第41卷第7期 中国科学技术大学学报 Vol. 41, No. 7
2011年7月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Jul. 2011

文章编号:0253-2778(2011)07-0589-05

一个具有完备前向安全性的基于口令认证密钥协商方案

郝 卓,俞能海

(中国科学技术大学电子工程与信息科学系,安徽合肥 230027)

摘要:在基于网络的分布式环境中,基于口令的认证密钥协商方案是一项基本的安全防护机制.对一个已有的基于口令的认证密钥协商方案[Chen T H, Hsiang H C, Shih W K. Security enhancement on an improvement on two remote user authentication schemes using smart cards. Future Generation Computer Systems, 2011, 27(4): 337-380]做了安全分析,指出其易受离线口令猜测攻击,并且不具备完备的前向安全性.在此基础上,提出了一个安全性增强的远程口令认证密钥协商方案.所提出的方案继承了已有方案的优良性质,能够抵抗离线口令猜测攻击,并且具有完备的前向安全性.经过安全分析,论证了所提出的方案具有强安全性,适合于在分布式环境中对用户和服务器提供双向认证和密钥协商.

关键词:认证密钥协商;口令认证;完备前向安全性;离线口令猜测攻击

中图分类号:TP393.08 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2011.07.004

A password-authenticated key agreement scheme with perfect forward secrecy

HAO Zhuo, YU Nenghai

(*Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei* 230027, *China*)

Abstract: In a distributed network environment, password-authenticated key agreement schemes are fundamental security mechanisms. A security analysis of Chen et al.'s scheme [Chen T H, Hsiang H C, Shih W K. Security enhancement on an improvement on two remote user authentication schemes using smart cards. Future Generation Computer Systems, 2011, 27(4): 337-380] was presented. It was found that Chen et al.'s scheme cannot resist offline password guessing attacks, and does not have perfect forward secrecy. A security enhanced password-authenticated key agreement scheme was thus proposed. The proposed scheme maintains the good properties of Chen et al.'s scheme, is resistant to offline password guessing attack and provides perfect forward secrecy. A security analysis of the proposed scheme demonstrated that it is capable of strong security. It is suitable for providing mutual authentication and key agreement between the user and the server in a distributed environment.

Key words: authenticated key agreement; password authentication; perfect forward secrecy; offline password guessing attack

收稿日期:2011-04-28;**修回日期**:2011-06-23

基金项目:国家科技重大专项(2010ZX03004-003)资助.

作者简介:郝卓,男,1985年生,博士生. 研究方向:计算机网络安全. E-mail: hzhuo@mail.ustc.edu.cn

通讯作者:俞能海,博士/教授. E-mail: ynh@ustc.edu.cn

0 引言

在互联网技术高度发达的今天，人们随时随地都可以通过网络访问各种应用程序和服务. 在访问这些服务时，不可避免会遇到身份认证和会话机密性的问题. 基于口令的认证密钥协商方案能够在用户和服务器之间进行身份认证，并提供会话密钥使用户和服务器之间能够进行秘密会话. 最近 Chen 等[1]提出了一个基于口令的认证密钥协商方案，该方案的安全性基于单向函数的抗碰撞性. Chen 等的方案通过使用基于智能卡的口令认证增强了身份认证的安全性，并通过在协议中仅使用哈希函数和异或操作使方案具有很高的效率. Chen 等的方案能够抵抗伪装攻击、并行会话攻击和重放攻击等，并达到了双向认证.

我们对 Chen 等的方案作了密码分析，发现 Chen 等的方案不能抵抗离线口令猜测攻击，并且不具有完备前向安全性[5]. 在此基础上，我们提出了一个安全性增强的方案，解决了存在离线口令猜测攻击的问题，并达到了完备的前向安全性. 方案的安全性基于单向哈希函数的性质和计算 Diffie-Hellman 假设[4].

文章内容安排如下：节 1 介绍预备知识；节 2 回顾 Chen 等的方案；节 3 对 Chen 等的方案进行安全分析；节 4 提出一个安全性增强的方案；节 5 对所提出的方案进行安全分析；最后我们在节 6 给出结论.

