doi: 10.7690/bgzdh.2014.03.012

基于口令的三方密钥交换协议的分析与研究

刘保菊[1]，刘家磊[2]
（1. 平顶山学院国际教育交流学院，河南 平顶山 467000；
2. 安阳工学院计算机科学与信息工程学院，河南 安阳 455000）

摘要：针对计算机中较短易记的口令容易受到“口令猜测”攻击的问题，提出一种基于口令的三方密钥交换协议。在分析了已有的三方密钥交换协议不足的基础上，进一步完善 DML-3PAKE 协议，并从协议效率和安全性 2 方面进行分析。分析结果表明：新协议虽然在执行效率方面增加了计算开销，但在防御在线字典攻击、离线字典攻击、中间人攻击等方面与之前协议相比更为安全。

关键词：口令；网络安全；协议
中图分类号：TP393.08　　**文献标志码：**A

Analysis and Research on Three-Party Key Exchange Protocol Based on Password

Liu Baoju[1], Liu Jialei[2]
(1. *College of International Education & Exchange*, *Pingdingshan University*, *Pingdingshan*, 467000, *China*;
2. *College of Computer Science & Information Technology*, *Anyang Institute of Technology*, *Anyang* 455000, *China*)

Abstract: The password which is short and easy to remember is easily be attacked by “password guessing”, put forwards three-party exchange protocol based on password. Based on analysis of lack of three-party exchange protocol, further improve of DML-3PAKE protocol, then analyze protocol efficiency and security. The analysis result shows that although new protocol increases calculation cost in executing probability, it is safer in defense of online dictionary attack, offline dictionary attack, and inter-mediator attack.

Keywords: password; network security; protocol

0　引言

基于口令的安全协议可以应用在多种场合下，尤其是在一些缺乏相关硬件设备来储存一些随机长期密钥的情况下。安全协议中口令的选取由用户决定，口令实质上是一个较短的易记忆的长期对称密钥。人们选择的口令一般都是比较容易记忆的，所以这些口令又往往容易受到“口令猜测”的攻击，任何一个攻击者攻击的目的就是为了得到用户口令，并且能够验证口令的正确性。口令认证密钥交换（password key exchange，PAKE）协议能够使用户通过一个安全性不够高的信道上相对安全的生成共享的高熵口令，而用户也不必具有存储长对称密钥和相关公钥的硬件设施，由于使用的便利性，所以成为众多密码学研究者的研究重点[1]。

1　常见的攻击

具有较高可扩展性的 3PAKE 协议也可能遭受各类攻击，主要包括 3 类[2-3]：可察觉在线攻击、不可察觉在线攻击、离线攻击。在以上 3 种攻击方法中，不可察觉在线攻击是对 3PAKE 协议最严重的攻击方式。而各种攻击方法之所以能成功主要因为在协议中把服务器当作一个用来加密和解密的工具，无法区分合法的消息和伪造的消息。为了有效应对各种攻击，就需要设计安全有效的协议。而安全协议设计的困难性主要在于[4-5]：1) 安全目标本身的微妙性；2) 攻击者行为的多变性；3) 协议运行时不能泄漏关于口令的任何信息；4) 协议运行时不能泄漏关于口令的任何信息。实际过程中，处于各种安全原因的考虑，使得协议的设计和分析工作极具挑战性。邓淼磊等[6]在 Lowe[7]所提出的基于口令的安全协议（称之为 LMB 协议）的基础上进行了改进，以后简记为 DML-3PAKE，又对此协议进行了改进。下面先回顾一下邓淼磊等人改进后的协议。

2　DML-3PAKE

2.1　LMB协议

$$(1)\ A \rightarrow B : \{k_{AB}\}_{pw(A,B)}$$
$$(2)\ B \rightarrow A : \{\{k\}_{k_{AB}}\}_{pw(A,B)}$$
$$(3)\ A \rightarrow B : \{n_A\}_k$$
$$(4)\ B \rightarrow A : \{n_A \| n_B\}_k$$
$$(5)\ A \rightarrow B : \{n_B\}_k$$

收稿日期：2013-10-06；**修回日期：**2013-11-02
作者简介：刘保菊（1980—），女，河南人，硕士，讲师，从事网络安全研究。

这里 k_{AB} 是协议生成的 A 和 B 共享的对称密钥，$pw(A,B)$ 是 A 和 B 事先共享的口令，k 是秘密值(也用作密钥)，n_A 和 n_B 分别是 A 和 B 生成的临时值。

