<<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.

<<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.

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。

<<网际安全技术构架>>

书籍目录

<<网际安全技术构架>>

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.

<<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。

版权说明