基于数字签名的安全认证存取控制方案*

施荣华

(中南大学 计算机科学与技术系,湖南 长沙 410075)
E-mail: shirh@263.net
http://www.csu.edu.cn

摘要: 基于 Harn 数字签名方案和零知识证明,针对信息保护系统构造了一种认证存取控制方案.该方案与已有的存取控制方案相比要更加安全.因为在该方案中,用户与系统不必暴露秘密信息就可以进行双向认证,并且其共享密钥可用于认证用户访问保密文件的请求合法权限.该方案能够在动态环境中执行像改变存取权限和插入/删除用户或文件这样的存取操作,而不影响任何用户的保密密钥.

关 键 词: 数字签名;零知识证明;安全认证;存取控制;信息保密系统
中图法分类号: TP393 文献标识码: A

在多用户网络系统中,信息保护系统主要由一组文件、一组客体及一个存取控制表三部分组成.在存取控制表中,任一元素 a_{ij} 表示用户 i 对客体 j 的存取权限.从表 1 中可以看出,用户 1 对文件 4 无任何访问权;用户 3 对文件 3 有执行权等.

Table 1 4×5 access control table

表 **1** 4×5 存取控制矩阵

	File j					Note①
User i	1	2	3	4	5	0—No access right②
1	4	3	2	0	1	1—Reading③
2	3	2	4	3	2	2—Writing④
3	0	2	3	4	4	3—Executing⑤
4	1	1	0	0	3	4—Reading,writing,executing⑥

①注解,②无任何存取权,③可读,④可写,⑤可执行,⑥可读,可写,可执行.

近年来,有关学者提出了几种实现存取控制的方案[1~4].在这类方案中,建立信息系统的计算复杂,更严重的是整个建立起来的信息保护系统在动态环境中,进行像改变访问权限和插入/删除用户或文件等操作时,要不断进行重建,即动态特性差.这类方案的另一不足之处是用户不能对欲进入的系统进行认证[1~5],系统也不能对需访问保护文件而进入系统的用户进行认证,也就是说,这些方案的抗攻击性差.

本文为克服上述缺点,结合零知识证明的思想[6],提出了一种基于数字签名方案的安全认证存取控制方案.

1 数字签名方案[7~9]

1994 年,Harn 提出了一种基于离散对数的数字签名方案.该方案签名生成过程简单,签名验证速度快.方案如下:

p 是一个大素数,a 是 $GF(p)$中的一个本原元,f 是单向出数.签名者 A 的密钥为 x,这里 $x\in[1,p-1]$且 $gcd(x,p-1)=1$,公钥为 $y=a^x(\mathrm{mod}\ p)$.

设 m 为需签发的消息,签名者 A 选择随机数 $k\in[1,p-1]$,计算 $r=a^k(\mathrm{mod}\ p)$及 $s=x\cdot f(m)-k\cdot r(\mathrm{mod}\ p-1)$,则$(r,s)$为

* 收稿日期: 2000-04-21; 修改日期: 2000-09-26
基金项目: 国家自然科学基金资助项目(60173041)
作者简介: 施荣华(1964－),男,湖南安乡人,教授,主要研究领域为计算机网络技术,计算机通信保密技术.

消息 m 的数字签名.

任何用户一旦接收集合$\{m,r,s\}$就可以利用检查下式是否成立来验证签名者 A 对消息 m 的签名:

$$y^{f(m)}=r^r\cdot a^s(\mathrm{mod}\ p). \tag{1}$$

2 基于身份的双向认证

本节将利用 Harn 数字签名方案,结合零知识证明[6]的思想构造基于身份的系统与用户的双向认证方案.该方案由初始化、注册及认证 3 个阶段组成.

2.1 初始化阶段

网络中密钥认证中心 KAC(key authentication centre)先选择一个单向函数 f,一个大素数 p 及 $GF(p)$上的本原元 a,再选择一个随机数 x 作为自己的密钥,这里 $x\in[1,p-1]$且 $gcd(x,p-1)=1$.于是 KAC 的公钥为 $y=a^x(\mathrm{mod}\ p)$.注意,p 的选择应满足 $p=2p'+1$,其中 p'也是一个大素数[5].然后,系统公开 f,p,a,y 这 4 个参数.

