开放式网络环境下的访问认证问题研究*

张龙军[1,2], 黄继武[3]
(1. 上海交通大学 计算机科学与工程系, 上海 200030;
2. 中国科学院信息安全国家重点实验室, 北京 100039;
3. 中山大学 信息科学与技术学院, 广东 广州 510275)

摘 要: 对开放式网络环境下的访问认证中存在的安全问题进行了分析和研究。为了防止这些问题的发生, 设计了一个安全认证系统并分析了其安全性和复杂性。该系统具有安全性强、形式简单、运算简便以及便于实现的特点。

关键词: 开放式网络; 访问控制; 安全认证
中图分类号: TP393.08 文献标识码: A 文章编号: 0529-6579 (2003) 06-0019-05

随着社会活动和经济活动电子化、信息化的不断发展, 计算机网络上的各种访问行为与日俱增, 与之相应地需要各种访问控制系统。认证系统是访问控制系统的基础, 目前的访问认证系统已有很多, 这些系统在设计上也许没有明显的漏洞, 但是其加密算法或数字签名算法都是基于 DES、RC4、MD5 等私钥密码体制或 RSA 公钥密码体制。由于私钥密码体制本身的局限如密钥管理困难以及 RSA 公钥密码体制所面临的安全威胁, 使得这些访问认证系统在底层存在着一定的安全隐患[1]。本文针对现有访问认证系统存在的安全隐患, 从底层入手, 设计了一个具有较低复杂性和较高安全性的访问认证系统。

1 开放式网络环境下的访问安全问题分析

在开放式网络环境下, 由于交换和拨号功能的加入, 影响并降低了访问网络的安全性。这主要体现在: ①如何对授权用户的身份进行认证; ②如何确定信息是安全的。

目前开放式网络不安全的主要原因主要有: ①网络自身的安全缺陷; ②网络的开放性; ③黑客攻击。在开放式网络中, 系统本身的安全及系统传送的信息的安全都会受到严重的威胁。在开放式网络环境下, 非法用户普遍采用的是主动攻击模式, 即非法用户可以任意地截获并修改网络层的数据, 甚至将原数据删除而用伪造的数据取代。或者采取身份伪装的方法, 非法用户采用欺骗的方法伪装成系统中一个合法用户, 截取并处理系统发送给该合法用户的信息。但是, 如果采用数据完整性检验和身份认证等密码技术就可以有效防止这些攻击。目前, 除了防止对系统进行破坏的攻击以外, 最大的安全隐患就是非法用户对系统的访问。也就是说非法用户采用欺骗或破获合法用户密码等方法对系统进行非法访问已经成为必须解决的重点问题。因此, 为了确保开放式网络的安全, 必须能够提供一个强有力的访问认证系统。

一个安全的认证系统应当能够提供如下的服务: ①访问控制: 非法用户被拒绝使用系统资源, 合法用户只能访问系统授权使用的资源; ②可信性: 信息的来源是真实可信的; ③不可抵赖性: 信息的发送方和接收方不能否认他们所发出的或已收到了信息; ④完整性: 信息接收者能够确信所获得的信息在传输过程中没有被修改或替换。

2 信息加密算法与数字签名算法

访问认证系统的核心技术是信息加密和数字签名技术, 因此加密和签名算法的安全性就成为访问认证系统安全性的重要保证。不同的网络系统的资源不同, 对认证系统的具体要求不同。但是, 有效

* 收稿日期: 2002-12-02
基金项目: 国家自然科学基金重点资助项目 (60133020); 国家自然科学基金资助项目 (69975011, 60172067); "863" 计划项目 (2002AA144060); 教育部博士点基金项目 (20020558038); 教育部跨世纪优秀人才基金广东省自然科学基金重点项目 (013164)
作者简介: 张龙军 (1964 年生), 男, 博士, 副教授; 通讯联系人: 黄继武; E-mail: isshjw@zsu.edu.cn

