高效的基于口令的三方密钥交换协议

许春香，何小虎

(电子科技大学计算机科学与工程学院 成都 611731)

【摘要】基于口令的三方密钥交换协议，通过一个保存了客户的口令或是关于口令的验证值的可信第三方服务器，实现了两个需要相互通信的客户的身份认证和密钥协商。但由于口令的低熵性，使得现有的很多基于口令的三方密钥交换协议容易遭受字典攻击。在现有协议的基础上，利用对称加密算法和Diffie-Hellman两方密钥交换方法，提出了一个高效的基于口令的三方密钥交换协议。该协议能抵御各种现有的攻击，并提供完美的前向安全性。

关 键 词 身份认证； 密钥交换； 口令； 三方

中图分类号 TP309 **文献标识码** A doi:10.3969/j.issn.1001-0548.2012.04.023

Efficient Three-Party Password-Based Authenticated Key Exchange Protocol

XU Chun-xiang and HE Xiao-hu

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 611731)

Abstract Three-party password-based authenticated key exchange protocols allow two clients to authenticate each other and establish a shared session key through a trusted server who preserves clients' passwords or verifiers about passwords. However, because of the low entropy of passwords, password-based authenticated key exchange protocols are vulnerable to dictionary attacks. Based on available protocols, a new efficient three-party password-based authenticated key exchange protocol is proposed by combining the symmetric encryption algorithm with the method of two-party key exchange protocol of Diffie-Hellman. Results indicate that and the proposed protocol can resist against various attacks and provide the perfect forward security.

Key words ID authentication; key exchange; password; three-party

当通信双方需要在公开信道上安全通信时，需要在通信前协商一个会话密钥。由于基于口令的密钥交换协议只需要通信双方保存一个简单易记的口令，因此该协议得到了更广泛的应用。但是由于口令的低熵性，使得其更容易遭受字典攻击。字典攻击可分为以下3类[1]：

1) 在线可检测字典攻击：攻击者尝试猜测客户的口令并进行在线通信来验证其猜测口令的正确性，一旦攻击者口令猜测失败很容易被发现。

2) 在线不可检测字典攻击：攻击者尝试猜测客户的口令并进行在线通信来验证其猜测口令的正确性，攻击者口令猜测失败也不会被发现。因此该情况下攻击者可以实施多次口令猜测攻击。

3) 离线字典攻击：攻击者猜测客户的口令并在离线情况下验证猜测口令的正确性。

安全的基于口令的密钥交换协议应该能有效抵御在线不可检测字典攻击和离线字典攻击。

文献[2]首先提出了一个基于口令的两方密钥交换(2PAKE)协议，通过通信双方共享的口令，该协议成功实现了通信双方的相互认证和密钥交换。此后，人们又提出了大量的2PAKE协议[3-4]。

但是由于两方的密钥交换协议适合“客户–服务器”模式的系统，却不适合于像P2P这样有大量客户需要互相通信的系统。文献[5]提出了一个基于口令的三方密钥交换(3PAKE)协议，但是文献[1]指出该协议不能抵御在线不可检测字典攻击，同时文献[6]指出该协议同样不能抵御离线字典攻击，并提出了一个基于公钥技术的改进协议。文献[7]提出了一个新的不需要公钥技术的3PAKE协议，但是该协议比之前的基于公钥的改进协议多执行两轮。文献[8]提

收稿日期：2010 – 09 – 25； 修回日期：2011 – 11 – 08
基金项目：保密通信重点实验室基金(9140C110301110C1103)；部级预研基金(9140A04020311DZ02)
作者简介：许春香(1965 –)，女，教授，博士生导师，主要从事信息安全与密码学方面的研究.