2.2 注册阶段

网络中,用户 u_i 及系统 s 需向 KAC 提交自己的身份标识 Idu_i 及 Ids,经 KAC 确认身份后,KAC 为 u_i 及 s 计算 (r_{u_i},s_{u_i})及(r_s,s_s)如下:

$$r_{u_i}=a^{k_{ui}}\ (\mathrm{mod}\ p), \tag{2}$$

$$s_{u_i}=x\cdot f(Id_{u_i})-k_{u_i}\cdot r_{u_i}\ (\mathrm{mod}\ p-1), \tag{3}$$

$$r_s=a^{k_s}\ (\mathrm{mod}\ p), \tag{4}$$

$$s_s=x\cdot f(Id_s)-k_s\cdot r_s(\mathrm{mod}\ p-1), \tag{5}$$

这里, k_{u_i} ,k_s 是随机数,且 k_{u_i} ,$k_s\in[1,p-1]$.

KAC 由可靠的信道把 (r_{u_i},s_{u_i}) 及(r_s,s_s)分别交给 u_i 与 s.其中 s_{u_i} 是 u_i 的秘密参数,s_s 是 s 的秘密参数.u_i 与 s 可以通过以下两个方程是否成立来验证 (r_{u_i},s_{u_i}) 及(r_s,s_s)是否由 KAC 给出:

$$y^f(Id_{u_i})=(r_{u_i})^{r_{ui}}\cdot a^{s_{ui}}\ (\mathrm{mod}\ p), \tag{6}$$

$$y^f(Id_s)=(r_s)^{r_s}\cdot a^{s_s}\ (\mathrm{mod}\ p). \tag{7}$$

2.3 认证阶段

现假定 u_i 与 s 需向对方证实各自的身份.为防止攻击者假冒骗取 u_i 与 s 的秘密信息,认证方案设计的关键在于如何保证 u_i 与 s 双向证实各自身份的同时不致于暴露自己的秘密信息 s_{u_i} 与 s_s,这是零知识证明的思想在身份认证方案设计中的应用.该双向认证方案属于一种“问答式”协议.

双向认证的步骤如下:

第 1 步:u_i 选择一个随机数 v_{u_i} ,它满足 $v_{u_i}\in[1,p-1]$且 $gcd(v_{u_i},p-1)=1$.计算:

$$v_{u_i}=a^{v_{ui}}\ (\mathrm{mod}\ p), \tag{8}$$

把$(Id_{u_i},r_{u_i},w_{u_i})$发送给 s.

第 2 步:s 收到$(Id_{u_i},r_{u_i},w_{u_i})$之后,选择一个随机数 v_s,它满足 $v_s\in[1,p-1]$且 $gcd(v_s,p-1)=1$.计算:

$$w_s=a^{v_s}\ (\mathrm{mod}\ p), \tag{9}$$

$$\delta_s=(w_{ui})^{s_s}\ (\mathrm{mod}\ p), \tag{10}$$

把(Id_s,r_s,w_s,δ_s)发送给 u_i.

第 3 步:u_i 收到(Id_s,r_s,w_s,δ_s)之后,验证等式

$$y^{f(Id_s)}=(r_s)^{r_s}\cdot(\delta_s)^{(v_{u_i})^{-1}}\ (\mathrm{mod}\ p), \tag{11}$$

是否成立.若式(11)成立,则说明 s 身份真实.然后,u_i 计算:

$$\delta_{ui}=(w_s)^{s_{ui}} \pmod p, \tag{12}$$

并把 δ_{u_i} 发送给 s.

第 4 步:s 收到 δ_{u_i} 之后,验证等式:

$$y^{f(Id_{u_i})}=(r_{u_i})^{r_{ui}}\cdot(\delta_{u_i})^{(v_s)^{-1}} \tag{13}$$

是否成立.若式(13)成立,则说明 u_i 身份真实.

通过上述步骤,u_i 与 s 之间就双向认证了对方的身份.式(11)的证明如下:

证明:由式(10)和式(8),有

$$\begin{aligned}\delta_s&=(w_{u_i})^{s_s} \pmod p\\&=(a^{v_{ui}})^{s_s} \pmod p\\&=(a^{v_s})^{v_{ui}} \pmod p,\end{aligned}$$

于是

$$(\delta_s)^{(v_{u_i})^{-1}}=a^{s_s} \pmod p. \tag{14}$$

又由式(7),有

$$y^{f(Id_s)}\cdot(r_s^{r_s})^{-1}=a^{s_s} \pmod p,$$

于是再由式(14),得

$$y^{f(Id_s)}\cdot(r_s^{r_s})^{-1}=\delta^{(v_{u_i})^{-1}} \pmod p,$$

从而得式(11). □

同理,可证明方程式(13)成立.

