·计算机工程与应用·

关于S-3PAKE协议的漏洞分析

许春香，罗淑丹

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】通过分析一种基于CCDH假设的简单三方密钥交换协议(S-3PAKE 协议)，指出了该协议未对攻击者可能的身份进行全面考虑，缺乏完备认证机制的缺陷，阐明了当攻击者本身就是与服务器共享一对认证口令的合法用户时，该协议不能有效地抵抗在线口令猜测攻击，并提出了一种对S-3PAKE协议进行在线口令猜测攻击的具体方法。使用该方法，攻击者只需与服务器进行通信，即可对其他用户的口令进行猜测分析。

关 键 词 身份认证； 密钥交换； 在线猜测攻击； 口令

中图分类号 TP393.08 **文献标识码** A doi:10.3969/j.issn.1001-0548.2009.04.025

Security Analysis on S-3PAKE Protocol

XU Chun-xiang and LUO Shu-dan

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract The three-party password-based authenticated key exchange protocol based on the CCDH assumption is analyzed. It is demonstrated that this protocol has security vulnerabilities from on-line guessing attack and lacks a perfect authentication mechanism. This paper presents an attack scheme to the protocol. Our attack scheme shows that an adversary can get other legitimate user's password successfully by on-line guessing cyclically.

Key words ID authentication; key exchange; on-line guessing attack; password

随着计算机网络技术的不断发展，网络的应用日益广泛，网络通信中的安全问题受到越来越多的关注。文献[1]指出电子商务作为当前一种重要的网络应用，以密码学为基础的各种加解密技术和通信协议是其安全基础。在安全通信领域里，密钥协商协议(也称密码交换协议)是其中一种重要的密码学机制，是两个实体在公共网络上协商通信密钥的协议，协议的最终结果是双方都能确认，只有对方才能拥有协商好的通信密钥，而其他第三方均无法获得通信密钥。文献[2]提出了第一个密钥协商协议(D-H协议)，但是由于该协议没有提供认证机制，因此很容易受到中间人攻击。文献[3]提出了一种基于用户口令的两方加密密钥交换协议(2PAKE协议)，但是由于2PAKE协议只适用于“客户–服务器”结构，许多研究者又将其扩展为适用于“客户–服务器–客户”结构的基于口令认证的三方密钥交换协议(3PAKE协议)。在3PAKE协议中，每个用户都与一个可靠的服务器共享一个口令，在需要进行通信时，通信双方都通过服务器对对方的身份进行认证，并生成会话密钥。文献[4]基于Diffie-Hellman密钥交换的思想，用双线性对简单地完成了三方密钥协商。针对文献[4]的方案不能抵抗中间人攻击的情况，文献[5]在文献[4]的方案中引入证书以实现通信三方的认证功能。文献[6]提出了基于ID的可验证双方密钥协商方案。文献[7]指出文献[6]的方案不具备完善的前向安全性，并提出了改进方案，但改进方案仍存在中间人攻击。文献[8]提出了两种不需要公钥技术的三方加密密钥交换协议(3PEKE协议)。文献[9]运用Weil对提出了一种基于口令认证的三方密钥加密协议(3PAKE协议)，并指出它们的协议具有可证明的安全性。然而，文献[10]发现了3PAKE协议并不能抵抗中间人攻击的漏洞。文献[11]提出了一种基于CCDH假设[12]的S-3PAKE协议，其设计者声称，该协议能够抵抗平凡攻击、在线猜测攻击、回放攻击

收稿日期：2008 – 03 – 22；修回日期：2009 – 05 – 04
基金项目：国家863计划(2009AA01Z415)；现代通信国家重点实验室基金(9140C1107010604)
作者简介：许春香(1970 –)，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.

等多种类型的攻击，并且具有比其他类似的协议更优越的特性。但文献[13]却指出S-3PAKE协议具有发起者伪装攻击、响应者伪装攻击以及中间人攻击3个漏洞。除此之外，经过分析还发现，由于该协议未对攻击者可能的身份进行全面考虑，缺乏完备的认证机制，如果攻击者本身就是与服务器共享一对认证口令的合法用户，那么S-3PAKE协议并不能够有效地抵抗在线猜测攻击。

本文首先介绍S-3PAKE协议，然后提出一种对S-3PAKE协议进行在线口令猜测攻击的具体方法。通过对该方法的描述，充分论证了S-3PAKE协议中，当攻击者本身就是与服务器共享一对认证口令的合法用户时，不能抵抗在线口令猜测攻击的漏洞。

