Design and Application of Authentication Scheme for Span Field Net Based on Public Key Certification

HU Wei, WEI Guoheng, QIN Yanlin, LIAO Wei

Department of Information Security, Naval Univ. of Engineering, Wuhan, China

e-mail: Huwei-1212@126.com

Abstract: According to the requirement of span field net authentication, the authentication scheme for span field net based on public key certification is designed. It combines the authentication technology based on secret information and that based on authenticating objects. It concludes secret information carrier selection, trusted third-party selection, certification make and distribution, span field net authentication protocol, and certification logout. This authentication scheme is used in span field authentication of computer security defense system. It can offer better safeguard in span field authentication.

Keywords: public key certification; span field authentication; authentication

基于公钥证书的跨域身份认证方案设计与应用

胡　卫，魏国珩，秦艳琳，廖　巍

海军工程大学信息安全系，武汉，中国，430033

e-mail: Huwei-1212@126.com

【摘　要】针对用户跨域身份认证的需求，将基于秘密信息的认证技术和基于信物的认证技术进行结合，设计了基于公钥证书的跨域身份认证方案，包括秘密信息载体选择、可信第三方的选择、证书的生成与颁发、跨域认证协议和证书注销全过程。并在计算机桌面安全防护系统跨域认证时进行了应用，较好的解决了跨域身份认证的安全性。

【关键词】公钥证书；跨域认证；身份认证

1 引言

信息安全包括认证、操作系统安全、数据库安全、访问控制和数据加密等。其中认证体制作为访问控制的一个重要内容，一直为人们所关注。认证通常分为实体认证和数据源认证。实体认证又叫身份认证，它是信息系统的第一道安全屏障，也是实施访问控制的基础，因此具有十分重要的作用。

根据被认证方赖以证明身份的秘密的不同，身份认证可以分为四大类：基于秘密信息的身份认证技术、基于信物的身份认证技术、零知识身份认证和基于生物特征的身份认证技术。本文将基于秘密信息的认证技术和基于信物的认证技术进行结合，设计了基于公钥证书的身份认证方案，并在计算机桌面安全防护系统跨域认证时进行了应用。

资助信息：国家“863”计划基金资助项目（2007AA12Z208）；中国博士后科研基金项目（20080431384）

2 安全管理体系

安全管理体系是保证身份认证方案有效的重要部分。完善的管理体系可以增强身份认证的安全性，防止非法用户通过认证。

本认证方案的管理体系分为三个层次：超级管理层、二级管理层、一般用户层。超级管理层的主体对象是超级管理员，二级管理层的主体对象是二级管理员，一般用户层的主体对象是合法用户。管理体系层次如图1所示。

超级管理员可对二级管理员进行管理，负责对二级管理员的资格进行审查。资格审查通过后，超级管理员为二级管理员生成私钥、颁发公钥证书、配发电子钥匙。

二级管理员可对其信任域的一般用户进行管理：包括审查资格、生成用户私钥、颁发用户公钥证书、分析和审计一般用户的使用情况、取消用户资格等。

一般合法用户可以修改其用户名和用户口令，以及

978-1-935068-06-8 © 2009 SciRes.

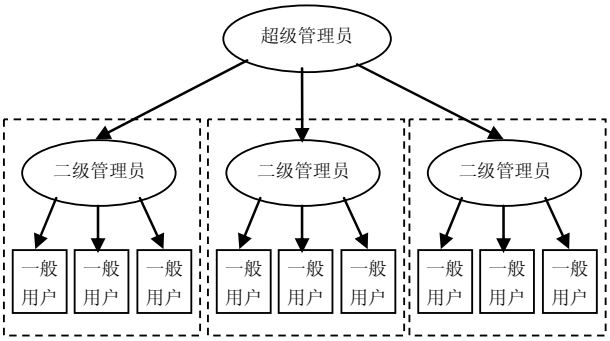

Figure 1. Manage system levels
图 1. 管理体系层次

合法的操作。

3 跨域身份认证协议设计

3.1 秘密信息载体选择

电子钥匙内置的带有密码保护的专用存储器可对用户存储的重要信息提供安全保护。身份认证方案所使用的用户标识、口令、私钥和公钥证书等信息采用电子钥匙存储。表 1 二级管理员电子钥匙中存储的内容，表 2 一般用户电子钥匙中存储的内容。

