted Socket Layer (TSL)	115
14.4	TSL Working Principle	116
14.5	TSL Address Authentication	118
14.6	Comparison	120
Chapter 15	Router Trust Connecting	121
15.1	Principle of Router	122
15.2	Requirements of Trusted Connection	123
15.3	Fundamental Technology	124
15.4	Origin Address Authentication	124
15.5	Encryption Function	127
15.5.1	Encryption Process	127
15.5.2	Decryption Process	128
15.6	Requirement of Header Format	128
15.7	Trusted Computing Environment	129
15.7.1	Evidence of Software Code	129
15.7.2	Authentication of Software Code	129
Conclusion		129

Part Six Trust e-Commerce

Chapter 16	e-Bank Authentication	132
16.1	Background	132
16.2	Counter Business	133
16.3	Business Layer	134
16.4	Basic Technology	135
16.5	Business at ATM	136
16.6	Communication Between ATM and Portal	137
16.7	The Advantages	138
Chapter 17	e-Bill Authentication	140

17.1	Bill Authentication Network	140
17.2	Main Technologies	141
17.3	Application for Bills	141
17.4	Circulation of Bills	143
17.5	Verification of Check	143

Part Seven Trust Logistics

Chapter 18	e-Tag Authentication	146
18.1	Background	146
18.2	Main Technology	147
18.3	Embodiment (I)	148
18.4	Embodiment (II)	149
Chapter 19	The Design of Mywallet	151
19.1	Two Kinds of Authentication Concept	151
19.2	System Configuration	152
19.3	TAG Structure	153
19.3.1	Structure of Data Region	153
19.3.2	Structure of Control Region	154
19.4	TAG Data Generation and Authentication	155
19.4.1	KMC	155
19.4.2	Enterprise	155
19.4.3	Writer and Reader	155
19.5	Protocol Design	156
19.6	Conclusion	157

Part Eight File & Network Management

Chapter 20	e-Mail Authentication	160
20.1	Main Technologies	160
20.2	Sending Process	161
20.3	Receiving Process	162
Chapter 21	Data Storage Authentication	163
21.1	Security Requirements	163
21.2	Basic Technology	164