一种分布式网络环境下单点登录模型①

任传伦[1,2]，李忠献[1,2]，钮心忻[1]，杨义先[1]

[1](北京邮电大学 网络与信息攻防技术教育部重点实验室，北京 100876)
[2](天津市国瑞数码安全系统有限公司，天津 300384)

摘 要：提出一种基于 USB Token 和数字证书的分布式网络下的身份认证协议，它能够实现分布式网络环境下的单点登录功能，并且对重放攻击是安全的，保证了用户身份的真实性和用户票据的保密性。

关键词：密码；单点登录；身份认证；密码攻击；安全分析

Single Sign-On Model in Distributed Network

REN Chuan-Lun[1,2], LI Zhong-Xian[1,2], NIU Xin-Xin[1], YANG Yi-Xian[1]

[1](Key Laboratory of Network and Information Attack & Defence Technology of MOE, Beijing University of Posts and Telecommunications, Beijing 100876, China)
[2](Tianjin National Cybernet Security Limited, Tianjin 300384, China)

Abstract: An USB Token & Certificate-Based Authentication Protocol (TCBAP) was proposed, which implements single sign-on in distributed network and is secure against replay attacks. It ensures authenticity of users' identity and the privacy of users' ticket.

Keywords: cryptography; single sign on; authentication; attack; security analysis

1 引言

如何使一个内部用户既能访问到处于不同地理位置的、不同业务、不同级别的系统又能得到相应的权限控制，是电子政务应用系统建设中需要解决的一个重要课题，在这样的应用环境中，安全的单点登录显得尤其迫切。

借助安全的单点登录系统，用户仅仅需要记住一个口令即可在登录到一个应用系统后访问所有有权限的应用系统而不需要重新登录。

当前的单点登录系统，无论是国外 CA 公司的 eTrust、RSA 公司的 clearTrust、HP 公司的 Select Access，还是在[1-7]中提及的单点登录，存在着以下的缺陷：

* 要么单点登录仅局限于局域网环境，不适于电子政务下分布式的广域网环境；

* 要么使用的是弱认证方式，在电子政务中应该使用受密码保护的强认证方式；

本文提出了一种基于数字证书高强度认证协议的单点登录模型。该模型不但适用于电子政务大规模的分布式的广域网环境，而且大大满足了电子政务的安全需求：不仅采用了受高强度密码保护的强认证方式，而且对重放攻击是安全的。

2 单点登录模型

针对网络环境下的身份认证，人们提出了多种方法，主要有以下几种：

(1) 基于口令的用户身份认证

基于口令的用户身份认证一直是分布环境中最广泛使用的一种认证方法。但不幸的是，它对于重放攻击和字典攻击[8]没有抵抗力。到现在为止，人们已经提出了多种基于口令认证的方案[8-19]，但是这些方案所运用的技术并不比公钥密码体制[20]和 Diffie-Hellman

① 基金项目:国家重大科技专项(2009ZX03004-003-03);国家高技术研究发展计划(2007AA01Z430)
收稿时间:2010-05-24;收到修改稿时间:2010-07-06

密钥交换技术[20,21]更先进，而且它们还对整个系统造成了更加严重的计算开销。

(2) S/key[22]认证

每一次认证时系统产生的一次性口令不同,这样即使口令被窃听也无关紧要。然而使用 S/key 的用户需输入一次性口令，因而使用起来比较烦琐。

(3) Kerberos 身份认证

在分布式计算环境下，用户访问系统时的位置是可变的，同时用户所要访问的系统资源也不是固定的。Kerberos 给出了一种具有较高安全性能的用户身份认证和资源访问认证的机制。但是文献[23]指出了 Kerberos 存在的安全缺陷，而且这种协议的使用需要复杂的设置。

此外，还有基于智能卡的身份认证和基于 X.509 数字证书[24]的身份认证。本文中，我们基于单点登录的目标，结合公钥和对称密码技术，提出了一种基于 USB Token 和 X.509 数字证书的认证协议(Token&Certificate-Based Authentication Protocol)，以下简称 TCBAP 协议。每个需要认证的用户持有一个储存有本人数字证书的 USB Token，用户登录应用系统时仅需输入 USB Token 的保护 PIN 码即可登录。这个协议能够实现系统用户的单点登录，对重发攻击是安全的，能够保证用户身份信息的真实性和身份票据的保密性。

2.1 符号说明

本文中用到下列符号：

A 用户的身份标识，其中包含用户所在地信息。

S_L 本地认证服务器的身份标识。

S_R 异地认证服务器的身份标识，与用户不属于同一地区。

I_A 用户 A 的个人信息。

R 随机数。

$Cert_A$ 用户 A 的数字证书。

$E_K(m)$ 使用公钥为的 RSA 算法对明文 m 加密。$D_{K^{-1}}(c)$ 使用私钥为 K^{-1} 的RSA算法对密文C解密。$S_{K^{-1}}(m)$ 使用私钥 K^{-1} 为的RSA 算法对明文m签名。$V_K(c)$ 使用公钥为的RSA 算法对签名信息C进行签名验证。

