Journal of Computer Applications
计算机应用,2012,32(11):3147-3148,3152
ISSN 1001-9081
CODEN JYIIDU
2012-11-01
http://www.joca.cn

文章编号:1001-9081(2012)11-3147-02
doi:10.3724/SP.J.1087.2012.03147

改进的双方密钥协商协议

张龙翔*
(临沂大学 信息学院,山东 临沂 276001)
(*通信作者电子邮箱 zhanglongxiang@lyu.edu.cn)

摘　要:双方认证密钥协商是生成会话密钥的重要手段。分析了赵建杰等于2011年提出的一个可证明安全的双方认证密钥协商协议,指出如果敌手持有原协议的长期私钥,协议是不安全的。提出一种改进的协议,新协议将影响安全性的公开参数保护起来,避免了长期私钥的泄露,并对新协议的安全性和计算量进行了讨论。分析结果表明,新协议在减少计算量的前提下实现了协议双方的安全密钥协商。

关键词:密码学;认证;密钥协商;前向安全性;可证明安全
中图分类号:TP 309　　**文献标志码**:A

Improved two-party authenticated key agreement protocol

ZHANG Long-xiang*
(*School of Information, Linyi University, Linyi Shandong* 276001, *China*)

Abstract: Two-party authenticated key agreement is one of the methods to generate session keys. In this paper, the authors analyzed a new provably secure two-party authenticated key agreement protocol proposed in 2011 by Jianjie Zhao *et al.* and pointed out that this protocol was not secure if the adversary can obtain the long-term key of a participant. Then an improved protocol was presented, and in the new scheme, the parameters that may leak the long-term keys were encrypted. The authors also discussed the security and computational cost of the new scheme. The result shows that the new protocol realizes the secure key agreement with lower computational cost.

Key words: cryptography; authentication; key agreement; forward secrecy; provable security

0　引言

密钥建立协议是密码协议的重要组成部分。密钥建立协议是指两个或多个参与者在公开的网络上建立临时的秘密会话密钥的过程。密钥建立是保证后续通信安全的一种重要机制。利用密钥建立协议得到的会话密钥,参与者们可以在开放的网络中建立安全信道,从而保证传输信息的安全性。

根据会话密钥生成方式不同,密钥建立协议通常分为两种:密钥传输协议和密钥协商协议。在密钥传输协议中,密钥的分发者(参与者或可信的第三方)生成一个会话密钥,并将其通过安全信道秘密地发送给各个参与者。这种做法简单,而且也有一些场合(如参与者不同时在线)必须依赖此类协议,但缺点也是显而易见的,接收会话密钥的参与者需要信任密钥的分发者或者必须存在一个可信的第三方,这种要求在现实中很难实现,或者需要较高的成本;另外,维护安全信道也加重了系统的负担。而在密钥协商协议中,会话密钥由所有的参与者共同协商而成,其中任何一方在密钥协商结束前都无法预测或决定会话密钥的值。尽管这种做法有计算量和通信量相对较大的缺点,但密钥协商不需要参与会话密钥生成的可信第三方和安全信道,协议的参与者也无需信任其他参与者。本文将重点研究这类协议。

自从 Diffie 等[1]自1976年提出公钥密码体制后,认证密钥协商就得到了蓬勃发展。1986年,Matsumoto 等[2]扩展了 Diffie-Hellman 协议,提出了三个双方认证密钥协商协议:MTI/A0、MTI/B0 和 MTI/C0。这些协议能够通过巧妙的消息传递而不需要签名,为通信双方产生能够抵抗被动攻击者攻击的双向认证的会话密钥。Menezes 等[3]和 Law 等[4]指出了 MTI 系列协议的漏洞,并证明 MTI/A0 和 MTI/C0 容易受到小子群攻击和未知密钥共享攻击。为此,他们提出了一种高效的可认证密钥协商协议 MQV。这一协议被许多权威机构,如 ANSI(美国国家标准学会)、IEEE(美国电气与电子工程师学会)等广泛采纳为密码标准。但遗憾的是,这一协议也被证明是不安全的[5]。