出了一个3PAKE协议，但文献[9]很快指出该协议容易遭受中间人攻击。文献[10]提出了一个3PAKE协议，该协议能抵御各种攻击，并提供完美的前向安全性。文献[11]基于CCDH假设提出了一个简单高效的3PAKE协议，该协议能抵御各种攻击。但随后人们分析发现该协议不能抵御中间人攻击[12-13]、在线不可检测字典攻击[14-15]，以及离线字典攻击[16]。

1　文献[10]的3PAKE协议介绍

1.1　协议中用到的符号说明

(G,g,p)表示有限循环群，g为Z_p^*的生成元，p是一个大素数；A、B代表协议中需要协商密钥的两个客户；S代表可信第三方服务器；pw_A表示A的口令；pw_B表示B的口令；$h()$是一个将任意长度消息转化为固定长度消息的哈希函数；$E_K(M)$、$D_K(M)$分别表示用对称密钥K对消息M进行加密和解密；为了简便起见，在协议描述中省略了“mod p”。

1.2　3PAKE协议

3PAKE协议具体步骤如下：

1) A选择一个随机数$a \in_R Z_p^*$，并计算$X_A=g^a$，然后将A、X_A发送给B。

2) B收到A、X_A后，B选择一个随机数$b \in_R Z_p^*$，并计算$X_B= g^b$，然后将A、X_A、B、X_B发送给S，将X_B发送给A。

3) S收到A、X_A、B、X_B后，首先产生随机数$c,d \in_R Z_p^*$，并运用S预先保存的A和B的基于口令的验证信息$v_A = g^{h(A,S,pw_A)}$，$v_B = g^{h(B,S,pw_B)}$计算$X_{SA}=(v_A)^c \oplus v_A$，$X_{SB}=(v_B)^d \oplus v_B$，分别将$X_{SA}$、$X_{SB}$发送给$A$、$B$。然后计算并保存$K_{SA}=(X_A)^c=g^{ac}$，$K_{SB}=(X_B)^d=g^{bd}$。

4) A、B收到S发送的X_{SA}、X_{SB}后，分别运用自己保存的$t_A=h(A,S,pw_A)$，$t_B=h(B,S,pw_B)$，A计算$K_{SA} = (X_{SA} \oplus v_A)^{t_A^{-1} \cdot a} = g^{ac}$和$V_{AS}=h(A,B,S,X_A,X_B,X_{SA},K_{AS})$，$B$计算$K_{SB} = (X_{SB} \oplus v_B)^{t_B^{-1} \cdot b} = g^{bd}$和$V_{BS}=h(B,A,S,X_B,X_A,X_{SB},K_{BS})$。然后$A$, B分别将V_{AS}, V_{BS}发送给S。

5) S收到A、B发送的V_{AS}、V_{BS}后，分别验证$V_{AS} \stackrel{?}{=} h(A,B,S,X_A,X_B,X_{SA},K_{SA})$, $V_{BS} \stackrel{?}{=} h(B,A,S,X_B,X_A,X_{SB},K_{BS})$，如果验证相等则$S$分别计算$V_{SA}=h(S,A,B,X_A,X_B,K_{BS})$，$V_{SB}=h(S,A,B,X_A,X_B,K_{SB})$，并分别将$V_{SA}$、$V_{SB}$发送给$A$、$B$。

6) A、B收到S发送的V_{SA}、V_{SB}后，分别验证$V_{SA} \stackrel{?}{=} h(S,A,B,X_A,X_B,K_{SA})$, $V_{SB} \stackrel{?}{=} h(S,A,B,X_A,X_B,K_{SB})$，如果相等则$A$、$B$分别计算$K_{AB}=(X_B)^a=g^{ab}$，$K_{BA}=(X_A)^b=g^{ab}$。$A$, B双方计算会话密钥$K=h(A,B,S,K_{AB})=h(A,B,S,K_{BA})=h(A,B,S,g^{ab})$。

文献[10]的3PAKE协议能够抵御现有的各种攻击，并在计算量上和以前的协议比较有很大的提升，但通信过程还是相对复杂。本文提出一个新的3PAKE协议，该协议在通信时间和通信过程的复杂度上有所改善。

2　新的三方密钥交换协议

本文以文献[8,10]的3PAKE协议为基础，并结合对称加密，提出了一个新的三方密钥交换协议。协议开始前，A、B通过安全的通信信道用pw_A、pw_B向S注册，S保存$h(pw_A)$, $h(pw_B)$。新协议的具体步骤如下：

1) A发送A、B给S。

2) S收到A、B后，首先S产生随机数$a,b \in_R Z_p^*$，计算$S_A = E_{h(pw_A)}(g^a)$，$S_B = E_{h(pw_B)}(g^b)$，然后将S_A、S_B分别发送给A、B。

