基于口令认证的密钥交换协议的安全性分析

李 莉[1],薛 锐[2],张焕国[1],冯登国[2],王丽娜[1]
(1. 武汉大学计算机学院,湖北武汉 430072;2. 中国科学院软件所信息安全国家重点实验室,北京 100080)

摘 要: 在串空间理论模型引入了描述 DH 问题的方法以及分析猜测攻击的攻击者能力,对基于口令认证的密钥交换协议的安全性进行了形式化分析。提出一个对 DH-EKE 协议的简化,并证明了该协议的安全性:口令的秘密性,认证性,以及会话密钥的秘密性. 根据分析给出基于口令认证的密钥交换协议抵抗猜测攻击的基本条件. 将分析方法应用到基于口令的三方密钥交换协议上,给出单纯基于口令进行密钥交换协议的安全性需要满足的一个必要条件.

关键词: 密钥交换协议; 口令猜测攻击; 串空间模型; DH 密钥协商
中图分类号: TN393 **文献标识码**: A **文章编号**: 0372-2112 (2005) 01-0166-05

Security Analysis of Authenticated Key Exchange Protocol Based on Password

LI Li[1,2], XUE Rui[2], ZHANG Huan-guo[1], FENG Deng-guo[2], WANG Li-na[1]
(1. *School of Computer Science, Wuhan University, Wuhan, Hubei* 430072, *China*; 2. *State Key Laboratory of Information, IOS, CAS, Beijing* 100080, *China*)

Abstract: This paper gives a formal analysis on the authenticated key exchange protocol based on password using the theory of the strand space model. We introduce the ability on modeling the DH problem and the guessing attack, and then give a proof on secrecy of the password, authentication and the secrecy of the session key of the simplified DH-EKE protocol. Based on the analysis, we propose a basic condition of the key exchange protocol based on password on resisting the guessing attack. Extending the method to the three-party case, a necessary condition is concluded to guarantee the security of the three-party authenticated key exchange protocol based on the pure password.

Key words: key exchange protocol; guessing attack; strand space; DH key agreement

1 引言

在基于口令认证的密钥交换协议中,用户通常事先共享一个口令,用来在通信中进行彼此的身份认证,并协商一个短期的会话密钥. 基于口令的方案可以避免复杂的密钥管理,无需额外的公钥设施或者安全硬件. 目前已经有许多基于口令实现的方案[1~9],包括著名的 Kerberos 协议. 但是因为口令是由用户选择,存在不足够长且容易记忆的特点,使得基于口令的协议都存在可能的猜测攻击,如文献[10]中指出 Kerberos 不能抵抗离线的猜测攻击,文献[5,6]中指出的文献[4]中提出的三方协议存在漏洞,以及本文指出的文献[3]中提出的三方协议存在猜测攻击. 如何有效的抵抗攻击者对口令进行猜测攻击成为设计这类协议的目标之一.

基于口令的密钥交换协议需要满足协议运行过程中不能泄漏关于口令的安全准则. 攻击者即使获取合法方通信的消息报文,也无法通过字典攻击来猜测口令. 大多文献只对这类安全性给出了非形式化的分析,直到文献[11]首次基于一个非对称的混合模型给出了对这类协议的安全性证明,其后文献[12,13]也给出了不同模型下协议的安全性证明. 虽然这类证明有效且是很强的,但是这类基于计算复杂性理论的可证安全性方法比较复杂,不好操作. 文献[14]首次提出使用 CSP 来描述和分析猜测攻击,对安全性进行形式化分析,但是其分析中只单纯考虑了离线攻击. 本文基于 Guttman 等人提出的串空间模型[15,16]来分析基于口令认证的密钥交换协议,并对于基于 DH 问题的密钥协商问题给出了描述和分析.

2 串空间理论模型

本节首先简单介绍串空间(Strand Space,简称 SS)理论模型[15,16],并将其进行扩展以增加其分析密钥交换协议的能力和描述猜测攻击的能力. 有关串空间的详细讨论和相关证明可以参见文献[15,16].

2.1 消息代数

基于口令的密钥交换协议中可以利用 Diffie-Hellman 问题进行密钥交换. 在最简单的 DH 体制中,假设通信双方已经知道了一个大的循环群 G 和其生成元 g. A 和 B 可以如下进行密钥协商: A 在 $\{1\cdots|G|\}$ 范围内随机选择一个值 x,计算 g^x 并发送给 B; B 在 $\{1\cdots|G|\}$ 范围内随机选择一个值 y,计算 g^y 并发送给 A,其中 $|G|$ 表示循环群的阶. 经过两次交互后,A

收稿日期:2003-07-16;修回日期:2004-10-07
基金项目:国家自然科学基金(No. 90104005,No. 60373048);国家 863 项目(No. 2002AA144050);教育部博士点基金(No. 20020486046).

