无双线性对双向认证密钥协商协议①

黄朝阳

(厦门海洋学院 信息技术系, 厦门 361100)

摘 要: 为提高公钥密码体制下身份认证协议的性能, 将杂凑函数结合到认证过程中, 提出一种高性能的交互认证密钥协商协议. 协议设计认证双方通过两次信息交换即可实现双向认证, 显著降低通信代价. 协议的运算复杂度与传统公钥密码体制下身份认证协议相当. 通过针对已知攻击形式化推演的方法和数学推导证明了协议能抵御拒绝服务攻击、内部攻击在内的各种已知攻击. 协议还设计了登录认证成功后的一次性对称会话密钥协商机制.

关键词: 公钥密码体制; 杂凑函数; 挑战应答机制; 双向认证; 密钥协商; 无双线性对

Mutual Authentication and Key Agreement Protocol without Bilinear Pairing

HUANG Chao-Yang

(Department of Information and Technology, Xiamen Ocean College, Xiamen 361100, China)

Abstract: To improve the performance of identity authentication protocol using public key cryptography effectively, a new secure and effective mutual authentication key agreement protocol combined with one-way hash function is proposed. The communication cost is reduced clearly in this protocol, because the two parties of authentication needs only message exchange twice. The computation complexity of the agreement is equivalent as classical protocol using public key cryptography. The security of this protocol is proved by mathematical derivation and the formal deduction which aims at all- known attacks. In this protocol, a secure one-time symmetric key is generated after successful authentication.

Key words: public key cryptography; hash function; challenge response mechanism; mutual authentication; key agreement; without bilinear pairing

在信息安全的木桶理论中, 身份认证是网络化系统安全的第一道屏障. 公钥密码体制作为一种成熟的安全技术广泛应用于各种身份认证协议中. 传统的公钥密码体制下的双向认证协议及利用挑战应答机制[1]通过四次信息交互以实现双向认证, 这被认为是最有效的交互次数[2]. 挑战应答机制结合公钥密码体制的认证方案层出不穷, 但都存在一定的效率或安全缺陷[3,4]. 文献[5]方案的注册阶段需通过安全信道传递信息, 且存在无法有效抵御拒绝服务攻击[1,6]、内部攻击[6]等弊端. 文献[6]方案还有多次散列效率低下的缺陷. 文献[7]虽然引入服务器的端登录时间记数器解决了拒绝服务攻击问题, 但还是延用四次的信息交互方式.

杂凑函数的单向性和高效性可以有效保障认证信息的完整性, 本文将杂凑运算结合到公钥密码体制下的双向认证协议中, 保障认证安全的同时有效降低认证过程通信代价. 通过巧妙地改进双向认证的信息交互格式及流程以保证高效性, 实现双向认证仅需两次信息传递, 同时还协商了后续会话一次性对称密钥.

1 双向认证密钥协商协议

本文协议在不明显增加计算复杂度的前提下, 把公钥密码体制下双向认证通信交互次数减少一半的同时, 要保障双向认证的安全性并协商产生一次性会话对称密钥.

① 基金项目:福建省中青年教师教育科研项目(JA13409)

收稿时间:2015-07-21;收到修改稿时间:2015-11-02 [doi:10.15888/j.cnki.csa.005157]

协议的认证安全基于数字证书非对称加密体系和杂凑函数,双向认证过程所协商产生的一次性会话对称密钥的构成包含有双方的随机信息且密钥协商过程中没有将的一次性对称密钥以明文的方式在公网上传输或在 AS 上存储. 认证过程由用户注册、双向认证、密钥协商、口令值更新四个阶段组成.

约定本文所用符号如下:*AS*－远程服务器; U_i－用户 *i*; $Kpub\_X$、$Kpri\_X$－*X* 的公、私钥; $Cert\_X$－*X* 的数字证书; ID_i、K_i、$SecretInfo\_U_i$－用户 *i* 的帐号、密码及密码保护信息; H(*)－单向杂凑函数; R_n－生成的随机数; ‖－字符串连接; $Kpub\_X${m}以 $Kpub\_X$ 非对称加密信息 m; K_i(m)以 K_i 对称加密信息 m; *Result*－注册、认证或信息修改的结果信息, 以 0 或 1 表示失败或成功; K_{X-Y}^{k} －*X* 与 *Y* 第 *k* 次双向认证成功后的一次性会话密钥.

1.1 用户注册

(1) U_i 构造并公网发送注册申请消息.