$F(m)$ 对消息 m 进行置换的置换函数。$F_i(m)$ 等价于 $\underbrace{F(F(F(...F(m)...)))}_{i次}$。

T_A 用户 A 通过身份认证后的身份票据，表明用户已经成功登录。该身份票据是动态变化的。$I(m)$ 通过对 m 和用户个人信息利用分组加密算法进行加密运算，产生用户的身份真实性信息，即证明该用户确实是他所宣称的身份，而不是假冒者。

$X \Rightarrow Y : M$ 从 X 向 Y 发送信息 M。

2.2 符号说明

TCBAP 协议包括两个阶段，认证阶段和身份真实性验证阶段。当用户登录应用系统时，执行身份认证过程；而当用户访问系统资源时，执行身份真实性验证过程。

2.2.1 身份认证阶段

用户在本地和异地登录应用系统时，用户需要与本地认证服务器和异地认证服务器进行信息交互，因此本文将其分为本地认证和异地认证阶段。

(1) 本地认证阶段

当用户在本地登录应用系统时，用户和本地认证服务器之间运行挑战-应答协议。图 1 表示 TCBAP 协议的本地认证阶段。

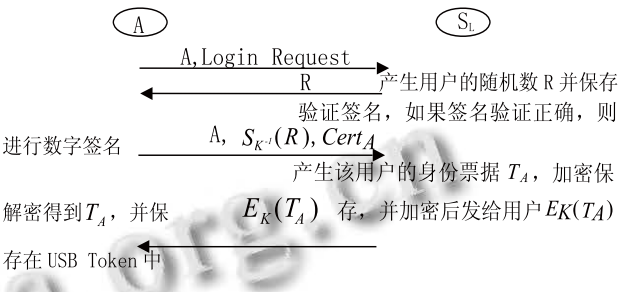

图 1 TCBAP 的本地认证阶段

具体认证过程如下：

① Login Request

用户向服务器发出登录请求。

② $S_L \Rightarrow A$： R 认证服务器 S_L 产生用户随机数 R，发送给 A，并在服务器中保存该随机数。

③ $A \Rightarrow S_L$： A，$S_{K^{-1}}(R)$，$Cert_A$ 用户对该随机数进行签名，并将用户的身份信息、签名信息以及公钥证书(A，$S_{K^{-1}}(R)$，$Cert_A$)发往认证服务器 S_L。

认证服务器 S_L 对用户的签名验证，如果签名验证正确，则产生该用户的身份票据 T_A，加密保存在服务器，并将密文 $E_K(T_A)$ 发给用户；如果用户签名不正确，则用户认证失败，不能登录。

④ $S_L \Rightarrow A$： $E_K(T_A)$

用户收到认证服务器 S_L 发来的信息 $E_K(T_A)$，解密后得到身份票据 T_A，并将其保存在用户 USB Token 中。

(2) 异地认证阶段

具体认证过程如下：

① $A \Rightarrow S_R$： A,Login Request

用户 A 向异地认证服务器 S_R 发出登录认证请求。

② $S_R \Rightarrow A$： R

认证服务器 S_R 产生用户随机数 R，将其发送给 A，并在服务器中保存该随机数。

③ $A \Rightarrow S_R$： A， $S_{K^{-1}}(R)$，Cert_A

用户对随机数签名，将用户身份信息、签名信息以及公钥证书(A, $S_{K^{-1}}(R)$,Cert_A)发往异地认证服务器 S_R。

异地认证服务器 S_R 判断如果用户登录的是异地认证服务器，那么通知用户重定向到本地认证服务器进行身份认证。

④ $S_R \Rightarrow A$：Redirection

异地认证服务器通知用户重定向。

⑤ $A \Rightarrow S_L$： A， $S_{K^{-1}}(R)$，Cert_A

用户收到重定向通知后，将用户认证信息重新发往用户的本地认证服务器 S_L。随后的过程如本地认证阶段所述。

⑥ $S_L \Rightarrow A$： $E_K(T_A)$

本步骤的处理同本地认证步骤的第四步。

2.2.2 身份真实性验证阶段

用户通过身份认证登录到应用系统后，每次访问系统资源都需要验证用户身份的真实性，即系统需要确认请求访问系统资源的用户确实是他宣称的身份，以防止非法用户假冒用户身份进行非法操作。