在该协议里，攻击者可以猜测 $pw(A,B)$ 的一个值，然后使用猜测的值解密消息(1)得到 k_{AB}。它再使用猜测的值解密消息(2)得到 $\{k\}_{k_{AB}}$，并使用前面得到的 k_{AB} 解密 $\{k\}_{k_{AB}}$，计算出 k。这样它就可以使用这个 k 值解密消息(3)和(4)，检查得到的 n_A 和 $[n_A \| n_B]_1$ 是否匹配，这里 $[n_A \| n_B]_1$ 是连接项 $n_A \| n_B$ 中的第一项，以验证猜测是否正确。当然，它也可以解密消息(4)和(5)，然后验证 n_B 和 $[n_A \| n_B]_2$ 是否匹配，所以这个协议是不安全的。

2.2　DML-3PAKE 对 LMB 协议的改进

接收方在接收到临时值 n_A 或 n_B 后，返回的是 n_A 或 n_B 的散列值。DML-3PAKE 修改后的协议如下：

$(1) A \to B : \{k_{AB}\}_{pw(A,B)}$

$(2) B \to A : \{\{k\}_{k_{AB}}\}_{pw(A,B)}$

$(3) A \to B : \{n_A\}_k$

$(4) B \to A : \{h_{n_A} \| n_B\}_k$

$(5) A \to B : \{h_{n_B}\}_k$

设 $pw(A,B)$ 的二进制长度为 L，一般来说口令的长度较小，攻击者攻击时总能通过随机选取一个猜测的口令值来假冒合法用户运行协议，其攻击成功的概率大于 $1/2^L$。DML-3PAKE 协议中使用的散列函数需要满足以下条件：$L<|h(n)|<<|n|$，这里 $|h(n)|$ 和 $|n|$ 分别表示 $h(n)$ 和 n 的二进制长度。例如假设 L 为 48 比特，而 n 为固定的 2 048 比特，$h(n)$ 为固定的 256 比特，亦即将有 $2^{1\,792}$ 个 n 值与 1 个 $h(n)$ 值相对应[7]。

DML-3PAKE 协议能否抵御口令猜测攻击，证明过程如下：

命题 1　设 C 是改进的 LMB 协议的丛，那么 C 中的口令猜测攻击是不可行的。

证明：这里并没有用 $pw(A,B)$ 而是用猜测值 g 替代 $pw(A,B)$，鉴于 $pw(A,B)$ 的弱密钥性。首先，攻击者可以由 $\{k_{AB}\}_{pw(A,B)}$ 得到 k_{AB}，因为 k_{AB} 使用口令 $pw(A,B)$ 加密的，并且 $k_{AB} \subset \{k_{AB}\}_{pw(A,B)}$，类似的可以得到：

$\{k\}_{k_{AB}}$，因为 $\{k\}_{k_{AB}} \subset \{\{k\}_{AB}\}_{pw(A,B)}$；

k，因为 $k \subset \{k\}_{k_{AB}}$，并且攻击者由 $\{k_{AB}\}_{pw(A,B)}$ 得到 k_{AB}；

n_A，因为 $n_A \subset \{n_A\}_k$，因为攻击者得到 k；

$h(n_A) \| n_B$，因为 $h(n_A) \| n_B \subset \{h(n_A) \| n_B\}_k$；

$h(n_B)$，因为 $h(n_B) \subset \{h(n_B)\}_k$

因此，相应 $pw(A,B)$：k_{AB}、$\{k\}_{k_{AB}}$、k、n_A、$h(n_A) \| n_B$、$h(n_B)$ 从 C 中的验证项是：$\{n_A\}_k$、$h(n_A) \| n_B\}_k$、$h(n_B)_k$。考察所有可以使用上述项构造的 G 串。

1) 因为攻击者得到的项中不包含具有 v、$\{v\}_p$. 形式的项，G_1 串不能被构造。k、$\{k\}_{k_{AB}}$ 不能用来构造 G_1，因为攻击者不知道真实的 k 值，所以即使用 k_{AB} 解密 $\{k\}_{k_{AB}}$ 得到 k，它也无法进行验证。

