基于图像认证的个性化用户认证方法研究*)

陈 龙[1,2] 蒋 溢[1] 江 伟[1]
(重庆邮电大学 计算机科学与技术学院 重庆 400065)[1]
(西南交通大学 信息科学与技术学院 成都 610031)[2]

摘 要 普适计算是未来的计算模式,人们可以随时、随地获得满意的服务。结合未来普适计算环境下设备的多样性和用户的个性化需求,对图像认证方法进行了扩展进而提出个性化认证方案,图像认证方法利用用户对图片的识别能力验证登录者是否为用户本人,从而可以抵抗重放攻击。该认证方案使用一种组合办法既减少每次认证暴露给第三方的信息,又提高了安全性,同时可提供多种媒体形式供用户识别,实验结果与分析表明该方法是可行的,用户可以接受这种认证方式。

关键词 图像认证,用户认证,基于知识的认证,网络安全,普适计算

Study on Personal User Authentication Method Based on Photographic Authentication

CHEN Long[1,2] JIANG Yi[1] JIANG Wei[1]
(College of Computer Sci. & Tech., Chongqing Univ. of Posts and Telecoms., Chongqing 400065)[1]
(School of Information Sci. & Tech., SouthWest JiaoTong University, Chengdu 610031)[2]

Abstract Pervasive computing is a computing paradigm for future, in which a user can get satisfied service at anytime and anywhere. Considering trends of user personalization and device diversity, a personal user authentication method by extending the photographic authentication method is proposed. Photographic authentication identifies the right user by user's ability to recognize personal photographs, so it can withstand replay attacks. This method can reduce information exposure and enhance system security with a combinatorial choosing objects scheme. Experimental results and security analysis show that this method is acceptable and viable. It can reasonably withstand replay attacks.

Keywords Photographic authentication, User authentication, Knowledge-based authentication, Network security, Pervasive computing

1 引言

用户认证是用来防止计算机系统(其他应用系统)被非授权用户使用或侵入的技术手段,属于系统安全的第一道防线。

用户认证的关键是核实用户提供的身份是否真实。一般而言,有三种类型的认证用户身份的基本方法:(1)用户知道的(秘密信息如:口令、个人识别号(PIN)或密钥),(2)用户拥有的(令牌如:银行卡或智能卡),和(3)用户本身的(生物特征如:语音特征、笔迹特征或指纹)。这些方法可以单独使用或联合使用。

这些认证方法有各自的优点和缺点。如用户口令通过网络传输时可能被第三者拦截并冒充该用户。一些公共场所的因特网访问点为人们上网提供了方便,但也为使用的人们带来了相当的安全风险。例如,一个攻击者可能会有意识地修改公用系统以截获用户的击键序列从而获得密码。问题还不止这些,许多网络服务系统或网站使用不频繁,用户非常容易忘记密码,结果是用户使用弱密码或使用相同的密码。

Pering[1]等人提出了图像认证(photographic authentication)方案增强在使用不可信终端访问因特网时的安全性。图像认证方法依赖于一个用户识别出个人图片的能力,系统给出若干组图片,用户从每组挑选出属于自己的一张图片(每组还有若干不属于该用户的图片)。虽然这种方案在数学意义上不如多字符密码安全,但是图像认证方法在用户每次登录时都用了不同的图片组合,可以抵抗重放攻击行为。

针对图像认证方案面临的挑战,应用相同的基本原理,本文设计了一个应用此类个性化知识的改进认证方案。

2 图像认证方法

一个人可以快速识别出自己的照片或与自己过去联系密切甚至记住的图片。Dhamija 等人研究了人的这种能力,并使用计算机合成的图像或人脸等预先选定的图片作为"密码"使用[2],进而对认证方法进行研究,主要考虑避免出现弱密码的问题。例如人们常将难于记忆的密码写下来,容易泄露。Pering 等应用一个人能识别出个人图片的能力提出了图像认证方法。该图像认证方案使用用户预先知道的,通常是用户自己拍摄(制作)并收藏的图片集合,另设置不属于用户的一个图片集合。该方案(下文需区别时称 P 方案)的原型系统使用 Web 浏览界面,每次提供 4 张图片,用户从中选出属于用户自己的那一张图片(对攻击者来说是要识别出属于假冒对象的图片),如此顺序显示 10 组图片作为一次认证或登录尝试。理论上这种方案可以达到使用 6 位数字作为密码的系统安全性[1],国内银行的 ATM 机上就是使用 6 位数字作为密码。

