一种基于隐藏证书的自动信任协商模型*)

廖振松　金　海　李赤松

(华中科技大学计算机学院 集群与网格计算实验室　武汉 430074)

摘　要　自动信任协商是一种通过逐步暴露证书和访问控制策略以确立协商双方信任关系的安全方法。隐藏证书采用椭圆曲线加密的原理,具有极好的安全保密性与数据完整性。本文将隐藏证书引入到自动信任协商系统中,提出了一种基于隐藏证书的自动信任协商模型(简称为 HCBATN)。该模型使用隐藏证书来携带并传递双方交换的证书、访问控制策略、资源等信息,充分保护了证书、策略的敏感信息以及用户个人隐私;同时具有单轮回证书交换、较小的网络开销、较低的证书保存、较高安全保密性等优点。

关键词　隐藏证书,自动信任协商,认证,策略,身份加密系统

A Hidden Credential Based Automated Trust Negotiation Model

LIAO Zhen-Song　JIN Hai　LI Chi-Song

(Cluster and Grid Computing Lab, School of Computer, Huazhong University of Science and Technology, Wuhan 430074)

Abstract　Automated Trust Negotiation, for short ATN, is an approach to establishing trust relationship between strangers through iterative disclosure of digital credentials and access control policies. Hidden credential is based on ellipse curve cryptography and has a high secure level. When hidden credential is introduced to ATN, a hidden credential based ATN model, called HCBATN, is presented in this paper. The model uses hidden credential to carry and transfer participants' digital credentials, access control polices and resource/service, which can greatly protect sensitive credentials and policies as well as user's privacy. Meanwhile, due to hidden credential's inherent characteristic, the model has many features of one-round credential exchange, little network cost, little spending on storing and finding credentials, high secure integrality etc.

Keywords　Hidden credential, Automated trust negotiation, Authentication, Policy, Identity-based encryption

1　引言

自动信任协商(Automated Trust Negotiation, ATN)是指通过逐步向对方暴露数字证书以在陌生者之间确立信任关系的一种访问控制方法[1~3]。当访问者与资源/服务不在同一个安全域时,常规的访问控制方法(如 RBAC、MAC 等)不能有效地对访问者的行为进行控制,自动信任协商则可为合法用户访问资源提供安全保障,防止非法用户的非授权访问。

然而,自动信任协商技术在为用户跨域访问资源带来便利的同时,也暴露了许多问题与不足[1~3]:(1)多轮回证书交换:为确立信任关系,协商双方需要进行多个轮回的证书交换;(2)较大的网络传输开销:确立信任关系时,证书的多次交换势必要带来较大的网络传输开销,同时,对于分布存储的数字证书,证书链的发现问题,也增加了网络负担;(3)较弱的证书安全保障:在非安全的 Internet 上传输证书,证书的安全将受到威胁;(4)数字证书中敏感信息保护欠缺:在向陌生人暴露证书时,很可能会泄露一些商业隐私或军事密等重要信息;(5)敏感的访问控制策略受到威胁:协商过程中,资源提供方将暴露访问控制策略,而这些策略在某种程度上来说是敏感的,如军事系统中的提示信息等。

针对当前自动信任协商系统的不足,结合隐藏证书的安全优势,将隐藏证书[4~6]引入到自动信任协商系统中,提出了一种基于隐藏证书的自动信任协商模型:HCBATN。用隐藏证书的优点来弥补自动信任协商中的不足,在后面的章节将会看到,HCBATN 具有单轮回证书交换、低网络开销、安全的证书保护、良好的证书信息和访问控制策略保护等优点。

后面的章节安排如下:第 2 节是对隐藏证书及其系统基本知识的相关介绍;第 3 节详细描述 HCBATN 模型的相关细节,包括组成部分、证书、策略等,并通过实例来说明了 HCBATN 协议的工作流程;在第 4 节里,对 HCBATN 的特征进行了分析;最后是对全文的总结。

