文章编号:1000 - 582x(2000)03 - 0062 - 04

Internet/Intranet 环境下的交互式强用户认证系统

秦　拯[1]，付　勇[1]，吴中福[1]，王　康[1]，周　兵[2]
（1. 重庆大学 网络中心，重庆　400044；2. 重庆商学院，重庆　400031）

摘　要：企业需要在 Internet/Intranet 环境下安全从事商务活动，用户认证是确保其安全性的基本前提。笔者通过对现有用户认证方法和协议的研究，在 Kerberos 协议的基础上，提出了一种基于数字证书与灵巧卡的、采用公钥密码体制的交互式强用户认证系统。该系统在满足交互式实时认证的速度要求的前提下，简化了密钥的管理、分配、存贮问题，也减轻了客户端的负担，较好地解决了 Kerberos 协议存在的几个不足。

关键词：认证 / 因特网；数字证书；灵巧卡；公钥密码体制
中图分类号：TP 393.08　　文献标识码：A

近年来，全球电子商务伴随因特网的发展而爆炸性增长。以 Internet 的 TCP/IP 协议和 WEB 技术为基础的 Intranet 也日益成为企业构网的最佳模式。Forester Research 预测到 2002 年，美国电子商务市场的交易额将达 2 万亿美元。在国内，因特网用户今年年初已达 210 万，约半年翻一番，电子商务也已在各地兴起。企业网上商务活动必将应势而上。国内一些大中型企业纷纷构建 Intranet 或用 Intranet 改造传统企业网络，并与 Internet 相连。企业选择 Internet/Intranet 作为商务平台，其主要原因是有利于各企业提高竞争力、帮助与雇员、顾客和商业伙伴建立紧密关系，降低从事商务活动的费用。然而当 Intranet 与 Internet 互连时，由于 Internet 固有的安全风险，诸如非授权用户访问、数据篡改和窃听等，因而，为防止受到攻击，保护企业至关重要的商务信息，必需一个强有力的安全解决方案。企业在 Internet/Intranet 环境下，尤其是从事商务活动时，正如国外一些安全专家所认为的那样——若没有以强用户认证作为基本前提，那么其他的安全方法，如加密和访问控制等，都将变得无效[1]。

1　认证与强用户认证

认证(Authentication)又称为鉴别、确认，它是认证某人或某事是否名副其实或是否有效的过程。认证的基本思想是通过验证称谓者的一个或多个参数的真实性与有效性，以达到认证的目的。认证的主要目的有二，即信源识别与信息完整性验证。安全可行的认证系统常建立在密码学的基础上，并结合数字签名技术。

用户认证可以识别合法用户和非法用户，从而阻止非法用户访问系统。用户认证往往是许多应用系统中安全保护的第一道设防，它的失败可能导致整个系统的失败。

强用户认证(Strong User Authentication，简称 SUA)通常依靠下述可能方法中的两种：① 用户保存的某些东西，如令牌和灵巧卡；② 用户知道的某些东西，如口令或个人识别号(PIN)；③ 用户唯一的某些专有特征，如可由生物统计学方法证实的指纹或视网膜扫描。SUA 的一个最大好处是迫使用户具有责任心，使得某个组织可以知道那些用户在进行什么活动。与允许用户共享口令且容易破解的单要素用户认证方法不同，SUA 方法(如 PIN + 灵巧卡)虽存在用户共享认证方法的问题，但共享的结果是，当另一用户在使用 SUA 方法时，原始用户就不能访问网络。口令易被泄露或破解，引起用户否认；而 SUA 则可使一个组织准确认定谁在访问网络，因为该用户拥有两个要素。

2　用户认证协议

· 收稿日期：1999-08-28
基金项目：宗申基金资助、重庆市科技攻关项目
作者简介：秦　拯(1969-)，男，湖南祁东人，重庆大学博士生，主要研究方向为计算机网络与通信、网络安全。

2.1 用户认证协议的研究现状简介

国外至今已提出多种用户认证协议，但其中大部分在安全性与可行性方面不能令人满意，且密钥的管理、分配、存储也是一个严重问题。A. Shamir 于 1984 年提出了"基于身份的密码系统"这一概念[2]后，出现了各种类型的用户认证协议。Okamoto 提出了基于身份的密钥分配协议[3]；Ohta 发展了 Okamoto 协议用于身份认证[4]；Tsujii 利用离散对数也提出了基于身份的认证协议[5]；Harn 和 Yang 提出了一种集用户认证、数字签名、密钥分配为一体的协议[6]。然而，上述这些协议均有不足之处[7]。