该认证技术使用一个可信的个人服务器(home server)

*)基金项目:重庆市自然科学基金重点项目(No. 2005BA2003)、重庆市教委科学技术研究项目(编号 KJ050509)资助,重庆市教委骨干教师资助计划资助。陈 龙 副教授,主要研究方向为智能信息处理,信息安全;蒋 溢 副教授,主要研究方向为宽带网络理论与技术,信息安全等;江 伟 硕士生,主要研究方向为网络安全。

进行配合，包括存储图片集合与用户信息，在必要时帮助用户进行其他需要的工作（如与其他系统进行传统安全认证后转发相关服务结果）。

这种系统的目标并不是提供具有很高安全性的认证方法，图像认证方法的目标是为系统提供相对意义上足够安全的认证手段，并且在特定的场合还具有其他认证方法不具有的优点。图像认证方法在用户每次登录都用了不同的图片组合，可以抵抗重放攻击行为。

3 个性化用户认证方法

3.1 个性化用户认证方法原理

基于图像的认证方法面临着一些挑战：首先，用户面临需要较大的图片集合以应对图片的重复性、可能出现的认证系统遭攻破等问题。但是每个用户得到一定数量图片以后要再增加是比较困难的（随意拍摄的图片用户自己难于识别和区分）。

其次，普适计算是信息空间与物理空间的融合，在这个融合的空间中人们可以随时随地、透明地获得数字化的服务[3]。普适计算时代的一个重要特点是多人共享多个（种）设备，从而有设备多样性的突出问题，同时也有使用不可信设备的问题。

尽管 Pering 等人有意区分了基于用户知识的（knowledge-based）方案如口令与基于用户识别的方案（recognition-based）如图像认证方法，但其本质都是基于用户所知、用户的知识。归纳用户知识的特性可以看出，人们拥有一些特殊的知识，这些知识与个人经历联系比较密切，容易回忆，甚至可以形成直觉，而且不易被他人获得。

人们拥有的各种各样的个人文档数量越来越多，其中有专门建立的易于记忆、识别的数字化收藏。这类涉及特殊经验、经历、记忆的数字化收藏对于其他人则很陌生，既不容易记忆，也不容易得到并进行推断。

分析图像认证方案，其本质是利用了用户个性化的容易回想、回忆起的特殊经验、经历、记忆的数字化收藏，进而可以进行识别。这种关于过去的特殊的经验、经历、“个性化知识”并不只是体现为照片（图片），往往也还体现为其他的各种形式——文字、声音、视频等。

个性化用户认证方法利用用户的个性化数字收藏来识别用户本人，认证识别过程使用组合方案来减少每次认证需要使用的媒体数量，相对地可以认为增加了媒体数量。媒体形式可以有图片、文本、视频、音频等。有关用户的多通道输入研究已经涉及到使用多媒体信息的“多媒体反馈模式”[4]。本方法同样可以根据用户终端的不同类型、不同工作模式选择适当的承载媒体，从而选择使用不同媒体或多种媒体相结合的认证方法。所以该方法具有终端设备的自适应性、可裁减性。

由于用户每次登录通过随机选取使用了不同的媒体信息，可以抵抗重放攻击。

3.2 原型系统

原型系统使用 Web 浏览界面，每一次认证或登录尝试共显示 32 条信息，其中属于该用户收藏的 8 条，不属于该用户收藏的 24 条，给认证用户的显示信息在可供选择的集合中采用随机的方式选取。每页显示 4 条信息，共分 8 页显示，用户从中挑出属于用户自己的那些图片（对攻击者来说是要识别出属于假冒对象的那些图片）。每页由用户确认提交。

与 P 方案的每一组有且只有一张属于用户的图片不同，本认证方法采用了从整体中选择一部分的组合方式，即只是在所有的 32 条信息中限定有 8 条属于用户收藏，单独的某一页上则完全不能确定有无属于用户收藏的信息。这种组合方案减少了暴露给攻击者的信息，相对地可以认为扩大了备选的媒体组成的信息空间，而不增加或很少增加用户识别上的困难。

3.3 安全性分析

安全性是所有认证机制的最重要的问题。用户个性化的知识（识别能力），实际上是不容易被人一次偷窃很多的知识，克服了密码方案的很多缺点。但是这类方案也肯定面临不少攻击，由于研究与使用的经验缺乏，其面临的攻击将造成多大的威胁以及其他没有设想到的攻击方案的可能性等还需要进一步研究。

