改进的基于身份认证密钥协商协议 *

舒 剑[1,2], 许春香[1]
(1. 电子科技大学 计算机科学与工程学院, 成都 611731; 2. 江西财经大学 电子商务系, 南昌 330013)

摘 要: 对标准模型下可证安全的基于身份认证密钥协商协议进行安全分析,指出由于传送消息存在冗余,协议不能抵御伪装攻击。为解决上述安全漏洞,提出一个改进的基于身份认证密钥协商协议,并在标准模型下分析其安全性。结果表明,新协议满足基于身份认证密钥协商协议的所有安全要求。

关键词: 基于身份; 伪装攻击; 冗余; 标准模型
中图分类号: TP918.1 **文献标志码**: A **文章编号**: 1001-3695(2010)01-0218-02
doi:10.3969/j.issn.1001-3695.2010.01.064

Improvement of ID-based authenticated key exchange protocol

SHU Jian[1,2], XU Chun-xiang[1]
(1. *School of Computer Science & Engineering, University of Electronic Science & Technology of China, Chengdu* 611731, *China*; 2. *Dept. of Electronic Commercial, University of Jiangxi Financial Economics, Nanchan* 330013, *China*)

Abstract: Analyzed the security of a recently proposed ID-based authenticated key exchange protocol without random oracles, it was shown that the protocol suffer from impersonation attacks due to redundancy of the exchange messages. To overcome this problem, presented an improved version of the protocol and gave security analyses in the standard model. Results show that it satisfies all the security requirements of an ID-based authenticated key exchange protocol.

Key words: ID-based; impersonation attacks; redundancy; standard model

密钥协商协议的目的是让两个用户在开放网络通过交互建立一个共同的密钥,从而实现安全通信。一般地,协议借助公钥机制生成一个短期会话密钥,在接下来的通信中,仅使用短期会话密钥进行加密或认证。但是,公钥机制需要可信第三方的参与。在某些特定的场合如紧急救援、军事行动中,由于缺少固定的安全基础设施,无法实现安全的密钥协商。

Diffie-Hellman 首先提出了无认证的两方密钥协商协议[1]。基于 Shamir 提出的基于身份密码系统[2]和 Boneh 等人利用双线性对提出的基于身份的加密方案[3],研究者利用双线对构造基于身份的认证密钥协商协议[4~6],文献[4~6]提出的协议是在随机预言机模型下证明其安全性的。随机预言模型自从于 1993 年被 Bellare 等人[7]提出以来,就成为可证安全领域的一项主要技术手段。在这个模型中,散列函数被看做一个完全随机的理想模型,是一个很强的要求。在随机预言机模型下是可证安全的方案,但在具体应用中却无法构造出相应的实例。因此,在无随机预言机下设计基于身份认证密钥协商协议更具有实际意义。

2007 年王圣宝等人[8]首先提出了标准模型下可证安全的基于身份密钥协商协议;汪小芬等人[9]对文献[8]中无会话密钥托管模式下的密钥协商协议进行安全性分析,指出恶意的密钥生成中心(PKG)能计算出所有的会话密钥,同时给出了一个改进的基于身份的认证密钥协商协议,并在标准模型下证明了协议的安全性。

1 背景知识

1.1 双线性对

一个可接受的双线性配对 e 是一个映射 $e: G_1 \times G_1 \to G_2$,其中,$G_1 = \langle g \rangle$ 和 G_2 分别是阶为素数 p 的乘法交换群。它满足下列三条性质:

a)双线性,若 $u, v \in G_1$ 且 $a, b \in Z_p^*$,则 $e(u^a, v^b) = e(u, v)^{ab}$;

b)非退化性,$e(g, g) \neq 1$;