著名的 Kerberos 协议[8]是 MIT 开发的用户认证协议，采用基于数论的对称密钥体制。由于 Kerberos 的设计毕竟是与 MIT 校园网环境相结合的产物，将它推广到 Internet/Intranet 这样一个分布式环境依然有其局限性[9]。首先，原有的认证码很有可能被存储或替换；其次，认证码的正确性是基于网络中所有的时钟保持同步，然而大多数网络的时间协议都不安全，这将在分布式网络环境中导致极为严重的问题；再次，Kerberos 防止口令猜测的能力也很弱。

尽管 Kerberos 协议存在一些局限性，然而因其设计风格优美，简单易行，且已有丰富的应用背景，因而被多方采用；而且一些对安全性要求较高的网络环境也采用了 Kerberos 协议，如 OSF(Open Software Foundation)于 1991 年推出的 DCE(Distributed Computing Environment)的认证就采用了它。笔者拟在 Kerberos 协议基础上引进公钥密码体制以适用于 Internet/Intranet 环境下的 SUA.

2.2 Kerberos 用户认证模型简介

Kerberos 用户认证模型如图 1 所示。

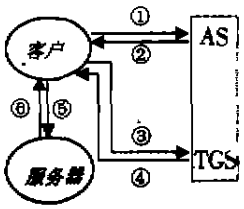

图 1　Kerberos 用户认证模型

图中：① C，TGS，t_{exp}，r；② $\{K_{C,TGS}, t_{exp}, r\} K_C$，$\{TGT\} K_{TGS}$；③ $\{TS,---\} K_{C,TGS}$，$\{TGT\} K_{TGS}$，S，t_{exp}，r；④ $\{K_{C,S}, S, t_{exp}, r\} K_{C,TGS}$，$\{T_{C,S}\} K_S$；⑤ $\{TS, CK, k\} K_{C,S}$，$\{T_{C,S}\} K_S$；⑥ $\{TS+1\} K_{C,S}$；TGS、AS 分别为票据授权服务中心和认证服务中心；K_C，K_S分别为用户 C，服务器 S 与 AS 共享的密钥；K_{TGS}是 TGS 的密钥，$K_{C,S}$是 C 和 S 的会话密钥；TS 是 AS 盖的时戳，CK 是校验和；$\{M\}K$ 表示用密钥 K 按单钥体制加密 M；t_{exp}为验证最后期限，r 为随机数；$K_{C,TGS}$是 C 与 TGS 的共享密钥；k 是用于其他交换的子会话密钥。

当 Client(简称 C)需要与 Server(简称 S)进行认证时，基本过程如下：1) C 向 AS 发送自己的身份信息，申请许可票据服务；2) AS 随机产生一个 KC，TGS 和一个 TGS 的票据证明，并将它们加密后传给 C；3) C 在本地用 KC 解密得到 KC，TGS，然后用票据证明访问 TGS，并请求访问 S 的票据证明；4) TGS 验证票据并向 C 签发服务票据；最后，C 与 S 相互认证。

3 Internet/Intranet 环境下一种强用户认证系统

3.1 选择认证方法

在构建 SUA 系统时，必须先选择合适的认证方法。尽管生物统计学方法可提供最高强度的用户认证，但目前技术上尚不成熟，且代价昂贵，因而这种方法现在不实用。笔者拟采用在电子商务中起关键作用的数字证书(Digital Certificate)，并与技术成熟、实用的灵巧卡(Smart Card)组合在一起共同完成 Internet/Intranet 环境下的 SUA。

数字证书是一份加密文件，其中包含了用户凭证(如用户公开密钥)及用户识别证明(如 PIN)，它是公钥密码体制的重要组成部分，已被电子商务广为采用。数字证书可提供比口令更好的安全性，但它不能提供 SUA，不能解决用户认证的根本问题[10]。对数字证书的颁发常根据用户名和口令进行，这样，能够访问用户工作站并具有口令的闯入者将能冒充该用户。根据口令而颁发的数字证书很像没有本人照片的护照。笔者将采取一定的策略，使数字证书的颁发避开口令操作。

灵巧卡不同于磁卡，磁卡不具备数据处理能力及数据保护机制，而灵巧卡的集成电路中包括 CPU、E2PROM、RAM、ROM 和 COS(Chip Operating System)，可以封装成各种便于人们携带的形式，可从最简单的单张卡片复杂到袖珍计算机。灵巧卡同时具有数据存储和处理能力，可进行复杂的加密、解密、签名、验证签名、认证等操作，可以采用复杂的认证协议。灵巧卡可用于贮存用户的秘密密钥，当与数字证书或 PIN 一起使用时，可提供 SUA 并优化基于公钥密码体制的安全性。