和 B 都可以计算出会话密钥 g^{xy}. DH 机制的安全性基于有限域的乘法群上求解离散对数的困难性,但这种简单的 DH 方案缺乏认证机制,基于口令认证的 DH 密钥协商机制可以利用口令提供有效的认证,如文献[1]中提出的 DH-EKE,以及文献[13]中的 PAK 协议.

为了能够描述基于 DH 问题的密钥交换协议,文献[17]中在串空间模型中引入对 DH 计算的描述,这里我们给出更一般的定义. 基于 DH 机制的密钥协商协议中具有以下三个条件:用户只有知道了相应的 g^x 和 y 或者 g^y 和 x 才能计算 g^{xy}; g^x 的产生者不会在协议中发送 x 值;合法参与者不发送 g^{xy},而只是将其作为一个密钥使用或者作为验证信息的一部分. 显然对于 g^{xy}的计算是一个单向函数. 我们在 SS 模型中增加一个新的数据类型集 D 来表示 DH 值,其中的元素为 d_1, d_2, …,每个元素表示为一个元组(m, n),满足 $m = g^n$,并定义计算 DH 值的操作 DH: $D \times D \to D$.

沿用文献[15]中的符号标识,用 A 表示协议中的信息空间的元素集合.

定义 1　设 A 表示协议的所有参与者交换的消息的全体组成的集合,称为项空间,A 中的元素称为项,其元素是由下述集合生成的:

- T:包括协议中可预见的原子项;
- K:包括协议使用的密钥,包括对称密钥、非对称密钥;
- D:用于计算的 DH 值.

其中 K,T,D 两两不相交. 在这些项上的操作包括:

- 加密运算 encr: $K \times A \to A$
- 连接运算 join: $A \times A \to A$
- 密钥逆运算 inv: $K \to K$
- DH 运算 DH: $D \times D \to D$.
- HASH 运算 Hash: $A^n \to A$.

后文将 encr(k, m)操作表示为$\{m\}_k$,其像空间记为 E,称为密文空间;将 join(a, b)表示为 ab,记为 C,表示项连接空间;将单向函数运算 Hash$(a_1, \cdots, a_n)$表示为 $H(a_1, \cdots, a_n)$,记为 H,称为散列值空间. 这些值空间互不相交.

在信息空间中,如下定义子项关系:

定义 2　M 是 N 的子项,记为 $M \subset N$,如果有:

(1) $M = N$

(2) 如果 $N = N' \hat{} N''$,则 $M \subset N$ 或者 $M \subset N''$

(3) 如果 $N = \{N'\}_k$,则 $M \subset N'$

(4) 如果 $N = \mathrm{DH}(d_1, d_2)$,则 $M = d_1$ 或者 $M = d_2$,其中, $M, N \in A$, $k \in K$, $d_1, d_2 \in D$.

对于基于 DH 问题的密钥交换,一般对于项 $g^x \in D$, x 是不会单独出现的,因此后文中对于 $d_1 \in D$ 直接使用 d_1. m 来描述 DH 值,即写成 g^n 的形式.

命题 1　给定 $K, K' \subseteq K$,如果 $K \neq K'$,且$\{h_1\}_K \subset \{h\}_{K'}$,则$\{h_1\}_K \subset h$.

定义 3　信息空间 A 上的一个串空间定义为集合 Σ和一个迹映射 tr,满足 tr: $\Sigma \to (\pm A)^*$,记为(Σ, tr). 集合 Σ的元素称为串空间中的串.

串空间模型使用从来描述协议的通信模型. 从 C 的高度,记为 $height(C)$,表示 C 中的串$\langle s, i\rangle$的最大的 i 的值.

2.2　攻击者的描述

攻击者的知识可以包括两个部分,一个是初始知识集 IK (Initial Knowledge),一个是攻击者根据 IK 和截获的消息动态生成的消息. 在基于口令的密钥协议中,我们将攻击者可能猜测的信息集合记为 G_P, K_p 表示攻击者知道的所有密钥,对于基于口令的 DH 密钥交换协议,攻击者可以生成的 DH 值,使用 D_p 来表示. 用 M_p 表示攻击者其他已知(截获)的信息. 这样有 $IK = K_P \cup G_P \cup D_P \cup M_P$.