由于采用了从整体中选择一部分的组合方式——在所有的 32 条信息中限定有 8 条属于用户收藏，所以如果采用理论上随机猜测的攻击方法，我们用少得多的媒体数量就达到了比 P 方案更加安全的效果。

对于随机猜测的攻击方法，P 方案有 4^{10} 即 1,048,576 种选择，猜中的概率约为百万分之一，本方案采用了从整体 32 条信息中选择 8 条信息的方式，即有 10,518,300 种选择，即全猜中的概率约为千万分之一，猜中概率后者只有前者的 1/10 左右。从这个角度说，比银行系统 6 位数的数字密码要更加安全。

考虑到用户本人也可能不会 100%准确地识别出自己的图片，假设认证系统把用户选错一个仍然视为通过认证，则两种方案都同在几万分之一的数量级上，相对而言，本方案里猜中的概率要小些。

和弱口令的存在一样，本系统的实际安全性可能比理论分析结果要弱。由于人们的自然分析能力、快速学习与识别能力，可能有许多快速猜测方法。由于视频信息包含的信息量大，也面临更多的攻击的可能。

4 实验结果及分析

实验中由七位用户准备了数字媒体信息，各类信息数量见表 1。

表 1 数字媒体信息集合

用户	文本片段	图片	视频片段	音频片段
A	40	107	47	60
B	73	247	16	101
C	152	869	12	60
D	71	754	49	50
E	16	768	66	0
F	101	308	23	90
G	102	353	13	89

实验中使用其他多个用户的数字媒体信息集合表示非用户本人的部分。

为了验证组合方案的有效性，使用图片集合进行了正式的测试。用户本人正式测试之前可以进行适当的练习和适应。每个用户分别进行 10 次认证，计算平均识别率和平均认证时间。

攻击实验开始前攻击者先理解认证方法、认证过程。在

（下转第 89 页）

Vu CanProve(*Vs* Says *Service*)

再根据假设 A5，又可以得到：

Vu CanProve(*Vs* Sends *Service*)

对于消息 4：根据假设 A1，*Vs* 可以确定是 *Vu* 发送了消息，即：

Vs CanProve(*Vu* Says *Acknowledge*)

然后根据假设 A6 得到：

Vs Canprove(*Vu* Received *Service*)

根据以上证明，交易过程的协议已经达到了可追究性的目标。

结论与展望 随着电子商务的发展，对于同时实现匿名性与可追究性的要求也越来越强烈。本文通过将 RBAC 的思想应用到电子商务交易的可信第三方的角色分配过程，并通过对注册用户真实信息加密并将加密密钥分段保存的方法实现了交易过程中的匿名性和可追究性要求。根据 RBAC 最小特权的原则对可信第三方的角色进行合理分配使其够协调工作又能相互牵制，既减弱了单个可信第三方的权力并将单个可信第三方出现问题造成的损失降到最低，又能实现匿名性与可追究性同时实现的要求。这种方法对于长期以来可信第三方安全假设要求过强的问题也提供了一些思路。

在下一步的工作中，需要进一步研究是投诉处理过程中的证据确认原则及各可信第三方之间的通信过程处理及协议。更长远的研究包括使用零知识证明等方法实现进一步的匿名要求。

参 考 文 献

1 Ferraiolo D F, Kuhn D R. Role Based Access Control. In: 15th National Computer Security Conference, 1992

2 Sandhu R S, Coyne E J, Feinstein H L, et al. Youman, Role-Based Access Control Models. IEEE Computer, 1999, 29(2): 38～47

3 Qing SH. Cryptography and Computer Network Security. Beijing: Thinghua University Press, 2001 (in Chinese)

4 Qing S H. TTP roles in electronic commerce protocols. Journal of Software, 2003,14(11):1936～1943

5 Qing, S H. Design and logical analysis of security protocols. Journal of Software, 2003,14(7):1300～1309 (in Chinese with English abstract)

6 Farkas C, Ziegler C, Meretei A, et al. Anonymity and Accountability in Self-Organizing Electronic Communities. In: WPES'02, Nov. 2002

7 Kailar R. Accountability in electronic commerce protocols. IEEE Transactions on Software Engineering, 1996,22(5):313～328