3.2 强用户认证系统

基于前文的分析，本节将在 Kerberos 协议的基础上，提出一个基于数字证书及灵巧卡的、采用公钥密码体制的交互式 SUA 系统。如同 Kerberos 认证模型，本

系统需要可信赖的第三方参加。第三方包括 KDC(Key Distributing Center)及 AS(Authentication Server)。KDC 和 AS 各有一对密钥,PM 表示 M 的公开密钥,S M 表示 M 的秘密密钥。为解决 Kerberos 协议存在的时间同步问题,本系统由用户自己加盖时戳(Timestamps)来代替一次性使用随机数(Nonces),从而可有效防止重播攻击(Replay Attack)[11]。

本系统采用 RSA 公钥密码体制的一种变形—Yaksha 体制[12]。Yaksha 体制也以(e_i, n_i)为公开密钥,但要求两个不同的秘密密钥:用户密钥 d_{ui} 和 Yaksha 服务器密钥 d_{vi},它们与原来的 RSA 的 d_i 有关,即 $d_{ui} \times d_{vi} = d_i \bmod n_i$,每个用户 i 有自己的 d_{ui}。同时,Yaksha 服务器保留相应的 d_{vi},并且两者不能相互推知。这里以 AS 作为 Yaksha 服务器,(e_i, n_i)表示 Yaksha 公开密钥,d_{vi}表示 KDC 传给 AS 的密钥。

3.2.1 初始化协议

用户首先向 KDC 发出联网申请,提交 AS 的名字和自己的公开密钥。KDC 验证其合法性并签署证书,向用户发送 Yaksha 公开密钥、秘密密钥、有效期以及用户 PIN 等信息;同时,将相应的 Yaksha 公开密钥、服务器秘密密钥等信息发送给 AS。用户得到证书并解密,然后向 AS 递交证书、PIN 等来证明自己的身份。初始化协议如下:

① KDC→A: $CertA = E_{SKDC}[ID_A, (e_a, n_a)$,有效期, EPA [daa]]

KDC AS: $E_{PAS}[ID_A, (e_a, n_a)$,有效期, day]

② A→AS: ID_A, KDC, CertA

其中,$E_K[M]$表示按 RSA 体制用 K 加密 M,ID_A 是 KDC 分配给 A 的名字代号,有效期给用户规定 Yaksha 公开密钥及秘密密钥的使用时间。任何人都可用 KDC 的公开密钥验证证书的合法性,但没有 KDC 的秘密密钥不能伪造或篡改证书。

初始化协议完成:1)用户访问 AS 并获得 Yaksha 密钥,用于实时认证;2)不键入口令,从而避免了口令所带来的安全问题;3)初始化定期进行,用户的密钥由灵巧卡存储并定期更换,这样也解决了密钥贮存与管理方面的问题。

3.2.2 交互式实时认证

用户 A 联网后,可以同已连网的用户 B 进行通信,执行以下实时认证协议:

① A→B: $ID_A, (T_a, ID_B)^{d_{aa}} \bmod n_a$

② B→AS: $(T_a, ID_B)^{d_{bb}} \bmod n_b$, $(T_b, ID_A)d_{bb} \bmod n_b$

③ AS→A: $(ID_B, T_b, T_a, K_{ab})\ d_{vi} \times e_i \bmod n_a$

AS→B: $(ID_A, T_a, T_b, K_{ab})\ d_{by} \times e_b \bmod n_b$

④ A→B: $\{T_b\}K_{ab}$ B→A: $\{T_a\}K_{ab}$

其中,$(M)^K$表示按 RSA 体制用 K 加密消息 M,$\{M\}_K$则表示按单钥体制用 K 加密消息 M,以提高加速度。T_a、T_b分别是 A、B 自己加盖的时戳。由于 T_a、T_b 是时间的函数,因而能有效的防止明文攻击。

在上述协议初始化和交互式实时认证过程中,用户 A、B 是采用灵巧卡完成签名、验证、加/解密、保存 Yaksha 公开密钥(e_i, n_i)与用户的秘密密钥 d_{ui}。

3.3 强用户认证系统安全性分析

上文提出的交互式 SUA 系统由于采用了双要素认证,具有很高的安全性。同时,在 Kerberos 认证模型的基础上引进了 Yaksha 体制的先进思想,将单钥体制与公钥体制进行了有机结合、简化了认证"手续",减少了认证次数,确保了较高的加密速度,较好地解决了 Kerberos 协议存在的几个不足。用户联网时不需要键入口令,使安全性得以提高;用户在认证过程中亲自加盖时戳,解决了 Kerberos 协议存在的时间同步问题,有效防止了重放攻击及已知明文的攻击。用户在客户端引入灵巧卡,不仅大大提高了 Internet/Intranet 环境下系统的安全性,而且使得密钥的管理、分配、存贮问题得以简化,也减轻了客户端的负担;而且,当需要改动加解密算法时,没有必要对客户端系统进行升级,只需对灵巧卡进行相应的改动即可。