性是衡量网络系统质量的一个重要标准。因此在保证认证系统安全性的前提下，保持高的效率是认证系统的追求目标，应当尽可能地采用计算简单的密码算法。私钥密码算法计算简单，实现速度快。但是又存在着密钥管理困难的问题，特别是在大型网络中这一问题显得尤为突出。而目前的主流公钥密码体制——RSA 密码算法虽然克服了私钥密码算法存在的密钥管理困难的问题，但又存在着运算量大、实现速度慢的问题。因此，在本文的认证系统中，信息加密和数字签名均基于密码学界公认的下一代公钥密码体制——椭圆曲线密码算法[2]。

2.1 信息加密算法设计

我们可以建立一种类 ElGamal 型椭圆曲线公钥密码体制，首先将有限域 F_p 上的两数相乘（即数 m 的 k 次幂）映射为椭圆曲线 E 上的两点相加（即点 P 乘 k），在这样的运算映射下，就可以将椭圆曲线离散对数问题对应于有限域上的离散对数而建立起安全简便的密码体制，进而设计出加密算法。

2.1.1 算法描述

(1) 构造有限域 F_p 上的一条椭圆曲线 E，群 $E(F_p)$ 的阶有大素因子，即保证椭圆曲线群上的离散对数是难解的。确定一个元素 $G \in E(F_p)$，G 是一个公开的固定点(即公开钥)，有一个易于计算的函数 $f: E(F_p) \to s \in F_p$，s 是信息单位组成的群——如有限域 F_p。

(2) B 选取任意一个随机整数 K_B（保密），计算出 $G_B = K_B * G$，并且公开 G_B。

(3) A 将明文消息 m 编码为椭圆曲线上的点 $P_m \in E$。设 $P_m = (x, y)$，l 是一个小整数，编码的过程即寻找 $x, y \in F_p$，$2^l m \leqslant x \leqslant 2^l (m+1)$，使得 x 和 y 满足 $E: y^2 = x^3 + ax + b$。

(4) A 另外选取一个随机整数 K_A（保密），计算 $G_A = K_A * G$ 及 $P_m + f(K_A * G_B) \in s$ 并把 $\{G_A, P_m + f(K_A * G_B)\}$ 发送给 B。

(5) B 收到 A 发送的信息以后，首先计算出函数 $f(K_B * G_A)$ 的值，在这里有 $f(K_B * G_A) = f(K_B * K_A * G) = f(K_A * G_B)$ 成立。再从收到的 s 的元素中减去 $f(K_B * G_A)$ 即可得到 P_m。

(6) B 从点 P_m 的 x 坐标中去掉最低 l 位，余下的便是明文消息 m。

2.1.2 安全性和复杂性分析

对于非法截取信息者，仅仅知道 $K_B * G$ 和 $K_A * G$ 以及 G，都无法获知 K_A 和 K_B，这是因为椭圆曲线离散对数问题是难解的。所以在不知道 K_A 和 K_B 的情况下就不能求得 $K_A * G_B = K_B * GA = K_B * K_A * G$，也就不可能非法获得明文信息。

在我们设计的类 ElGamal 型椭圆曲线密码体制里，需要发送 4 个域元素来传达只包含 2 个域元素的信息，所以其信息扩展系数为 2。如果有可用的寄存器（如在软件实现时），则可以通过预先计算 P 的乘法来大大加快计算 k_P 的速度。

2.2 数字签名算法设计

在实际应用中，签名信息是一长串输入序列。在这种情况下给系列中的每一个元素都加带签名是困难的。因此，首先用 hash 函数产生一个较小的消息摘要，而只在这个消息摘要上签名。hash 函数是一个公开知识，为防止伪造和模仿，必须不能找到两种导致相同输出的不同输入，同时也必须找不到输出为一给定值时的输入。