2　隐藏证书

隐藏证书的概念,最初由 Jason E. Holt 等在身份加密系统(Identity-Based Encryption, IBE)[7] 的基础上提出[4]。随后,Robert W 等提出了使用隐藏证书来隐藏复杂策略的解决方案,并分析该方案的协议性能等相关问题[5],Keith Frikken 等提出了使用隐藏证书隐藏访问控制策略[6]。隐藏证书基于椭圆曲线加密(Ellipse Curve Cryptography, ECC)[8] 的原理(即大素数相乘容易因式分解困难),具有很好的安全保密性与数据完整性。在这一节里,将对隐藏证书的相关知识进行介绍。

2.1　IBE

隐藏证书是在 IBE 的基础上形成的,因此了解 IBE 是理

*)国家自然科学基金重大专项(90412010)资助。廖振松　博士研究生,研究方向为网格(网络)安全、网格系统分析;金　海　教授,博士生导师,研究方向为计算机系统结构、集群与网格计算、高性能与外存储系统、网络安全等;李赤松　博士研究生,研究方向为网格计算、网格安全等。

解隐藏证书的前提。IBE模型由4个随机算法组成，这些算法分别描述为：

[1]Setup算法。向私钥产生器(Private Key Generator, PKG)输入一安全参数 k(k 包括对有限消息空间 M 和有限密文空间 C 的描述)，产生系统安全参数 *params* 和 *master-key* 值。其中，*params* 对外公布，而 *master-key* 仅为PKG所知。

[2]Extract算法。输入 *params*、*master-key* 以及由0和1组成的任意长度字符串 $ID\in\{0,1\}^*$；输出字符串 d。这里，ID 即为系统的公钥，而 d 是与之对应的私钥。Extract的作用即是为给定的公钥产生对应的私钥。

[3]Enctypt算法。输入 *params*、ID 以及欲传送的消息 m；输出为与 m 对应的密文 c，即 m 由 c 进行保护。

[4]Decrypt算法。输入 *params*、密文 c 以及 d；输出为消息明文 m。

对这4个算法的约束为：

$\forall m\in M$: $Decrypt(params,c,d)=m, c=Encrypt(params,ID,m)$

2.2 隐藏证书系统

在满足IBE的定义和约束的基础上，Dan Boneh等提出了两种改进(主要对系统参数改进)的IBE系统：BasicIdent和FullIdent[7]。而隐藏证书系统则是在FullIdent基础上提出的。一个基本的隐藏证书系统包括：

[1]证书创建函数 $CA\_Create()$：与PKG作用类似，创建证书机构或发布者。

[2]证书发布函数 $CA\_Issue(nym,attribute)$：创建证书，证书的主体为 *nym*，其具有属性 *attribute*。

[3]加密函数 $CT=HC_E(R,nym,Policy)$：对资源 R 进行加密，R 由策略 *Policy* 进行保护，R 的接收者为 *nym*。CT 为加密后的密文。

[4]解密函数 $R=HC_D(CT,P\{Cred_1,\cdots,Cred_n\})$：对密文 CT 进行解密，当且仅当证书 $\{Cred_1,\cdots,Cred_n\}$ 包含有 *nym* 的证书且满足策略 P 时，解密为资源 R。

3 HCBATN

HCBATN建立在隐藏证书的基础上，通过将隐藏证书系统引入到自动信任协商，为证书交换、策略暴露以及消息传输提供安全保密性保障。在这一节里，对HCBATN进行详细介绍，如HCBATN对隐藏证书系统进行改进、证书格式等，并通过实例来说明HCBATN协议的工作流程。