3.2 可信任第三方选择

由于是采用基于公钥证书的身份认证方案，而可信任第三方是建立跨域网络环境下信任保证的基础，是信息加密、身份鉴别、密钥协商等安全策略实现的前提，所以可信任第三方的选择与建立是整个身份认证方案的基石和核心。由可信任第三方负责对系统中的用户进行公钥证书的生成、颁发、管理以及注销等操作，其签名保证了用户公钥的真实性和数据完整性。由于每个子域的管理员都有其安全信任域，域中的用户都充分信任

Table 1. Secondary manager USBKey file content
表 1. 二级管理员电子钥匙文件单元

文件 ID	文件大小	读权限	写权限	文件信息
1000	5	ALWAYS	MKEY	钥匙分配，管理员标识，位置参数
1001	20	PIN	PIN	管理员用户名
1002	20	PIN	PIN	密码
2000	3072	PIN	MKEY	用户信息
3000	SN 长度	PIN	MKEY	二级管理员私钥和模数
4000	证书长度	PIN	MKEY	二级管理员证书

Table 2. User USBKey file content
表 2. 一般用户电子钥匙文件单元

文件 ID	文件大小	读权限	写权限	文件信息
1000	5	ALWAYS	MKEY	钥匙分配，管理员标识，位置参数
1001	20	PIN	PIN	一般用户用户名
1002	20	PIN	PIN	密码
4000	证书长度	PIN	MKEY	二级管理员证书
5000	SN 长度	PIN	MKEY	一般用户私钥和模数
6000	证书长度	PIN	MKEY	一般用户证书

Figure 2. Certification format
图 2. 证书格式

本子域的管理员，因此我们选择每个子域的管理员为可信任第三方。由他对本子域中的用户进行公钥证书的生成，颁发以及注销等操作。公钥证书格式如图 2 所示。证书的签名采用 1024 位的 RSA 公钥算法模拟实现。

3.3 秘密信息载体选择

超级管理员的公钥直接保存在系统中，超级管理员在对二级管理员的身份和资格进行严格的审查后，为每个二级管理员生成并签发公钥证书，分配二级管理员的电子钥匙。同样，二级管理员在对本信任域内一般用户的身份和资格进行严格审查后，为其生成并签发公钥证书，同时将二级管理员自己的公钥证书传递给一般用户，并为用户分配电子钥匙。颁发证书流程如图 3 所示。

每个合法用户都拥有自己的电子钥匙，用于存放二级管理员的公钥证书以及二级管理员为用户签发的

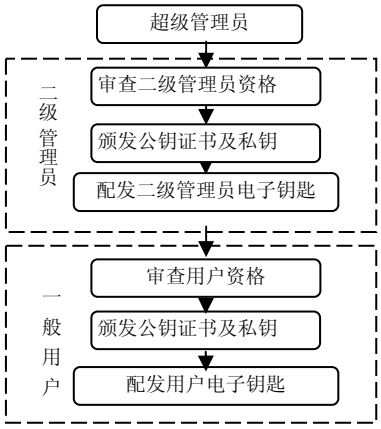

Figure 3. Certification distribution
图 3. 颁发证书流程

公钥证书、用户私钥等信息。

3.4 证书的注销

二级管理员可以对本信任域内的一般用户证书进行有效的管理，可以为证书过期的用户重新颁发证书或者直接注销该用户证书。由于每个用户在使用本系统时，都要先进行登录，即与本域二级管理员进行联系，如果是非法用户或者用户的证书已过期，系统将自动拒绝该用户登录系统，用户必须与二级管理员进行联系，生成新的合法用户证书。

3.5 跨域身份认证协议

设 E 是签名算法，D 是 E 的逆算法，S_i 是私钥，P_i 是公钥，N_i 是模数，ID_i 是用户名，$Date_i$ 是证书有效期，$Cert_i$（Mi，P_i，N_i，ID_i，$Date_i$）=Es_0（Mi，P_i，N_i，ID_i，$Date_i$）是超级管理员 SuperM 用 S_0 为二级管理员 Mi 签发的证书，$Cert_{ij}$（User ij，P_{ij}，N_{ij}，ID_{ij},$Date_{ij}$）=Es_i（User ij，P_{ij}，N_{ij}，ID_{ij},$Date_{ij}$）是管理员 Mi 用 S_i 为用户 $User_{ij}$ 签发的证书。

