基于零知识证明的匿名身份认证机制

李 琳[1] 岳建华[2]
(中国矿业大学计算机科学与技术学院 徐州 221116)[1]
(中国矿业大学资源与地球科学学院 徐州 221116)[2]

摘 要 近年来,随着互联网的快速发展,匿名身份认证对保护用户的隐私和信息安全发挥着越来越重要的作用。对现有身份认证机制进行了分析,指出其存在的缺点,并在此基础上,提出了改进方法,给出了基于Wang的使用数字签名的零知识证明的匿名身份认证方案。该方案既降低了通信流量,又具有更高级别的安全性。

关键词 匿名,身份认证,数字签名,零知识证明
中图法分类号 TP393 **文献标识码** A

Anonymous Authentication Mechanisms Based on Zero-knowledge Proof

LI Lin[1] YUE Jian-hua[2]
(School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China)[1]
(School of Resources and Earth Science, China University of Mining and Technology, Xuzhou 221116, China)[2]

Abstract With the rapid development of Internet, anonymous authentication plays more and more important roles during the users' privacy protection and information security. Based on the analysis of existed authentication scheme, this paper pointed out the existing shortcomings and proposed the improved one. In addition, the paper gave the zero-knowledge proof of the scheme with digital signatures proposed by Wang. The proposed scheme greatly reduces the traffic and increases the security.

Keywords Anonymous, Authentication, Digital signature, Zero-knowledge proof

1 引言

随着互联网应用的发展,网络安全越来越成为关注的焦点,相关的安全技术及安全协议也不断被提出。但是这些安全技术和安全协议主要应用于对网络通信内容的保护,忽略了通信双方的匿名性。事实上,在许多情况下人们都需要对其他参与者或可能存在的窃听者隐藏自己的真实身份从而保护个人和信息安全。因此,匿名身份认证在生活中有着重要的作用。

文献[1,2]提出使用密钥分配的分布式网络用户认证机制,但该方案不能抵御伪装攻击和因身份泄漏引起的攻击。文献[3]提出了一种基于口令的匿名身份认证密钥交换协议,但该方案在服务器端使用密码表,需要大量的指数运算,效率不高。文献[4]提出了一个新的基于匿名口令的密钥交换协议,该方案能够抵御伪装攻击和离线字典攻击,文中还对新方案的安全性进行了分析。文献[5]发现之前提出的匿名身份认证和密钥交换协议存在一些安全漏洞。如果用户和服务器之间的连接已经建立,服务器要猜测用户的真实身份的可能性是100%。该文提出了一种基于环签名的匿名身份认证协议。然而,该方案中提到获取所有用户的公钥是不现实的。本文在上述文献的基础上,利用零知识证明内容提出了一种新的匿名身份认证方案,并对该协议的安全性和计算效率进行了实验验证。

2 基于零知识证明的匿名身份认证机制

2.1 零知识证明

使用DSA数字签名的零知识证明方案可以用来阻止数字签名的任意分布。

以下设DSA数字签名算法的系统参数是 p,q,g(p 和 q 分别是1024及160比特的大素数,且 $q|p-1$;$g\in z_p$,阶为 q;一般可取 $g\triangleq h^{(p-1)/q} \bmod p$,$(1<h<p-1, h\in z)$。设证明者 P(即签名者)的公钥是 $y=g^x \bmod p$。公钥可通过X.509或其它公钥证书获得,对公钥的信任来源于对签发证书的根CA的信任。$x\in R, Z_p$ 是证明者 P 的私钥,代表了签名者的身份信息。

由DSA算法知道证明者 P 对信息 M 的签名 (r,s),其中

$$\begin{cases} r=(g^k \bmod p) \bmod q; k\in RZ_q \\ s=[k^{-1}(H(M)+xr)] \bmod q \end{cases} \tag{1}$$

式中,$H(\cdot)$为安全哈希函数SHA-1。DSA数字签名的验证为判定下式是否成立。

$$\{[g^{(H(M)s^{-1} \bmod q)} y^{(rs^{-1} \bmod q)}] \bmod p\} \bmod q=r \tag{2}$$