3 认证存取控制方案

设信息保密系统 s 中有 m 个用户,n 个文件.令 a_{ij} 是用户 u_i 对文件 f_j 的访问特权.先按第 2.2 节中的方法,获得(r_s,s_s)及 (r_{u_i},s_{u_i}).这里 i=1,2,…,m.

设 q 是比所有 a_{ij} 中最大值还要大的数.

3.1 建立过程

第 1 步:按第 2.3 节中的方法,系统 s 和所有用户进行双向认证.

第 2 步:计算由系统 s 和用户 u_i 所共享的密钥

$$k_{s\cdot u_i}=(\delta_{u_i})^{s_s\cdot(v_s)^{-1}(\bmod p-1)} \pmod p,\ i=1,2,\ldots,m. \tag{15}$$

第 3 步:计算

$$r_{ij}=((k_{s\cdot u_i}+j)\bmod q)\oplus a_{ij},\ i=1,2,\ldots,m;\ j=1,2,\ldots,n. \tag{16}$$

第 4 步:将 r_{ij} 放入表 2 中.

Table 2 The public information table which s manage

表 2 s 管理的公用信息表

	f_j				
u_i	1	2	…	…	n
1	r_{11}	r_{12}	…	…	r_{1n}
2	r_{21}	r_{22}	…	…	r_{2n}
⋮	⋮	⋮	…	…	⋮
m	r_{m1}	r_{m2}	…	…	r_{mn}

建立过程的主要目的是构成由 s 分别和各用户所共享的密钥.与此同时,这些共享密钥也确立了各用户针对每个文件的访问权.

3.2 认证存取控制的实现

公用信息表一旦建立起来,便可以实现认证存取控制.即 s 与 u_i 在实现双向认证的前提下,u_i 能以特权 a^*_{ij} 去存取所需的文件 f_j.

认证存取过程:

第 1 步: s_i 与 u_i 进行双向认证,只要任何一方身份不真实便终止 u_i 请求进入 s 或 s 拒绝 u_i 访问请求.

第 2 步: s 重新计算 u_i 与 s 的共享密钥

$$k_{s\cdot u_i}=(\delta_{u_i})^{s_s v_s-1(\bmod p-1)}\ (\bmod p).$$

第 3 步: s 计算用户 u_i 对文件 f_j 的存取特权.利用"异或"运算的特性,由式(16)可得

$$a_{ij}=((k_{s\cdot u_i}+j)\bmod q)\oplus r_{ij}. \tag{19}$$

第 4 步: s 检查用户 u_i 提供的对文件 f_j 的访问特权 a^*_{ij} 是否与 a_{ij} 相同,若相同,则接受请求;否则,拒绝请求.

4 认证存取控制方案动态特性描述

现在考虑认证存取控制方案在动态环境[5]中的特性.

(1) 把用户 u_i 对文件 f_j 的存取权改为 a'_{ij}.系统 s 只要计算

$$r'_{ij}=((k_{s\cdot u_i}+j)\bmod q)\oplus a'_{ij},$$

并把表 2 的变元 r_{ij} 改为 r'_{ij} 即可.

(2) 从系统 s 中删除用户 u_t.系统 s 只要从表 2 中删除所有的 $r_{tj}(j=1,2,\ldots,n)$便可.

(3) 从系统 s 中删除文件 f_t.系统 s 只要从表 2 中删除所有的 $r_{it}(i=1,2,\ldots,m)$便可.

(4) 把文件 f_t 插入到系统 s 中.系统 s 先计算

$$r_{it}=((k_{s\cdot u_i}+j)\bmod q)\oplus a'_{ij},\ i=1,2,\ldots,m,$$

再把所算得的所有 r_{it} 填入表 2 即可.

(5) 把用户 u_t 插入到系统 s 中.先由网络系统的 KAC 按照 u_t 的注册请求,按第 2.2 节计算 (r_{u_t},s_{u_t}),并由可靠信道交给 u_t,u_t 验证 (r_{u_t},s_{u_t}) 由 KAC 所给的话,再按第 3.1 节中建立过程,计算出 $r_{tj}(i=1,2,\ldots,n)$,系统 s 最后把算得的所有 r_{tj} 填入表 2 即可.

可见,该方案的动态特性良好.

5 认证存取控制方案的安全性分析与计算复杂性说明

5.1 认证存取控制方案的安全性分析

攻击者可以用以下方式攻击上述认证存取控制方案.

