

一种安全的两方口令认证的密钥交换协议

项顺伯

(广东石油化工学院 计算机与电子信息学院, 茂名 525000)

摘要 对于口令认证密钥交换协议的服务器泄漏伪装攻击, 提出一个针对该攻击的两方口令认证的密钥交换协议, 并分析了该协议的安全性。所提出的协议中, 用户保存自己的口令明文, 服务器存储用户口令明文的验证值, 用户和服务器之间通过身份标识和含有口令验证值的信息来认证对方。分析表明, 所提出的协议是安全的。

关键词 口令认证 密钥交换 泄漏伪装攻击 验证值

中图分类号 TP309; **文献标志码** A

两方口令认证的密钥交换协议是指参与协议的两方共享一个低熵的口令或口令验证值来建立一个会话密钥, 从而实现不安全信道上的安全通信。1992年, Bellovin等首次提出能抵抗在线口令字典攻击的两方口令认证的密钥交换协议EKE^[1], EKE协议以Diffie-Hellman密钥交换协议为基础, 实现两方之间的认证以及会话密钥的建立过程。文献[2]所提出的协议是EKE的改进。随后, 大量的两方口令认证的密钥交换协议被提出^[3-7]。两方口令认证的密钥交换协议中的两方是指用户和服务器, 采用的口令为用户的口令明文或者口令的验证值。文献[5]提出一种两方口令认证密钥交换协议PAKA-X, 文献作者声称PAKA-X能抵御服务器泄漏伪装攻击。文献[6]指出PAKA-X存在服务器泄漏伪装攻击和离线口令猜测攻击, 并各给出一种有效的攻击形式, 但没有提出对PAKA-X的改进。文献[7]提出一种适用于TLS协议的基于口令验证值的两方口令认证密钥交换协议, 该协议是一轮且可证明安全的。本文在文献[5]和文献[6]的基础上, 提出一个新的两方口令认证的密钥交换协议。

1 PAKA-X的协议内容

文献[5]中, 假设PAKA-X的协议参与方为Alice和Bob, 简称A和B, A为用户, 其身份标识为 ID_A ; B为服务器, 其身份标识为 ID_B 。 π 是A的口令明文, H 是抗碰撞的单向杂凑函数。为抵御服务器泄漏伪装攻击, B存储A口令的验证值。A计算口令验证值 $V = g^{H(ID_A || ID_B || \pi)}$, 通过秘密通道传到B上保存。协议执行过程如下: 1) A随机选择 $a \in {}_R Z_p^*$, 计算 $X_A = g^a \oplus V$, 然后发送 ID_A 和 X_A 给B; 2) 收到A的消息后, B从口令文件中取出V, 选择 $b \in {}_R Z_p^*$, 计算 $X_B = V^b \oplus V$, 发送 X_B 给A; 等待的时间内, A计算 $K_B = (X_A \oplus V)^b = g^{ab}$, 计算 $V'_A = H(ID_A || X_B || K_B)$ 和 $V_B = H(ID_A || X_A || K_B)$; 3) 收到B的消息后, A计算 $K_A = (X_B \oplus V)^{aH(ID_A || ID_B || \pi)^{-1}} = g^{ab}$ 和 $V_A = H(ID_A || X_B || K_A)$, 发送 V_A 给B; 等待的时间内, B计算 $V'_B = H(ID_B || X_A || K_A)$; 4) 收到 V_A 后, B验证 $V_A \stackrel{?}{=} V'_A$ 是否成立, 如果成立, B确信 K_A 得到证实, 然后发送 V_B 给A; 5) 收到 V_B 后, A验证 $V_B \stackrel{?}{=} V'_B$ 是否成立, 如果成立, A确信 K_B 得到证实; 6) 最终A和B计算出共同的会话密钥 $K = H(K_A) = H(K_B) = H(g^{ab})$ 。

2 PAKA-X存在的服务器泄漏伪装攻击

文献[6]指出攻击者能对PAKA-X协议实施服务器泄漏伪装攻击。假设攻击者Eve获得了服务器

2012年4月23日收到 广东省自然科学基金(02525000002000001)

资助

作者简介: 项顺伯(1979—), 男, 汉, 安徽枞阳人, 讲师, 硕士, 研究方向: 计算机网络与密码协议。

的口令文件,从中得到 A 的口令验证值 V , Eve 能向服务器冒充是 A 。攻击过程如下:

1) Eve 随机选择 $a \in {}_R Z_p^*$, 利用口令验证值 V , 计算 $X_A = V^a \oplus V$, 然后发送 ID_A 和 X_A 给 B ;

2) 收到 Eve 的消息后, B 从口令文件中取出 V , 选择 $b \in {}_R Z_p^*$, 计算 $X_B = V^b \oplus V$, 发送 X_B 给 Eve; 然后, A 计算 $K_B = (X_A \oplus V)^b = V^{ab}$, $V'_A = H(ID_A || X_B || K_B)$ 和 $V_B = H(ID_B || X_A || K_B)$;

