《CPK公钥体制与标识鉴别》

图书基本信息

书名：《CPK公钥体制与标识鉴别》

13位ISBN编号：9787121174858

10位ISBN编号：7121174855

出版时间：2012-7

出版社：电子工业出版社

作者：南相浩

页数：316

《CPK公钥体制与标识鉴别》

内容概要

《CPK公钥体制与标识鉴别(英文)》讨论了未来“网际安全”的关键技术——基于标识鉴别的可信系统，也讨论了与此相关的自证性公钥体制、信任逻辑，以及信任逻辑在可信接入、可信计算、可信交易、可信物流。网络管理中的应用，以及在互联网和物联网构成的网际空间中建立互信的基本技术。

《CPK公钥体制与标识鉴别》

书籍目录

《CPK公钥体制与标识鉴别》

章节摘录

版权页： 插图： Development and spread of horizontally structured networking and end to end transmission technology such as store-forward communication and packet switching raise many new issues to the authentication system.The issues can be summarized as follows:scalability of proof and immediacy of verification in digital signature.Different domains and classifications were defined in the networks in the past but now the horizontal management i.e.the management over the Grid authentication network has become the new trends.To meet the new requirement it must be supported by new technology and theory. 7.1.2 Communication Key Since the authentication network is a grid network with no center,and the modern communication is individualized and end to end communication,on the open public network(such as Internet,telephone network),it is redundant to divide the network or data into function domains(e.g.longitudinal multi-layered division,horizontal internal-external network division),and to divide personnel and data into different classifications(except for private network). Despite all that,in view of the actual situation of coexistence of private network and public network,it is acceptable to remain function domain division of keys and registration classification of personnel. Communication key is a main parameter variable that ensures commumcation between the communicating parties.The keys are divided into symmetric keys and asymmetric keys. 1)Symmetric Key:A common key shared by both communicating parties. 2)Asymmetric Key:The decryption key is owned by the designated party. 7.1.3 Classification of Keys In generally,there is no need to define different classifications for the communication network and computer facilities in public network.It is the same as above mentioned authentication network.But if the keys are used in file management then files may be classified different levels to realize different encryption. The keys are classified by roles and domain.Role is divided into 1)System administrator 2)Senior employees 3)Mid-level employees 4)General employees 5)Customers Domain is divided into 1)Global domain 2)District domain Different keys are distributed to different classes and domain for enabling different access control.

《CPK公钥体制与标识鉴别》

编辑推荐

《CPK公钥体制与标识鉴别(英文)》讨论了新一代信息安全的概念和下一代绿色网络安全的发展方向，《CPK公钥体制与标识鉴别(英文)》适合网络技术方面的教授和研究人员做为参考文件，也适合学生，工程师和全部对网络技术感兴趣的人士阅读。

《CPK公钥体制与标识鉴别》