

校园网络身份认证技术平台研究

叶汝军

(浙江商业职业技术学院, 浙江 杭州 310053)

摘 要: 研究校园网络平台中安全身份认证技术问题, 提出基于快速密钥生成算法的身份认证方式. 这种认证方式只需要在初次进行身份认证时从网络平台服务方得到密钥, 运用奇数筛选理论减少了身份验证的计算量, 提高了校园网络平台中安全身份认证的效率. 实验证明, 该算法能够实时认证操作者的身份, 进一步保证校园网络平台的安全.

关键词: 校园网络; 身份认证; 快速密钥生成

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2012)03-0155-04

Campus Network the Identity Authentication Technology Platform

YE Ru-jun

(Zhejiang Vocational College of Commerce, Hangzhou 310053, China)

Abstract: Research campus network platform of the safety in the identity authentication technology. This paper puts forward the key generation algorithm based on rapid identity authentication, the authentication way need only in the first time when the identification from the network platform service party, using an odd number of screening key theory reduced the identity authentication of calculation and improve the safety in the campus network platform identity authentication of the efficiency. Experimental results show that this algorithm can real-time the authentication of the operator, further ensure that the campus network as the safety of the platform.

Key words: campus network; identity authentication; session key

1 引言

随着校园网络的不断发展, 基于校园网络的应用越来越多, 这对校园网络的安全性提出了更高的要求. 当前的平台多是基于身份认证技术的认证管理模式. 使用传统方式进行身份认证需要有一个作为媒介的服务器, 在服务器中将校园网络平台数据库中的相关数据信息与使用者输入的相关数据信息进行配准, 从而识别使用者的身份^[1]. 在识别使用者身份的过程中, 需要两次使用作为媒介的服务器, 在服务器中通过运算获取密钥, 并且将获取的结果与数据库中的密钥进行对比分析, 从而完成校园网络平台中使用者身份的识别. 因为数据库中密钥的数据量非常大, 所以对比次数非常多, 计算量很大, 导致识别时间过长, 识别效率过低, 频繁的计算导致安

全性能得不到很好的保证. 所以, 快速识别校园网络平台中使用者身份是校园网络平台安全问题的核心^[2-6].

2 身份认证技术原理

在校园网络平台的环境中, 通常采用密钥生成加密方式, 为了外界恶意攻击, 保证校园网络的安全, 而密钥的产生往往具有身份认证的要求. 校园网络身份核对分为具体步骤为^[7-8]:

(1) 第一步需要构建一个产生密钥的随机素数群: 随机选取 2 个不超过极致的素数, 设为 p, q , 素数群设为 Z_p . 其中密码的发起方设为 A, 服务器设为 B; 认证的认证过程设为 $H: \{0, 1\}^\infty \rightarrow \{0, 1\}^n$. A 通过得到的密钥对其合法性进行有效的验证. 方法如下: $r' = b^x = g^{xy}$, 反馈合法性通知: $K = H(g^{xy} \parallel A$

|| B). 有些复杂的密钥验证系统会产生多重密钥:

$$K_1 = H(g^{xy} || A || B), \dots, K_m = H(g^{xy} || K_{m-1} || A || B) \quad (1)$$

(2) 服务器接到验证要求后, 为了保证自身的安全性, 也会产生一个密钥, 方法如下:

$$h_1 = H(r' \oplus b^r \oplus g^{xy} || A ||) \quad (2)$$

最后一步是完成验证对比识别, 方法如下:

$$\frac{h_1 - \sum_{j=1}^{\infty} K_j}{K_i} < 0.5 \quad (i = 1, 2, \dots, \infty) \quad (3)$$

如果匹配成功, 那么通过验证, 否则拒绝请求.

(3) 如果密钥发送方和接收到都满足了相互的要求, 至此就完成了通信双方的身份认证.

传统的校园网络安全认证技术, 通过自建立服务器, 设定认证规则, 和安全数据库, 完成合法性身份验证, 最终保证校园网络用户的安全性. 但是, 通过以上原理可以看出: 步骤(2)、(3)中, 需要多次和服务器进行轮转密钥对比, 由 $h = H(r' \oplus b^r \oplus g^{xy} || A ||)$ 完成, 去验证用户的合法性, 需要进行大规模的密钥对比分析, 找到用户的身份是否是合法的, 这种方法中, 会大量占用服务器资源, 如果遇到用户恶意身份验证, 会耗尽服务器资源给认证安全带来危险, 另外, 验证效率也极其低.