U_i 生成随机数 R_0, 计算出自己密码和密保信息的杂凑值 H(K_i)和 H($SecretInfo\_U_i$), 将三者连接打包后用自己的私钥加密形成 M_1=$Kpri\_U_i${R_0‖H(K_i)‖H($SecretInfo\_U_i$)}. U_i 将自己的帐号 ID_i、数字证书 $Cert\_U_i$、R_0 与 M_1 连接打包后, 使用 *AS* 的公钥加密形成注册信息.

U_i 通过公共信道向 *AS* 发送注册信息:

$Kpub\__{AS}${ID_i‖$Cert\_U_i$‖R_0‖$Kpri\_U_i${R_0‖H(K_i)‖H($SecretInfo\_U_i$)}}

(2) *AS* 审核注册申请并返回注册结果.

AS 用 $Kpri\__{AS}$ 解密注册信息得到 $Cert\_U_i$ 及 $R_0^{'}$, 用查询获得的 $Kpub\_U_i$ 解密 M_1, 并获得 $R_0^{''}$. 通过比对 $R_0^{'}$ 和 $R_0^{''}$ 以验证注册用户的合法性. 将拆包所得注册内容 ID_i、$Cert\_U_i$、$R_0^{''}$、H(K_i)、H($SecretInfo\_U_i$)存储在本地数据库, 注册成功并返回注册结果信息 *Result*. 如 $R_0^{'}$ 和 $R_0^{''}$ 比对失败则拒绝注册请求并终止会话.

1.2 双向认证及一次性对称密钥协商

(1) U_i 生成并发送登录请求消息.

U_i 输入保护私钥的 PIN 码即用户密码 K_i, 以获得的 $Kpri\_U_i$ 使用权, 并生成随机数 R_1. U_i 构造登录请求消息并通过公共信道发往 *AS*:$Kpub\__{AS}${ID_i‖R_0‖H(K_i){R_0}‖R_1}.

(2) *AS* 验证登录请求来源合法性并认证 U_i, 生成后续会话对称密钥, 构造发送双向认证消息.

AS 使用 $Kpri\__{AS}$ 解密登录请求消息获得 ID_i、‖R_0、H(K_i){R_0}、$R_0^{'}$. *AS* 通过比对 $R_0^{'}$ 和 $R_0^{''}$ 以验证登录请求消息来源合法.

根据 ID_i 查询本地数据库中的 $Cert\_U_i$、H(K_i)和 $R_0^{''}$, 继而获取对应的 $Kpub\_U_i$. *AS* 计算 H(K_i){ $R_0^{''}$ },并与 H(K_i){R_0}比对以认证 U_i.

AS 生成 K_{AS-Ui}^{1} =H(K_i){ID_i‖ID_{AS}‖ $R_0^{''}$ ‖ $R_1^{'}$ }作为 U_i 登录成功后的双方一次性对称会话密钥.

AS 构造并通过公共信道发给 U_i 双向认证消息: $Kpub\_U_i${ID_{AS}‖ $R_1^{'}$ ‖*Result*}, 同时暂存 $R_1^{'}$ 于本地.

(3) U_i 认证 *AS* 的合法性,生成后续会话对称密钥.

U_i 使用 $Kpri\_U_i$ 解密来自 *AS* 的信息获得 $R_1^{''}$. 通过比对本地 R_1 与收取的 $R_1^{''}$ 是否相同来认证 *AS* 的合法性, 否则终止登录认证过程.

U_i 生成 K_{Ui-AS}^{1} =H(K_i){ID_i‖ID_{AS}‖R_0‖R_1}作为登录 *AS* 成功后的双方一次性对称会话密钥.

1.3 口令值更新

口令值更新前首先要进行双向认证以确认双方身份的合法性, 认证过程详情参照上一小节.

口令值更新前首先要进行双向认证以确认双方身份的合法性, 认证过程详情参照上一小节.

(1) U_i 发送 *AS* 登录请求消息:

$Kpub\__{AS}${ID_i‖H(K_i){R_0}‖R_m}

(2) *AS* 认证 U_i 后, 返回双向认证消息:

$Kpub\_U_i${ID_{AS}‖ $R_m^{'}$ ‖*Result*}

(3) U_i 通过比对 R_m 认证以 *AS* 的合法性,构造并发送更新的注册信息.

生成新的随机数 R_x, 构造并发送以下信息:

$Kpub\__{AS}${ID_i‖H($SecretInfo\_U_i$) ‖ (R_0 ⊕ R_x) ‖ (H(K_i) ⊕ H($K_i^{'}$))}

为保障数据安全, 协议设计新的存储值均为与原存储值异或后的形式出现:R_0 ⊕ R_x、H(K_i) ⊕ H($K_i^{'}$). 这样既不影响 *AS* 对新值的提取, 又可保障传输过程的安全.