3) 收到 B 的消息后, Eve 计算 $K_A = (X_B \oplus V)^a = V^{ab}$ 和 $V_A = H(ID_A || X_B || K_A)$, 发送 V_A 给 B ; 等待时间内, B 计算 $V'_B = H(ID_B || X_A || K_A)$;

4) 收到 V_A 后, B 验证 $V_A \stackrel{?}{=} V'_A$ 是否成立。因为 $K_A = K_B$, 所以 $V_A = V'_A$, B 确信 K_A 得到证实, 然后发送 V_B 给 A , 接着 B 计算会话密钥 $K = H(K_B) = H(V^{ab})$;

5) 收到 V_B 后, A 验证 $V_B \stackrel{?}{=} V'_B$ 是否成立, 如果成立, A 确信 K_B 得到证实; 因为 $K_A = K_B$, 所以 $V_B = V'_B$, Eve 成功向服务器 B 冒充 A , 并计算会话密钥 $K = H(K_A) = H(V^{ab})$ 。

3 新的两方口令认证的密钥交换协议

针对 PAKA-X 协议的缺陷, 提出一个新的两方口令认证的密钥交换协议, 简称 NPAKA, 协议中, H 和 H_1 是抗碰撞的单向杂凑函数, $H: \{0, 1\} \rightarrow Z_p^*$, $H_1: \{0, 1\} \rightarrow Z_p^*$ 。NPAKA 的实现过程如下:

1) A 随机选择 $a \in {}_R Z_p^*$, 计算 $X_A = g^a \oplus V$, 然后发送 ID_A 和 X_A 给 B ;

2) 收到 A 的消息后, B 选择 $b, c \in {}_R Z_p^*$, 从口令文件中取出 V , 计算 $X_B = V^b \oplus V$ 和 $X_C = g^c \oplus V$, 发送 ID_B , X_B 和 X_C 给 A ; 接着 B 计算 $K_B = (X_A \oplus V)^b = g^{ab}$, $K_C = (X_A \oplus V)^c = g^{ac}$, $V'_A = H(ID_A || X_B || K_B || K_C)$ 和 $V_B = H(ID_A || X_A || K_B || K_C)$;

3) 收到 B 的消息后, A 计算 $K_A = (X_B \oplus V)^{aH(ID_A || ID_B || \pi)^{-1}} = g^{ab}$, $K_D = (X_C \oplus V)^c = g^{ac}$, $V_A = H(ID_A || X_B || K_A || K_D)$, 发送 V_A 给 B , 等待的时间内, A 计算 $V'_B = H(ID_B || X_A || K_A || K_D)$;

4) 收到 V_A 后, B 验证 $V_A \stackrel{?}{=} V'_A$ 是否成立, 如果成立, B 确信 K_A 得到证实, 然后发送 V_B 给 A ;

5) 收到 V_B 后, A 验证 $V_B \stackrel{?}{=} V'_B$ 是否成立, 如果成立, A 确信 K_B 得到证实;

6) 最终 A 和 B 计算出共同的会话密钥 $SK = H_1(ID_A || ID_B || K_A || K_D) = H_1(ID_A || ID_B || K_B || K_C) = H_1(ID_A || ID_B || g^{ab} || g^{ac})$ 。

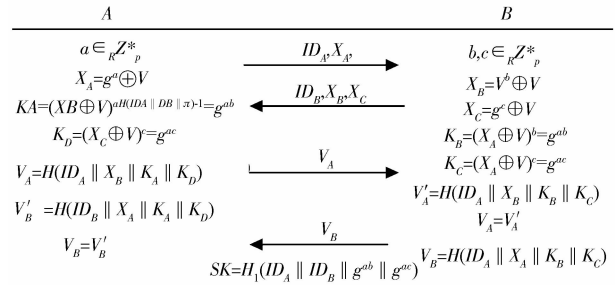


图1 NPAKA 实现过程图

4 新的两方口令认证密钥交换协议安全性分析

定义1 CDL 困难问题: 设 G 表示一个阶为素数 p 的群, 给定二元组 (g, g^a) , 其中 $a \in {}_R Z_p^*$, 计算 a 是困难的。定义解决 CDH 困难问题的优势是可忽略的。

定义2 CDH 困难问题: 设 G 表示一个阶为素数 p 的群。给定三元组 (g, g^a, g^b) , 其中 $a, b \in {}_R Z_p^*$, 计算 g^{ab} 是困难的。定义解决 CDH 困难问题的优势是可忽略的。

定理1 NPAKA 具有完美前向安全性。

证明 NPAKA 的完美前向安全性是指某次会话过程中, 即使 A 的口令明文 π 泄漏给攻击者 Eve, Eve 也不能计算出该会话之前的会话密钥, 因为, 假如 Eve 已知某次会话过程的口令 π , 通过窃听, Eve 获得了该次会话之前的通信消息 $g^a \oplus V, V^b \oplus V$ 和 $g^c \oplus V$, Eve 通过计算知道 g^a, V^a 和 V^b , 但他无法计算出 g^{ab} , 因为这是 CDL 困难问题或 CDH 困难问题。

定理2 NPAKA 对于 Denning-Sacco 攻击是安全的。

证明 对于 Denning-Sacco 攻击是安全的, 是指一个密码协议在运行过程中, 即使某一次的会话密钥泄漏, 攻击者无法利用此会话密钥计算出用户的口令, 也无法确定所猜测用户口令的正确性。NPA-