3.1 HCBATN模型

隐藏证书系统并不是一个固定的系统，可以根据具体的应用或需求对其进行修改。为适应自动信任协商的需求，HCBATN是对隐藏证书系统改造。

3.1.1 系统安全参数 *params* 的定义

$params=\langle q,G_1,G_2,\hat{e},n,P,H_1,H_2,\varepsilon,D\rangle$

其中，q 为是一个大素数；G_1 与 G_2 为两组群，其生成元为 q。$\hat{e}$ 为一可管理的线性映射，即 $\hat{e}$ 满足：(1)线性：$\hat{e}: G_1\times G_1\to G_2$；(2)非退化性：若 $\forall p\in G_1$，$\hat{e}(P,P)\in G_2$；(3)可计算性：对于任意的 $P,Q\in G_1$ 存在着有效的算法能快速计算 $\hat{e}(P,Q)$，且满足公式 $\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$。$n$ 指明了消息(M)和密文(C)空间大小，即 $M=\{0,1\}^n$，$C=G_1^*\times\{0,1\}^n$ ($G_1^*=G_1\backslash\{O\}$)。P 是 G_1 中的随机元素 $\forall P\in G_1$，用来产生公钥与私钥。H_1、H_2、ε 和 D 为4个哈希函数，满足 $H_1: \{0,1\}^n\to G_1^*$，$H_2: G_2\to\{0,1\}^n$，以及 $D_s(\varepsilon_s(m))=m$(ε、D 为对称的加密/解密函数，s 为密钥)。

3.1.2 用户证书的格式

在隐藏证书系统中，证书没有固定格式，一般是根据实际的应用自行定义。为了不失一般性，在HCBATN中，证书格式由具体的应用发布证书模板生成，如可将证书模板定为“主体 + 属性”。如在CGCL实验室，贵重仪器的使用权限根据使用者的角色来定的，则可将隐藏证书的格式定为：(*user_name*) : *CGCL* : (*user_role*) : (*current_date*)(括号里的部分表示为发布证书时需要填写的信息)，如 *Tom* : *CGCL* : *phd* : 20/12/2005 表示CGCL实验室的博士Tom可在2005年12月20日使用设备。

3.1.3 HCBATN描述

HCBATN是在隐藏证书系统的基础上进行改进，因此，按照隐藏证书系统的要求，将HCBATN设计为4个组成部分：

[1] 创建CA：$CA\_Create()$，创建证书发布机构，发布证书格式模板

为证书发布者(即证书机构CA)随机选取私钥 $P_{sec}\in z_q^*$ ($z_q^*=z_q\backslash\{0\}=\{1,2,\cdots,q-1\}$，表示为整除 q 的余，除0外)，同时选取 $P_{pub}\in P$ 作为CA的与 P_{sec} 相对应的公钥。同时，根据具体的应用或应用的不同需求，发布一个方便证书生成与读取的模板，如CGCL实验室发布的证书模板为：(*user_name*) : *CGCL* : (*user role*) : (*current_date*)。

[2]证书生成：$CA\ \ Issue(nym,role,date)$，为用户 *nym* 生成具有角色 *role* 可在 *date* 使用的隐藏证书 *Cred*

根据隐藏证书模板的格式，为用户生成与其身份相对应的隐藏证书。输出 *Cred* 为对证书加密的密文 $Cred=P_{sec}H_1(nym\,\|\,role\,\|\,date)$。这里要求 *nym* 是一个长度受限(如要求长度不超过10位)且在一次协商过程中名称唯一；要求 *role* 是系统中有效的角色，否则证书将是无效的；*date* 是指当前的日期，格式为：日/月/年。*role*、*date* 的组合便成了用户的属性信息 $attribute=(role\,\|\,date)$。

[3]消息加密：$CT=HC_E(R,nym,Policy)$，在资源提供端，对由策略 *Policy* 保护将发送给用户 *nym* 的资源 R 进行加密

R 指广义上的资源/服务，可将其理解为明文消息 m 或使用软件的注册码等。在该过程中，首先，随机产生一字符串 $s\in\{0,1\}^n$ 以及一任意值 $r\in Z_q^*$。接着，计算加密密文 $CT=\langle V,\varepsilon_s(R)\rangle$，其中，$V=s\oplus\sigma$，$\sigma=H_2(\hat{e}(P_{pub},Q)^r,n)$，$Q=H_1(nym,attribute)$，策略描述为 $Policy=\{attribute,P_{Pub}\}$。

[4]密文解密：$R=HC_D(CT,Cred)$，在消息接收端，恢复资源 R

对资源 R 的密文 CT 进行解密，$R=Decrypt(params,CT,Cred)$。即根据用户提交的隐藏证书，通过 *attribute* 来计算 V 与 σ，再根据 $s=V\oplus\sigma$ 便可计算 $D_s(R)$，从而恢复传输的资源 R。