1 S-3PAKE协议介绍

1.1 S-3PAKE协议中使用的符号含义

假设(G,g,p)表示有限循环群G，$G\subseteq Z_p^*$；g为Z_p的生成元；p为一个大素数。并假设S-3PAKE协议中使用的符号的含义如下：

M和N分别表示G中的两个元素；

S表示一个可靠的服务器；

A和B分别表示在一次协议执行过程中的发起者与接收者，也即两个用户的身份，此外A也可以扮演攻击者；

pw_A表示A与S之间共享的口令；

pw_B表示B与S之间共享的口令；

$H()$是一个$\{0,1\}^*\to Z_{p-1}$的哈希函数。

1.2 CDH和CCDH假设

(1) CDH假设。

从Z_p中随机地选取两个元素u和v，并计算出g^u和g^v的值。CDH假设是指：在u和v保密的前提下，即使已知g^u和g^v，仍不可能计算出g^{uv}的值。一般将CDH假设记为CDH(g^u, g^v)。

(2) CCDH假设。

CCDH假设是对CDH假设的一种变形，该假设考虑的情况是攻击者已知G中的3个随机元素M、N和X，并且其目标是要找出三元组(Y,u,v)的值，其中，u=CDH(X,Y)，v=CDH(X/M,Y/N)。CCDH假设认为，即使攻击者通过选择$Y=g$来得到$u=X$，或者通过选择$Y=gN$得到$v=X/M$，但是却不可能同时得到u和v的值。

1.3 S-3PAKE协议

S-3PAKE协议的具体步骤如下：

(1) A选择一个随机数$x\in Z_p$，并计算$X\leftarrow g^x M^{\mathrm{pw}_A}$，然后将$A\|X$发送给$B$；$B$收到消息后，也选择一个随机数$y\in Z_p$，并计算$Y\leftarrow g^y N^{\mathrm{pw}_B}$，然后将$A\|X\|B\|Y$发送给服务器$S$。

(2) 服务器S收到$A\|X\|B\|Y$后，首先运用pw_A和pw_B分别计算出$g^x\leftarrow X/M^{\mathrm{pw}_A}$和$g^y\leftarrow Y/N^{\mathrm{pw}_B}$，然后选择一个随机数$z\in Z_p$，并计算出$g^{xz}\leftarrow (g^x)^z$和$g^{yz}\leftarrow (g^y)^z$，再计算出$X'\leftarrow g^{yz}H(A,S,g^x)^{\mathrm{pw}_A}$和$Y'\leftarrow g^{xz}H(B,S,g^y)^{\mathrm{pw}_B}$，并把$X'\|Y'$发送给$B$。

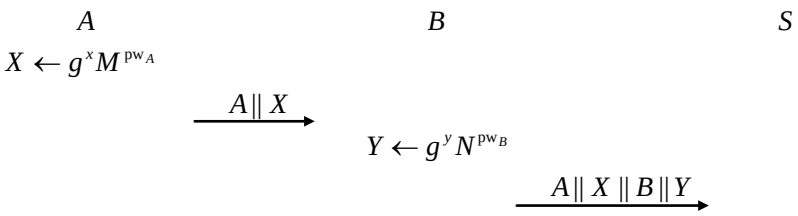
B收到$X'\|Y'$后，运用pw_B计算出$g^{xz}\leftarrow Y'/H(B,S,g^y)^{\mathrm{pw}_B}$，然后通过$y$计算$g^{xyz}\leftarrow (g^{xz})^y$，$B$计算出$\alpha\leftarrow H(A,B,g^{xyz})$，并将$X'\|\alpha$发送给$A$。

(3) A收到$X'\|\alpha$后，计算出$g^{yz}\leftarrow X'/H(A,S,g^x)^{\mathrm{pw}_A}$、$g^{xyz}\leftarrow (g^{yz})^x$和$H(A,B,g^{xyz})$，如果$H(A,B,g^{xyz})$与收到的$\alpha$相等，那么$A$就可确认$g^{xyz}$是有效的；否则，$A$将终止这次协议的运行。然后$A$计算出$\beta\leftarrow H(B,A,g^{xyz})$，并将$\beta$回传给$B$。同时，$A$将会计算出$\mathrm{SK}_A\leftarrow H'(A,B,g^{xyz})$，作为之后与$B$进行安全通信的会话密钥。

B收到β后，计算出$H(B,A,g^{xyz})$，如果$H(B,A,g^{xyz})$与收到的β相等，那么B将会计算出$\mathrm{SK}_B\leftarrow H'(A,B,g^{xyz})$，作为之后与$A$进行安全通信的会话密钥；否则，$B$也将终止这次协议的运行。