KA 中,假设 Eve 获得某次的会话密钥 $H_1(ID_A || \times ID_B || g^{ab} || g^{ac})$,通过 $H_1(ID_A || ID_B || g^{ab} || g^{ac})$ 和获得的信息 $g^a \oplus V$ 、 $V^b \oplus V$ 和 $g^c \oplus V$ 以及 V_A 和 V_B ,试图计算出口令 π 或确认所猜测口令的正确性,可 Eve 无法做到,因为 $H_1(ID_A || ID_B || g^{ab} || g^{ac})$ 不含任何的口令信息,Eve 无法通过计算获得 a 、 b 、 c 、 ab 和 ac ,因为他无法解决 CDL 困难问题或 CDH 困难问题,因此 NPAKA 针对 Denning-Sacco 攻击是安全的。

定理 3 NPAKA 可抵御服务器泄漏伪装攻击。

证明 NPAKA 中的服务器泄漏伪装攻击是指攻击者 Eve 获得 A 存储在服务器中的口令验证值 V ,伪装成 A 登录 B 。由于 Eve 不知道 A 的口令 π ,无法计算 $(X_B \oplus V)^{aH(ID_A || ID_B || \pi)^{-1}} = g^{ab}$,也就无法伪装成 A 与 B 会话,从而计算出 A 与 B 的会话密钥,因此 NPAKA 是能抵御服务器泄漏伪装攻击。

定理 4 NPAKA 可抵御各种字典攻击。

证明 字典攻击是指攻击者对用户口令的猜测,分为在线字典攻击和离线字典攻击两种。NPAKA 中,假设 Eve 选择 π' 来猜测口令 π ,通过 π' 计算出 V' ,更改 $X_A = g^a \oplus V'$, $X'_A = (V')^a \oplus V'$ 和 $X_B = (V')^b \oplus V'$ 。对于 A ,计算 $K_A = (X_B \oplus V)^{aH(ID_A || ID_B || \pi)^{-1}}$, $K'_A = (X_B \oplus V)^a$;对于 B ,计算 $K_B = (X_A \oplus V)^b$, $K'_B = (X'_A \oplus V)^b$,明显 $K_A \neq K'_A$, $K_B \neq K'_B$,则 $V_A \neq V'_A$, $V_B \neq V'_B$,以致 A 与 B 之间无法互相确认从而终止协议的执行,因此攻击者无法实施针对 NPAKA 的在线字典攻击。如果攻击者对 NPAKA 实施离线字典攻击,则攻击者必须解决

CDL 困难问题或 CDH 困难问题,攻击者无法解决这两个难题,因而离线字典攻击无效。因此,NPAKA 可抵御攻击者发起的各种字典攻击。

5 结论

针对文献[5]的 PAKA - X 协议中存在的服务器泄漏伪装攻击,提出一种改进的协议,通过分析表明,改进的协议 NPAKA 具有完美前向安全性,能抵御服务器泄漏伪装攻击和各种字典攻击以及其他的针对两方口令认证的密钥交换协议的攻击形式。

参 考 文 献

- 1 Bellovin S M, Merritt M. Encrypted key exchange: password-based protocols secure against dictionary attacks. IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, USA, 1992:72—84
- 2 Belkovic S, Merritt M. Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password-file compromise. Proceedings of CCS'93. New York: ACM Press, 1993: 244—250
- 3 Boyko V, Mackenzie P, PATEL S. Provably-secure password-authenticated and key exchange using Diffie-Hellman. EUROCRYPT2000, LNCS 1807, Berlin Springer-Verlag, 2000:156—171
- 4 Katz J, Ostrovsky R, Yung M. Efficient password-authenticated key exchange using human-memorable passwords. EUROCRYPT 2001, Berlin: Springer-Verlag, 2001
- 5 Lee S W, Kim W H, Kim H S, et al. Efficient password-based authenticated key agreement protocol. ICCSA'04. LNCS 2045: Springer - Verlag, 2004:475—494
- 6 Shim K A, Seo S H. Security analysis of password-authenticated key agreement protocols. CANS 2005, LNCS 3810: Springer-Verlag, 2005:49—58
- 7 Kwon J O, Sakurai K, Lee D H. One-round protocol for two-party verifier-based password-authenticated key exchange. Communications and Multimedia Security, LNCS 4237, 2006:87—96

A Secure Two-party Password-authenticated Key Exchange Protocol

XIANG Shun-bo

(College of Computer and Electronic Information, Guangdong University of Petrochemical Technology, Maoming 525000, P. R. China)

[Abstract] Password authenticated key exchange protocol for the server leaks disguised attack against the attacks, a two-party password authenticated key exchange protocol is proposed, and the security of the protocol is analyzed. The proposed protocol, the user expressly preserve their own password, the server stores user passwords in clear text authentication value, between the user and the server identity and by the value of information with password authentication to authenticate each other. Analysis showed that the proposed protocol is secure.

[Key words] password - authenticated key exchange compromising attack authentication value