(4) *AS* 验证注册信息更新权限, 存储新的口令值和随机数.

AS 比对收到的 H($SecretInfo\_U_i$)与本地存储的密保信息值以确定是否允许修改注册信息. 计算(H(K_i) ⊕ H($K_i^{'}$)) ⊕ H(K_i)=H($K_i^{'}$)、(R_0 ⊕ R_x) ⊕ $R_0^{''}$ =R_x,用两新值替换本地数据库对应数据, 并返回口令值更新的结果 *Result*. 口令值修改完成.

协议的用户注册、双向认证及一次性密钥协商、口令值更新时序图(含消息交换格式)如图 1 所示.

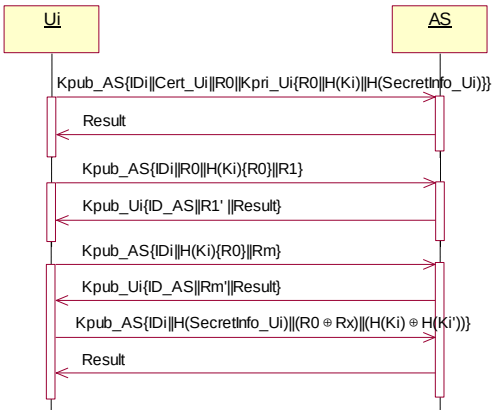

图 1　本文提出的双向认证密钥协商协议

2　性能证明和效率分析

2.1 等式正确性证明

$$K^1_{Ui-AS} = \mathrm{H}(K_i)\{ID_i \| ID\_{AS} \| R_0 \| R_1\}$$
$$= \mathrm{H}(K_i)\{ID_i \| ID\_{AS} \| R_0^{''} \| R_1^{'}\} = K^1_{AS-Ui}$$

说明在双向认证成功后，U_j、AS 各自计算的后续一次性会话对称密钥是相等的.

2.2 安全性证明

命题 1. 协议能抵御拒绝服务攻击

证明: 针对 AS 的拒绝服务攻击分以下几种情景.

情景 1. 非法用户 U_j 假冒合法用户 U_i 恶意抢注. 如果攻击者 U_j 能伪造 U_i 的注册信息抢先进行注册，会造成 U_i 无法正常注册的情况[1][6]. 由于协议所设计的注册信息 $Kpub\_{AS}\{ID_i \| Cert\_U_i \| R_0 \| M_1\}$ 中的 $M_1 = Kpri\_U_i\{R_0 \| \mathrm{H}(K_i) \| \mathrm{H}(SecretInfo\_U_i)\}$，需要由 $Kpri\_U_i$ 加密生成，U_j 在伪装成合法用户 U_i 进行注册时，虽然能获得 $Kpub\_{AS}$ 进行注册信息的外层加密，但是由于没有 $Kpri\_U_i$ 无法伪造 M_1，必然出现后续 AS 执行 $R_0^{'}$ 和 $R_0^{''}$ 比对的失败. 如果 U_j 反复恶意抢注，可以封锁其 IP 连接从而有效抵御拒绝服务攻击.

情景 2. 传统的数字证书认证过程可能存在由于攻击者 U_j 频繁发送无效登录请求消息给 AS，造成由疲于应答，性能下降并最终无法提供正常服务的拒绝服务攻击[5,6]. 本协议在 U_i 成功注册后曾在 AS 上存储有 $R_0^{''}$，当 AS 收到登录请求消息的后，第一步即比对 $R_0^{'}$ 和 $R_0^{''}$ 以验证登录请求消息来源合法性. 由于非法用户 U_j 无法提供正确的 R_0 以供比对，AS 可以立即拒绝并记录其错误次数，超限后封锁其 IP 连接从而有效抵御拒绝服务攻击.

命题 2. 协议能抵御内部攻击

证明: AS 内部授权人员获取用户相关信息 $Cert\_U_i$ 和 $\mathrm{H}(K_i)$后无法完成认证过程.

通用 $Cert\_U_i$ 只能查询获取对应的 $Kpub\_U_i$ 用于加密发送给 U_i 的信息，除非 $Kpri\_{AS}$ 也被盗取，否则无法完成后续双向认证. 因为用户的密码 K_i 是以杂凑值的形式出现，基于杂凑函数的单向安全性[8]，授权的内部人员根本无法获得用户的密码信息，从而能抵御内部攻击.

命题 3. 协议能抵御冒充攻击

证明: 注册阶段的 R_0 是经过公钥加密后传输的. 由于攻击者无法获取 R_0，根本无法生成合法的登录请求消息，所有冒充攻击无法实施.