攻击者利用消息项进行攻击,产生攻击者的迹,其定义如下:

定义 4　攻击者的串包括:

M. 产生原子消息:$\langle + t\rangle$, $t \in T$

F. 接收消息:$\langle - g\rangle$

T. 接收并多次发送消息:$\langle - g, + g, + g\rangle$

C. 级联消息:$\langle - g, - h, + gh\rangle$

S. 拆分消息:$\langle - gh, + g, + h\rangle$

K. 发送密钥:$\langle + K\rangle$, $K \in K_p$

G. 发送口令:$\langle + P\rangle$, $P \in G_p$

E. 加密消息:$\langle - K, - h, + \{h\}_K\rangle$, $K \in K_p$

D. 解密消息:$\langle - \{h\}_K, - K^{-1}, + h\rangle$, $K \in K_p$

V. 发送值:$\langle + b\rangle$, $b \in V_p \subseteq V$

f. 计算单向函数:$\langle - x_1, - x_2, \cdots, - x_n, + f(x_1, x_2, \cdots, x_n)\rangle$, f 表示单向计算.

其中 G 事件表示攻击者猜测口令的操作;V 事件表示攻击者可以产生用于计算单向函数的值. V 是 A 的一个子集,函数满足 $f: V^n \to V$ 表示单向运算. 如果 f 是 DH 运算,则 V 为 D, n 为 2,如果 f 是 HASH 运算,则 V 为 A. 这里 f 函数类似于文献[18]中的诚实函数. 如果攻击者可以对$(x_1, x_2, \cdots, x_n)$计算单向函数的值,即 $f(x_1, x_2, \cdots, x_n) \in IK$,则一定已经有 $x_1, x_2, \cdots, x_n \in IK$.

公理 1　对于定义 1 中的集合 E 和 C,假设 $V \cap C = V \cap E = \phi$.

(Σ, P)来表示存在攻击者的串空间,其中 $P \subseteq \Sigma$表示对所有的 $p \in P$, tr(p) 是一个迹,也就是串主体的一个动作序列. 攻击者可以通过猜测的值来构造新的项,并试图验证此次猜测,因此我们定义一个新的关系 ——匹配关系来描述攻击者进行猜测时进行的验证操作.

定义 5　M 是 N 可匹配的,记为 $M \overset{\pm}{\rightrightarrows} N$,如果有:

(1) M, N 为同一类原子项;

(2) $N = N' \hat{} N''$,且 $M \overset{\pm}{\rightrightarrows} N'$ 或者 $M \overset{\pm}{\rightrightarrows} N''$;

(3) $M = \{M'\}_k$, $N = \{N'\}_k$,且 $M' \overset{\pm}{\rightrightarrows} N'$

(4) $M = f(M'_1, \cdots, M'_n)$, $N = f(N'_1, \cdots, N'_n)$,存在 i 使得 $M'_i \overset{\pm}{\rightrightarrows} N'_i$,且 $M'_j = N'_j$,其中 $1 \leq i, j \leq n$ 且 $j \neq i$.

定义 6　如果 $k \subseteq$K,I 是 A 的一个子集,对于所有 $h \in$I, $g_1, g_2, \cdots, g_n \in$A,且 $K \in k$,有:

(1) $hg_1, g_1 h \in$I

(2) $\{h\}_K \in$I

(3) 如果 $h \in V, g_2, \cdots, g_n \in V$,则 $f(h, g_2, \cdots, g_n) \in I$

则称 I 是 A 的一个 k 理想,记为 $I_k[h]$. 如果 $S \subseteq A$,则 $I_k[S]$定义为包括 S 的最小 k 理想.

定义 7 集合 $I \subseteq A$ 对于一个丛 C 是诚实的,当且仅当只要 I 的入口点是一个攻击者节点 p,则 p 是一个 M 节点、K 节点或者 V 节点.

定理 1 假设 C 是 A 上的一个丛; $S \subseteq T \cup K \cup V$, $k \subseteq K$, $K \subseteq S \cup k^{-1}$, f 是 C 上的一个单向函数,如果有 $y = f(x_1, x_2, \cdots, x_n)$产生于 C 中的一个攻击者结点,则 $y \in I_k[S]$可推出至少存在一个 $x_i (1 \leq i \leq n)$, $x_i \in I_k[S]$,则 $I_k[S]$是诚实的.

证明 假设 m 是一个攻击者节点,并且是 I 的入口点,证明该节点只能是 M 节点、K 节点或者 V 节点. 文献[16]证明了除 V 和 f 的攻击者迹,这里只分析假设 m 源于 f 的情况,则显然〈f, $n+1$〉为 $I_k[S]$的入口点. 但是根据条件, $y \in I_k[S]$可推出至少存在一个 $x_i (1 \leq i \leq n)$, $x_i \in I_k[S]$,不妨设 $i = h$,也就是说如果〈f, $n+1$〉$\in I_k[S]$,则已经有〈f, h〉$\in I_k[S]$,显然〈$f, n+1$〉不是 $I_k[S]$的入口点,即 y 不是 $I_k[S]$的入口点.