c)可计算性,若 $u, v \in G_1$,存在多项式时间算法计算配对 $e(u, v) \in G_2$。

1.2 复杂性假设

判定性 q-ABDHE[10](augmented bilinear Diffie-Hellman exponent)问题。给定一个 $q+3$ 个元素的向量 $(g', g'^{a^{q+2}}, g, g^a, \cdots, g^{a^q}) \in G_1^{q+3}$ 作为输入,其中 g, g' 是群 G_1 的生成元。一个输出为 $b \in \{0,1\}$ 的算法 B 若满足下列不等式 $|pr[B(g', g'^{a^{q+2}}, g, g^a, \cdots, g^{a^q}, e(g^{a^{q+1}}, g')] = 0; -pr[B(g', g'^{a^{q+2}}, g, g^a, \cdots, g^{a^q}, Z)] = 0 \geqslant \varepsilon$,称算法 B 以优势 ε 解决判定性 q-ABDHE 问题。

2 Wang 协议及安全性分析

1)系统建立 G_1, G_2 是阶乘法群,$e: G_1 \times G_1 \to G_2$ 是一个双线性对,$H: \{0,1\}^* \to \{0,1\}^k$ 是哈希函数。密钥生成中心(PKG)随机选取两个生成元 $g, h \in G_1$;PKG 随机选取 $\alpha \in Z_p^*$ 作为私钥,计算公钥为 $g_1 = g^\alpha$;系统公开参数 $\{P, G_1, G_2, e, g, g_1, h, H\}$。

2)用户密钥对生成 对应身份 $ID \in Z_p$,PKG 生成私钥方式如下:随机选择 $r_{ID} \in Z_p$,计算 $h_{ID} = (hg^{-r_{ID}})^{1/(\alpha - ID)}$,则私钥

收稿日期: 2009-03-29; **修回日期**: 2009-05-04 **基金项目**: 国家"863"计划资助项目(2009AA012415)

作者简介:舒剑(1972-),男,江西南昌人,博士研究生,主要研究方向为密码学与信息安全(mikeshujian@uestc.edu.cn);许春香(1965-),女,湖南宁乡人,教授,博导,主要研究方向为密码学与信息安全.

为 $d_{ID}=\langle r_{ID},h_{ID}\rangle$。对每一个身份 ID,固定 r_{ID},且保证 $\alpha\neq ID$。

3)密钥协商协议　Alice(身份为 IDA,私钥为 $d_{IDA}=\langle r_{IDA},(hg^{-r_{IDA}})^{1/(\alpha-IDA)}\rangle$)与 Bob(身份为 IDB,私钥为 $d_{IDB}=\langle r_{IDB},(hg^{-r_{IDB}})^{1/(\alpha-IDB)}\rangle$)进行密钥协商。它们计算公开参数 $g_T=e(g,g)$。

a) Alice 随机选择 $x\in Z_P$,计算 $T_{A1}=(g_1g^{-IDB})^x$,$T_{A2}=g_T{}^x$,$T_{A3}=g^x$。然后将(T_{A1},T_{A2},T_{A3})发送给 Bob;Bob 随机选择 $y\in Z_P$,计算 $T_{B1}=(g_1g^{-IDA})^y$,$T_{B2}=g_T{}^y$,$T_{B3}=g^y$。然后将(T_{B1},T_{B2},T_{B3})发送给 Alice。

b) Alice 计算共享秘密 $K_{AB1}=e(T_{B1},(hg^{-r_{IDA}})^{1/(\alpha-IDA)})T_{B2}{}^{r_{IDA}}e(g,h)^x$ 和 $K_{AB2}=T_{B3}{}^x$;Bob 计算共享秘密 $K_{BA1}=e(T_{A1},(hg^{-r_{IDB}})^{1/(\alpha-IDB)})T_{A2}{}^{r_{IDB}}e(g,h)^y$ 和 $K_{BA2}=T_{A3}{}^y$。

c) Alice 计算会话密钥

$$SK_{AB}=H(IDA\parallel IDB\parallel T_A\parallel T_B\parallel K_{AB1}\parallel K_{AB2})$$

Bob 计算会话密钥

$$SK_{BA}=H(IDA\parallel IDB\parallel T_A\parallel T_B\parallel K_{BA1}\parallel K_{BA2})$$