2) 显然，G_3 和 G_4 串也不能被构造。

3) 攻击者可以构造 G_2 串：$G_2=\langle -\{n_A\}_k, -\{h(n_A) \| n_B\}_k, -k, +[h(n_A) \| n_B], +n_A \rangle$。然后攻击者验证 $n_A \approx [h(n_A) \| n_B]_1$ 是否成立(即验证 n_A 和 $h(n_A)$ 中的 n_A 是相同的项)。如果攻击者实施的口令猜测攻击可行，那么就有 $\Pr(n_A \approx [h(n_A) \| n_B]_1 \mid g = pw(A,B)) \geqslant \varepsilon_1$ 和 $\Pr(g = pw(A,B) \mid n_A \approx [h(n_A) \| n_B]_1) \geqslant \varepsilon_2$，但是这里 $n_A \approx [h(n_A) \| n_B]_1$ 不一定成立，并且任一散列值 $h(n_A)$，都存在 n_A，使得它们具有相同的散列值。特别是当 $\varepsilon_1 = \varepsilon_2 = 1$ 时，$\Pr(g = pw(A,B))$ 和 $\Pr(n_A \approx [h(n_A) \| n_B]_1)$ 相同，都等于一个非常小的值 $1/n$，这里 n 是满足条件的 n_A 的个数。所以使用 G_2 串的猜测攻击是不可行的。

最终 C 中的攻击无法实施。

2.3　对DML-3PAKE协议的分析

文献[6]在形式化模型下证明了 DML-3PAKE 协议可以抵御口令猜测攻击。但文中指出改进后的 DML-3PAKE 给出的改进协议仍旧是不安全的，还是难于抵抗不可察觉在线字典攻击。设外部攻击者 E 想要猜测用户 A、B 的口令，重复执行下述步骤：

1) 首先攻击者 E 猜测用户 A、B 的口令对为 $p(w_A^*, w_B^*)$，然后选择 2 个随机值 $x, y \in z_p^*$，计算 $x^* = g^x . m^{pw_A^*}$，$y^* = g^y . n^{pw_B^*}$ 并伪装成用户 B 发送消息 $\langle \mathrm{id_A}, x^*, \mathrm{id_B}, y^* \rangle$ 给服务器 S。

2) 服务器 S 在收到消息后，判断认为用户 A 和用户 B 正在进行密钥交换，从而它利用口令 pw_A, pw_B 计算 $x = x^* / m^{pw_A}, y = y^* / n^{pw_B}$。此时服务器 S 选择随机值 $z \in z_p^*$，计算 $x' = (x)^z . h_1(id_A, id_B, id_s, x)^{pw_A}$，$y' = (x)^z . h_1(\mathrm{id_B}, \mathrm{id_A}, \mathrm{id_s}, y)^{pw_B}$ 并发送消息 (x', y') 给用户 B。

3) 攻击者拦截上述消息 (x', y')，利用第 1 步中猜测的口令对 (pw_A^*, pw_B^*) 计算 $\bar{x} = x' / h1(\mathrm{id_A}, \mathrm{id_B}, \mathrm{id_Z}, g^x)^{pw_A^*}$，

$\bar{y}=y'/h1(\mathrm{id_B},\mathrm{id_A},\mathrm{id_Z},g^y)^{pw_B^*}$，进一步验证 $\bar{x}^x=\bar{y}^y$ 是否成立，如果成立，攻击者 E 成功地猜对用户 A、B 的口令对为 $p(w_A^*,w_B^*)$；否则，攻击者 E 成功地排除口令对 $p(w_A^*,w_B^*)$，然后选择另外一个口令对重复前述步骤。在上述攻击过程中，攻击者 E 通过数次拦截用户 A，B 的口令并伪造消息欺骗服务器 S，而服务器 S 也不会察觉到用户 E 的多次不成功的猜测，所以攻击者 E 可以成功地实施不可察觉在线字典攻击。

3 改进的 3PAKE 协议

3.1 符号说明

(I,g,p)表示有限循环群，g 为 Z_p^*的生成元，p 是一个大素数。$h()$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。以 DML-3PAKE 协议为基础，结合对称加密的相关内容，提出一个新的三方密钥交换协议。在协议开始执行前，用户 A、B 通过安全的通信信道用 $pw(A,B)$ 向 S 注册，服务器 S 保存 $h(pw_A),h(pw_B)$。

3.2 具体步骤

1) A 发送 A、B 给服务器 S。

2) 服务器 S 在收到 A、B 后，先产生随机数 $a,b\in_R Z_P^*$，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} 发送给服务器 S。