3 实例分析

我们对文献[1]中提出的四步的 DH-EKE 进行了简化,给出一个只需三步的两方协议,简称为 SEKE:

A → B: $A, \{g^x\}_{pwd}$

B → A: $B, \{g^y\}_{pwd}, H_1(A, B, g^{xy}, g^x)$

A → B: $H_2(B, A, g^{xy}, g^y)$

其中 pwd 是双方共享的口令, H_1、H_2 和 H_3 都是安全的 HASH 函数,在协议中利用 H_1 和 H_2 进行消息的认证,如果验证都通过,A 和 B 使用 H_3 计算 $K = H_3(g^{xy})$,作为双方的会话密钥.

对于这个协议的分析包括:口令的秘密性,会话密钥的秘密性,以及通信双方的认证性. 如前所述,口令的秘密性需要保证口令不会被猜测者猜测成功. 我们首先定义如下两个不相交的串空间:

定义 8 令 $\sum$为一个串空间,则有

1. Init$[pwd, g^{xy}, g^x, g^y, A, B]$是发起者的串,其迹为:

〈$+A\{g^x\}pwd, -B\{g^y\}_{pwd}H_1(A, B, g^{xy}, g^x), +H_2(B, A, g^{xy}, g^y)$〉, $\sum_{init}$是初始者串集合;

2. Resp$[pwd, g^{xy}, g^x, g^y, A, B]$是响应者的串,其迹为:

〈$-A\{g^x\}_{pwd}, +B\{g^y\}_{pwd}H_1(A, B, g^{xy}, g^x), -H_2(B, A, g^{xy}, g^y)$〉, $\sum_{resp}$是响应者串的集合;

则 SEKE 协议的串空间记为 $(\sum, P)_{SEKE} = \sum_{init} \cup \sum_{resp} \cup P$,其中 P 是攻击者的串集合.

在猜测攻击中,攻击者需要利用猜测构造相应的消息. 在两方通信协议中,攻击者利用与某一合法方交换,以获取尽可能多的验证信息来验证猜测是否成功,但这种在线攻击很容易被检测,所以在两方协议中不考虑这种情况,只考虑离线攻击. 假设能被猜测的只是口令,并假设 DH 计算所选的群是安全的,DH 值 g^x 中随机选取的值 x 是满足安全长度的随机变量,攻击者不能使用猜测攻击进行猜测.

如果协议可以抵抗猜测攻击,即证明通过猜测 pwd 无法找到可用于验证的项,也就是说如果协议中存在可匹配的项,则猜测的项至少有两个. 显然在 SEKE 协议中,可用来验证的匹配项集合是:$\{A, \{g^x\}_{pwd}, B, \{g^y\}_{pwd}, H_1(A, B, g^{xy}, g^x), H_2(B, A, g^{xy}, g^y)\}$,定义为 VI. 令 O 表示攻击者根据猜测以及 IK 构造的集合.

定理 2 (口令的秘密性):假设 C 是 $(\sum, P)_{SEKE}$上的丛, g^x, g^y 唯一源于 C 上的正常串, $g^x \neq g^y$, $pwd \notin K_p$, H_1、H_2 是 HASH 函数,且 DH 问题是难解的,如果存在 $n \in O$, $m \in VI$, $n \neq m$,则 $|G_p| > 1$.

证明 攻击者必须根据 VI 中的集合来构造猜测项,以便实现验证. 根据项产生的因果关系,不妨从串的最高节点开始分析. 显然存在 $s \in \sum_{init}$,使得 $unterm(\langle s, 1\rangle) = (A, \{g^x\}_{pwd})$, $unterm(\langle s, 2\rangle) = (B, \{g^y\}_{pwd}, H_1(A, B, g^{xy}, g^x))$, $unterm(\langle s, 3\rangle) = H_2(B, A, g^{xy}, g^y)$. 假设 $unterm(n) = H^2(B', A', g^{xy'}, g^{y'})$,如果 $unterm(n) \neq unterm(\langle s, 3\rangle)$, H_2 是单向函数,则攻击者需要知道 g^{xy}, g^y,则 $G_p = \{g^{xy}, g^y\}$. 因为 g^y 唯一源于 C 上的正常串,存在 $r \in \sum_{resp}$, g^y 源于节点$(r, 2)$,形为$\{g^y\}_{pwd}$. 攻击者猜测 pwd,获取相应的 $g^{y'}$,这时 $G_p = \{g^{xy}, pwd\}$. 攻击者还必须知道 x 才能计算 g^{xy},或者求解 DH 问题,根据假设求解 DH 问题是困难的,所以攻击者必须猜测 x. 而 g^x 唯一源于 C 上的正常串,形式为$\{g^x\}_{pwd}$,由于 $pwd \in G_p$,可以得到 $g^{x'}$,但是对于 g^x, x 从不单独出现且 DH 问题是难解的,所以攻击者只能猜测 x',这时 $G_p = \{x, pwd\}$. 同样的如果将 $H_1(A, B, g^{xy}, g^x)$作为验证项, $G_p = \{y, pwd\}$. 如果将$\{g^x\}_{pwd}$和$\{g^y\}_{pwd}$作为验证项,分别得到 $G_p = \{g^x, pwd\}$和 $G_p = \{g^y, pwd\}$. 对于所有的 $m \in VI$,都有$|G_p| > 1$. 定理得证.