1 预备知识

因为 Chen 等的方案[1]和本文所提出的方案的安全性基于单向哈希函数的性质，在这一部分我们介绍单向哈希函数的定义. 此外，我们介绍群上的计算 Diffie-Hellman 假设[4].

1.1 单向哈希函数

定义 1.1(单向哈希函数) 单向哈希函数 h: $\{0,1\}^* \to \{0,1\}^l$ 是一个具有下面 4 条性质的函数：

①函数的输入是任意长度的消息，输出是固定长度的消息；

②对任意给定消息，计算消息摘要很容易，但是对于给定的消息摘要，计算消息本身是计算上不可行的；

③给定一个消息 s，寻找 s' 使得 $s \neq s'$ 但是 $h(s)=h(s')$ 在计算上是不可行的；

④试图寻找两个消息 s 和 s'，使得 $s \neq s'$ 但是 $h(s)=h(s')$ 在计算上是不可行的.

除了定义中所给出的 4 条性质之外，单向哈希函数通常还具有雪崩性. 雪崩性是指函数输入的每一比特对输出的每一比特都有影响. 当输入仅发生一比特变化时，输出的消息发生很大变化. SHA-1，SHA-256 等[6]是目前应用比较广泛的单向哈希函数.

1.2 计算 Diffie-Hellman 假设

令 p,q,g 表示 3 个公有参数，其中 p 和 q 是大素数，并且 q 整除 $(p-1)$. g 是乘法群 Z_p^* 中阶数为 q 的一个元素，$\{1,g,g^2,g^3\cdots,g^{q-1}\}$ 构成一个 q 阶的循环子群，记这个群为 G_q. 下面定义群 G_q 上的计算 Diffie-Hellman 假设.

定义 1.2(G_q 上的计算 Diffie-Hellman 假设[4]) 群 G_q 上的计算 Diffie-Hellman 算法 $\mathcal{A}$ 是一个概率多项式时间算法(以 $|p|$ 为参考)，该算法对某个固定的 $\alpha>0$，和充分大的 n，有

$$\Pr(\mathcal{A}(p,q,g,g^a,g^b)=g^{ab})>\frac{1}{n^\alpha},$$

其中 a,b 从 $[1,q-1]$ 随机选取. G_q 满足计算 Diffie-Hellman 假设，是指在 G_q 上不存在这样的算法.

2 Chen 等的方案回顾

在这一部分我们首先介绍在本文中用到的符号，然后对 Chen 等的方案进行回顾.

2.1 符号介绍

本文中所用到的符号介绍如下：

U：用户.

ID：用户身份标识.

PW：用户口令.

S：服务器.

x：服务器的长期密钥.

$h()$：一个单向哈希函数.

$h_k()$：一个带有密钥的哈希函数，其中 k 作为密钥.

$\Rightarrow$：安全信道，表示在其中传输的消息或智能卡受到保护，使敌手不能窃听.

$\to$：一般信道，表示在其中传输的消息或智能卡不受保护.

$\|$：二进制串连接操作.

2.2 Chen 等的方案[1]回顾

Chen 等的方案分为 4 个阶段，分别为注册阶段、登录阶段、验证阶段和口令更改阶段.

2.2.1 注册阶段

当 U 向服务器注册身份的时候，注册阶段被调

用.其包括以下步骤：

①U 选择自己的身份标识 ID 和口令 PW，生成一个随机数 b，并计算 $h(b\oplus PW)$.

②U⇒S：ID，$h(b\oplus PW)$.

③S 执行下面的计算：

$$P = h(ID \oplus x),$$
$$R = P \oplus h(b \oplus PW),$$
$$V = h_P(h(b \oplus PW)).$$

④S⇒U：包含 V，R，$h()$和 $h_k()$的智能卡.

⑤U 将 b 写入智能卡.智能卡中最后包含 V，R，b，$h()$和 $h_k()$.

2.2.2　登录阶段

当 U 需要登录到 S 时，登录阶段被调用，其包含以下步骤：

①U 将智能卡插入智能卡读取器，并输入 ID 和 PW.

②U 的智能卡计算 $P=R\oplus h(b\oplus PW)$，并检验 $h_P(h(b\oplus PW))$是否和存储在智能卡中的 V 相等.如果不相等，智能卡立刻终结本次登录过程.