因此, 优化原始的方法, 降低校园网络双方认证中密钥对比次数, 避免与服务器数据库中大量密钥的轮番比较, 减少算数运算的计算量, 就能提高校园网络身份认证的效率. 针对传统校园网络平台中, 身份认证技术的缺点, 提出一种快速密钥生成算法的身份认证策略. 通过运用伪随机数验证、一次性会话密钥技术, 运用生成多组素数, 对产生的密钥产生源进行有效的筛选, 从选取更有效的素数, 快速生产密钥, 另外, 在对比过程中, 只一次从中心服务器中获取密钥, 无需与数据库中的用户身份密钥轮番对比, 避免轮转服务器带来的资源浪费、计算量大、验证效率低的问题. 实验证明, 这种校园网络身份验证技术不仅能快速生成密钥, 而且验证过程简单, 取得了很好的效果.

3 基于校园网络平台的快速身份认证策略

网络身份认证技术, 是通过身份信息的对比完成相应的认证操作.

3.1 快速密钥的生成技术

密钥生成的速度和选取的素数有很大的关系, 如果想要加快生成速度, 可以对选取的素数进行筛

选, 方法如下: 计算交互密钥 $n = pq$ 以及密钥生成函数 $\Psi(n) = (p-1)(q-1)$, 先选择一个素数, 以此作为密钥加密的基础参数, 密钥的二重加密函数可以做如下表示: $\gcd(e, \phi(n)) = 1$. 选取一个非 0 偶数 k , 满足 $de - k\phi(n) = 1$, 根据密钥生成方法, 对应的解密公式如下所示:

$$d = 1 + k \lfloor \phi(n)/e \rfloor + [k(\phi(n) \bmod e)] \bmod (e-1) \quad (4)$$

可以计算出 K 的值:

$$k = (-\phi(n)^{\phi(e)-1}) \bmod e \quad (5)$$

具体的计算步骤如下:

(1) 为了简化密钥生成的时间, 可以对密钥的多个数据项进行简化处理, 即: $e = e_1^{a_1} e_2^{a_2} \dots e_n^{a_n}$, 其中 $e_1, e_2, \dots$ 是多个素数, $a_1, a_2, \dots$ 是 n 个正整数.

(2) 分解的方式如下:

$$m = c^d \bmod n \quad (6)$$

其中 e_i 为反加密的密钥

$$d_1, d_2, \dots, d_n.$$

(3) 解密密钥的计算方法如下:

$$d = \prod_{i=1}^n d_i^{a_i} \bmod \phi(n) \quad (7)$$

其中令 $i = 1, 2, \dots, n$, 根据快速加密方法得到: $e_i d_i = 1 \bmod \phi(n)$

通过分解可以得到多个小多项式, 即 $(e_1 e_2 \dots e_n) (d_1 d_2 \dots d_n) \equiv 1 \bmod \phi(n)$ 和 $ed \equiv 1 \bmod \phi(n)$. 进行带入运算可以得到:

$$d_i = 1 + k_i \lfloor \phi(n)/e_i \rfloor + [k(\phi(n) \bmod e_i)] \bmod (e_i - 1) \quad (8)$$

$$\phi(e) = \phi(e_1) \phi(e_2) \dots \phi(e_n) = (e_1 - 1)(e_2 - 1) \dots (e_n - 1) \quad (9)$$

因为 $\phi(e_i)$ 和无正比关系 $\phi(e)$. 因此, 计算量较小, 生产的密钥快速. 可以准确产生出了解密密钥 d . 最后, 删除之前产生的密钥, 完成快速密钥生成操作.

3.2 通信双方的身份认证

在完成校园网络认证的过程中, 最为重要的一步是根据密钥完成双方身份的识别, 确定认证对象是否合法, 这个需要交易方和服务器的通信机制完成, 具体方法如下:

$$(1) D_0 = S - F_{L_q}(D_{je}) / F_{L_q}(Q_k) \quad (10)$$

通过上述表达式可以得知, 将 D_{je} 与操作者本次认证的口令 Q_k 在节点 A 内, 利用此节点进行加密处理后, 在节点 B 内将上述处理结果与 D_{je} 和随机取值 S 利用此节点进行加密处理, 将加密结果传

输至节点 B. 完成上述过程后, 复制 S 的相关数据存储在用户器的存储器中, 并设置保存时间, 假设在保存时间内, 没有获取节点 B 传输的回复数据, 则删除保存内容; 假设在保存时间内, 获取了节点 B 传输的回复数据, 则将其核对后删除存储器中的保存内容.

$$(2) N_1 = E_{L_q}(D_1)/S = (N_2 + E_{L_q}(D_1))/S \\ = (F_{L_q}(D_{je}) + F_{L_q}(Q_k))/(F_{L_q}(D_{je}) \cdot S) \quad (11)$$

获取 D_1 相关数据后, 在节点 B 内, 通过此节点进行解密处理, 能够获取与节点 A 加密相关的信息参数 N_2 , D_{je} 及 S . 通过 D_{je} 能够获取与节点 A 对应的加密函数 L_q , 这个加密函数的获取对后续的两个节点相关数据核对奠定了基础.

$$(3) N = \sqrt{E_{L_q}(N_2)} \\ = \sqrt{E_{L_q}(D_{je})F_{L_q}(Q_k)} \quad (12)$$

利用与节点 A 对应的加密函数对 N_2 做解密处理, 能够获取 D_{je} 和使用者本次操作的口令.