3) A、B收到S_A、S_B后，解密S_A、S_B得到$g^a = D_{h(pw_A)}(S_A)$，$g^b = D_{h(pw_B)}(S_B)$。然后A, B分别产生随机数$x, y \in_R Z_p^*$，并计算$V_{AS} = E_{h(pw_A)}(g^x, h(g^{ax}, A, B, S)), V_{BS} = E_{h(pw_B)}(g^y, h(g^{by}, A, B, S))$。最后分别将$V_{AS}$、$V_{BS}$发送给$S$。

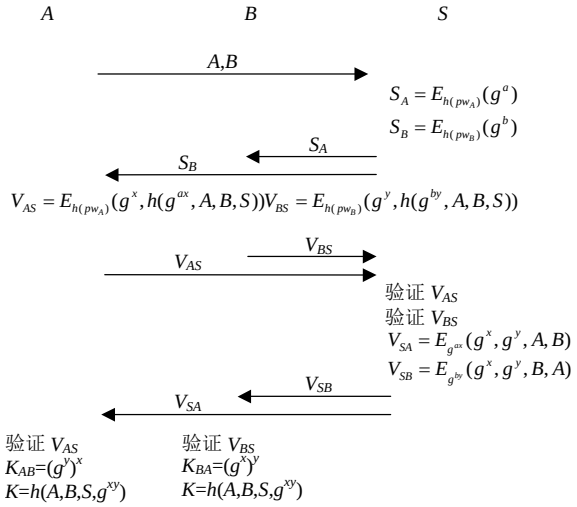

图1　新协议的流程

4) S收到A、B发送的V_{AS}、V_{BS}后，分别计算$D_{h(pw_A)}(V_{AS})$，$D_{h(pw_B)}(V_{BS})$得到解密后的前半部分g^x, g^y，然后利用自己保存的a、b计算$h(g^{ax},A,B,S)$, $h(g^{by},A,B,S)$，并分别验证是否与解密后的后半部分相等，若相等，S计算$V_{SA} = E_{g^{ax}}(g^x, g^y, A, B)$，$V_{SB} = E_{g^{by}}(g^x, g^y, B, A)$。然后分别将$V_{SA}$、$V_{SB}$发送给$A$、$B$。

5) A、B收到V_{SA}、V_{SB}后，分别利用保存的g^{ax}、

g^{by}对它们解密，计算$D_{g^{ax}}(V_{SA})$，$D_{g^{by}}(V_{SB})$，A验证解密后的消息中是否含有g^x，B验证解密后的消息中是否含有g^y，若验证都含有，则A，B计算$K_{AB}=(g^y)^x$，$K_{BA}=(g^x)^y$。A、B双方的会话密钥$K=h(A,B,S,K_{AB})=h(A,B,S,K_{BA})=h(A,B,S,g^{xy})$。

新协议的流程如图1所示。

3 新协议的安全性分析

假设攻击者具有窃听、重放、冒充、伪造等手段对协议进行攻击，本文从现有的协议常遭受的几种攻击来分析新协议的安全性。

1) 假设攻击者截获了A、B、S_A、S_B、V_{AS}、V_{BS}、V_{SA}、V_{SB}，除了身份外其他消息都进行了对称加密，攻击者无法在不知道密钥的情况下得到任何其他有用的信息。

2) 假设攻击者试图冒充A、B，但是在协议执行步骤2)中S用$h(pw_A)$, $h(pw_B)$分别加密g^a、g^b产生了S_A、S_B，攻击者在不知道口令的情况下无法对S_A、S_B解密，所以无法得到g^a、g^b，所以攻击者无法产生用于冒充的消息V_{AS}、V_{BS}。

3) 假设攻击者试图冒充S，但是在协议执行步骤3)中A、B分别用$h(pw_A)$、$h(pw_B)$分别加密了g^x、g^y产生了S_{AS}、S_{BS}，攻击者在不知道口令的情况下无法对V_{AS}、V_{BS}解密，所以无法得到g^x、g^y，所以攻击者无法产生用于冒充的消息V_{SA}、V_{SB}。