8 Kailar R. Reasoning about Accountability in Protocols for Electronic Commerce. Security and Privacy. In: Proceedings, 1995 IEEE, 1995

9 O'Toole K R. The Internet Billing Server Transaction Protocol Alternative. Carnegie Mellon University Information Networking Institute, INI TR, 1994

10 Backes M, Camenisch J, Snommer D. Anonymous yet Accountable Access Control. In: VPES05, 2005 ACM, Nov. 2005

11 Keesom K A. Anonymity, Accountability. In: InfoSecCD Conferece'04, ACM, 2005

(上接第 85 页)

正式进行攻击测试之前，攻击者先试用一次该系统，攻击者可以事先花一定时间查看假冒对象的某一次认证记录结果。每个攻击者轮流假冒每个用户一次，测试过程中还可以查看该假冒对象的相应认证记录结果。正常用户与被假冒时针对该用户的平均识别率和平均认证时间结果分别见图 1 和图 2。

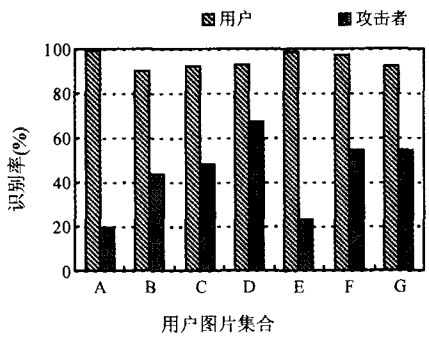

图 1 正常用户和攻击者识别率比较

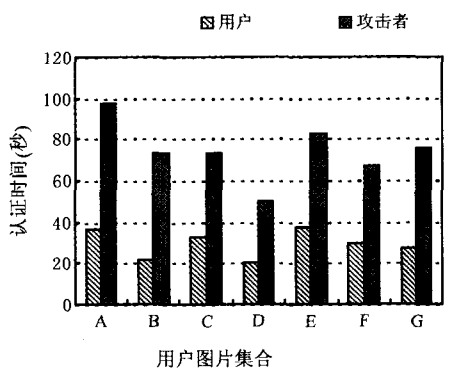

图 2 正常用户和攻击者登录的花费时间比较

由图 1 和图 2 所示结果，从对图片的识别率和平均认证时间两个方面看，攻击者和用户都可以比较明显地进行区分。P 方案中攻击者识别率相对较高，多数达到 60%左右。从图 1 可以看出，本方案显著降低了攻击者对图片的识别率。实验结果显示这种组合方案会在用户最初使用该系统时会出现漏选个别信息的错误。

其他一般性实验显示单独使用一种类型的数字媒体时，使用文本方式时用户识别率略高而攻击难度大，图片次之，视频和音频差一些。如果只提供一种形式的媒体供用户选择，图片为用户的首选。相对传统认证方式，用户本人制作、生成个人收藏集合还是有一定困难，用户总体上感到此种认证方式新颖、有趣，感觉比较安全。但也有部分人担心数字媒体信息集合全部被他人获得，从而可能暴露个人隐私。

结论 本文个性化认证方法由于用户每次登录通过随机选取使用了不同的媒体信息组合，可以抵抗重放攻击。分析与实验结果表明该方法是可行的，安全性得到提高，用户可以接受这种认证方式。该实现方案增加了用户灵活的媒体形式选择，解决了设备多样性问题，同时减少了暴露给攻击者的信息，相对地可以认为扩大了备选的媒体组成的信息空间。

未来可能的研究工作包括改进用户参与配置系统的方式、攻击方法及其对抗措施等。

参 考 文 献

1 Pering T, et al. Photogranphic Authentication through Untrusted Terminals. IEEE PERVASIVE computing,2003,2(1): 30～36

2 Dhamija R, Perrig A. DejaVu: A User Study Using Images for Authentication. In: Proc. 9th Usenix Security Symp., Usenix, Aug. 2000. 45～58

3 徐光佑，史元春，谢伟凯. 普适计算. 计算机学报，2003,26(9): 1042～1050

4 王悦，岳玮宁，王衡，董士海. 手持移动计算中的多通道交互. 软件学报，2005,16(1):29～36

5 Deb S, Zhang Yanchun. An overview of content-based image retrieval techniques. In: 18th International Conference on Advanced Information Networking and Applications, Volume 1, 2004. 59～64