命题 4. 协议能抵御重播攻击

证明: 协议延用挑战应答机制实现双向认证，重播登录请求消息可以获取对方应答，但应答消息是经过公钥加密的，没有合法私钥无法获取详细内容，从而无法完成后续认证过程.

命题 5. 实现双向认证，有效抵制中间人攻击

证明: 只有合法的 U_i 才可能构造出正确的登录请求消息，只有真正的 $Kpri\_X$ 私钥所有者才可能解密对方的非对称加密认证消息，认证双方通过非对称密钥加解密运算来验证应答消息的正确性，实现了双向认证，有效抵制中间人攻击.

命题 6. 协议协商了安全的一次性会话密钥

证明: U_i 首次登录且双向认证成功后，双方各自计算出 K^1_{Ui-AS}、K^1_{AS-Ui} 作为后续会话对称密钥，会话密钥的构造包含$\{K_i, ID_i, ID_{AS}, R_0, R_1\}$多种信息，既包含 U_i 的编号 ID_i、密码 K_i 信息，又包含了 AS 的编号 ID_{AS} 信息，同时还设计有一次性随机数信息，即使是同一用户与服务器间的两次不同的登录认证后，所生成的会话密钥也会因 R_1 或用户修改了 $\mathrm{H}(K_i^{'})$而不相同. 而且会话密钥的所有组成部分均不以原始信息的形式出现在公共信道上，可实现真正安全的一次一密.

2.3 性能分析

从图 1 观察本文协议通信交互次数，在登录和认证阶段仅需认证双方共两次的信息交换，通信代价明显低于文献[1]和文献[7]的信息交换次数.

本协议所需计算量如表 1 所示. 其中，AEA、ADA: 非对称加解密运算; SEA:对称加密运算; H:杂凑运算.

表 1 本文协议的计算量

协议阶段	U_i	AS
注册	2AEA+2H	2ADA
登录	1SEA+1AEA	
认证 Ui		1ADA+1SEA+1AEA
认证 AS	1ADA	
密钥协商	1SEA	1SEA

对协议效率的考量, 取决定性作用的是登录和双向认证阶段的运算量, 特别是 AS 端的运算量[9]. 在本协议未引入计算量较大的双线性对进行改良[10], 协议登录和双向认证阶段, AS 和 Ui 端的运算量均为 1ADA+1SEA+1AEA. 传统的非对称密钥双向认证协议中, 双方的运算量至少均需要 1ADA+1AEA. 两种协议在运算量上没有明显区别.

通过上述分析, 本协议的与传统协议相比, 通信交互次数减少一半, 运算复杂度相当. 本协议比传统协议效率更高.

3 结语

本文将杂凑函数结合到基于公钥密码体制的身份认证协议中, 既实现双向认证又完成一次性密钥协商. 协议的安全性建立在杂凑函数的单向安全性和公私钥对难题基础上, 能有效抵御已知的各种攻击, 认证安全性高; 协议仅设计需两次的信息交互来实现双向认证, 通信代价低; 认证过程仅使用少量简单杂凑运算、非对称加解密运算, 与传统的基于公钥密码体制认证协议相比运算复杂度无明显变化. 该协议具有良好的安全性和实用价值. 后续工作是选取适当的非对称加密方式以期进一步降低计算复杂度.

参考文献

1 赵铭伟,季晓玉,江荣安.一种高效安全的动态口令认证方案.计算机应用与软件,2009,26(5):255−257.

2 Lai XJ. Security requirements on authentication protocols using challenge-response. Journal of the Graduate School of the Chinese Academy of Sciences, 2002, 19(3): 246−253.

3 聂旭云,徐赵虎,廖永建等.多变量公钥密码扩展方案的安全性分析.计算机学报,2013,36(6):1177−1182.

4 张福泰,孙银霞,张磊等.无证书公钥密码体制研究.软件学报,2011,22(6):1316−1332.

5 陈航,周剑岚,冯珊.基于SHA和RSA算法 实用有效的双向身份认证系统.计算机安全,2006,(4):6−8.

6 曹晓静.S / KEY 认证系统的分析与改进.计算机安全,2007,(4):31−33.

7 刘怀兰,侯昕,王佳.改进的基于USBKey的动态身份认证方案. 华中科技大学学报:自然科学版,2010,38(11):41−43.

8 贾小英,李宝,刘亚敏.随机谕言模型.软件学报,2012,23(1):140−151.

9 谌双双,陈泽茂,王浩.基于 PKI 的通用无线认证协议研究.计算机科学,2012,39(7):74−77.

10 岳泽轮,韩益亮,杨晓元.基于 Paillier 公钥密码体制的签密方案.小型微型计算机系统,2013,34(10):2310−2314.