3.1.4 约束条件

为保证隐藏证书系统的一致性，需对HCBATN的相关函数进行约束。首先，ε 和 D 为是一对对称加密解密函数，因此，必须满足 $D_s(\varepsilon_s(m))=m$(s 为密钥)。其次，资源/消息密文 $CT=HC_E(R,nym,Policy)$，解密后的资源/消息 $R=HC_D(CT,Cred)$，则隐藏证书的两函数 HC_E 与 HC_D 必须满足 $R=HC_D(HC_E(R,nym,Policy),Cred)$。第三，为了保护敏感策略，要求证书具有不可分辨性，即如果 $Policy_1$ 与 $Policy_2$

是不同的两个策略，对任何不持有与策略 $Policy_1$ 或 $Policy_2$ 相关证书的用户，则都不可辨别密文 CT_1 与 CT_2，其中 $CT_1 = HC_E(R, recipient, Policy_1)$，$CT_2 = HC_E(R, recipient, Policy_2)$。

3.2 HCBATN 协商规则

在对 HCBATN 模型进行描述后，需定义相关的协商规则来规范策略操作以及定义相关的函数。

3.2.1 简单策略与复合策略

在上述 HCBATN 的描述中，都是针对单一策略（即元策略或简单策略）的。而实际应用中，很少是简单策略的。因此，在 HCBATN 中，继续沿用 Jason E. Holt 等在文[4]中提供的三个谓词，用来将简单策略组成为复合策略。

[1] 连接谓词 AND：表示两者均要满足。如 C_1 AND C_2 表示同时需要 C_1 与 C_2。

[2]并列谓词 OR：表示两者取一。如 C_1 OR C_2 表示只需要 C_1 与 C_2 之一即可。

[3]取舍谓词 $MofN(m, C_1, C_2, \cdots, C_n)$：表示需要具有 n 个证书中的任意 m 个。如 $MofN(2, C_1, C_3, C_5, C_6)$ 表示需要具有 C_1, C_3, C_5, C_6 证书中的任意两个。

[4]3 个谓词的混合运用：如 $(C_1$ AND $C_2)$ OR $(MofN(2, C_3, C_4, C_5))$ 表示要么同时具有证书 C_1 与 C_2，要么具有 C_3, C_4, C_5 中的任意两个证书。

3.2.2 函数 HC_E

策略 Policy 有简单策略和复合策略之分，HC_E 提供了相关的规则来处理复合策略。

[1] 若 P 是简单策略（即 P 只需要一个证书即可满足），则直接使用 $CT = HC_E(R, nym, P)$

[2] 若 $P = (P_1$ OR $P_2)$，则 $HC_E(R, nym, P) = \{HC_E(R, nym, P_1), HC_E(R, nym, P_2)\}$

[3]若 $P = (P_1$ AND $P_2)$，则 $HC_E(R, nym, P) = HC_E(HC_E(R, nym, P_1), nym, P_2)$

[4]若 $P = MofN(m, P_1, \cdots, P_n)$，则 $CT = HC_E(R, nym, P)$ 可描述为：

$$HC_E(R, nym, P) = MofN(m, (HC_E(R, nym, P_1), \cdots, HC_E(R, nym, P_n)))$$

3.2.3 函数 HC_D

在具体的协商过程中，策略密文的产生是加密过程，而策略的协商（即证书满足策略需求）则是解密过程。HC_D 对策略的操作与 HC_E 类似。值得一提的是，解密过程是层层解密，逐步进行。如 $P = (P_1$ AND $P_2)$，则必须使用证书 C_1 来解密 $\langle CT_1, P_1\rangle$ 后，才能恢复出 $\langle CT_2, P_2\rangle$。在后面的协议实例里，将会有相关的说明。