(1) 本地身份真实性验证阶段

用户访问本地系统资源时的身份真实性验证如图 3 所示。

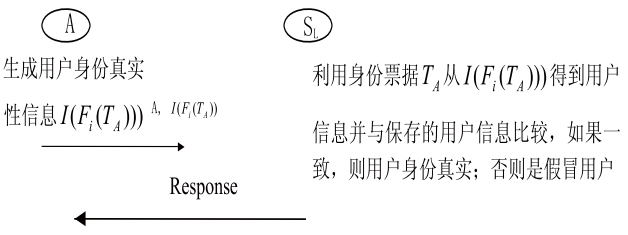

图 3　TCBAP 的本地身份真实性验证阶段

具体验证过程如下：

① $A \Rightarrow S_L$： A, $I(F_i(T_A))$

用户利用保存在 Token 中的身份票据 T_A 和身份信息，得到用户身份真实性信息 $I(F_i(T_A))$ 发到本地认证服务器。

② $S_L \Rightarrow A$：Response

认证服务器 S_L 安全的利用用户票据从 $I(F_i(T_A))$ 得到用户信息并与保存的用户信息比较，如果一致，则用户身份真实，返回应答允许用户访问系统资源；否则是假冒用户，返回应答信息，要求用户进行身份认证，因此转到本地身份认证。

(2) 异地身份真实性验证阶段

用户访问异地系统资源时的身份真实性验证如图 4 所示。

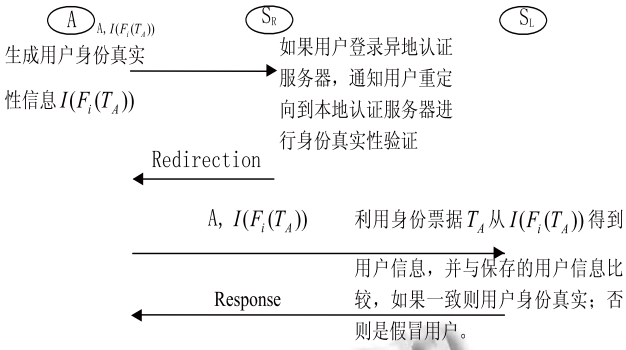

图 4　TCBAP 的异地身份真实性验证阶段

具体验证过程如下：

① $A \Rightarrow S_R$： A, $I(F_i(T_A))$

用户利用保存在 Token 中的身份票据 T_A 和身份信息，得到用户身份真实性信息 $I(F_i(T_A))$ 发到异地认证服务器。

异地认证服务器 S_R 收到身份真实性信息后，判断如果用户登录的是异地认证服务器，通知用户重定向到本地认证服务器。

② $S_R \Rightarrow A$：Redirection

异地认证服务器发送给用户重定向请求。

③ $A \Rightarrow S_L$： A, $I(F_i(T_A))$

用户收到重定向通知后，将用户身份真实性信息重新发往用户的本地认证服务器 S_L。随后的过程如本地认证阶段所述。

④ $S_L \Rightarrow A$：Response

该处理同本地身份真实性验证的第二步。

3 安全性分析

下面我们讨论模型对单点登录的可适用性，评估 TCBAP 协议中用户身份的真实性和用户身份票据的保密性，以及对重放攻击的安全性。

3.1 模型对单点登录功能的适用性

当用户登录成功后，就获得了一个该用户的有效的登录票据，即保存在 Token 中的身份票据 T_A。当用户登录另外一个不同的应用系统时，按照第 2.2.2 节所述，用户与认证服务器之间会运行一个对用户透明的交互协议，如果该用户是合法的，那么不需要用户作任何操作即可登录到另外一个应用系统，既实现了单点登录。

3.2 用户身份的真实性

在 TCBAP 协议中，我们使用的 RSA 算法和对称密码算法在计算上是安全的。因而攻击者无法获得用户的私钥信息，从而无法在认证阶段假冒用户的签名。在身份真实性验证阶段，密码算法的安全性也使攻击者无法通过获得用户的身份票据假冒用户身份，从而用户身份的真实性能够得以保证。

3.3 身份票据的保密性

身份票据是在密码卡内产生的，身份票据出卡后都是以密文的状态存在：

在服务器端，攻击者无法解密票据；

在发往用户的过程中，身份票据是以用户的公钥加密的，RSA 算法的安全性使得只有该用户能够解密；

在用户端，该身份票据是保存在 USB Token 中，非法用户没有办法得到它；

因此 TCBAP 保证了用户身份票据的保密性。

3.4 重放攻击

在用户身份认证阶段，假设攻击者截获到用户的身份认证信息(A，$S_{K^{-1}}(R)$，$\mathrm{Cert_A}$)，并重新发送到认证服务器。认证服务器取不到随机数(用户登录成功后，用户的随机数被删除)，所以拒绝该攻击者的登录请求，攻击者的重发攻击失败。