若式(2)成立,则签名正确,否则为无效签名。注意到以

到稿日期:2013-03-20 返修日期:2013-06-20 本文受"十二五"国家科技支撑计划资助项目(2013BAK06B01)资助。
李 琳(1982—),女,博士生,讲师,主要研究方向为信息安全、地质资源与地质工程,E-mail:lilin@cumt.edu.cn;岳建华(1964—),男,博士,教授,主要研究方向为地球探测与信息技术、地质资源与地质工程、煤矿安全。

上运算在 z 中的模 P 运算，g 的阶为 q，故本文为简便起见以下均省去模符号，于是式(2)简记为：

$$Z_p g^{(H(M)s^{-1})} y^{rs^{-1}} = r$$

证明者 P 欲使验证方确信他或她拥有对信息的数字签名(r,s)，而不泄漏有关 r 和 s 的任何有用信息，证明者 P 与验证方执行零知识证明(zero knowledge proof)协议。由 DSA 的验证式(2)，证明者 P 与验证者须执行以下的零知识证明协议。

$$ZPK\{\alpha,\beta|[(g^{(H(M)\beta^{-1}) \bmod q} y^{(r\beta^{-1}) \bmod q}) \bmod p] \bmod q=\alpha\} \tag{3}$$

式中，α 和 β 代表证明者的秘密信息，这里分别是证明者拥有的对信息的 DSA 数字签名 $r,s;p,q,g,y,H(\ )$ 为证明者 P 与验证者的共享信息。

式(3)所示的零知识协议较为困难，本文给出一个蕴涵式(3)成立的零知识证明协议，这在零知识证明方面是首次提出。

首先证明者计算对签名者之一 r 的承诺值：

$$Z := (y^r \bmod p) \bmod q \tag{4}$$

并且证明者公开该承诺，即将该承诺发送给验证者。则式(3)蕴涵于下式所示的零知识证明协议：

$$ZPK\{\alpha,\beta \mid z[(y^{\alpha}) \bmod p] \bmod q \wedge (g^{H(M)\beta^{-1} \bmod q} y^{\alpha\beta^{-1} \bmod q}) \bmod p] \bmod q=\alpha\} \tag{5}$$

我们也应该注意下面的式子：

$$[(g^{H(M)\beta^{-1}} y^{\alpha\beta^{-1}}) \bmod p] \bmod q = \alpha \Leftrightarrow [(y^{[(g^{H(M)}z)^{\beta^{-1} \bmod p] \bmod q}}) \bmod p] \bmod q=z \tag{6}$$

$z=y^{\alpha}$

式(6)显然是成立的，因此式(5)可以等价为下面的式子。

$$ZPK\{\alpha,\beta|z=[(y^{\alpha}) \bmod p] \bmod q \wedge z\} = [(y^{[(g^{H(M)}z)^{\beta^{-1} \bmod p] \bmod q}}) \bmod p] \bmod q \tag{7}$$

$$b := g^{H(M)} z \bmod p \tag{8}$$

式(7)可以使用式(9)代替：

$$ZPK\{\alpha,\beta|z=y^{\alpha} \wedge z=y^{b^{\beta^{-1}}}\} \tag{9}$$

式(9)所表示的零知识协议的具体含义为：

$$ZPK\{\alpha,\beta|z=y^{\alpha} \wedge z=y^{b^{\beta^{-1}}}\}=\{c,d,s_1,\cdots,s_l\} \in \{0,1\} \times z_q^{l+1} \tag{10}$$

式中，α 和 β 分别代表证明者的对信息 M 的 DSA 数字签名 r 和 s。

2.2 基于零知识证明的匿名身份认证机制

传统的匿名身份认证机制主要研究两个实体，即服务器和用户。对于服务器来说，因所有的用户数据全部存储在服务器端，得知用户的身份信息较为容易。对于用户来说，如果用户直接向服务器发送数字签名 r 和 s，服务器根据数字签名信息可能计算出用户的身份信息。