在对这个定理的证明中我们很容易得出,如果攻击者不能成功猜测口令,也就是他无法对 B 冒充 A 的身份和 A 通信,即提供了 A 对 B 的认证,同理,也可以保证 B 对 A 的认证.

命题 2 如果对于 $k \in Kr$, $Kr \cap K_p = \varnothing$,如果 k 不是 C 中任何结点的项,则对于任意的 $m \in A$,$\{m\}_k$ 一定产生于正常结点.

证明:假设$\{m\}_k$ 产生于一个攻击者结点,则显然唯一可能源于的攻击者串 p 是类型为 E 的攻击者串〈$-K, -h, +\{h\}_K$〉,假设$\{m\}_k$ 产生于结点〈$p, 3$〉,则如果$\{m\}_k = \{h\}_K$,则有 $k \subset \langle p, 1\rangle$,与条件矛盾,所以由$\{m\}_k \subset \{h\}_K$ 推出$\{m\}_k \subset h$,与假设矛盾,所以$\{m\}_k$ 一定产生于正常结点.

定理 3 假设 C 是 $(\sum, P)$ 上的丛,A ≠B, g^y 唯一源于 C 上的正常串, $g^x \neq g^y$, $pwd \notin K_p$,且 DH 问题是难解的, H_1 和 H_2 是单向 HASH 函数. 如果 $r \in$Resp$[pwd, g^{xy}, g^x, g^y, A, B]$的高度为 3,则存在 $s \in$Init$[pwd, g^{xy}, g^x, g^y, A, B]$的高度为 3.

证明 根据假设,令 $tr(r) = \langle(A\{g^x\}_{pwd}, +B\{g^y\}_{pwd}H_1(A, B, g^{xy}, g^x), -H_2(B, A, g^{xy}, g^y)\rangle$,因为 g^y 唯一源于 C 上的正常串,由假设知 $g^y \subset \langle r, 2\rangle$,因为 $g^x \neq g^y$,所以 g^y 源于〈$r, 2$〉. 下面证明 $H_2(B, A, g^{xy}, g^y)$源于正常节点. 对于集合 $S = \{n \in C: H_2(B, A, g^{xy}, g^y) \subset term(n)\}$. 显然节点$(r, 3) \in S$,所以 S 不为空,这样 S 至少有一个 ≤最小元素 n_1,其符号为

正.显然 n_1 不可能源于 M,F,T,C,S,K,G,E,D 类型的攻击者串.则考虑 n_1 可能位于的攻击者串为 f:〈- B, - A, - g^{xy}, - g^{y}, + $H_2(B, A, g^{xy}, g^{y})$〉.因为 g^{y} 唯一源于〈r,2〉,形为 $\{g^{y}\}_{pwd}$,并且 $pwd \notin K_p$,由命题 2 知攻击者无法获取 g^{y},n_1 只能是正常节点.因为 $A \neq B$,存在 $s \in \mathrm{Init}[pwd, g^{xy}, g^{x}, g^{y}, A, B]$,$n_1$ 是$(s,3)$,也就是说存在 $s \in \sum_{init}$的高度为 3.

定理 4　假设 C 是$(\sum, P)$上的丛,$A \neq B$,g^{x} 唯一产生于 C 上的正常串,$g^{x} \neq g^{y}$,$pwd \notin K_p$,且 DH 问题是难解的,H_1 和 H_2 是单向 HASH 函数,如果 $s \in \mathrm{Init}[pwd, g^{xy}, g^{x}, g^{y}, A, B]$的高度为 3,则存在 $r \in \mathrm{Resp}[pwd, g^{xy}, g^{x}, g^{y}, A, B]$的高度为 2.