3.2.4 HCBATN 协商过程

HCBATN 采用单轮回的协商方式，除协商双方的第一次相互交换 nym 外，整个协商过程中只需要进行一次信息互换：访问者向资源方发送资源访问请求（为保证敏感信息不泄露，该请求可由相关策略进行保护）；资源方接收到访问请求后，使用满足要求的证书来解密访问请求，并将对资源加密的密文发送给访问者。访问者再使用证书进行解密。在下面的一节里，将通过一个实例来说明 HCBATN 的协商过程。

3.3 HCBATN 协议

在这一节里，以一个实例来说明 HCBATN 的协商协议与应用。

3.3.1 场景描述

CGCL 实验室（分布在几个不同的地方，处于不同的局域网里）的高性能设备的开放策略为，实验室的老师、博士可直接使用；对于硕士研究生，若是课题组长，亦可直接使用；对于其他人员，满足（负责人授权，合作伙伴 HP 的成员，科研项目）的任两条方可使用。

3.3.2 策略描述

HCBATN 中，所有的证书都是临时性的（即一般只在一次协商会话中使用），记所有证书的集合为 $Creds = \{C_1, C_2, \cdots, C_n\}$，$C_{iP}$、$P_{Ci}$ 分别表示证书 C_i 可满足的策略以及保护证书 C_i 的策略。则上述场景中，$Creds = \{C_{users}, C_{CGCL}\}$ 策略可描述为：

$$P = (C_{1P} \text{ OR } C_{2P}) \text{OR } (C_{3P} \text{ AND } C_{4P}) \text{OR } MofN(2, C_{5P}, C_{6P}, C_{7P})$$

其中，证书 $C_1 = (nym) : CGCL : (Teacher) : (10/9/2005) = \{user.\ role = Teacher\}$，$C_2 = \{user.\ role = Phd\}$，$C_3 = \{user.\ role = Ms\}$，$C_4 = \{user.\ role = Teamleader\}$，$C_5 = \{user.\ role = Assist\}$，$C_6 = \{user.\ role = HP\}$，$C_7 = \{user.\ role = Sciproject\}$。

Tom 是 HP 公司的一个员工，他需要使用集群进行一次图像匹配算法的测试。向 HCBATN 中心申请并通过身份认证后，Tom 获得 C_6 与 C_7 证书，即 $C_{Tom} = \{C_6, C_7\}$。同时，Tom 在这次测试中，涉及到了一些公司的机密信息，他要求使用 HP 公司捐赠的集群服务器，即 $P_{Request} = (C_{8P}$ AND $C_{9P}\}$，其中 $C_8 = \{device.\ role = CGCL\}$，$C_9 = \{device.\ role = HP\}$。因 CGCL 实验室除了 HP 公司捐赠的仪器外，还有来自 IBM、Intel 的，因此，$C_8, C_9 \in C_{CGCL}$。

3.3.3 协议描述

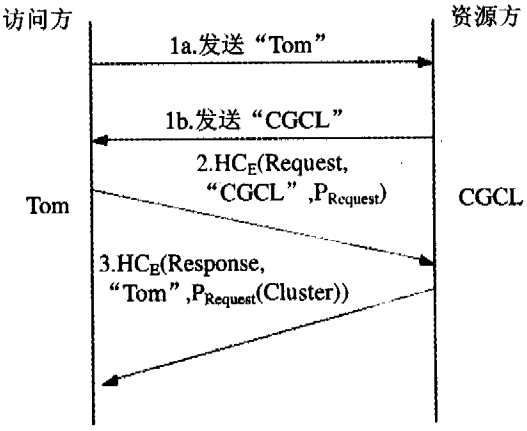

图 1 HCBATN 协议

HCBATN 的协议如图 1 所示。对其解释为：

①资源访问者 Tom 与资源提供方 CGCL 进行"名片"互换，为进一步的协商提供消息接受者；

② Tom 向 CGCL 发送资源访问请求，请求接收者为 CGCL，请求由策略 $P_{Request}$ 保护；

③ CGCL 接收到访问请求后，使用自己所拥有的证书进行解密，以便为 Tom 的访问分配资源；同时，将分配的资源以密文的形式发送给接收方 Tom。

3.3.4 协商描述

在 Tom 与 CGCL 交换名称后，Tom 发出了访问请求 $HC_E(Request, "CGCL", P_{Request})$。在此请求中，$P_{Request}$ 是使用 $params$ 中的加密 ε 进行加密的。CGCL 收到访问请求后，