本文提出的基于零知识证明的匿名身份认证通过引入中间第三方代理和使用 2.1 节中的零知识证明来实现服务器与用户之间的安全通信。用户想要访问服务器的时候，就向代理服务器发送信息 M。代理服务器验证用户的身份，通过私钥生成数字签名 r 和 s。用户收到数字签名以后，选择一定的参数经过变形计算后产生新的验证数字，该数字发送给服务器，服务器端通过零知识证明的方法计算验证该用户是否合法。首先介绍协议所用的标识符：

$A \rightarrow B:M$：A 向 B 发送消息 M；

r_i：表示协议中所选取的随机数；

$c[i]$：表示由 0 和 1 组成的二进制序列；

s：数字签名；

p、q：大素数；

c、d：用户端加密参数；

t_i：时间戳。

用户从代理服务器收到数字签名后，按如下步骤进行：

1. 首先，用户选择一系列的随机数，如：$r_0,r_1,\cdots,r_l \in R$，Z_q，然后用户开始计算：

$c := H(g|p|q|z|y^{r_0}|\cdots|y^{\theta_i})$

$(c=c[l]\cdots c[1] \in \{0,1\}^l$；

$[(y^{\theta_l \bmod q}) \bmod p] \bmod q, i=1,\cdots,l;\theta=b^{r_i})$

2. 计算出结果后，用户使用自己的秘密信息(即数字签名 r 和 s)秘密计算：

$$d=r_0 \cdot cr \bmod q$$

$$s_i=\begin{cases} r_i, & c[i]=0 \\ r_i-s^{-1}, & c[i]=1 \end{cases}, (i=1,2,\cdots,l)$$

我们得到结果 c、d 和 s，它们是零知识证明的组成部分。

3. 用户通过和服务器之间的安全隧道将零知识证明$\{c,d,\cdots,s_1,s_t\}$发送给服务器端。

4. 服务器端收到零知识证明以后，使用共享的信息 p,q,g,y,M,z,b 来验证下式是否成立。

$$c \stackrel{?}{=} H(g|p|q|y|z|z^c y^d|t_1|\cdots|t_l) \tag{11}$$

$$t_i=\begin{cases} [(y^{b^{s_i} \bmod q}) \bmod p] \bmod q, & c[i]=0 \\ [(z^{b^{s_i} \bmod q}) \bmod p] \bmod q, & c[i]=1 \end{cases}, (i=1,\cdots,l)$$

服务器根据式(11)来判断与用户端的通信是否合法：如果式(11)成立，则服务器端得知该用户是合法的。如果上式不成立，服务器端和用户端不能建立通信连接。通过以上零知识方案的证明我们可以发现，当式(11)成立时，p,q,g,y,M,z,b 等共享信息的哈希值与值 c 必然相等，同理，根据 t_i 的值也可以通过判断 i 与 c 数组的相等情况。当 t 个参数的属性值与共享信息值连接操作后可以得出 c 的值。用户和服务器认证阶段如图 1 所示。

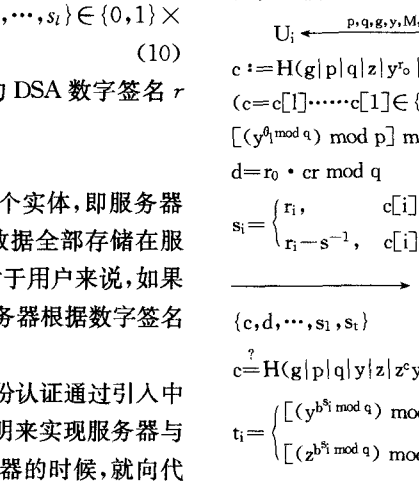

图 1 用户认证阶段

上文提出的基于零知识证明的匿名身份认证机制的应用过程详细步骤如下：

某一用户 Jane 想要从某一网页 Bob 上下载一些文件。

然而，他不想要暴露自己的身份。我们假设 Peter 是一个充当认证中心的可信第三方。

(1)Jane 想要发送信息 M 给 Bob，首先 Peter 使用他的私钥生成数字签名信息 r 和 s 并发送给 Jane。

(2)当 Jane 收到数字签名 r 和 s 以后，选择一系列的随机数像 $r_0, r_1, \cdots, r_t \in R, Z_q$，开始利用他的密钥进行秘密计算，然后生成零知识证明 $\{c, d, \cdots, s_1, s_t\}$。