(4) 判断使用者本次操作口令是否正确. 根据本次操作口令获取的方法, 能够利用相同方法获取口令 Q'_k . 将 Q'_k 与 Q_k 进行核对, 假设二者不完全一致, 那么拒绝本次操作, 假设二者完全一致, 则可以开始本次操作.

$$(5) D_2 = (F_{L_q}(T_{je}) - F_{L_q}(T_{je}))^2/S \quad (13)$$

将 T_{je} 与随机参数 S , 通过节点 B 的加密函数进行加密处理, 将获取的结果与 T_{je} 相结合, 通过节点 A 的加密函数让其构成一个数据集合, 并传输到节点 A 中.

$$(6) N_3 = \frac{E_{L_q}(D_2)}{3} = N_4 + \frac{T_{je}}{3} \\ = \frac{(F_{L_q}(T_{je}) - F_{L_q}(S))/T_{je}}{3} \quad (14)$$

(7) 当节点 A 获取从节点 B 传输的回复数据后, 利用节点 A 的加密进行解密处理, 获取相关信息参数数据集合 N_4 和 T_{je} .

$$N_5 = E_{L_q}(N_4)/4 = (E_{L_q}(T_{je}) - F_{L_q}(S))/4 \quad (15)$$

通过上述方法可以获取 T_{je} , 进行解密处理后能够获取加密函数 L_q . 利用得到的加密函数 L_q , 将 N_4 解密, 获取 T_{je} 和 S . 将随机取值 S 与存储器中的内容进行核对, 假设二者完全一致, 则可以进行认证, 假设二者不完全一致, 则拒绝进行认证.

3.3 实时身份认证

为了加速认证, 需要加密函数更新: 根据相关协

议获取几个不同的加密函数, 利用表达式 $n = F_{L_1}(S)/n$ 更新加密函数. 加密函数可以隐藏自身的构造方式等相关信息, 能够加强对网络平台认证的保护, 提高网络平台认证的安全性. 加密函数协商: 根据节点 A 和节点 B 中与安全信息有关的系数能够获取二者都可以使用的加密函数. 在 h_{ab} 和 h_b 传输信息的过程中, 使用的加密方式是二者共同拥有的加密函数, 因为 h_{ab} 是两个节点共同拥有的, 所以也只有这两个节点能够得到 $L = I \cdot \left(h_{ab} - \frac{vt_1}{vt_2} \right)$. 利用加密函数实现使用者身份核对后, 获取加密函数的配准结果.

双方核对: 双方节点同时传输数据 $F_{Q_{x2}}(vt_1, vt_2, t, b)$, $F_{Q_{x2}}(vt_1, vt_2, t, c)$ 及 N_c . 因为 $F_{Q_{x2}}(vt_1, vt_2, t, b)$ 只能利用节点 A 的加密函数进行解密, $F_{Q_{x2}}(vt_1, vt_2, t, c)$ 只能利用节点 B 的加密函数进行解密, 导致 N_c 必须根据两个节点获取和核对, 从而完成双方核对的任务.

4 实验结果及分析

传统的基于 PKI 身份认证技术的网络平台认证验证方法, 通过与服务器数据库中的密钥轮番对比, 这种方法的弊端很大, 计算量聚到, 经常导致身份认证缓慢, 服务器压力大. 而基于本文方法的校园网络平台身份认证技术无需多次访问中心服务器, 无需在生成密钥上占据大量时间, 大大降低了认证技术的复杂性, 实现了校园网络的安全性和时效性.

由图 1、图 2 比较可知, 本文提出的身份认证技术无需多次查询服务器, 提高了身份认证的效率, 降低了服务器负荷.

分别用两种方法进行校园网络的身份认定, 统计不同方法的效率和执行实现, 两种不同方法得到的趋势效果如图 3 所示.