（下转第 74 页）

6 ÄOzdo~gano~glu H, Vijaykumar T N, Brodley C E, et al. SmashGuard: A Hardware Solution to Prevent Security Attacks on the Function Return Address. School of Electrical and Computer Engineering 465 Northwestern Ave, Purdue University, November 2003
7 Cowan C, Pu C, Maier D, et al. StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks. http://www.immunix.org/documentation.html.
8 Richarte G. Four different tricks to bypass StackShield and StackGuard protection. Core Security Technologies, April 9, 2002 - June 3, 2002
9 Bulba Kil3r. Bypassing StackGuard And StackShield, May, 2000. http://www.phrack.org/show.php? p=56&a=5 (April 9, 2002).
10 Richarte G. Four different tricks to bypass StackShield and StackGuard protection. Core Security Technologies, April 9, 2002
11 Bergeron J, Debbabi M, Desharnais J, et al. Detection of Malicious Code in COTS Software: A Short Survey. In: First International Software AssuranceCertification Conference (ISACC'99), Washington D C, Mar. 1999
12 Bergeron J, Debbabi M, Erhioui M M, et al. Static Analysis of Binary Code to Isolate Malicious Behaviors. In: Proccedingsof the 8th Workshop on Enabling Technologies on Infrastructure for Collaborative Enterprises, pages, 1999. 184~189
13 尚明磊,黄皓. 缓冲区溢出攻击的分析与实时检测. 计算机工程, 2005, 31 (12): 36~38
14 Intel. IA-32 Intel Architecture Software Developer's Manual Volume 2A: Instruction Set Reference, A-M. http://www.intel.com, 2004
15 AMD. AMD64 Architecture Programmer's Manual Volume 2: System Programming. http://www.amd.com, 2003
16 刘昌勇. CPU 原理分析. http://www.itdoor.net/pages/27, 21932,1,1076917028.html, 2004-02-16
17 Fiskiran A M, Lee R B. Runtime Execution Monitoring (REM) to Detect and PreventMalicious Code Execution. IEEE International Conference on Computer Design ICCD'04), 2004. 452~457
18 Gassend B, Suh G E, Clarke D, et al. Caches and Hash Trees for Efficient Memory Integrity Verification. In: Proc. Int Symposium on High-Performance Computer Architecture (HPCA), 2003. 295~306
19 Burger D, Austin T M. The SimpleScalar Tool Set, Version 2.0. Computer Architecture News, 1997. 13~25
20 Austin T, Larson E, Ernst D. Simplescalar- an infrastructure for computer system modeling. IEEE, February 2002. 59~67

(上接第 61 页)

使用 HC_D 将其恢复(过程中将使用到 *params* 中的解密 D): $\langle CT_8, \langle CT_X \rangle\rangle$。由于 $C_8 \in C_{CGCL}$, CGCL 使用 C_8 将继续看到 $\langle CT_9 \rangle$, 同样的道理, CGCL 使用 C_9 后将可看到访问请求 Re *quest*。

此时, CGCL 为 Tom 的此次访问分配资源 *Cluster*(如"以用户名 CGCL、密码 HP 从 8754 端口登录 192.168.1.240 集群"), 并将使用 Re *sponse* 返回给 Tom。同样, Tom 将使用 Re *sponse* 解密 $P_{Re\ sponse}(Cluster)$ 得到 $P_{Cluster}$; 在提供他的证书来满足便可恢复 *Cluster*。此时, 一个完整的信任协商便成功了。

4 HCBATN 特征分析

隐藏证书在信任协商中, 可带来许多优势, 如: (1)可解决基于 PKI 认证系统中的"谁先"的问题: 自动信任协商系统中, 协商双方都不愿意先暴露自己的策略; (2)访问控制策略不会让非授权的接收者所了解: 策略、资源信息都是密文, 窃听者无法解开, 或者说解密代价太大, 获得信息后已失去意义; (3)证书没固定的格式, 可随意创建和使用等。