4) 服务器 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，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 在收到 V_{SA}、V_{SB} 后，分别利用保存的 g^{ax}、g^{by} 对它们进行解密，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 $K=h(A,B,S,K_{AB})=h(A,B,S,K_{BA})=h(A,B,S,g^{xy})$。

3.3 协议效率分析

判断任何一个协议设计的成功与否，最后都要归结到计算开销和通信开销 2 个方面进行衡量。在所提出的新协议中 c 每生成一个会话密钥，每个用户需要进行 4 次运算；服务器需要进行 3 次运算。而协议每执行一次，用户和服务器之间需要 3 轮交互，与 DML-3PAKE 协议相比，虽然增加了运算量，但提供了更好的安全性。

3.4 协议安全性分析

3.4.1 在线字典攻击

如果攻击者试图进行在线字典攻击，一般攻击者首先通过拦截合法用户的消息并且伪造消息 PW_A'、PW_S' 进行欺骗，但是合法用户在验证 V_{SA}、V_{SB} 时发现这种攻击者的口令猜测攻击，服务器能在验证 V_{AS}、V_{BS} 时发现这种攻击者冒充 A 或 B 的口令猜测攻击，因此提出的改进协议可检测在线字典攻击。

3.4.2 防御离线字典攻击

由于随机数 a,b,x,y 的任意性，同时攻击者也不可能获得服务器 S 的私钥，因此攻击者无法算出 S_A、S_B，从而也无法对 V_{AS}、V_{BS} 进行解密，即无法对 PW_A 与 PW_B 进行离线字典攻击[8]。笔者提出的改进协议可防御离线字典攻击。

3.4.3 中间人攻击

攻击者在 A 和 B 发送信息给 S 的过程中实施攻击，S 可以通过对 A、B 的身份进行认证来提前发现攻击。当攻击者在 S 发信息给 A、B 的过程中实施攻击时，由于 A 和 B 要对密钥进行解密计算确认，可有效地避免中间人攻击，即攻击者不能计算出 V_{SA}、V_{SB}；因此，从而也无法最终计算出会话秘钥 K。

4 结束语

笔者通过分析改进后的 DML-3PAKE 协议的安全性，并且证明了此协议仍难于抵抗不可察觉的在线字典攻击。该协议最终并没有通过严格的数学推理对协议的各种攻击进行规约，只是通过形式化模型的方法对某些用户实例和攻击者攻击进行了形式化，并且仅限于对协议的“诱导”层次上。笔者对该协议做了安全性验证，发现它并不能抵御在线字典攻击。笔者最后给出了一种新改进的协议，虽然在执行效率方面增加了计算开销，但新协议在防御在线字典攻击、离线字典攻击、中间人攻击安全性等方面与 DML-3PAKE 协议相比更为安全。

参考文献：

[1] Boyd, Mathuria keyestablishment[M]. Berlin: SpringPress, 2003: 24-266.

[2] 李洪敏, 李宇明, 葛杨. 虚拟化数据中心的安全设计[J]. 兵工自动化, 2012, 31(8): 49-51.

[3] Chien H Y. SASI: a new ultralightweight RFID authentication protocol providing strongauthentication and strong integrity[J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4(4): 337-340.

[4] Corin R, Doumen J, Etalle S. Analyzing password protocol security against off-line dictionary attacks[J]. Electronic Notes in Theoretical Computer Science, 2005, 121(4): 47-63.

[5] 卿斯汉. 安全协议. 20 年研究进展[J]. 软件学报, 2003, 14(10): 1740-1752.

[6] 邓淼磊, 王玉磊, 等. 通用可组合的三方口令认证密钥交换协议[J]. 电子与信息学报, 2010.

[7] Lowe G. Analyzing protocols subject to guessing attack. Journal of Computer Security, 2004, 12(1): 83-98.

[8] 屈峰, 杨华, 王立军, 等. 无线传感器网络及其应用[J]. 四川兵工学报, 2013, 34(2): 111-113.