4 结束语

企业在 Internet/Intranet 环境下从事商务活动必须解决安全性,而解决的前提和基础是采用 SUA 方法。为此,本文在 Kerberos 协议的基础上结合 Yaksha 体制的先进思想,在客户端引用灵巧卡,提出了一种安全、高速、简单易行的交互式 SUA 系统。Forrester Research 公司指出,有关厂商正计划将灵巧卡阅读器与 PC 机或膝上机"捆绑"提供给用户,这将导致使用灵巧卡的代价大大降低,基于灵巧卡的 SUA 系统也必将被广泛采用。

参 考 文 献

[1] ITSS PRICE WATER HOUSE COOPERS. The case for strong user authentication[EB/OL]. http://www.utexas.edu/computer/rcl/journals.html.

[2] SHAMIR A. Identity-based cryptosystem and signature schemes [A]. SALTZER J H. Crypto 84. Santa Barbara[C]. CA: Spring-Verlag, 1984: 47 ~ 53.

[3] OKAMOTO E、TANAKE K. Key distribution system based on

identification information [J]. IEEE J Select Areas Comm, 1989,7(4):481 ~ 485.

[4] OHTA K. Efficient identification and signature schemes[J]. Electtron Lett,1988,24(2):115 ~ 116.

[5] TSUJJ S, ITOH. An ID-based cryptosystem based on the discrete logrithm problem[J]. IEEE J Select Areas Comm,1989,7(4):467 ~ 473.

[6] HARN L, YANG S B. ID-based cryptographic schemes for user identification, digital signature, and key distribution[J]. IEEE J Select Areas Comm.1993,11(5):543 ~ 549.

[7] LEE WEI-BIN, CHANG CHIN-CHEN. Three-based information security functions[J]. Corp Comm.1997(20):36 ~ 41.

[8] MILLER S P, NEUMAN C, SCHILLER J I, et al. Kerberos Authentication and Athorization System[P]. America: MIT, Cambridge, Mass, July, 1987.

[9] INFORMATION SECURITY GARTER GROUP. The role of certificate authorities in information security[EB/OL]. http://www.mcom.com/info.

[10] BELLOVIN S M, MERRIT M. Limitation of the kerberos authentication system[J]. ACM SIGCOMM Computer Comm Review, 1990,20(5):119 ~ 132.

[11] NEUMAN B C, STUBBLEBINE S G. A note on the use of timestamps as nonces[J]. ACM SIGOPS Operating System Review, 1993,27(2):10 ~ 14.

[12] GANESAN R. The Yaksha security system. Comm of the ACM,1996,39(3):55 ~ 60.

A Mutual Strong User Identification System in Internet/Intranet

QIN Zheng[1], *FU Yong*[1], *WU Zhong-fu*[1], *WANG Kang*[1], *ZHOU Bing*

(1. Network Research Center of Chongqing University, Chongqing 400044, China;
2. Chongqing Commercial College, Chongqing 400031, China)

ABSTRACT: An enterprise needs electronic commerce in Internet/Intranet environment whose security depends basically on User Identification. After studying on present identification methods and protocol, we present, in this paper, a mutual Strong User Identification system based on Kerberos protocol, public key cryptosystem, digital certificate and smart card. Several limitations of Kerberos protocal are overcome. This system satisfies the speed requirement of mutual real-time identification. Moreover, it can simplify the actions of key management, distribution and storage, relieves the client's burden.

KEYWORDS: identification / Internet; digital certificate; smart card; public key cryptosystem

(责任编辑　吕赛英)

·下期论文摘要介绍·

小波滤波器的统一构造方法与软件

严 中 洪

(重庆大学 机械工程学院,重庆　400044)

摘　要：尽管小波分析与应用已十分深入,特别是紧支集上的小波变换已广泛应用在信号处理,如图象压缩、声音处理、文字识别等领域,但小波基或小波滤波器的构造却是一件十分艰苦的工作,它揭示了紧支集上任意长度正交小波基滤波器统一的解析结构。一种有限步递归构造分解方法可以非常容易地计算出任意多个参数的正交小波基滤波器参数。此后并验证了 Daubechies 等人的小波滤波器的构成参数,以及验证了已在具体应用中发挥重要作用的一些滤波器。小波滤波器的解析构造使得动态选择小波基变得极其容易,这一结果必将在小波理论及应用方面产生积极的作用。