证明　根据假设,令 $tr(s) = \langle + A\{g^{x}\}_{pwd}, - B\{g^{y}\}_{pwd} H_1(A, B, g^{xy}, g^{x}), + H_2(B, A, g^{xy}, g^{y})\rangle$.需要证明结点〈$s$,2〉产生于一个响应者串.假设〈$s$,2〉产生于攻击者串,根据命题 2,因为 $pwd \notin K_p$,所以$\{g^{y}\}_{pwd}$一定产生于正常结点;因为 g^{x} 唯一产生于 C 上的正常串,显然 g^{x} 产生于结点〈s,1〉,因为 $pwd \notin K_p$,所以攻击者不能获取 g^{x},因为 DH 问题是难解的,攻击者也不能获取 g^{xy},对于单向函数 H_1,$H_1(A, B, g^{xy}, g^{x})$产生于正常结点.因为 A ≠B,存在 $r \in \mathrm{Init}[pwd, g^{xy}, g^{x}, g^{y}, A, B]$,$\{g^{y}\}_{pwd}$和 $H_1(A, B, g^{xy}, g^{x})$都产生于〈r,2〉,也即$(B\{g^{y}\}_{pwd} H_1(A, B, g^{xy}, g^{x}))$产生于〈$r$,2〉,也就是说存在 $s \in \sum_{resp}$的高度为 2.

定义 $S = \{g^{x}, g^{y}, g^{xy}, pwd\}$,$k = \mathrm{K} \setminus \{pwd, g^{xy}\}$,显然满足定理的条件 $K \subseteq S \cup k^{-1}$.因为我们假设了 g^{x}、g^{y} 唯一源于 C 上的正常串,所以满足定理 1 的条件:如果 g^{xy}源于 C 中的一个攻击者节点,则如果 $g^{xy} \in \mathrm{I}_k[S]$,则可以推出 g^{x} 和 g^{y} 中至少有一个 $\in \mathrm{I}_k[S]$,因为 $g^{x}(g^{y})$的形式只有$(g^{x})_{pwd}((g^{y})_{pwd})$,$pwd \notin K_p$. $\mathrm{I}_k[S]$是一个诚实的理想,从而保证了 SEKE 协议的秘密性.因为会话密钥 $K = H_3(g^{xy})$,H_3 是单向 HASH 函数,只要 g^{xy}不会泄漏,K就不会泄漏.

在分析认证性的时候,以定理 3 为例,攻击者不知道 g^{y},所以 $H_2(B, A, g^{xy}, g^{y})$源于一个发起者串,其实攻击者即使知道 g^{y},如果不知道 g^{xy},攻击者一样不能生成 $H_2(B, A, g^{xy}, g^{y})$,证明仍然成立.因此第二步中的加密可以去掉,一样不能被猜测,g^{xy}不会源于攻击者节点,同样可以保证认证性.同样的,定理 4 也可以得到相同的结论.

4　基于口令的三方密钥交换协议

在两方通信系统中,每两个用户都需要共享一个口令,对于有 n 个用户的系统来说,每个用户需要用于 n 个口令,整个系统需要 $O(n^2)$ 个口令.基于这样的考虑,Steiner 等人提出了三方 EKE 协议[4],其中所有的用户只需要和一个可信方 S 共享一个口令,通过 S 的协助,用户 A 和 B 完成相互认证和会话密钥的交换[2~4,9,10].

与两方协议不同的是,三方协议中的攻击者可能是一个合法的用户,试图猜测其他合法用户和 S 共享的密钥.文献[5]将对这类协议的口令猜测攻击分为三类:可检测的在线口令猜测攻击;不可检测的在线口令猜测攻击;离线口令猜测攻击:攻击者离线的猜测口令和进行验证猜测.不可检测的在线口令猜测攻击和可检测的在线口令猜测攻击类似,不同的是服务器 S 无法区分诚实用户的响应和恶意用户的响应.一个安全的基于口令认证的三方密钥交换协议必须能够抵抗不可检测的在线口令猜测攻击和离线猜测攻击.在对这类协议分析时,如果对于串 $s \in \sum_{init}$或者 $s \in \sum_{resp}$,存在一个攻击者串 p,满足 $unterm(s, height(s)) = unterm(p, height(p))$,且存在 $n \in \mathrm{O}$,$m \in \mathrm{VI}$,$n \stackrel{\pm}{\neq} m$ 时 $G_p = \{pwd\}$,则该协议存在离线猜测攻击;如果对于 $s_1 \in \sum_{init}$和 $s_2 \in \sum_{server}$或者对于 $s_1 \in \sum_{resp}$和 $s_2 \in \sum_{server}$,存在攻击者串 p,满足 $unterm(s_1, height(s_1)) = unterm(p, height(p))$,或者 $unterm(s_2, height(s_2)) = unterm(p, height(p))$,且 $height(p) = height(s_1) + height(s_2)$.如果这里其中 s_2 的高度是满的,也就是完整运行了一个实例,且存在 $n \in \mathrm{O}$,$m \in \mathrm{VI}$,$n \stackrel{\pm}{\neq} m$ 时 $G_p = \{pwd\}$,则存在不可检测的在线攻击,否则为可检测的在线攻击.