4) 假设攻击者试图进行在线字典攻击，攻击者可以选择可能的口令pw'_A、pw'_B来冒充A、B或S，但是A、B能在验证V_{SA}、V_{SB}时发现攻击者冒充S的口令猜测攻击，S能在验证V_{AS}、V_{BS}时发现这种攻击者冒充A或B的口令猜测攻击，因此该在线字典攻击是一种可检测的在线字典攻击。

5) 假设攻击者得到了口令pw_A或pw_B，攻击者无法计算出以前的会话密钥K，因为攻击者想要得到以前的会话密钥就必须解一个离散对数问题，而这个问题是现在公认的难解问题。所以该协议提供了完美的前向安全性。

4 新协议的效率分析

新协议以文献[8,10]的3PAKE协议为基础，不仅能够抵御现有的各种攻击，在效率上也得到了较大的提高。将新协议与文献[8,10]的3PAKE协议进行效率对比，结果如表1所示。对比指标包括随机数个数、指数运算次数、非对称加密/解密次数、交换轮数和执行时间。因为对称加密/解密和哈希函数的计算量很小，相较于非对称加密/解密和指数运算可以忽略不计，所以这里也不做分析。通常认为非对称加密/解密和指数运算的计算量相当，可以看出新协议的计算量与文献[8,10]的协议相当，但随机数个数少于文献[8]协议。在新协议的执行中S_A、S_B、g^x、g^y可以预先计算出(其他两个协议也做同样考虑)，所以在执行新协议时只需要3次指数运算(用3E表示，E表示非对称加密/解密次数和指数运算次数)的时间就能完成，优于文献[8,10]的协议。且新协议只需执行4次信息交换，在交换轮数上要优于文献[8,10]的协议。

表1 效率对比

协议	文献[8]协议			文献[10]协议			新协议		
	A	B	S	A	B	S	A	B	S
随机数个数	1	1	3	1	1	2	1	1	2
指数运算次数	2	2	2	3	3	4	3	3	4
非对称加密/解密次数	1	2	1	0	0	0	0	0	0
交换轮数	5			5			4		
执行时间	8E			5E			3E		

5 总 结

本文提出了一个新的基于口令的三方密钥交换协议，通过对其进行安全性分析，该协议能够抵御现有的攻击，如离线字典攻击、在线不可检测字典攻击、冒充攻击等，并且提供完美的前向安全性。通过对其进行效率分析，该协议在整体执行效率上要优于文献[8,10]协议。

参 考 文 献

[1] DING Y, HORSTER P. Undetectable on-line password guessing attacks[J]. ACM SIGOPS Operating Systems Review, 1995, 29(4): 77-86.

[2] BELLOVIN S M, MERRITT M. Encrypted key exchange: password-based protocols secure against dictionary attacks[C]//Proc of the 1992 IEEE Symposium on Research in Security and Privacy. Oakland: IEEE Computer Society Press, 1992: 72-84.

[3] BELLARE M, POINTCHEVAL D, ROGAWAY P. Authenticated key exchange secure against dictionary attacks[C]//Proc of the Advances in Cryptology-Eurocrypt 2000, LNCS 1807. Berlin Heidelberg: Springer-Verlag, 2000: 139-155.

[4] KATZ J, OSTROVSKY R, YUNG M. Efficient password-authenticated key exchange using human-memorable passwords[C]//Proc of the Advances in Cryptology-Eurocrypt 2001, LNCS 2045. Berlin Heidelberg: Springer-Verlag, 2001: 475-494.

(下转第604页)

4 结 论

本文提出一种构建集成电路工艺设备仿真系统的方法，设计了一套通用的设备气路子模块的仿真系统。该气路仿真系统包含功能层、逻辑层和外部通信接口层，采用了符合SEMI标准的通信与设备模型管理方法，使得系统具有一定通用性的同时，既可以满足单独设备的功能仿真需求，也能对整个系统的功能进行仿真验证。仿真系统能保存仿真信息，便于对这些信息的查看与调试。该系统实现了对PVD系统中，气路中阀门的闭合动作及气流变化等的实时仿真分析。实现结果表明该仿真系统能够准确有效地仿真实际系统的功能。

参 考 文 献

[1] SEMATECH. Guidelines for simulator-based control system testing[EB/OL]. [2011-01-15]. http://www.sematech. org.