除上述特点外, HCBATN 还具有如下特征:

[1]灵活的证书形式, 为证书的创建和使用带了便利。相比 X.509、SPKI/SDSI 等证书, 隐藏证书的使用更为简单、便捷;

[2]没有发现证书的网络开销。在 PKI 信任协商系统中, 证书链的发现, 带来了大量的网络传输开销。同时, 也影响了信任协商的效率和成功率。而在 HCBATN 中, 证书一般只限于一次协商会话, 是临时的, 由协商双方集中管理的, 没有发现证书的网络开销;

[3]减少管理证书的开销。在 HCBATN 中, 证书的创建和使用是任意的, 不需要像 PKI 一样使用 OLAP 来管理发布的证书和 CRL 来管理过期的证书;

[4]单轮回证书交换, 提高了协议的性能。在 HCBATN 中, 除最初一次名称的交换外, 整个过程证书的交换只有一个轮回, 这极大地提高了信任协商的协议性能, 提高了协商效率;

[5]具有更高的证书安全保密性。HCBATN 中, 信息都是以密文的形式进行的, 保证了传递信息、策略的安全性; 同时, 也有效地保护了用户隐私。

结束语 自动信任协商为资源共享、服务调用、商业交易等提供了跨域的安全保障, 是访问控制技术又一道防线。针对当前自动信任协商系统的不足, 本文引入了隐藏证书, 提供了一种基于隐藏证书的自动信任协商模型。HCBATN 对隐藏证书系统进行了改造, 使得其更接近于现实的应用。文中对 HCBATN 的组成与工作原理进行了详细的描述, 介绍了其操作规范, 并通过一个实际的例子来说明其 HCBATN 协议以及其工作流程, 总结了 HCBATN 的特征。

在下一步的工作中, 主要是将 HCBATN 应用到实际的系统中, 或在应用中体现 HCBATN 优势。针对中国教育网格支撑平台[9](ChinaGrid Supporting Platform, CGSP)的多域(一个大学可看作为一个域)、资源复杂、操作系统异构等特征, 将 HCBATN 引入到 CGSP 中, 为校园之间的资源共享与访问提供更高的安全保障。

参 考 文 献

1 Winsborough W H, Li Ninghui. Safety in Automated Trust Negotiation. In: Proceedings of the 2004 IEEE Symposium on Security and Privacy, IEEE Press, 2004. 123~135
2 Winsborough W H, Li N. Protecting sensitive attributes in automated trust negotiation. In: Proceeding of ACM Workshop on Privacy in the Electronic Society, ACM Press, 2002. 102~113
3 Winsborough W, Seamons K, Jones V. Automated Trust Negotiation. In: Proceeding of DARPA Information Survivability Conference and Exposition, ACM Press, 2000. 156~182
4 Holt J E, Bradshaw R, Seamons K E. et al. Hidden crdentials. In: Proceedings of 2nd ACM Workshop on Privacy in the Electronic Society, ACM Press, 2003. 1~8
5 Bradshaw R W, Holt J E, Seamons K E. Concealing Complex Policies with Hidden Credentials. In: Proceedings of the 4th ACM Conference on Computer and Communications Security, ACM Press, 2004. 245~253
6 Frikken K, Atallah M, Li Jiangtao. Hidden Access Control Policies with Hidden Credentials. In: Proceedings of the 3rd ACM Workshop on Privacy in the Electronic Society, ACM Press, 2004. 130~131
7 Boneh D, Franklin M. Identity based encryption from the Weil pairing. In: Proceedings of Crypto2001, Advances in Cryptology, Lecture Notes in Computer Science, Vol 2139, Springer-Verlag, 2001. 213~229
8 Gura N, Eberle H, Shantz S C. Generic implementations of elliptic curve cryptography using partial reduction. In: Proceedings of the 9th ACM Conference on Computer and Communications ecurity, ACM Press, 2002. 1771~89
9 中国教育科研网格公共支撑平台工作组. 中国教育科研网格公共支撑平台设计规范. 北京: 清华大学出版社, 2004