2011年,赵建杰等[6]提出了一种新的双方认证密钥协商协议,并在最新的 eCK 模型[7]下证明了该协议的安全性可以规约为计算式 Diffie-Hellman 问题。本文的研究发现,如果协议参与者双方的长期私钥全部泄露,该协议是不安全的。为此指出了这一安全漏洞,并提出了改进方案。与原方案相比,改进后的方案还具有较好的执行效率。

1　AKA-eCK 方案与安全性分析

本章简要介绍文献[6]提出的 AKA-eCK 方案,并分析其安全性。

1.1　AKA-eCK 方案

在介绍该方案之前,先定义一些本章用到的表示:

ID_A,ID_B 表示参与者 A 和 B 的身份符号;

p,q 表示在阶为 q 的循环群 G 中,p 为该群的生成元;

$H_1:\{0,1\}^* \rightarrow \mathbf{Z}_q^*$ 表示一个随机预言,用于隐藏参与者的长期私钥和临时公钥;

$H:\{0,1\}^* \rightarrow \{0,1\}^\lambda$ 表示一个理想的 Hash 函数;

参与者 A 和 B 为了得到协商得到的会话密钥 SK,将执行如下步骤:

收稿日期:2012-05-28;修回日期:2012-06-18。
作者简介:张龙翔(1976-),男,山东临沂人,讲师,硕士,主要研究领域:网络安全、模式识别。

Journal of Computer Applications 计算机应用

1)A 随机选取 $a \in \mathbf{Z}_q^*$ 作为自己的长期私钥,计算 $\bar{A} = g^a \bmod p$ 作为其长期公钥,并公布 $(\bar{A}, ID_A)$;同理,B 随机选取 $b \in \mathbf{Z}_q^*$ 作为自己的长期私钥,计算 $\bar{B} = g^b \bmod p$ 作为其长期公钥,并公布 $(\bar{B}, ID_B)$。

2)A 随机选取 $\tilde{x} \in \mathbf{Z}_q^*$ 作为自己的临时私钥,并计算 $x = H_1(a, \tilde{x})$,$K_A = (\bar{B})^x \bmod p$,$s_A = \dfrac{x}{(K_A + a)} \bmod q$,$R_A = g^{K_A} \bmod p$,将 (R_A, s_A) 发送给 B。

3)收到 (R_A, s_A) 后,B 计算 $K_A = (R_A \bar{A})^{hs_A} \bmod p$ 并验证等式 $R_A = g^{K_A} \bmod p$ 是否成立。若成立,则 B 随机选取 $\tilde{y} \in \mathbf{Z}_q^*$ 作为自己的临时私钥,并计算 $y = H_1(b, \tilde{y})$,$K_B = (\bar{A})^y \bmod p$,$s_B = \dfrac{y}{(K_B + b)} \bmod q$,$R_B = g^{K_B} \bmod p$。计算 $K = R_B^{K_A} \bmod p$ 及 $SK = H(K, s_B, s_A, ID_B, ID_A)$,将 (R_B, s_B) 发送给 A。

4)收到 (R_B, s_B) 后,A 计算 $K_B = (R_B \bar{B})^{as_B} \bmod p$ 并验证等式 $R_B = g^{K_B} \bmod p$ 是否成立。若成立,计算 $K = R_A^{K_B} \bmod p$ 以及 $SK = H(K, s_A, s_B, ID_A, ID_B)$。

1.2 AKA-eCK 方案安全性分析

在原协议的安全性证明中,作者指出如果长期私钥泄露前的会话没有被敌手破坏,即使参与者的长期私钥被敌手获得,敌手也无法获得这类会话的会话密钥。但本文的研究发现如果主动攻击者 E 如果拥有了参与者 A 和 B 的长期私钥 a 和 b,原协议的会话密钥可以被计算出来。

1)敌手利用公开信道中的 (R_A, s_A) 和 (R_B, s_B) 计算 $K_A = (R_A \bar{A})^{hs_A} \bmod p$ 和 $K_B = (R_B \bar{B})^{as_B} \bmod p$;

2)利用 $K_A \bmod p$ 和 $K_B \bmod p$ 计算 $K' = {R_A}^{K_B} \bmod p$ 和 $K' = {R_B}^{K_A} \bmod p$,从而得到了会话密钥。