(3)Jane 通过安全的隧道向 Bob 发送零知识证明 $\{c, d, \cdots, s_1, s_t\}$。

(4)当 Bob 接收到零知识证明以后，使用共享信息 p, q, g, y, M, z, b 来验证用户 Jane 是否是合法用户。如果 Jane 是合法的，Bob 会和 Jane 建立连接进行通信。

3 安全性分析

本文提出了基于零知识证明的匿名身份认证机制，现就其认证的安全性进行分析如下。

1. 安全性：在我们的方案中，假扮成一个合法的用户向服务器端发出请求服务是不可行的。因为只有合法的用户才可以在代理服务器获得数字签名。某一个用户如果想成为合法用户，必须在代理服务器端完成注册。因此，代理服务器可以识别一个用户是否合法，然后给合法用户发送数字签名信息。如果该用户是不合法的，那他得不到数字签名信息 r 和 s。也就是说不合法的用户不能和服务器进行通信。除此之外，服务器和代理服务器之间不能进行相互通信。因此服务器不能从代理服务器获得合法用户的任何身份信息。因此我们说用户是不可以被伪造的。

2. 匿名性：在我们的方案中，如果合法的用户没有暴露其数字签名，任何验证方不能确定该用户是否是合法的。用户随机选取一系列的随机数 $r_0, r_1, \cdots, r_t \in R, Z_q$ 来计算。然后计算数字签名发送给服务器。然而服务器不能够计算零知识证明，因为零知识证明 $\{c, d, \cdots, s_1, s_t\}$ 由用户使用数字签名 r 和 s 秘密计算而来。除此之外，用户从代理服务器获得数字签名 r 和 s。服务器和代理服务器之间没有任何连接。因此服务器不能得知是哪个用户在访问，只能判断该用户是否是合法的。因此，我们的方案具有良好的匿名性。

3. 不可关联性：攻击者假扮成服务提供商来获取用户的身份信息在我们的方案中是不可行的。既然用户和服务器之间使用零知识证明，那么服务器能够确信用户是合法的但不能知道关于数字签名 r 和 s 的任何相关信息。每次服务器接收到零知识证明，他开始使用共享信息 p, q, g, y, M, z, b 进行验证，而这些共享信息不含有任何用户的私密信息，因此服务器不能获得用户的身份信息。即便用户连续访问服务器，服务器也不能够计算用户的身份信息，因为用户每次选择的随机数一般是不同的。因此我们说用户和服务器之间是不可关联的。

4 实验验证及分析

为验证本文提出的基于零知识证明的匿名身份认证机制的安全性和效率，我们做了该方案的实验验证。

4.1 仿真实验环境

为模拟实际的网络应用，仿真实验设计了 3 组类型的匿名身份认证：一个用户验证多个网站(一对多)、多个用户验证同一网站(多对一)以及多个用户验证多个网站(多对多)，以此来综合验证该认证协议在不同网络应用下的实际性能。仿真环境硬件平台为 Core2 Duo 2.8GHz 的 CPU 和 1GB 的内存，操作系统为 Windows XP。鉴于文献[1,7]提供了对自身协议计算性能的分析，仿真实验结果将与其进行对比。

4.2 认证协议计算代价仿真实验

在互联网通用的 C-S 架构中，服务器作为信息提供者承担了大部分的计算量。考虑到整个网络信息资源的不对称性，我们通过分析用户在整个协议运行过程中的计算量来测试该协议的运行效率和可行性(比较结果如表 1 所列)。

表 1 协议效率对比

协议	文献[1]	文献[7]	本文协议
哈希运算次数	2	3	1
模指数运算次数	4	2	2
交互次数	3	2	2
对称加密/解密	3	2	0
公钥加密/解密	0	1	1
随机参数选取次数	3	3	2
协商密钥	3	2	1