在S-3PAKE协议中，虽然通信双方A、B以及服务器S需要在公开信道(不安全信道)上传输数据(X,Y,X',Y',α,β)，但是基于CCDH假设、离散对数难解问题、哈希函数的单向性，以及每次通信所使用的x、y和z均是一些随机数等因素，S-PAKE协议仍然具有前向安全性及已知密钥安全性，能够有效地抵抗平凡攻击、离线猜测攻击和重放攻击。

S-3PAKE协议的流程如下：



$$
\begin{array}{ccc}
 & & g^{x} \leftarrow X / M^{\mathrm{pw}_A} \\
 & & g^{y} \leftarrow Y / N^{\mathrm{pw}_B} \\
 & & g^{xz} \leftarrow (g^{x})^{z} \\
 & & g^{yz} \leftarrow (g^{y})^{z} \\
 & & X' \leftarrow g^{yz} H(A,S,g^{x})^{\mathrm{pw}_A} \\
 & & Y' \leftarrow g^{xz} H(B,S,g^{y})^{\mathrm{pw}_B} \\
 & & \xleftarrow{X' \| Y'} \\
 & g^{xz} \leftarrow Y' / H(B,S,g^{y})^{\mathrm{pw}_B} & \\
 & g^{xyz} \leftarrow (g^{xz})^{y} & \\
 & \alpha \leftarrow H(A,B,g^{xyz}) & \\
 & \xleftarrow{X' \| \alpha} & \\
g^{yz} \leftarrow X' / H(A,S,g^{x})^{\mathrm{pw}_A} & & \\
g^{xyz} \leftarrow (g^{yz})^{x} & & \\
\text{验证 } B: & & \\
H(A,B,g^{xyz}) & & \\
\beta \leftarrow H(B,A,g^{xyz}) & & \\
 & \xrightarrow{\beta} & \\
 & \text{验证 } A: & \\
 & H(B,A,g^{xyz}) & \\
\mathrm{SK}_A \leftarrow H'(A,B,g^{xyz}) & & \mathrm{SK}_B \leftarrow H'(A,B,g^{xyz})
\end{array}
$$

2　S-3PAKE协议漏洞分析

密码协议的漏洞分析主要是针对协议消息交互产生的漏洞[14]，在漏洞分析的一般方法中，协议攻击者被赋予以下能力：

(1) 可以得到任何网络上传输的消息。

(2) 是网络的合法用户，可以与任何其他用户发起会话。

(3) 有机会成为某个用户的消息接收者。

S-3PAKE协议的设计者声称，该协议能够抵抗平凡攻击、在线猜测攻击、回放攻击等多种类型的攻击，并且具有比其他类似的协议更优越的特性。但文献[13]却指出，该协议不能抵抗发起者伪装攻击、响应者伪装攻击和中间人攻击3种攻击。任何一个用户C，只要是与S共享一对认证口令的合法用户，都可以冒充对话的发起者A、或者响应者B、或者作为中间人窃听甚至篡改另外两方的对话内容，来实现发起者伪装攻击、响应者伪装攻击和中间人攻击3种类型的攻击，因此S-3PAKE协议是不安全的。

除了文献[13]提出的3种攻击之外，经过分析还可发现，如果S-3PAKE协议中的发起者A本身就是攻击者，那么，由于该协议不具备服务器与用户之间的认证机制，用户A就可以通过循环运行该协议，假冒B的身份对用户B与服务器S共享的口令pw_B进行在线猜测分析，从而最终窃取B的口令达到冒充B的目的。

S-3PAKE协议进行在线口令猜测攻击的具体方案如下：

$$
\begin{array}{ccc}
A & B & S \\
\text{猜测：} \mathrm{pw}'_B & & \\
X \leftarrow g^{x} M^{\mathrm{pw}_A} & & \\
Y \leftarrow g^{y} N^{\mathrm{pw}'_B} & & \\
 & \xrightarrow{A \| X \| B \| Y} & \\
 & & g^{x} \leftarrow X / M^{\mathrm{pw}_A} \\
 & & Q \leftarrow Y / N^{\mathrm{pw}_B} \\
 & & g^{xz} \leftarrow (g^{x})^{z},\ Q^{z}
\end{array}
$$