③智能卡生成一个随机数 r，并计算下面两个值：

$$C_1 = P \oplus h(r \oplus b),$$
$$C_2 = h_p(h(r \oplus b) \| T_u).$$

其中 T_u 是 U 的当前时间戳，根据当前系统时间生成.

④U→S：$C=\{ID, C_1, C_2, T_u\}$.

2.2.3　验证阶段

在消息 C 被 S 接收到以后，S 和智能卡执行以下步骤：

①S 根据自己的当前系统时间生成时间戳 T_s，之后检查 ID 的格式和时间戳.如果 ID 无效或 $T_u=T_s$，S 就拒绝 U 的登录请求.如果 $(T_s-T_u)>\Delta T$（ΔT 是客户和服务器之间的传输延迟期望值），那么 S 拒绝 U 的登录请求.

②S 计算 $P=h(ID\oplus x)$，$C_1'=P\oplus C_1$ 和 $C_2'=h_P(C_1'\| T_u)$.S 判断 C_2'与接收到的 C_2 是否相等.如果 $C_2'=C_2$，则 S 接受 U 的登录请求，并计算 $C_3=h_P(C_1'\oplus T_s\| P)$；否则 S 拒绝 U 的登录请求.

③S→U：T_s，C_3.

④在 U 接收到消息$\{T_s, C_3\}$之后，U 检验 T_s 的有效性.如果 T_s 是无效的，或者 $T_s=T_u$，则 U 立即终止本次会话.否则 U 计算 $C_3'=h_P(h(r\oplus b)\oplus T_s\| P)$并比较 C_3'和接收到的 C_3 是否相等.如果相等，则 S 的身份得到验证；否则 U 终止当前会话.$C_1'=h(r\oplus b)$被用作 U 和 S 的共享密钥.

2.2.4　口令更改阶段

当 U 需要更改口令时，U 调用口令更改阶段.本阶段包括以下步骤：

①U 将智能卡插入到智能卡读取器，输入 ID 和 PW，请求更改口令.

②U 的智能卡计算 $P^*=R\oplus h(b\oplus PW)$和 $V^*=h_{P^*}(h(b\oplus PW))$.

③U 的智能卡验证 V^* 和存储在智能卡中的 V 是否相等.如果相等，则提示 U 选择新口令；否则 U 的智能卡拒绝口令更改请求.

④U 输入新口令，记为 PW_{new}.U 的智能卡计算 $R_{new}=P^*\oplus h(b\oplus PW_{new})$和 $V_{new}=h_{P^*}(h(b\oplus PW_{new}))$.之后 U 的智能卡用 R_{new}和 V_{new}替换智能卡中的 R 和 V.

3　对 Chen 等的方案的安全分析

我们对 Chen 等的方案做了安全性分析，发现其不能抵抗离线口令猜测攻击，并且缺乏完备前向安全性.其中离线口令猜测攻击发生在敌手获取到用户丢失的智能卡的情况下.敌手使用功率分析的方法[2-3]能够获取到智能卡当中存储的全部数据（我们指出这是一个合理的情景，在很多文章中被使用，例如文献[8-12]），根据这些数据敌手能够对用户口令进行猜测.完备前向安全性[5]是指当某个协议方的长期密钥被敌人发现之后，他不能利用该长期密钥获取以前会话中所协商出来的密钥.

3.1　离线口令猜测攻击

在敌手获取到用户 U 丢失的智能卡以后，通过功率分析的方法，敌手获取到存储在其中的秘密信息，包括 V，R 和 b.其中

$$R = P \oplus h(b \oplus PW),$$
$$V = h_P(h(b \oplus PW)).$$

敌手按照以下步骤编写程序进行离线口令猜测攻击：

①选择一个可能的口令 PW′，计算 $h(b\oplus PW')$.

②计算 $P'=R\oplus h(b\oplus PW')$和 $V'=h_{P'}(h(b\oplus PW'))$.

③比较 V′和 V.如果 $V'=V$，则 PW′为用户口令；否则再选一个新的可能的口令，重复执行以上步骤，直至找到用户口令.