超级管理员 SuperM：S_0，P_0，N_0

二级管理员 M_1：S_1，$Cert_1$（M1，P_1，N_1，ID_1，$Date_1$），PIN_1，P_0，N_0

二级管理员 M2：S_2，$Cert_2$（M2，P_2，N_2，ID_2，$Date_2$），PIN_2，P_0，N_0

二级管理员 Mn：S_n，$Cert_n$（Mn，P_n，N_n，ID_n，$Date_n$），PIN_n，P_0，N_0

一般用户 $User_{11}$：S_{11}，$Cert_1$（M1，P_1，N_1，ID_1，$Date_1$），$Cert_{11}$（$User_{11}$，P_{11}，N_{11}，ID_{11}，$Date_{11}$），PIN_{11}，P_0，N_0

一般用户 $User_{ij}$：S_{ij}，$Cert_i$（Mi，P_i，N_i，ID_i，$Date_i$），$Cert_{ij}$（$User_{ij}$，P_{ij}，$N_{ij\ j}$，ID_{ij},$Date_{ij}$），PIN_{ij}，P_0，N_0

设 A 为发送端，Ma 是 A 的二级管理员，B 为接收端，Mb 是 B 的二级管理员。当两个用户的二级管理员不同时，即两个用户在不同的管理域，但在同一个超级管理员的管辖范围时，需要进行跨越管理域的身份认证。

在实现跨域认证时，需要进行二级管理员证书的传输与认证，这就需要建立跨域身份认证协议，从而实现跨域身份认证。跨域身份认证协议如下：

① A：$Cert_{Ma}$（M_{Ma}，P_{Ma}，N_{Ma}，ID_{Ma}，$Date_{Ma}$），$Cert_A$（$User_A$，P_A，N_A，ID_A，$Date_A$），随机数 R_A→B；

B 使用 p_0 计算 Dp_0（$Cert_{Ma}$（M_{Ma}，P_{Ma}，N_{Ma}，ID_{Ma}，$Date_{Ma}$））得到 A 的二级管理员 M_{Ma} 的公钥 P_{Ma}、模数 N_{Ma}，用户名 ID_{Ma} 及其证书有效期 $Date_{Ma}$，B 对证书有效期进行判断，若已过期则退出连接，若在有效期内则继续执行

B 使用 P_{Ma} 计算 Dp_{Ma}（$Cert_A$（$User_A$，P_A，N_A，ID_A，$Date_A$））得到 A 的公钥 P_A、模数 N_A，用户名 ID_A 及其证书有效期 $Date_A$，B 对证书有效期进行判断，若已过期则退出连接，若在有效期内则继续执行

计算 X=Es_B（R_A）。

② B：$Cert_{Mb}$（M_{Mb}，P_{Mb}，N_{Mb}，ID_{Mb}，$Date_{Mb}$），$Cert_B$（$User_B$，P_B，N_B，ID_B，$Date_B$），X，随机数 R_B→A；

A 使用 p_0 计算 Dp_0（$Cert_{Mb}$（M_{Mb}，P_{Mb}，N_{Mb}，ID_{Mb}，$Date_{Mb}$））得到 A 的二级管理员 M_{Mb} 的公钥 P_{Mb}、模数 N_{Mb}，用户名 ID_{Mb} 及其证书有效期 $Date_{Mb}$，A 对证书有效期进行判断，若已过期则退出连接，若在有效期内则继续执行

A 使用 P_{Mb} 计算 Dp_{Mb}（$Cert_B$（$User_B$，P_B，N_B，ID_B，$Date_B$））得到 B 的公钥 P_B、模数 N_B，用户名 ID_B 及其证书有效期 $Date_B$，A 对证书有效期进行判断，若已过期则退出连接，若在有效期内则继续执行

计算 R_A=Dp_B（X），比较 R_A=R_A'?，若 R_A=R_A'，则继续执行；否则认证失败，退出连接。

③ A：计算 Y=Es_A（R_B）→B；

B 计算 R_B'=Dp_A（Y），比较 R_B=R_B'?，若 R_B=R_B'，则认证成功；否则认证失败。

978-1-935068-06-8 © 2009 SciRes.