[2] 王戟, 王兵. 半导体设备通讯标准GEM的应用. 机电工程, 2008, l25(7): 34-36, 54.
WANG Ji, WANG Bing. Application of GEM in semiconductor equipment[J]. Mechanical & Electrical Engineering Magazine, 2008, 25(7): 34-36, 54.

[3] 王戟. SECS/GEM在半导体生产计算机集成制造系统中的应用研究[D]. 浙江: 浙江工业大学, 2008.
WANG Ji. Research and development of semiconductor production computer integrated manufacturing systems based on SECS/GEM[D]. Zhejiang: Zhejiang University of Technology, 2008.

[4] 王延辉, 姜建国, 王宇. 基于GEM/SECS协议的数据采集系统设计与实现[J]. 计算机工程与设计, 2008, 29(12): 3218-3223.
WANG Yan-hui, JIANG Jian-guo, WANG Yu. Design and implementation of data acquisition based on GEM/SECS[J]. Computer Engineering and Design, 2008, 29(12): 3218-3223.

[5] SECREST J, GHISELLI J. SECS communications handbook[S]. SECS and GEM implementation seminar: [s.n.], 1996.

[6] Global Information & Control Committee. SEMI E5-1104, SEMI equipment communications standard 2 message content[S]. 2006.

[7] Global Information & Control Committee. SEMI E30-1103, generic model for communications and control of manufacturing equipment[S]. 2003.

[8] Global Information & Control Committee. SEMI E37-0303, high-speed SECS message services (HSMS) generic services[S]. 2003.

编 辑 漆 蓉

(上接第598页)

[5] STEINER M, TSUDIK G, WAIDNER M. Refinement and extension of encrypted key exchange[J]. ACM SIGOPS Operating Systems Review, 1995, 29(3): 22-30.

[6] LIN C L, SUN H M, HWANG T. Three-party encrypted key exchange: attacks and a solution[J]. ACM SIGOPS Operating Systems Review, 2000, 34(4): 12-20.

[7] LIN C L, SUN H M, STEINER M, et al. Three-party encrypted key exchange without server public-keys[J]. IEEE Communication Letters, 2001, 5(12): 497-499.

[8] SUN H M, CHEN B C, HWANG T. Secure key agreement protocols for three-party against guessing attacks[J]. Journal of Systems and Software, 2003, 75(1/2): 63-68.

[9] NAM J, KIM S, WON D. A weakness in Sun-Chen-Hwang three-party key agreement protocols using passwords [EB/OL]. [2010-9-19]. http://eprint.iacr.org/2004/ 348.

[10] LEE S W, KIM H S, YOO K Y. Efficient verifier-based key agreement protocol for three parties without server's public key[J]. Applied Mathematics and Computation, 2005, 167(1): 996-1003.

[11] LU Rong-xing, CAO Zhen-fu. Simple three-party key exchange protocol[J]. Computers and Security, 2007, 26(1): 94-97.

[12] CHUNG H R, KU W C. Three weaknesses in a simple three-party key exchange protocol[J]. Information Sciences, 2008, 178(1): 220-229.

[13] GOU hua, LI Zhou-jun, MU Yi, et al. Cryptanalysis of simple three-party key exchange protocol[J]. Computers and Security, 2008, 27(1): 16-21.

[14] PHAN R C W, YAU W C, GOI B M. Cryptanalysis of simple three-party key exchange protocol(S-3PAKE)[J]. Information Sciences, 2008, 178(13): 2849-2856.

[15] 许春香, 罗淑丹. 关于S-3PAKE协议的漏洞分析[J]. 电子科技大学学报, 2009, 38(4): 583-587.
XU Chun-xiang, LUO Shu-dan. Security Anaysis on S-3PAKE Protocol[J]. Journal of University of Electronic Science and Technology of China, 2009, 38(4): 583-587.

[16] NAM J, PAIK J, KANG H K, et al, An off-line dictionary attack on a simple three-party key exchange protocol[J]. IEEE Communications Letters, 2009, 13(2): 205-207.

编 辑 漆 蓉