2.2.1 算法描述

(1) 系统初始化：

构造椭圆曲线 $E: y^2 = x^3 + ax + b$（$a, b \in F_p$，p 是一个素数），为了保证安全性，该椭圆曲线必须是非超奇异的；

选择一个公开的基点 $P \in E(F_p)$；

其阶为 $l = \mathrm{ord}(P)$。

(2) 密钥生成：

A 随机选取一个整数 s 作为秘密钥，将公开点 $P_A = sP$ 作为公开钥。

(3) 签名生成：

A 随机选取一个整数 $k \in \{1, 2, \cdots, l-1\}$，计算：$R' = kP$，并将 R' 传送给 B；

B 随机选取一个整数 $r_1 \in \{1, 2, \cdots, l-1\}$，计算：$R = r_1 R' = (r_x, r_y)$，其中 r_x 和 r_y 分别是 R 的 x 坐标和 y 坐标；

B 随机选取一个整数 $r_2 \in \{1, 2, \cdots, l-1\}$，并且计算：$m' = mr_2 \bmod l$ 和 $r = r_2 r_x \bmod l$，并且将 m' 和 r 传送给 A；

A 计算：$y' = k^{-1}(m's + r) \bmod l$，将 y' 传送给 B；

B 计算：$y = (r1^{-1} r_2^{-1 \otimes y'}) \bmod l$，输出签名 (R, y)。

(3) 签名验证：检验 $yR = mP_A + r_x P$ 是否成立，若成立则签名正确，否则签名不正确。

2.2.2 安全性和复杂性分析

这种数字签名算法的安全性是基于椭圆曲线离散对数问题的，如果非法用户要想伪造签名则他就要设法使得验证等式 $yR = mP_A + r_x P$ 成立，但这是不可能的。因为在等式

$yR = mP_A + r_xP$ 中，如果非法用户先确定 r_x，则求解 y 相当于求解椭圆曲线离散对数问题，至少在目前来看他是无法求解的。如果非法用户先确定 y 再求解 r_x，则相当于他要求解一个指数问题，这在目前也没有有效解法。因而，这种基于椭圆曲线密码体制的数字签名算法是安全的，并且具有形式简单、运算简便的特点。

值得注意的是，当加密和数字签名相结合时，加密和数字签名过程的顺序不一样将导致不同的安全强度。如果要求 A 给 B 发送消息时不仅要对消息进行签名而且还要对消息进行加密，那么在这种情况下，A 可以采用如下两种方式发送消息：一种是先签名，后加密；另一种是先加密，后签名。假设给定明文消息 x，在第一种方式中，A 先对 x 进行签名 $y = \mathrm{Sig}A\ (x)$，然后使用 B 的公开加密变换对 x 和 y 进行加密 $z = E_B\ (x, y)$，最后 A 将密文 z 传送给 B。当 B 收到 z 时，首先利用他的解密变换对 z 进行解密获得 (x, y)，然后使用 A 的公开验证函数检测 $\mathrm{Ver}A\ (x, y) = \mathrm{true}$ 是否成立。在第二种方式中，A 先利用 B 的公开加密变换对 x 进行加密 $z = E_B\ (x)$，然后对 z 进行签名 $y = \mathrm{Sig}A\ (z)$，最后 A 将 (z, y) 发送给 B。B 解密 z 获得 x，然后使用 $\mathrm{Ver}A$ 验证 A 对 x 的签名 y。用第二种方式就会产生一个问题，如果一个敌手 O 获得一对 (z, y)，他就可以用 $y' \mathrm{Sig}O\ (z)$ 代替 y 得到一对 (z, y')，将 (z, y') 发送给 B，B 先对 z 解密，然后使用 O 的验证算法 $\mathrm{Ver}O$ 验证签名的合法性。这样，B 就会误认为消息 x 来自于 O。由于存在这种潜在的危险，因而最好是先签名后加密。

3　安全认证系统设计

为叙述方便，本文约定以下符号：AC 为系统认证服务器 (Authentication Center)；S 为访问服务器 (Server)；C 为远程用户 (Client)；e 表示加密算法；d 表示解密算法；Sig 表示数字签名算法。