4 身份认证方案应用实例

计算机桌面安全防护系统由单机安全防护分系统、网络安全防护分系统和安全管理分系统组成。本文设计的跨域身份认证方案在计算机桌面安全防护系统网络安全防护跨域认证时进行了应用。网络安全防护功能实现基于计算机网络的相关安全防护，包括操作事件伪装、传输加密保护、文件安全传输、网络流量监视等功能。

在传输加密保护和文件安全传输之前，均需要进行身份认证和会话密钥的协商。当两个用户处理不同的二级管理域时，则需要用到跨域身份认证协议，以实现用户身份的鉴别，跨域身份认证应用如图 4 所示。

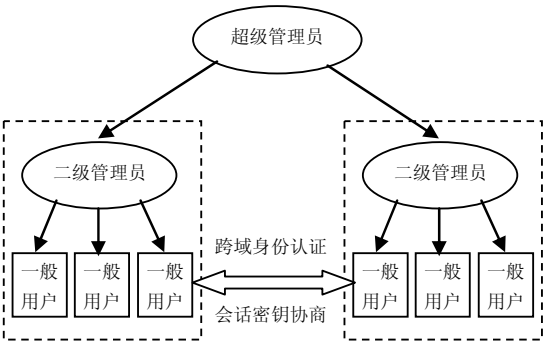

Figure 4. Span field authentication application

图 4. 跨域身份认证应用

5 结束语

本文提出了一种基于公钥证书的跨域身份认证方案，并在计算机桌面安全防护系统网络安全防护跨域认证中得到了应用。本文将公钥证书的思想应用于身份认证方案中，并选择电子钥匙作为存储证书的安全载体，能够较好的保护用户的私密信息和数据完整性。本方案也可用于其他需要身份鉴别的系统。

致谢

在这里首先感谢我的研究生导师信息工程大学的张明清副教授，在我读研期间的悉心指导。同时感谢与我共同完成论文的魏国珩、秦艳琳和廖巍，在论文写作过程中给我很多的帮助和建议。

References (参考文献)

[1] SONG Zhen DOU Wen-hua. New inter-realm authentication protocol and its formalization verification[J].Computer Engineering and Design.2007,(23):31-33.
宋震,李斌,窦文华.新的域间身份认证协议及其形式化验证[J].计算机工程与设计.2007,(23):31-33.

[2] LIU Feng, GAO Dong-ming, CHENG Xue-han. Design of divisible publicly verifiable secret sharing based on electronic cash schemes[J].Journal of Lanzhou University(Natural Sciences) .2007,(6): 75-78.
刘锋,高冬梅,程学翰. 基于可公开认证密钥共享的电子现金系统[J].兰州大学学报(自然科学版). 2007,(6): 75-78.

[3] Ren Jiang-chun, Dai Kui, Wang Zhiying. Research on the trust enhancement for general-purpose computer[J]. Journal of Huazhong University of Science and Technology. 2005,(S1): 308-311.
任江春,戴葵,王志英.通用计算机系统的可信增强研究[J].华中科技大学学报(自然科学版).2005,(S1): 308-311.

[4] WANG Liang, LI Xing-Guo. Research on PMI-based model of EAC exchanging for E-government[J]. Microcomputer Information. 2007,(36):151-153.
王靓,李兴国.电子政务系统属性证书交换模型研究实现[J].微计算机信息.2007,(36):151-153.

[5] WU Jian-wu. Novel remote password authentication scheme based on smart card[J]. Computer Engineering and Applications. 2007,(33):162-164.
吴建武.一种基于智能卡的远程口令认证方案[J]. 计算机工程与应用. 2007,(33):162-164.

[6] MO Xiao-li, SHI Qing-hua. New type of active security management[J]. Computer Engineering and Design. 2005,(5):93-95.
莫笑丽,史清华.一种新型的主动安全管理[J].计算机工程与设计.2005,(5):93-95.

[7] WANG Li-min, LI Yi-fa. Research of identity-based key agreement protocols[J]. Application Research of Computers. 2007,(9): 99-101+104.
王力民,李益发.基于身份的密钥协商协议研究[J]. 计算机应用研究.2007,(9): 99-101+104.

[8] WU Cheng-bo, KOU Ya-nan, TANG Li. Design of embedded network cipher security system based on smart card[J]. Computer Engineering and Design. 2007,(14): 158-161.
吴成波,寇雅楠,汤黎.基于智能卡的嵌入式网络加密安全系统设计[J].计算机工程与设计.2007,(14): 158-161.

[9] Liu Xiu-mei, Zhou Fu-cai, Chang Gui-ran. Improved key exchange protocol for three-party based on verifier authentication [J]. Journal of Southeast University(English Edition), 2008, (3): 72-74.

[10] WU Shu-Hua, ZHU Yue-Fei. Three-Party Password-Based Authenticated Key Exchange with Forward-Security [J]. Chinese Journal of Computers, 2007, (10): 193-201.