(1) 任何人均可得到 $p,w_s,w_{u_i},\delta_s,\delta_{u_i}$ 的值,在系统 s 与用户 u_i 进行双向认证时,若试图从式(9)、式(10)、式(11)和式(13)四式中求解密信息 v_{u_i},v_s,s_s,s_{u_i},其计算的困难性等价于计算 $GF(p)$中离散对数的困难性[7,8].

(2) 攻击者可能试图在不知道 s_{u_i} 及 s_s 的情况下冒充 u_i 及 s.其方法是收集以往认证过程中的信息,然后通过以往的认证信息计算本次认证信息 δ_{u_i} 及 δ_s.

例如,攻击者收集了某次认证过程的 $w_{u_i1}=a^{v_{s1}}\ (\bmod\ p)$及 $w_{u_i1}=(w_{u_i1})^{s_{u_i}}\ (\bmod\ p)$,然后,攻击者向 s 发送(Id_i,r_{u_i}).根据协议,s 生成访问信息 $w_{s1}=a^{v_{s1}}\ (\bmod p)$,攻击者试图通过 $w_{u_i1},\delta_{u_i1},w_{s1}$ 计算

$$\begin{aligned}\delta_{s1}&\equiv(w_{s1})^{s_{u_i1}}(\bmod p)\equiv(a^{v_{s1}})^{s_{u_i1}}(\bmod p)\equiv(a^{v_{u_i1}\cdot(v_{u_i1})^{-1}\cdot v_{s1}})^{s_{u_i1}}(\bmod p)\\&\equiv(a^{v_{u_i1}\cdot s_{u_i1}})^{(v_{u_i1})^{-1}\cdot v_{s1}}(\bmod p)\equiv((w_{u_i1})^{s_{u_i1}})^{(v_{u_i1})^{-1}\cdot v_{s1}}(\bmod p)\\&\equiv(\delta_{u_i1})^{(v_{u_i1})^{-1}\cdot v_{s1}}(\bmod p)\end{aligned},$$

但攻击者想通过 w_{u_i1},w_{s1},求解 v_{u_i1} 及 v_{s1} 的困难性也等价于计算离散对数[9,11].

(3) 攻击者若想由公开信息(Id_i, r_{u_i} ,y,Ids,r_s)及验证式(11)及式(13)求出保密密钥 s_{u_i} 及 s_s,其计算困难也等价于计算离散对数[11].

(4) 攻击者可能试图选择两个整数 s'_{u_i} 及 s'_s,然后由如下两个方程

$$y^{f(Id_i)} \equiv (r_{u_i})^{r_{u_i}} \cdot a^{s'_{u_i}} (\mathrm{mod}\ \ p)\ ,\quad y^{f(Id_s)} \equiv (r_s)^{r_s} \cdot a^{s'_s} (\mathrm{mod}\ \ p)$$

分别求出 r_{u_i} 及 r_s,其计算困难比求解离散对数要难[9,11].

(5) 用户 u_i(i=1,2,…,n)中有 m 人合作试图导出 KAC 的密钥.对于每一个 u_i 的(r_{u_i} ,s_s)及系统 s 的(r_s,s_s),由式(3)和式(5)可构成 m+1 个方程.但由于 k_{u_i} ,k_s,x 均为未知数,而且对于每个 u_i,s 相应的 k_{u_i} ,k_s 均不相同,因此 x 不能唯一决定[12].

(6) 攻击者可能利用式(16)求得 $k_{s\cdot u_i}$.而由式(18)有:

$$k_{s\cdot u_i} \equiv a^{s_s \cdot s_{u_i}} (\mathrm{mod}\ \ p)\ ,$$

但要从上式求出 s_s 及 s_{u_i} 的计算困难性比求解离散对数也要难[9,11].

可见,基于公认的“求解离散对数是计算困难问题[7~9,11]”这一前提下,本文所给方案是安全的.

5.2 计算复杂性说明[5,9~12]

在所给方案中,认证存取控制系统 s 的建立仅需要(s_s·s_{ui}−1)次乘法、一次加法、一次“异或”操作及两次模运算.为了检验一次存取请求,需要[(s_s· s_{u_i} −1)+(v_{u_i} ·s_s−1)]次乘法、一次加法、一次“ 异或 ”操作和两次模运算.

References:

[1] Jan, J.K. A single key access control scheme in information systems. Information Science, 1990,51(1):1~11.

[2] Laih, C.S., Harn, L., Lee, J.Y. On the design of single-key-lock mechanism base on newton’s interpololating polynomials. IEEE Transactions on SE, 1989,SE-15(5):1135~1137.