在设计访问认证系统时，一个需要考虑的重要因素是通信双方的计算能力往往是不对等的。通常，认证的客户端——访问服务器 S 往往具有较低的计算能力，而认证的服务器端——认证中心 AC 则具有较高的计算能力。因此，在设计和实现具体的认证系统时，应当充分考虑降低用户端的计算复杂性。

3.1　安全认证系统的体系结构

本文的安全认证系统由认证中心 AC、访问服务器 S 和客户机 C 组成，客户机 C 与访问服务器之间通过开放式公共网络进行通信。访问服务器 S 主要用于为用户提供访问网络资源的接入服务，并且可以作为访问用户向认证服务器请求认证的代理，它是实现访问的关键设备。认证中心 AC 把多个用户的信息和访问服务器的有关信息集中起来进行统一管理，对向访问服务趋发出访问请求的用户进行认证，根据不同用户的级别提供不同的访问权限。本文的安全认证系统具有 Client/Server 结构，访问服务器 S 作为认证系统的客户端，认证中心 AC 作为认证系统的服务器端。这种结构为安全认证提供了理想的分布式解决方案。系统可将用户和 AC 的所有敏感信息放在单一的、集中的数据库，而不是分散在网络的不同设备中。在单个安全操作系统平台上运行的认证服务器比遍及网络的若干访问服务器更容易确保安全。在系统中，用户的认证及访问授权和实际访问是分开的，并且重要数据集中保存，这样大大提高了系统的安全性和灵活性。

3.2　安全认证的过程

本文中安全认证系统的实现不需要特殊的物理设备，惟一的设备要求是各个参与者之间可以通过网络进行通信。对通信网络也没有特殊的要求，公共网络就可以满足要求。认证过程如下：

3.2.1　初始化

(1) 构造椭圆曲线 $E: y^2 = x^3 + ax + b\ (a, b \in F_p, p$ 是一个素数)，该椭圆曲线是非超奇异的；

(2) 选择一个公开的基点 $P \in E(F_p)$，其阶为 $l = \mathrm{ord}(P)$。

(3) 客户 C 随机选取一个整数 $d_C \in \{0, 1\}$ 作为秘密钥，计算 $e_C = d_CP$，将 e_C 作为其公开钥。客户 C 同时拥有椭圆曲线签名方法 $\mathrm{Sig}C$。

(4) 访问服务器 S 随机选取一个整数 $d_S \in \{0, l\}$ 作为秘密钥，计算 $e_S = d_SP$，将 e_S 作为其公开钥。访问服务器 S 同时拥有椭圆曲线签名方法 $\mathrm{Sig}S$。

(5) 认证中心 AC 随机选择一个整数 $d_A \in \{0, l\}$ 作为其秘密钥，计算 $e_A = d_AP$，将 e_A 作为其公开钥。同时 AC 也拥有椭圆曲线数字签名方法 $\mathrm{Sig}A$。

3.2.2　认证

(1) 注册：用户应当首先到认证中心进行注册，具体过程是：

C 生成由名字和口令组成的标识符 V，并选择一个随机整数 r_1，计算 $M = e_A(r_1 V \bmod l)$。

C 向 AC 发出请求准予访问系统信息 R，并用椭圆曲线签名方法进行签名，即计算 $C_R = \mathrm{Sig}C(R)$。将 (C_R, M) 发送给 AC。

AC 对 (C_R, M) 进行签名验证，以判断确实是 C 所发的信息还是冒名者入侵。

AC 随机选择一个整数 $k \in \{1, \cdots, l-1\}$, 计算 $Q = kP$ 并加签名后传送给 C;