1. 计算次数：本文方案中，用户在选择随机参数和计算零知识证明 $\{c, d, \cdots, s_1, s_t\}$ 时共需进行 1 次哈希函数计算和 2 次模指数运算。从表 1 可以看出，除文献[1]中因用户提前与服务器协商过密钥，公钥加密/解密运算次数计为 0 外，本文方案计算开销明显小于其他协议。

2. 交互次数：在一般的认证协议中，为保证匿名通信过程中涉及的通信实体是合法的，经常需要实现双向认证。本文方案在会话密钥建立过程中，只需用户向服务器发送经过计算的零知识证明 $\{c, d, \cdots, s_1, s_t\}$，实现了单向安全认证，降低了网络通信的代价，效率更高。

为验证理论分析的结果，本节对该匿名认证协议在 3 种网络应用下的计算代价进行了仿真实验。在协议仿真实现时，选取 SHA-1 作为哈希算法，DSA 为数字签名算法。为减少用户主机性能对协议执行效率的影响，仿真实验的客户端主机统一采用主频 2.8GHz 的 CPU，同时每类型验证方式分别执行 100 次。

图 2 为上述 3 种协议分别在不同应用场景中的平均执行时间对比图。由仿真结果可知，本文提出的匿名认证协议较文献[1,7]，效率提升 30%～40%。如具体分析 3 种网络应用中的不同性能，当出现多对多的验证需求时，该匿名认证协议效率是其他协议的 1 倍多。在所有仿真结果中，本文所提出的协议最少用时仅为 80ms，而最大用时也不到 100ms，远低于文献[1,7]中协议的执行时间。因此，仿真实验结果表明，本文提出的匿名身份认证协议具有较好的计算性能，

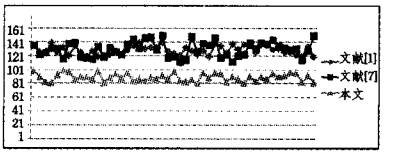

图 2 协议计算代价仿真结果

4.3 认证协议安全性能仿真实验

作为身份认证协议最基本的性质，运行的安全性直接决定了协议在实际网络环境中的可用性。为验证该协议在不同

(下转第 214 页)

进行编码和解码，这一过程不与任何特定的代码形式或它们的执行顺序有关。因此，即使通过语义变换，改变代码的形式或顺序，只要功能不变，上述永假式的构造不会遭到破坏。同时，0、1 串是用随机函数产生的，每次运行都不一样，无法穷举，所以无法确切地统计相关信息，以找到规律发现虚方法的存在，因而能抵抗统计攻击和单步跟踪调试攻击。与语义变换攻击一样，在程序中增加其它代码对本方法不会产生任何影响。对于减少代码攻击，如果减去的不是与永假式构造有关的代码，则不会对本程序产生影响；如果减去的代码与 0、1 串编解码的过程有关，由于不能正确进行编解码，将会导致程序出错，无法正常运行，这对于攻击者而言也没有意义，因为攻击者的目的是要盗用程序，若盗取的程序无法完成预定的功能，攻击便失去意义和效果。

结束语 本文针对基于字节码的 Java 软件水印算法，提出了一种永假式的设计构造方法，用于植入虚方法进行水印信息的嵌入，有效地解决了虚方法的隐藏和抗攻击问题，使得该水印方案更加完备，可实际应用于 Java 程序的版权保护。根据本文提出的方法以及相关水印嵌入、提取技术，我们已设计开发出用于对实际 Java 应用程序进行版权信息嵌入与提取的软件系统。

参 考 文 献

[1] Collberg C, Thomborson C. Watermarking, tamper-proofing, and Obfuscation—Tools for Software Protection[J]. IEEE Transactions on Software Engineering, 2002, 28(8): 735-746

[2] 张立和，杨义先，钮心忻. 软件水印综述[J]. 软件学报，2003，14(2)：268-277

[3] Zhu W, Thomborson C, Wang F. A Survey of Software Watermarking[C] // IEEE International Conference on Intelligence and Security Informatics. 2005: 454-458

[4] Hamilton J, Danicic S. A survey of static software watermarking [C]//IEEE World Congress on Internet Security. 2011: 100-107