根据双线性对的性质,容易得出 $K_{AB1}=K_{BA1}=e(g,h)^{x+y}$,$K_{AB2}=K_{BA2}=g^{xy}$,因此它们计算出相同的会话密钥:

$$SK=H(IDA\parallel IDB\parallel T_A\parallel T_B\parallel e(g,h)^{x+y}\parallel g^{xy})$$

改进的协议发送信息增加了 $T_{A3}=g^x$ 和 $T_{B3}=g^y$,则恶意的 PKG(拥有私钥 α)按下式计算:

$$T_{A1}{}^{(\alpha-IDB)^{-1}}=(g^{\alpha-IDB})^{x(\alpha-IDB)^{-1}}=g^x$$

$$T_{B1}{}^{(\alpha-IDA)^{-1}}=(g^{\alpha-IDA})^{y(\alpha-IDA)^{-1}}=g^y$$

增加的发送信息则对恶意的 PKG 没有任何帮助,PKG 无法计算 g^{xy},其困难等价于 CDH 问题。攻击者无法计算正确的会话密钥,改进的协议具备无密钥托管属性和 PKG 前向安全性。然而,攻击者可以利用 T_{A3},T_{B3}进行伪装攻击,攻击过程如下:

假设攻击者伪装成 Alice 与 Bob 进行密钥协商,攻击者随机选择 $x\in Z_P$,计算 $T_{A1}=(g_1g^{-IDB})^x$,$T_{A2}=g_T{}^x$,$T_{A3}=g^x$。然后将(T_{A1},T_{A2},T_{A3})发送给 Bob。在收到 Bob 发送的信息(T_{B1},T_{B2},T_{B3})后,攻击者计算(攻击者知道 x)$K_{AB1}=e(T_{B3},h)e(g,h)^x=e(g^y,h)e(g,h)^x=e(g,h)^{x+y}$和 $K_{AB2}=T_{B3}{}^x=g^{xy}$。攻击者和 Bob 计算出相同的会话密钥。

3　改进的基于身份密钥协商协议

针对无密钥托管的认证密钥协商协议的所有安全要求,提出一个无密钥托管的认证协商协议。系统建立阶段和用户密钥对生成阶段与文献[9]相同。

3.1　密钥协商协议

Alice(身份为 IDA,私钥为 $d_{IDA}=\langle r_{IDA},(hg^{-r_{IDA}})^{1/(\alpha-IDA)}\rangle$)与 Bob(身份为 IDB,私钥为 $d_{IDB}=\langle r_{IDB},(hg^{-r_{IDB}})^{1/(\alpha-IDB)}\rangle$)进行密钥协商。它们计算公开参数 $g_T=e(g,g)$。

a) Alice 随机选择 $x,x'\in Z_P$,计算 $T_{A1}=(g_1g^{-IDB})^x$,$T_{A2}=g_T{}^x$,$T_{A3}=g^{x'}$,然后将(T_{A1},T_{A2},T_{A3})发送给 Bob;Bob 随机选择 $y,y'\in Z_P$,计算 $T_{B1}=(g_1g^{-IDA})^y$,$T_{B2}=g_T{}^y$,$T_{B3}=g^{y'}$,然后将(T_{B1},T_{B2},T_{B3})发送给 Alice。

b)Alice 计算共享秘密 $K_{AB1}=e(T_{B1},(hg^{-r_{IDA}})^{1/(\alpha-IDA)})^xT_{B2}{}^{x\cdot r_{IDA}}$ 和 $K_{AB2}=T_{B3}{}^{x'}$;Bob 计算共享秘密 $K_{BA1}=e(T_{A1},(hg^{-r_{IDB}})^{1/(\alpha-IDB)})^yT_{A2}{}^{y\cdot r_{IDB}}$ 和 $K_{BA2}=T_{A3}{}^{y'}$。

c) Alice 计算会话密钥

$$SK_{AB}=H(IDA\parallel IDB\parallel T_A\parallel T_B\parallel K_{AB1}\parallel K_{AB2})$$