在身份真实性验证阶段，假设攻击者在用户进行第次身份认证时，截获到发送到认证服务器的身份真实性信息 A，$I(F_i(T_A))$，并重新发送到认证服务器企图登录。但是由于服务器端保存的用户身份票据已经变化，所以认证服务器不能从 $I(F_i(T_A))$ 得到用户真正的个人信息，从而身份真实性验证失败，攻击者无法访问系统资源。

总之，攻击者没有机会利用重发攻击假冒的身份登录和使用应用系统。

4 结论

本文给出了一种能够实现安全单点登录的协议模型，它对重放攻击是安全的，能够保证用户身份的真实性和身份票据的保密性，而且最大程度地减少了用户的负担，对于电子政务的安全应用不失为一种好的解决方案。

参考文献

1 Furukawa J, Sako K, Obana S. IC card-based single sign-on system that remains secure under card analysis. Proc. of the 5th ACM workshop on Digital identity management, 2009. 63－72.

2 van der Horst TW, Seamons KE. Simple authentication for the web. Proc. of the 16th International Conference on World Wide Web, 2007. 1217－1218.

3 Fleury T, Basney J, Welch V. Single sign-on for Java Web start applications using MyProxy. Proc. of the 3rd ACM workshop on Secure web services SWS'06. November 2006. 95－101.

4 黄琛,李忠献,杨义先,等.一种新的兼容多种身份认证方式的 Web 单点登录方案.北京邮电大学学报,2006,29(5):130－134.

5 毛捍东,张维明.一个基于 Web 服务的单点登录系统.计算机工程与应用,2004,40(24):18－20,50.

6 邱航,权勇.基于 Kerberos 的单点登录系统研究与设计.计算机应用,2003,23:142－144.

7 任栋,刘连忠.一种 WEB 应用环境下安全单点登录模型的设计.计算机工程与应用,2002,38(24):174－176,256.

8 Abdalla M, Bresson E, Chevassut O, et al. Provably secure password-based authentication in TLS. Proc. of the 2006 ACM Symposium on Information, Computer and Communications Security ASIACCS'06, March 2006. 35－45.

9 Ku WC. A hash-based strong-password authentication scheme without using smart cards. ACM SIGOPS Operating Systems Review, January 2004,38(1):29－34.

10 Bellovin SM, Merritt M. Encrypte key exchange: Password-based protocols secure against dictionary attacks. Proc. of IEEE Symposium on Research in Security and Privacy, 1992. 72－84.

11 Bellovin SM, Merritt M. Augmented encrypted key exchange: A password-based protocols secure against dictionary attacks and password file compromise. Proc. of ACM Conf. Comp. & Comm. Security. 1993. 244－250.

12 Gong L, Lomas M, Needham R, et al. Protecting poorly chosen secrets from guessing attacks. IEEE J. Sel. Areas Commun., 1993,11(5):648－656.

13 Gong L. Optimal authentication protocols resistant to password guessing attacks. Proc. 8th IEEE Computer Security Foundation Workshop. 1995. 24－29.

14 Steiner M, Tsudik G, Waidner M. Refinement and extension of encrypted key exchange. ACM Operating Systems Review, 1995,29(3):22－30.

15 Jablon D. Strong password-only authenticated key exchange. ACM Computer Communications Review, 1996,20(5):5－26.

16 Jaspan B. Dual-workfactor encrypted key exchange: Efficiently preventing password chaining and dictionary attacks. Proc. Sixth Annual USENIX Security Conference. 1996. 43－50.

17 Kwon T, Kang M, Song J. An adaptable and reliable authentication protocol for communication networks. Proc. IEEE INFOCOM'97. 1997. 737－744.

18 Kwon T, Kang M, Jung J, et al. An improvement of the password-based authentication protocol (K1P) on security against replay attacks. IEICE Trans. Commun., 1999, E82-B(7), 991－997.

19 Kwon T, Song J. Secure agreement scheme for gxy via password authentication. Electron. Lett., 1999,35(11):892－893.

20 Diffie W, Hellman ME. New directions in cryptography. IEEE Trans. Inf. Theory, 1976,IT-22(6):644－654.

21 Diffie W, Hellman ME. Multiuser cryptographic techniques. Proc. of AFIPS National Computer Conference, 1976:109－112.

22 Haller NM. The S/KEY One-time Password System. RFC 1760, 1995.

23 Bellovin SM, Merritt M. Limitation of Kerberos authentication system. ACM Computer Communications Review, 1990,20(5):119－132.

24 Housley R, Polk W, Ford W, Solo D. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Internet Engineering Task Force Request For Comments 3280, IETF Website, 2002. http:// www. ietf. org/rfc/rfc3280.txt.