2 改进后的新协议

从上述的攻击可以看出,过早地将 R_A 和 R_B 暴露,导致敌手可以利用已经获得的长期私钥计算得到会话密钥。为此,适当调整策略,将 R_A 和 R_B 隐藏起来,并对会话密钥的计算过程进行简单的改造,即可避免上述问题。

1)A 随机选取 $a \in \mathbf{Z}_q^*$ 作为自己的长期私钥,计算 $\bar{A} = g^a \bmod p$ 作为其长期公钥,并公布 $(\bar{A}, ID_A)$;同理,B 随机选取 $b \in \mathbf{Z}_q^*$ 作为自己的长期私钥,计算 $\bar{B} = g^b \bmod p$ 作为其长期公钥,并公布 $(\bar{B}, ID_B)$。

2)A 随机选取 $\tilde{x} \in \mathbf{Z}_q^*$ 作为自己的临时私钥,并计算 $x = H_1(a, \tilde{x})$,$K_A = g^x \bmod p$,$\hat{x} = H_1(K_A)$,$s_A = \dfrac{x}{(\hat{x} + a)} \bmod q$,将 (K_A, s_A) 发送给 B。

3)收到 (K_A, s_A) 后,B 计算 $H_1(K_A)$ 并验证等式 $(g^{H_1(K_A)} \bar{A})^{s_A} = K_A$ 是否成立。若成立,则 B 随机选取 $\tilde{y} \in \mathbf{Z}_q^*$ 作为自己的临时私钥,并计算 $y = H_1(b, \tilde{y})$,$K_B = g^y \bmod p$,$\hat{y} = H_1(K_B)$,$s_B = \dfrac{y}{(\hat{y} + b)} \bmod q$。计算 $K = (K_A \cdot \bar{A})^{b+y} \bmod p$ 及 $SK = H(K, s_B, s_A, ID_B, ID_A)$,将 (K_B, s_B) 发送给 A;

4)收到 (R_B, s_B) 后,A 计算 $H_1(K_B)$ 并验证等式 $(g^{H_1(K_B)} \bar{B})^{s_B} = K_B$ 是否成立。若成立,计算 $K = (K_B \bar{B})^{a+x} \bmod p$ 以及 $SK = H(K, s_A, s_B, ID_A, ID_B)$。

3 安全性与性能分析

3.1 安全性分析

协议的安全性是协议可以得到应用的前提和必要条件,而合理准确的安全目标是设计安全协议的首要条件。一般,密钥协商协议应实现的安全目标包括[8] AKA 安全、弱的完美前向安全性、抗密钥泄露伪装攻击、抗未知密钥共享攻击、抗密钥复制攻击。这些安全目标在文献[6]中都有详细定义,此处不再赘述。

3.1.1 弱的完美前向安全性和 AKA 安全

由于敌手在获得参与者的长期私钥后,可以利用在公开信道中传输的信息获得会话密钥。在改进的方案中,将计划用于会话密钥计算的 K_A 和 K_B 利用理想的 Hash 函数隐藏起来,从来避免了敌手的攻击,确保了协议弱的完美前向安全性[5, 9-10]。

3.1.2 抗密钥泄露伪装攻击[11]

抗密钥泄露伪装攻击是指当参与者一方的长期私钥泄露后虽然其可以被敌手冒充与对方进行交互,但这一密钥泄露不得反过来向其冒充为其他参与者。在本文中,由于没有改变其他秘密参数的生成方式,因此新协议仍然满足抗密钥泄露伪装攻击的安全性要求。

3.1.3 抗未知密钥共享攻击[12]和冒充攻击

协议可抵抗未知密钥共享攻击的核心在于在每条传输的信息中添加身份信息,以确保敌手无法利用截获的信息转发来冒充参与者。在新协议中,仍然将参与者的身份信息添加到了会话密钥 $SK = H(K, s_A, s_B, ID_A, ID_B)$ 中,从而避免了未知密钥共享攻击。

如果协议传输的信息是一成不变的,那么敌手就可以利用在这次会话中截获的 (K_A, s_A) 和 (K_B, s_B) 直接计算会话密钥而跳过验证环节。在新协议中,会话密钥中添加了当前会话的随机值 s_A 和 s_B,从而避免了冒充攻击。