Bob 计算会话密钥

$$SK_{BA}=H(IDA\parallel IDB\parallel T_A\parallel T_B\parallel K_{BA1}\parallel K_{BA2})$$

根据双线性对的性质,容易得出 $K_{AB1}=K_{BA1}=e(g,h)^{xy}$,$K_{AB2}=K_{BA2}=g^{x'y'}$,因此它们计算出相同的会话密钥 $SK=H(IDA\parallel IDB\parallel T_A\parallel T_B\parallel e(g,h)^{xy}\parallel g^{x'y'})$。

3.2　安全分析

新协议增加了两个变量 x'、y',传送信息为 $g^{x'}$、$g^{y'}$,而不是 g^x、g^y,消除了信息冗余,从而消除了伪装攻击。Alice 和 Bob 计算共享秘密分量 $K_{AB1}=K_{BA1}=e(g,h)^{xy}$而不是 $e(g,h)^{x+y}$。因为 PKG 根据传送信息(T_{A1},T_{A2},T_{B1},T_{B2})就能算出 $e(g,h)^x$、$e(g,h)^y$,从而计算出 $e(g,h)^{x+y}$。但 PKG 无法计算 $e(g,h)^{xy}$,这等价于 G_2 上的 CDH 问题。除非是恶意的 PKG,它知道 g、h 之间的离散对数 $u=\log_g h$,然后计算 $g^x=T_{A1}{}^{(\alpha-IDB)^{-1}}$,$g^y=T_{B1}{}^{(\alpha-IDA)^{-1}}$,才可以计算出 $e(g,h)^{xy}=e(g^x,g^y)^u$。

基于 q-ABDHE 假设,攻击者无法获得的任何信息,改进协议是一个安全的基于身份认证密钥协商协议。

4　结束语

在标准模型下设计认证协议具有更实际的意义。本文对文献[9]提出的标准模型下可证安全的基于身份认证密钥协商协议进行安全性分析,指出由于传送消息存在冗余,协议无法抵御伪装攻击。本文给出一个改进的基于身份认证协议,在标准模型下安全分析表明,新协议满足认证协议的所有安全需求。

参考文献:

[1] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Trans on Info Theory, 1976, 22(6): 644-654.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Proc of CRYPTO'84. Berlin: Springer-Verlag, 1984: 47-53.

[3] BONEH D, FRANKLIN M. Identity based encryption from the Weil pairing[C]//Proc of CRYPTO 2001. Berlin: Springer-Verlag, 2001: 213-229.

[4] CHEN L, KULDA C. Identity based authenticated key agreement protocols from pairing[C]//Proc of the 16th IEEE Computer Security Foundations Workshop. New York: IEEE Press, 2003: 219-233.

[5] MCCULLAGH N, BARRETO P. A new two party identity-based authenticated key agreement[C]//Proc of RSA Conference. Berlin: Springer-Verlag, 2005: 262-274.

[6] CHOIE Y, JEONG E, LEE E. Efficient identity-based authenticated key agreement protocol from pairings[J]. Journal of Applied Mathematics and Computation, 2005, 162(1): 179-188.

[7] BELLARE M, ROGAWAY P. Random oracles are practical: a paradigm for designing efficient protocols[C]//Proc of the 1st ACM Conference on Computer and Communication Security. New York: ACM Press, 1993: 62-73.

[8] 王圣宝,曹珍富,董晓蕾. 标准模型下可证安全的身份基认证密钥协商协议[J]. 计算机学报, 2007, 30(10): 1842-1852.

[9] 汪小芬,陈原,肖国镇. 基于身份的认证密钥协商协议的安全性分析与改进[J]. 通信学报, 2008, 29(12): 16-21.

[10] GENTRY C. Practical identity-based encryption without random oracles[C]//Proc of EUROCRYPT2006. Berlin: Springer-Verlag, 2006: 445-464.