$$X' \leftarrow Q^z H(A,S,g^x)^{\mathrm{pw}_A}$$

$$Y' \leftarrow g^{xz} H(B,S,Q)^{\mathrm{pw}_B}$$

$$\xleftarrow{X' \| Y'}$$

$$Q^z \leftarrow X' / H(A,S,g^x)^{\mathrm{pw}_A}$$

$$Q^{xz}$$

$$R \leftarrow Y' / H(B,S,g^y)^{\mathrm{pw}'_B}$$

判断 $R^y ? = Q^{xz}$

若 $R^y = Q^{xz}$，则 $\mathrm{pw}_B = \mathrm{pw}'_B$

若 $R^y \neq Q^{xz}$，则重新猜测 pw'_B

在线口令猜测的具体过程如下：

(1) A选择两个随机数 $x, y \in Z_p$，并通过 pw_A 计算出 $X \leftarrow g^x M^{\mathrm{pw}_A}$；同时，$A$猜测$B$与$S$的共享口令为 pw'_B，计算出 $Y \leftarrow g^y N^{\mathrm{pw}'_B}$，然后假冒 B 将 $A \| X \| B \| Y$ 发送给S。

(2) 当服务器S收到 $A \| X \| B \| Y$ 之后，首先运用 pw_A 和 pw_B 分别计算出 $g^x \leftarrow X / M^{\mathrm{pw}_A}$ 以及 $Q \leftarrow Y / N^{\mathrm{pw}_B}$；然后，选择一个随机数 $z \in Z_p$，并计算出 $g^{xz} \leftarrow (g^x)^z$ 和 Q^z，再计算出 $X' \leftarrow Q^z H(A,S,g^x)^{\mathrm{pw}_A}$ 以及 $Y' \leftarrow g^{xz} H(B,S,Q)^{\mathrm{pw}_B}$，并把 $X' \| Y'$ 发送给B，此时，A截获信息 $X' \| Y'$。

(3) A收到 $X' \| Y'$ 以后，首先通过 pw_A 算出 $Q^z \leftarrow X' / H(A,S,g^x)^{\mathrm{pw}_A}$ 以及 Q^{xz}，然后通过事先猜测的 pw'_B 算出 $R \leftarrow Y' / H(B,S,g^y)^{\mathrm{pw}'_B}$ 以及 R^y，如果 $R^y = Q^{xz}$，则说明 $\mathrm{pw}_B = \mathrm{pw}'_B$，即$A$已获得$B$的口令，否则，$A$继续猜测 pw_B，即重新开始第一步。

由上述过程不难发现，在用户A对用户B的口令进行猜测的过程中，并不需要用户B的参与，攻击直接发生在服务器S与攻击者A之间的。在S-3PAKE协议中，由于服务器无法验证用户身份，也无法终止协议的运行，在没有B的参与下，A可以一直循环冒充B，猜测B的口令，向服务器发出请求，直到最终确认了B的口令为止。因此，本文认为，当攻击者本身就是与服务器享有一对认证口令的合法用户时，S-3PAKE协议并不能有效地抵抗在线口令猜测攻击。

3 结 束 语

针对文献[12]提出的简单三方密钥交换协议(S-3PAKE协议)中的漏洞，即当攻击者本身就是与服务器共享一对认证口令的合法用户时，该协议不能有效地抵抗在线口令猜测攻击，本文提出了实现在线口令猜测攻击的具体方法。通过对该方法的描述，充分论证了S-3PAKE协议存在的安全漏洞，从而也说明了S-3PAKE协议并不如其设计者所声称的那样无论在效率上还是在安全性方面，都具有比其他类似的协议更优越的特性。因此，该协议仍需进一步改进才能具备更高更可靠的安全性能。

本文研究工作得到华为公司科技基金(YJCB2006053DC)和计算机网络与信息安全教育部重点实验室基金资助，在此表示感谢。

参 考 文 献

[1] QIN Zhi-guang, LUO Xu-cheng, GAO Rong. A survey of E-Commerce security[J]. Journal of Electronic Science and Technology of China, 2004, 2(3): 173-176.

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

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

[4] JOUX A. A one round protocol for tripartite Diffie-Hellman[C]//Proc of Fourth Algorithmic Number Theory Symposium, LNCS 1838. Berlin: Springer Verlag Press, 2000: 385-394.

[5] Al-RIYAMI S S, PATERSON K G. Authenticated three party key agreement protocols from pairings[EB/OL]. [2008-02-16]. http://eprint.iacr.org/2002/035.

[6] SMART N P. An identity-based authenticated key agreement protocol based on the weil pairing[J]. Electronics Letters, 2002, 38(13): 630-632.

[7] SHIM K. Efficient identity-based authenticated key agreement protocol based on the Weil pairing[J]. Electronics Letters, 2003, 39(8): 653-654.

[8] LEE T F, HWANG T, LIN C L. Enhanced three-party encrypted key exchange without server public keys[J]. Computers Security, 2004, 23(7): 571-577.