3.2 性能分析

除了安全性外,方案的性能也是制约协议推广的重要指标。同 AKA-eCK 方案,为了简便仅比较方案中最耗时的模指数运算的次数。记 T_{EXP} 表示一次模指数运算的时间,T_H 表示一次模指数运算的时间,如表 1 所示,新协议由于减少了计算 $K_A = (\bar{B})^x \bmod p$ 和 $K_B = (\bar{A})^y \bmod p$,因此每个参与者减少了一次模指数运算。但由于新协议为了隐藏 K_A 和 K_B 分别增加了一次 Hash 运算。需要指出的是,与模指数运算相比,Hash 运算是微不足道的。

表 1 新旧方案的计算量比较

计算	AKA-eCK 方案	新方案
模指数运算	$5T_{EXP}$	$4T_{EXP}$
Hash 运算	$2T_H$	$3T_H$

新协议在安全性和性能方面都优于原协议。

4 结语

本文分析了文献[6]的安全性,指出如果该协议中参与者的长期私钥泄露,敌手可以计算得到会话密钥,从而破坏了原协议的弱前向安全性。在此基础上,构造了一个全新的改进协议,并对新协议的安全性和性能进行了简单的分析,分析结果表明,新协议在安全性和性能方面均优于原协议。

本文注意到原协议作者对协议做了严格的可证明安全论证,但本文并未分析证明过程中的漏洞,这也是下一步需要进行的工作。

(下转第 3152 页)

Journal of Computer Applications 《计算机应用》

上放大倍数为 $b=(1.80\times100)/0.52\times3/4=461.5$。根据上述参数计算得到柱面反射镜形状，反射镜面垂直投影在 *XOY* 平面上的形状曲线如图 7 所示。沉浸感显示效果如图 8。

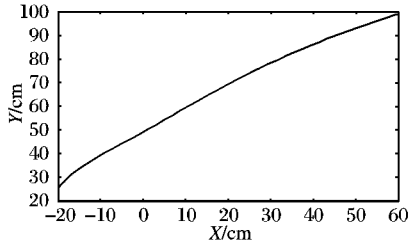
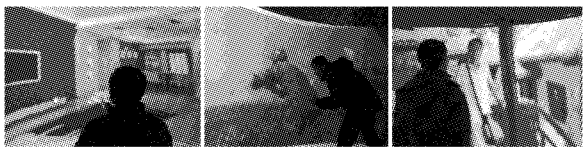


图 7 反射镜面在 *XOY* 平面上垂直投影曲线



(a) 虚拟漫游 (b) 三维游戏 (c) 面对面交流

图 8 沉浸感显示效果

5 结语

为了克服传统沉浸感显示系统中多投影仪或多显示器图像拼接困难以及运动范围受限等不足，本文设计并实现了一种基于单投影仪和柱面反射镜的沉浸感显示系统。该系统通过合理设计柱面反射镜形状和图像预变形，基本消除了投影画面的形变，实现了广角度虚拟场景的连贯显示。投影实验表明该系统能够获得良好的沉浸感显示效果。

本系统中反射镜实现了水平方向上投影画面的均匀放大，而垂直方向上通过图像修正消除形变。在加工精度足够高的情况下，可以制作在水平和垂直方向上都能对画面进行均匀放大的反射镜面，使图像变形算法得到进一步的简化，这是该系统进一步改进的方向。

参考文献：

[1] MEL S, ANTHONY S, YIORGOS C. 计算机图形学与虚拟环境[M]. 程成, 徐玉田, 译. 北京: 机械工业出版社, 2004.

[2] 黄东军, 伯斯科, 陈斌华. 沉浸感显示技术研究[J]. 计算机系统应用, 2007, 16(3): 43－46.

[3] MANIA K, CHALMERS A. The effects of levels of immersion on memory and presence in virtual environment: a reality centered approach[J]. CyberPsychology Behavior, 2001, 4(2): 247－264.

[4] LI KAI, CHEN HAN, CLARK D W, *et al*. Building and using a scalable display wall system[J]. IEEE Transactions on Computer Graphics and Applications, 2000, 20(4): 29－37.

[5] 梁嘉华, 董科军. 多屏显示墙可视化技术研究[J]. 中国科技信息, 2010(7): 99－101.