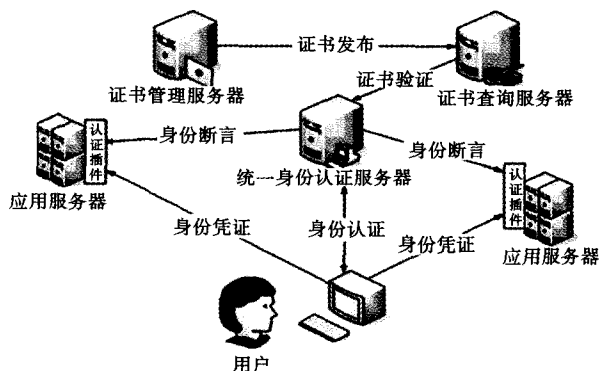


图1 PKI身份认证示意图

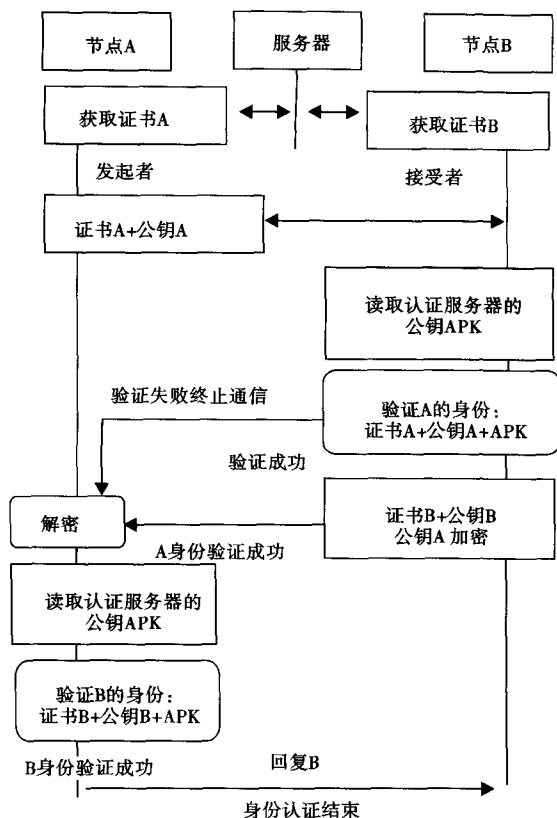


图2 本文身份认证序列图

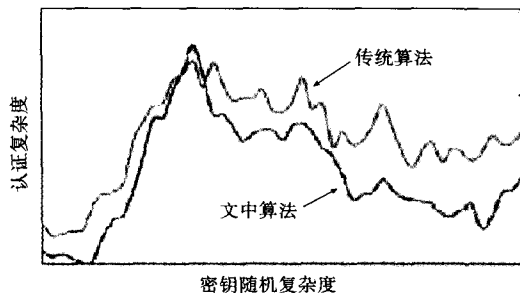


图3 两种方法计算量趋势图

由表1可知,本文的网络平台身份认证过程中计算复杂度要远远的低于传统算法,用的时间也比较少.可见,本文提出的基于校园网络平台的安全身份验证技术能够有效的克服传统方法的缺陷,实现了校园网络平台上身份的快速认证,保证了校园网络的安全性和时效性.

表1 测试结果比较

方法	计算次数	认证耗时/s
PKI 技术	1986	0.95
本文技术	421	0.35

5 结束语

本文通过研究校园网络平台中安全身份认证技术,研究了传统方式认证在校园网络平台中的缺陷,提出基于快速密钥生成算法的身份认证方式,这种认证方式只需要在初次进行身份认证时从网络平台服务方得到密钥,运用奇数筛选理论减少了身份验证的计算量,提高了校园网络平台中安全身份认证的效率.实验证明,该算法能够实时认证操作者的身份,进一步保证校园网络平台的安全.

参考文献:

- [1] 范林秀,陈舒娅,王喜进.基于PKI的身份认证在电子商务中的研究[J].电脑知识与技术,2007(16):979-980.
- [2] Ripeanu M, foster I, Iamnitchi A. Mapping the gnutella network: properties of lamescale peer-to-peer systems and implications for system design[J]. IEEE Internet Computinn, 2002(6):50-57.
- [3] 尹汉东,任邵东,周生炳.基于Web服务器的P2P服务器端实现[J].计算机仿真,2004(10):115-119.
- [4] 陈作聪,孙树峰.基于混沌算法的无线安全认证技术研究[J].微电子学与计算机,2007(12):133-134.
- [5] 刘日初,蒋嵘,张以皓.基于SOA的统一身份认证服务技术研究与应用[J].网络安全技术与应用,2011(05):48-49.
- [6] Ripeanu M, foster I, Iamnitchi A. Mapping the gnutella network: properties of lamescale peer-to-peer systems and implications for system design[J]. IEEE Internet Computinn, 2002(6):50-57.

作者简介:

叶汝军 男,(1972—),讲师.研究方向为校园信息化建设、计算机网络、实训室建设与管理.