C 在验证了 AC 的签名后另外选择一个随机整数 $r_2 \in \{1, \cdots, l-1\}$, 计算:

$$Q' = r_2 Q = (r_x, r_y)$$

$$r = (r_1 r_x) \bmod l$$

将 r 加签名后传送给 AC。

AC 由 M 解密得到 $r_1 V \bmod l$, 为 C 生成一个唯一的身份识别符 ID, 计算:

$$C_{ID} = S_A(ID)$$

$$y = k^{-1}(r_1 V d_A + r) \bmod l$$

$$A_{ID} = e_C(C_{ID} \mid y)$$

AC 将 A_{ID} 传送给 C。

C 得到 A_{ID} 以后, 解密得到 C_{ID} 和 y, 计算:

$$M' = (r_1^{-1} r_2^{-1} y) \bmod l =$$

$$r_1^{-1} k^{-1} (r_1 V d_A + r) \bmod l$$

(2) 访问系统：当用户欲访问系统即客户 C 向访问服务器 S 发请求访问信息时，系统首先要求用户输入合法用户标识符，C 将自己从认证中心 AC 处得到的标识符用访问服务器 S 的公钥加密后传送给 S，C 发出的访问信息中包含认证 (V, M')。访问服务器 S 从认证包中取出认证信息，然后将 C 的请求信息用 AC 的公钥进行加密，并用椭圆曲线数字签名方法进行签名，即计算 $S_R = \mathrm{Sig}S(R)$。随后将签名信息与加密后的请求信息一起放入请求数据包将发送给 AC 进行认证。

AC 用 S 的公开钥验证 S_R 是不是 S 的签名，即计算 $e_S(S_R)$，以证实消息是否确实来自 S；为确保进一步的安全，AC 还要向 S 发询问信息。询问包中的应答信息与访问请求包中的请求信息值应当相同，以表明它们是一对请求和应答。则 AC 对 S 发送来的 C 的请求信息用他的秘密钥解密后进行认证。否则，说明是非法入侵者冒名，则 AC 向 S 发送拒绝访问应答，拒绝 S 的操作申请。AC 对 S 传送过来的 C 的请求信息进行验证以判断其身份是否合法，即计算 $M'Q = Ve_A + r_x P$ 是否成立，如果正确，则说明 C 是合法用户，准予其访问系统；否则说明 C 是非法用户，拒绝其访问系统。将结果用 S 的公钥加密后进行签名发送给 S。S 收到 AC 发送来的应答包后，先将其用自己的秘密钥解密并用 AC 的公钥进行签名认证以确认为 AC 所发。若收到的是拒绝访问包，提示用户本次访问请求被拒绝；若收到的是接受包则表明 C 的访问被接受。

4 安全认证系统分析

4.1 防止攻击的安全措施

在本文的认证系统中 AC、S 及 C 之间传递数据包时，都使用了基于椭圆曲线密码体制的椭圆曲线数字签名技术，这样可以保证传递信息双方身份的相互确认和信息完整性确认，以防黑客假冒和对信息的修改或伪造。如果黑客要冒名顶替或者破坏信息的完整性，他就必须破解椭圆曲线数字签名技术，这至少在目前是无法实现的，这样就保证了系统的安全性。为防止非法窃听，在 AC、S 及 C 之间传递数据包时，对用户口令等重要信息都要利用椭圆曲线加密技术进行加密，这样就可以防止非法用户对重要明文信息的窃取。

4.2 安全性和复杂性分析

本文中认证系统的安全性是以椭圆曲线密码体制的安全性为保证的，而椭圆曲线密码体制的安全性是基于椭圆曲线离散对数问题的难解性之上的。由于目前还没有对椭圆曲线离散对数问题的有效解法，所以本系统是安全的。合法用户采用椭圆曲线加密方法和椭圆曲线数字签名方法处理请求信息和标识符之后，非法用户不能伪造合法用户的请求信息和标识，因为非法用户在不知道合法用户秘密钥的情况下是不能对椭圆曲线离散对数问题求解的，因而系统也就不会接受其访问请求。同样基于椭圆曲线离散对数的难解性，他也不可能得知双方交换信息的内容，也就无法对截获的信息进行流量分析、重传以及修改或伪造。

由于在认证过程中只涉及到有限域上椭圆曲线的模逆和点加，运算相对简单，因而实现也较为容易。具体应用时可以采用预处理的方法，给系统的每一个合法用户预先产生好身份标识符，当用户要访问系统时只要进行认证即可，这样可以减少计算时间。