[5] 鲍福良，彭俊艳，方志刚. Java 类文件保护方法综述[J]. 计算机系统应用，2007，6：124-126

[6] 周正虎，陈丹，周光霞，等. 基于病毒多态性的 Java 软件水印技术[J]. 计算机与数字工程，2011，39(11)：97-100

[7] Monden A, Iida H, Matsumoto K, et al. A Practical Method for Watermarking Java Programs [C] // The 24th International Computer Software and Applications Conference. 2000: 191-197

[8] 王春红，陈建平，王杰华，等. 基于字节码的 Java 软件水印的研究与实现[J]. 微电子学与计算机，2009，26(9)：146-149

[9] 樊昌信，曹丽娜. 通信原理[M]. 北京：国防工业出版社，2010

(上接第 199 页)

网络应用下的安全性能，本文设计如下仿真实验进行验证。首先，构造 500 对验证和应答请求，其中包含了协议所定义的参数极限值。然后，用 3 种协议分别执行这些验证数据，统计在 3 种网络应用环境下的验证正确率，由仿真结果可知，本文协议的正确率与文献[7]相当，较文献[1]则安全很多。协议安全性能仿真结果如图 3 所示。

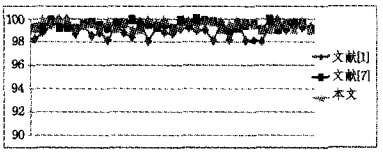

图 3 协议安全性能仿真结果

结束语 匿名身份认证对保护用户的隐私和信息安全发挥越来越重要的作用，本文提出了一个新的基于使用数字签名的零知识证明的匿名身份认证方案，通过引入中间第三方代理来完成服务器与用户之间的通信。该方案不需要知道所有用户的公钥，大大减少了通信量，同时很好地消除了安全漏洞，具有良好的匿名性、认证性和不可关联性。文中还对该协议的安全性和计算效率进行了实验仿真。经验证，该协议的安全性能优且较其他协议效率更高。

参 考 文 献

[1] Lee W B, Chang C C. The protocols guarantee user anonymity in distributed network user authentication and key distribution[J]. Computer Systems Science and Engineering, 1999, 15(4): 113-116

[2] Wu T S, Hsu C L. Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks[J]. Computers and Security, 2004, 23(2): 120-125

[3] Viet D Q, Yamamura A, Tanaka H. Anonymous authenticated key exchange protocol based on password: Advances in Cryptology INDOCRYPT, 2005[C]//LNCS, Vol. 3797. Berlin: Spring-Verlag, 2005: 244-257

[4] Yang Jing, Zhang Zhen-feng. New anonymous password-based authenticated key exchange protocol[C]//Chowdhury D R, Rijmen V, Das A, eds. INDOCRYPT, 2008. LNCS 5365, 2008: 200-212

[5] Cui Hui, Cao Tian-jie. A new anonymous identity authentication and key exchange protocols[J]. Journal of Network, 2003, 4(10): 985-992

[6] Bo Z, Wan Z G, et al. Anonymous secure routing for mobile ad hoc networks[C] // 29th Annual IEEE International Conference, 2004. 2004: 102-108

[7] Chien H Y, Chen C H. Remote authentication mechanism of guarantee user anonymity[C]//Proceedings of the 19th International Conference on Advanced Information Networking and Applications-AINA, 2005. 2005: 245-248

[8] Durresi A. Anonymous communications in the Internet [J]. Cluster Computing, 2007, 10(1): 57-66

[9] 王尚平，王育民，王晓峰，等. DSA 数字签名的零知识证明[J]. 电子学报，2004，32(5)：878-880

[10] Cesena E, Löhr H, Ramunno G, et al. Anonymous authentication with TLS and DAA[C]//Proceedings of the Third International Conference on Trust and Trustworthy Computing (TRUST'10), 2008. LNCS, vol. 6101, 2008: 47-62

[11] Chen L, Page D, et al. On the design and implementation of an efficient DAA scheme[C]//9th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Application (CARDIS'10), 2010. LNCS, vol. 6035, 2010: 223-237