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
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.

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 zlts@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, unforgetable, 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 (PITAC) 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 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-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

Part Two Crypto-systems

Part Three CPK System

Part Four Trust Computing

Part Five Trust Connecting

Part Six Trust e-Commerce

Part Seven Trust Logistics

Part Eight File & Network Management