在三方协议中如果 A 和 S、B 和 S 只共享口令,这样 A 和 S 以及 B 和 S 在进行密钥协商时,无法进行身份认证,所以这就意味着当密钥协商完成,A 和 B 需要进行密钥确认的步骤以实现对身份的认证,否则双方无法确保正确完成了协议的运行.显然,A、B 和 S 至少需要三步完成无认证的密钥协商,即 S 利用分别和 A、B 共享的口令为双方交换信息,当 A 和 B 获取相应的信息后,计算出会话密钥,再至少进行两步以进行互相的密钥确认.这样我们可以得到以下协议的一般形式(简称 SPK3):

$A \rightarrow B: f_1(p_a, A, B, R_a), r_a$

$B \rightarrow S: f_1(p_a, A, B, R_a), f_2(p_b, A, B, R_b)$

$S \rightarrow B: g_1(p_a, A, B, R_b, N), g_2(p_b, A, B, R_a, N)$

$B \rightarrow A: g_1(p_a, A, B, R_b, N), h_1(K, r_a, A, B), r_b$

$A \rightarrow B: h_2(K, r_b, A, B)$

由于口令不能泄漏,所以 f_1 操作表示利用 p_a 进行信息的秘密传送,如加密或者单向运算,r_a 是用于后续验证的信息,f_2 操作和 f_1 相同,R_a 和 R_b 用来协商密钥. g_2 是服务器利用口令 p_a 和 B 提交的协商密钥的信息 R_b 传递给 A,类似的,g_1 是服务器利用口令 p_b 和 A 提交的协商密钥的信息 R_a 传递给 B.后续两步是 A 和 B 分别利用 h_1 和 h_2 进行密钥确认.这里假设 f_1、f_2、g_1、g_2、h_1、h_2 运算的操作是公开的.密钥 K 由两种方式产生:或者 $K = f(R_a, R_b, N)$,即由 A 和 B 协商生成,或者 $K = f(N)$,由服务器分配,这时 R_a 和 R_b 分别是 A 和 B 产生的秘密信息,可以用来传递密钥,因为显然直接用口令来传递密钥 K 是不安全的.在第一种方式下,因为 S 和 A、B 只共享一个口令,S 只有通过口令来获取 R_a 和 R_b,同等的,对于攻击者 B 一样可以通过猜测一个口令,获取 R'_a,并设定 $R_b = R'_a$,则在第三步,B 获取服务器发回的 $g_1(p_a, A, R_a, N)$,从而得到可以计算 K 的 $f'(R_a, N)$,则 B 可以根据猜测的 p_a,$f'(R_a, N)$ 构造 $g_1(p_a, A, B, R'_a, N)$,比较 $g_1(p_a, A, B, R_a, N)$ 即可以验证猜测.在第二种方式下,B 仍然猜测 p_a,选择 R_a,产生 $f_1(p'_a, A, B, R_a)$,收到 S 发回的 $g_1(p_a, A, B, R'_a, N)$,通过 R'_a 获取 p_a, A, B, R'_a, N,验证是否格式匹配.在这两种情况下,攻击者 B 的 $G_p = \{p_a\}$,并且满足 $unterm(\langle Sserv, height(Sserv)\rangle) \stackrel{\pm}{\neq} unterm(\langle p. height(p)\rangle)$,所以存在在线猜测攻击.

如果协议的参与方 A 和 B 与服务器 S 只共享一个弱的口令,则若要保证 A 或者 B 的口令在三方密钥交换协议中不被泄漏,则三方交互的步骤一定大于 5 步,否则口令不能抵抗猜测攻击.

5 总结

我们使用 SS 模型对这类协议的安全性进行了形式化分析,分析了基于口令的密钥交换协议的安全性,包括口令的秘密性,认证性和交换的密钥的秘密性.根据这个分析方法,证明了 SEKE 协议的安全性,并指出了 SPK3 协议存在的不可猜测的在线攻击,并给出了一个一般性结论:如果用户只拥有最基本的口令,是不可能在 5 次交换中完成安全密钥交换的.根据分析基于口令认证的密钥交换协议的安全性的方法,我们可以得到设计这类协议的一些原则:口令和最后共享的密钥不能发生直接的关系,口令存在的消息必须存在一定形式的混淆方法,以避免给攻击者提供验证信息.