（上接第 33 页）

2) 集成性：金戈 I/O 系统将 OA 的邮件功能，主机登录身份认证功能，光盘刻录与审计功能等集成到一起，确保数据输入输出的安全高效。

金戈 I/O 系统的方案设计与技术实现，将 OA 办公系统、身份认证系统、“三合一”系统、光盘刻录与审计系统紧密结合，充分发挥各自功能的优势，便于用户使用，也利于安全保密管理，大大提高了工作效率和安全保密管理水平。

3) 智能性：在数据交换计算机上插入 USB-KEY 通过认证后直接登录系统，访问对应的功能模块，扫描数据输入输出的金戈 I/O 专用光盘上粘贴条码标签，个人的输入输出也记录在日志中并可以发送个性化的电子日志。

4　结束语

金戈 I/O 系统是严格按照国家安全保密管理要求，结合某军工集团公司自身业务特色，进行设计与实施的信息输入输出管理系统。它利用集团公司涉密信息系统内网目前的网络架构，借助 VLAN 机制实现安全子域管理；结合了 OA 办公系统、身份认证系统、“三合一”系统、光盘刻录与审计系统的优势功能，实现了硬件与软件相结合的系统化管理，通过集中管控和一环紧扣一环的安全审计，达到了内网信息输入输出管理的高效、安全、可控要求。

金戈 I/O 系统，促进了某军工集团公司安全保密管理水平的提升，很大程度上提高了内网信息输入输出管理的效率，解放了人力、物力，具有一定的安全价值及应用价值。

参考文献：

[1] 刘盛铭, 刘力天, 徐晋海. WiMAX 多跳网络中基于移动站节能的选路算法[J]. 兵工自动化, 2013, 32(2): 51-54.

[2] 李星, 钟志农, 景宁, 等. 复杂网络局部社区发现算法[J]. 兵工自动化, 2013, 32(4): 42-46.

[3] 张毅. 基于信息优化的加工过程神经网络控制[J]. 机电工程, 2013, 30(10): 1214-1217.

[4] 廖熹, 易克非. 基于嵌入式 Linux 系统下的 Qt 测试软件开发[J]. 兵工自动化, 2013, 32(8): 94-96.

[5] 李芳. 基于Matlab的螺纹参数检测软件[J]. 兵工自动化, 2013, 32(10): 95-96.

（上接第 35 页）

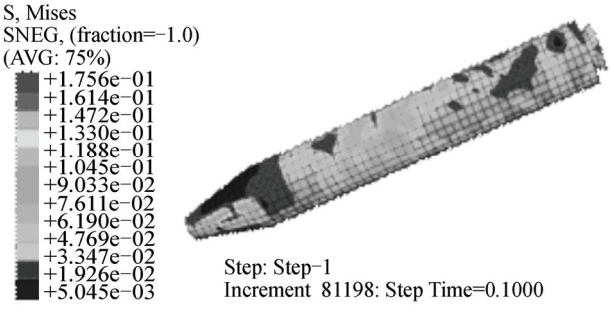

图 6　100 ms 时导弹应力图

4　结语

仿真结果表明：泡沫起到了良好的缓冲作用，使得 2 个发动机参考点上的垂直加速度峰值处在安全范围内，弹体的应力峰值也是安全的。

模拟结果为导弹的跌落试验以及弹体和包装箱的结构优化提供一定的参考。对导弹的导引头、飞控系统、舵机[9]和级间段壳体的具体结构可以进一步细化建模，以便获得更加准确的加速度和应力输出结果。

参考文献：

[1] 高廷如, 于鑫, 高欣宝. 新型炮弹缓冲包装计算方法[J]. 包装工程, 1999, 20(2): 33-35.

[2] 肖军, 樊来恩, 等. 机载导弹包装箱技术及其研究进展[J]. 包装工程, 2010, 31(13): 136-139.

[3] 邱莎莎, 蔡建, 张恒翔. 导弹缓冲包装设计与选材[J]. 包装工程, 2011, 32(9): 44-46.

[4] 高志远, 白修宇, 等. 弹载电子设备的缓冲包装设计及包装箱设计[J]. 国防技术基础, 2005(3): 34-37.

[5] 常新龙. 导弹总体结构与分析[M]. 北京: 国防工业出版社, 2010: 61-62.

[6] 龚艳霞, 沈晓红, 聂学俊. 基于 ABAQUS 的保险杠低速碰撞的仿真研究[J]. 北京工商大学学报, 2009, 27(3): 32-36.

[7] 徐文岷. 汽车碰撞过程的有限元数值模拟[D]. 哈尔滨: 哈尔滨工程大学, 2007: 15-16.

[8] 杨辛, 夏勇, 周青. 汽车低速碰撞下保险杠缓冲泡沫塑料件的损伤软化[C]. 北京: 2006 中国汽车安全技术国际研讨会, 2006: 148-152.

[9] 于翠. 某型导弹虚拟样机验模与仿真[J]. 兵工自动化, 2012, 31(10): 14-16.