[3] Chang, C.C. An information protection scheme based upon number theory. The Computer Journal, 1987,30(3):249~253.

[4] Chang. C.C. On the design of a key-lock-pair mechanism in information protection systems. Bit, 1986,26(4):410~417.

[5] Shi, Rong-hua. An authentication-double access control scheme based on one-way function. Journal of Electronics, 1997,19(2): 278~281(in Chinese).

[6] Li, Ji-hong, Xiao, Guo-zhen. A convertible undeniable signature scheme with perfectly Zero-Knowledge feature. Journal of China Institute of Communications, 1999,20(1):71~74 (in Chinese).

[7] Harn L. New digital signature scheme based on discrete Logarithm. Electron Letters, 1994,30(5):396~398.

[8] Harn L. Group Oriented (t,n) threshold digital signature scheme and digital multisignature. IEE Computers Digital Techniques, 1994,141(5):307~313.

[9] Qi, Ming, Xiao, Guo-zhen. A remote password authentication scheme based upon Harn’s signature scheme. Journal of China Institute of Communications, 1996,17(1):114~119 (in Chinese).

[10] Shi, Rong-hua. A redundant binary algorithm for RSA. Journal of Computer Science and Technology, 1996,11(4):416~420 (in Chinese).

[11] Shi, Rong-hua. A public key cryptosystem based on complex problems. Computer Engineering & Science, 1998,20(1):39~42 (in Chinese).

[12] Shi, Rong-hua, Hu, Xiang-ling. An authentication-doubled access control scheme based on compound problem. Mini-Micro Systems, 1998,19(7):49~52 (in Chinese).

附中文参考文献:

[5] 施荣华.一种基于单向函数的双重认证存取控制方案.电子科学学刊,1997,19(2):278~281.

[6] 李继红,肖国镇.一个具有完善零知识特性的可转换不可否认方案.通信学报.1999,20(1):71~74.

[9] 祁明,肖国镇.基于 Harn 签名方案的远距离通行字认证方案.通信学报,1996;17(1):114~119.

[10] 施荣华.一种针对 RSA 的冗余二进制算法.计算机科学技术学报,1996,11(4):416~420.
[11] 施荣华.一种基于复合问题的公钥密码系统.计算机工程与科学,1998,20(1):39~42.
[12] 施荣华,胡湘陵.一种基于复合问题的双重认证存取控制方案.小型微型计算机系统,1998,19(7):49~52.

A Secure Authentication Access Control Scheme Based on Digital Signature*

SHI Rong-hua

(*Department of Computer Science and Technology, Central South University, Changsha* 410075, *China*)

E-mail: shirh@263.net

http://www.csu.edu.cn

Abstract: Based on Harn's digital signature scheme and zero-knowledge proof, an authentication access control scheme for information protection system is presented in this paper. The scheme is safer than previously proposed one. In the scheme, two-way authentication may be done between a user and the system without exposing their secret information, and their sharing secret is used for authenticating the requesting user not to illegitimatimately access the protected file. The scheme can perform the access operation in dynamic environments, such as change access privileges and insert /delete users or files without implicating any user's secret key.

Key words: digital signature; zero-knowledge proof; secure authentication; access control; information protection system

* Received April 21, 2000; accepted September 26, 2000
Supported by the National Natural Science Foundation of China under Grant No.60173041

2002 全国软件与应用学术会议——软件工程专题(NASAC 2002)

征文通知

2002 年全国软件与应用学术会议由中国计算机学会软件工程专业委员会主办,将于 2002 年 11 月 4—6 日在北京召开.届时将进行软件工程等方面的技术与应用交流,会议将出版正式文集,并将优秀论文推荐到核心学术刊物上发表,欢迎大家踊跃投稿.

一、 征文范围(包括但不限于)

需求工程;软件过程;质量保障;软件工具与环境;软件工程实践;软件工程教育;操作系统;中间件;软件复用;软件语言;应用软件

二、 论文要求

1、 论文未曾在其他杂志、会议上发表或录用.
2、 论文长度:每篇限定在 6 页(A4)内.
3、 请以 PDF 或者 PS 格式提交论文.

三、 重要日期

征文征稿截止日期:2002 年 8 月 1 日
论文录用通知日期:2002 年 9 月 20 日

四、联系方式

联系地址:100871,北京大学软件工程研究所
联系电话:010-62757801-2 联系人:王千祥
E-mail:wqx@cs.pku.edu.cn http://www.sei.pku.edu.cn/academic/NASAC.htm