[6] HENDEN C, CHAMPION E, MUHLBERGER R, *et al*. A surround display warp-mesh utility to enhance player engagement[C]// ICEC 2008: Entertainment Computing, LNCS 5309. Berlin: Springer, 2009: 46－56.

[7] PAUL B. Spherical mirror: a new approach to hemispherical dome projection[J]. Planetarian, 2005, 34(4): 6－9.

[8] SIMON A, GÖBEL M. The i-Cone TM: A panoramic display system for virtual environment[C] // Proceedings of the 10th Pacific Conference on Computer Graphics and Applications. Washington, DC: IEEE Computer Society, 2002: 3－7.

[9] NANCY P Y, WILLIAM C T. Inexpensive immersive projection [C]// Proceedings of 2008 Virtual Reality Conference. Washington, DC: IEEE Computer Society, 2008: 237－240.

[10] PAUL B. Low cost projection environment for immersive gaming [J]. Journal of Multimedia, 2008, 3(1): 41－46.

[11] BRANISLAV S, CSABA S, STANISLAV S. The some problems solution by construction of multi-screen projection system[J]. Jounal of Computer Science and Control Systems, 2009, 2(1): 57－60.

[12] HASHIMOTO N, JEONG S, TAKEYAMA Y, *et al*. Immersive multi-projector display on hybrid screens with human-scale haptic and locomotion interfaces[C]// Proceedings of the 2004 International Conference on Cyberworlds. Washington, DC: IEEE Computer Society, 2004: 361－368.

[13] 陈柳叶, 常辉, 戴树岭. 多投影仪拼接显示技术综述[C]// 第四届全国虚拟现实与可视化学术会议论文集. 大连: 大连海事大学出版社, 2004: 250－254.

[14] HARLYN B, ZEYU L. Camera and projector arrays for immersive 3D video[C]// Proceedings of the 2nd International Conference on Immersive Telecommunications. New York: ACM, 2009: 1－6.

[15] HARVILLE M, CULBERTSON B, SOBEL I, *et al*. Practical methods for geometric and photometric correction of tiled projectors on curved surfaces[C]// Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop. Washington, DC: IEEE Computer Society, 2006: 5.

(上接第 3148 页)

参考文献：

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

[2] MATSUMOTO T, TAKASHIMA Y, IMAI H. On seeking smart public-key distribution systems[J]. Transactions on IECE, 1986, 69(2): 99－106.

[3] MENEZES A, QU M, VANSTONE S. Some new key agreement protocols providing mutual implicit authentication[C]// SAC'95: Proceedings of the Second Workshop on Selected Areas in Cryptography. New York: ACM, 1995: 22－32.

[4] LAW L, MENEZES A, QU M, *et al*. An efficient protocol for authenticated key agreement[J]. Designs, Codes and Cryptography, 2003, 28(2): 119－134.

[5] KRAWCZYK H. HMQV: A high-performance secure Diffie-Hellman protocol [C]// CRYPTO 2005: Proceedings of the 25th International Cryptology Conference, LNCS 3621. Berlin: Springer-Verlag, 2005: 546－566.

[6] 赵建杰, 谷大武. eCK 模型下可证明安全的双方认证密钥协商协议[J]. 计算机学报, 2011, 34 (1): 47－54.

[7] LAMACCHIA B, LAUTER K, MITYAGIN A. Stronger security of authenticated key exchange [C]// Proceedings of the 1st International Conference on Provable Security. Berlin: Springer-Verlag, 2007: 1－16.

[8] LAUTER K, MITYAGIN A. Security analysis of KEA authenticated key exchange protocol[C]// Public Key Cryptography 2006, LNCS 3958. Berlin: Springer, 2006: 378－39.

[9] 杨小东, 王彩芬. 前向安全的单向门限代理重签名[J]. 计算机应用, 2011, 31(3): 801－804.

[10] 高海英. 高效的基于身份的认证密钥协商协议[J]. 计算机应用, 2012, 32(1): 35－37.

[11] 周四方. 一种新的双方认证密钥协商协议的安全性分析[J]. 计算机应用, 2011, 31(11): 2994－2996.

[12] 侯孟波, 徐秋亮. 身份基认证密钥协商协议的分析与改进[J]. 计算机工程与应用, 2010, 46(7): 25－28.

《计算机应用》Journal of Computer Applications