4.3 椭圆曲线密码体制的安全性分析

由于其自身的优点，椭圆曲线密码学一出现便受到广泛关注。近年来，随着计算机网络，特别是 Internet 的发展，该学科也找到了它的应用领域。以椭圆曲线上的有理点构成的 Abel 群为背景实现密码体制已经是公钥密码学领域的一个重要课题，椭圆曲线密码体制逐渐成为一个十分令人感兴趣的密码学分支，以椭圆曲线构建密码体制的基础是椭圆曲线离散对数的难解性[3]。

一个群 G 上的离散对数问题是这样定义的：已知 α，$\beta \in G$，确定一个整数 x 使得 $\beta = \alpha^x$，若 x 存在，则 x 称作以 α 为底的 β 的离散对数。x 唯一

确定 α 的模的阶。用椭圆曲线 E 上的点的群替代 G，用群加法代替群乘法，用 E 上的点 P 代替 α，即可得椭圆曲线离散对数的定义：若 E 为 F_p 上的椭圆曲线，G 为 E 上一点，则 E 上关于 G 的椭圆曲线离散对数问题为：给定一点 $N \in G$，求解整数 x，使 $xG = N$。这里的 xG 表示数乘，即 x 个 G 相加。容易看出，对该系统的攻击依赖于在域 F_p 上求解方程：$G^x \equiv N \bmod p$ 或计算：$x = \log_G N \bmod (p-1)$。椭圆曲线离散对数问题比有限域上的离散对数问题更难求解，在一定条件下这一问题已经被证明是完全 NP 问题，被认为是几乎不能求解的[4]。椭圆曲线密码体制的强度主要依赖于椭圆曲线的阶 $E(F_p)$ 是否含有大素因子，因为对于 $\#E(F_p)$ 含有大量小素因子，已有 Pohiling Silver-Hellman 算法可解其椭圆曲线离散对数问题。而对于 $\#E(F_p)$ 有大素因子的椭圆曲线离散对数问题，目前还没有有效的攻击方法[5]。

5　结　语

针对开放式网络环境下的访问认证问题，本文从安全认证的底层入手设计了一个安全认证系统，克服了现有认证系统中存在的安全缺陷，提高了认证系统的安全性。本系统的主要设计考虑是安全性、对用户透明、便于管理和可扩充。本文设计的安全认证系统，不仅封堵了在协议上容易产生的安全漏洞，而且还加强了加密算法和数字签名算法的安全性。由于椭圆曲线密码体制的运算相对于目前通用的 RSA 密码体制较为复杂，因而本系统在运行速度上还有待进一步提高，对一些基本算法还应当结合具体的应用环境加以优化。

参考文献：

[1] GILMORE C, KORMANN D, RUBIN A D. Secure remote access to an Internet Web server[J]. IEEE Network, 1999, 13(6): 31—37.

[2] MENEZES A, Van OORSCHOT P, VANSTONE S. Handbook of applied cryptography[M]. New York: CRC Press, 1996.

[3] IEEE—P1363 Standard. Public Key Cryptographic Standard. 2000.

[4] MILLER V. Uses of elliptic curves in cryptography // Advances in Cryptology-CRYPTO'85[D]. Berlin: Springer-Verlag, 1986: 417—426.

[5] Elliptic Curve Cryptography. Standards for efficient cryptography group. http://www.secg.org.

Research on the Access Authentication in Open Network

ZHANG Long jun[1,2], *HUANG Ji wu*[3]

(1. Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200030, China;
2. The State Key Laboratory Of Information Security, Beijing 100039, China
3. School of Information Science and Technology, Sun Yat-sen University; Guangzhou 510275, China)

Abstract: Based on the analysis of the security in open network, a secure authentication system is designed to avoid the possible security problems. The security and the complexity of the proposed system is analyzed. The system has the merits of strong security, simple form, low computation complexity and easy to realize.

Key words: open network; access control; secure authentication