[9] WEN H A, LIN C L, HWANG T. Provably secure three-party password-authenticated key exchange using weil pairing[J]. IEE Proceedings-Communications, 2005, 152(2): 138-143.

[10] NAM J, LEE Y, KIM S, et al. Security weakness in a

three-party pairing-based protocol for password authenticated key exchange[J]. Information Sciences, 2007, 177(6): 1364-1375.
[11] LU Rong-xing, CAO Zhen-fu. Simple three-party key exchange protocol[J]. Computers Security, 2007, 26(1): 94-97.
[12] ABDALLA M, POINTCHEVAL D. Simple password based encrypted key exchange protocols[C]//Proc of CT-RSA 2005, LNCS 3376. Berlin: Springer-Verlag, 2005: 191-208.
[13] CHUNG Hao-rung, KU Wei-chi. Three weaknesses in a simple three-party key exchange protocol[J]. Information Sciences, 2008, 178(1): 220-229.
[14] 张 靖. 协议入侵者攻击能力的统一建模[J]. 电子科技大学学报, 2007, 36(3): 617-620
ZHANG Jing. Unified modeling of the intruder's attack ability based on the protocols[J]. Journal of University of Electronic Science and Technology of China, 2007, 36(3): 617-620.

编 辑 熊思亮

(上接第495页)

参 考 文 献

[1] YANG SHI-WEN, NIE ZAI-PING. A review of the four dimension antenna arrays[J]. Journal of Electronic Science and Technology of China, 2006, 4(3): 193-201.
[2] WALDSCHMIDT C, HAGEN J V, WIESBECK W. Influence and modelling of mutual coupling in MIMO and diversity systems[C]//Proc IEEE Antennas and Prop Soci Inte Symp. San Antonio, Texas: IEEE, 2002.
[3] FLETCHER P N, DEAN M, NIX A R. Mutual coupling in multi-element array antennas and its influence on MIMO channel capacity[J]. Eletronics Letters, 2003, 39(4): 342-344.
[4] CLERCKX B, VANHOENACKER J D, OESTGES C, et al. Mutual coupling effects on the channel capacity and the space-time processing of MIMO communication systems[C]//Proc IEEE Inte Conf, Commun (ICC.'03). [S.l.]: IEEE, 2003.
[5] 肖海林, 聂在平, 杨仕文. 衰落信道下的多天线最佳信道容量研究[J]. 电子科技大学学报, 2008, 7(1): 11-13.
XIAO Hai-lin, NIE Zai-ping, YANG Shi-wen. Optimize the capacity of multi-antenna in fading channels [J]. Journal of University of Electronic Science and Technology of China, 2008, 37(1): 11-13.
[6] 肖海林, 聂在平, 杨仕文. 室内MIMO无线信道: 模型和性能预测[J]. 电波科学学报, 2007, 27(3): 385-389.
XIAO Hai-lin, NIE Zai-ping, YANG Shi-wen. Indoor MIMO wireless channels: Models and performance prediction[J]. Chinese Journal of Radio Science, 2007, 27(3): 385-389.
[7] GUPTA I J, KSIENSKI A K. Effect of mutual coupling on the performance of adaptive arrays[J]. IEEE Trans Antennas and Propagation, 1983, 31(5):785-791.
[8] CLERCKX B, CRAEYE C, VANHOENACKER J D, et.al. Impact of antenna coupling on 2 $times$ 2 MIMO communications [J]. IEEE Transactions on Vehicular Technology, 2007, 56(3): 1009-1018.
[9] YANG Yao-qing, XU Guang-han, HAO Ling. An experimental investigation of wideband MIMO channel characteristics based on outdoor non-LOS measurements at 1.8 GHz[J]. IEEE Transactions on Antennas and Propagation, 2006, 54(11): 3274-3284.
[10] PAPOULIS A. Probability, random variables and stochastic processes[M]. 2nd ed. New York: McGram Hill, USA, 1984.
[11] FOSCHINI G J, GANS M J. On limits of wireless communications in a fading environment when using multiple antennas[J]. Wireless Personal Commun, 1998, 6(3): 311-317.
[12] XIN LI, ZAI-PING NIE. Mutual coupling effects on the performance of MIMO wireless channels[J]. IEEE Antennas and Wireless Propagation Letters, 2004, 3(16): 344-347.
[13] CHIU C Y, CHENG C H, MURCH R D, et al. Reduction of mutual coupling between closely-packed antenna elements[J]. IEEE Transactions on Antennas and Propagation, 2007, 55(6): 1732-1738.

编 辑 税 红