参考文献:

[1] S M Bellovin, M Merrit. Encrypted key exchange: password-based protocols secure against dictionary attacks[A]. Proceedings of the IEEE Symposium on Research in Security and Privacy[C]. Oakland, CA, IEEE Computer Society, 1992. 72 - 84.

[2] L Gong, T Mark, A Lomas, R M Needham, J H Saltzer. Protecting poorly chosen secrets from guessing attacks[J]. IEEE Journal on Selected Areas in Communications, 1993, 11(5): 648 - 656.

[3] L Gong. Optimal authentication protocols resistant to password guessing attacks[A]. Proceedings of 8th IEEE Computer Security Foundations Workshop[C]. 1995. 24 - 29.

[4] M Steiner, G Tsudik, M Waidner. Refinement and extension of encrypted key exchange[J]. ACM Operating Systems Review, 1995, 29(3): 24 - 29.

[5] Y Ding, P Horster. Undetectable on-line password guessing attacks[J]. ACM Operating Systems Reviews, 1995, 29(4): 77 - 86.

[6] Chun-Li Lin, Hung-Min Sun, Tzonelih Hwang. Three-party encrypted key exchange: attacks and a solution[J]. ACM Operating Systems Review, 2000, 34(4): 12 - 20.

[7] Chun-Li Lin, Hung-Min Sun, Michael Steiner and Tzonelih Hwang. Three-party encrypted key exchange without server public-keys[J]. IEEE Communications Letters, 2001, 5(12): 497 - 499.

[8] D P Jablon. Strong password-only authenticated key exchange[J]. SIGCOMM Computer Communication Review, 1996, 26(5): 5 - 26.

[9] S Lucks. Open key exchange: how to defeat dictionary attacks without encrypting public keys[A]. Proceedings of the Workshop on Security Protocols[C]. Ecole Normale Superieure, 1997.

[10] T Wu. A real world analysis of Kerberos password security[A]. In NDSS '99.

[11] S Halevi, H Krawczyk. Public-key cryptography and password protocols[A]. ACM Transaction on Information and System Security[C]. New York, USA, ACM Press, 1999, 2(3): 230 - 268.

[12] M Bellare, D Pointcheval, P Rogaway. Authenticated key exchange secure against Dictionary Attacks[A]. Advances in Cryptology-Eurocrypt '00[C]. LNCS 1807, B. Preneel ed., Springer-Verlag, 2000.

[13] V Boyko, P Mackenzie and S Patel. Provably secure password authenticated key exchange using diffie hellman[A]. Proceedings of Advances in Cryptology-Eurocrypt 2000[C]. LNCS 1807, 2000. 156 - 171.

[14] G Lowe. Analysing protocols subject to guessing attacks[A]. Workshop on Issues in the Theory of Security (WITS '02)[C]. January 2002.

[15] F J Thayer Fabrega, J C Herzog, J D Guttman. Strand space: why is a security protocol correct[A]. IEEE Computer Symposium on Security and Privacy[C]. 1998.

[16] F J Thayer Fabrega, J C Herzog, J D Guttman. Strand space: proving security protocols correct[J]. Journal of Computer Security, 1999, 7(2, 3): 191 - 230.

[17] J C Herzog. The Diffie-Hellman key-agreement scheme in the strand space model[A]. Proceedings of 16th IEEE Computer Security Foundations Workshop[C]. IEEE CS Press, June 2003.

[18] Alfred P Maneki. Honest functions and their application to the analysis of cryptographic protocols[A]. Proceedings of the 1999 IEEE Computer Security Foundations Workshop[C]. IEEE Computer Society, Washington, DC, USA, 1999. 83 - 92.

作者简介:

李 莉 女,1976 年生于安徽芜湖,现为武汉大学博士生,主要研究领域:网络安全,密码协议分析. E-mail: ll_36@163.com.

薛 锐 男,1963 年出生,博士,研究员,主要研究领域:信息安全,密码协议分析.

张焕国 男,1946 年出生于河北,教授,博士生导师,主要研究领域:密码学,信息安全理论与技术.

冯登国 男,1965 年出生于陕西靖边,博士,博士生导师,研究员,主要研究领域:信息与网络安全.

王丽娜 女,1964 年出生于辽宁营口,博士,教授,主要研究领域:密码学,信息安全理论与技术.