3.2 缺乏完备前向安全性

敌手通过监听U和S之间的会话，获取了一系列消息，包括{ID，C_1，C_2，T_u，T_s，C_3}.其中C_1展开如下：

$$C_1 = h(\mathrm{ID} \oplus x) \oplus h(r \oplus b).$$

如果敌手获取了服务器方长期密钥x，则可以通过以前所监听到的ID和C_1计算得到以前的会话密钥，即$h(r \oplus b) = h(\mathrm{ID} \oplus x) \oplus C_1$.由此可见，Chen等的方案不具备完备的前向安全性.

4 安全性增强的方案

在这一部分我们针对Chen等的方案[1]存在的安全问题，提出一个安全性增强的方案.所提出的方案在Chen等方案的基础上进行改进，修改智能卡中存储的内容，并使口令修改建立在成功认证的基础上，从而避免了离线口令猜测攻击.另外，通过将Diffie-Hellman密钥交换[7]整合到方案中，达到了完备前向安全性.

安全性增强的方案包括以下4个阶段：注册阶段、登录阶段、验证阶段和口令更改阶段.

4.1 注册阶段

在注册阶段，用户向服务器完成身份登记，并从服务器获取智能卡.该阶段包括如下步骤：

①用户选择自己的ID，PW，生成一个随机数b，并计算$h(b \oplus \mathrm{PW})$.

②U⇒S：ID，$h(b \oplus \mathrm{PW})$.

③S选择3个公有参数p，q，g，其中p和q是大素数，并且q整除$(p-1)$，g是乘法群Z_p^*中阶数为q的一个元素.S执行如下计算：

$$P = h(\mathrm{ID} \oplus x),$$

$$R = P \oplus h(b \oplus \mathrm{PW}).$$

④S⇒U：一个包含p，q，g，R，$h()$和$h_k()$的智能卡.

⑤U将b写入智能卡中.此时智能卡中包括p，q，g，R，b，$h()$和$h_k()$.

4.2 登录阶段

当U需要登录到服务器时，登录阶段被调用.该阶段包括如下步骤：

①U将其智能卡插入到智能卡读取器，输入ID和PW.

②U的智能卡生成一个临时交互号r，生成一个随机数$r_u \in [1, q-1]$，并计算$R_u = g^{r_u} \bmod p$.之后U的智能卡取当前系统时间戳T_u，并计算下面一些值：

$$P = R \oplus h(b \oplus \mathrm{PW}),$$

$$C_0 = h(\mathrm{ID} \oplus P) \oplus R_u,$$

$$C_1 = P \oplus h(r \oplus b),$$

$$C_2 = h_P(h(r \oplus b) \| T_u \| R_u).$$

③U→S：$C = \{\mathrm{ID}, C_0, C_1, C_2, T_u\}$

4.3 验证阶段

当S收到来自U的验证请求时，S执行以下步骤：

①S检验ID的格式是否有效，如果ID无效，则S拒绝U的认证请求.S取当前系统时间戳T_s.如果$T_u = T_s$或$|T_s - T_u| > \Delta T$(ΔT是消息传输的最大可容忍延迟)，则S拒绝U的认证请求.

②S计算$P = h(\mathrm{ID} \oplus x)$，$R'_u = h(\mathrm{ID} \oplus P) \oplus C_0$，$C'_1 = P \oplus C_1$和$C'_2 = h_P(C'_1 \| T_u \| R'_u)$.之后S检验$C'_2$和接收到的$C_2$是否相等.如果二者相等，S接受U的认证请求.

③S随机生成$r_s \in [1, q-1]$并计算$R_s = g^{r_s} \bmod p$，$W_s = (R'_u)^{r_s} \bmod p$和$K_s = h(W_s \| C'_1)$.$K_s$是S和U之间的共享会话密钥.之后S计算$C_3 = h_P((C'_1 \oplus T_s) \| P \| R_s)$和$C_4 = h(\mathrm{ID} \| P) \oplus R_s$.

④S→U：T_s，C_3，C_4.

⑤当U收到S发来的消息{T_s，C_3，C_4}时，U取当前系统时间戳T'_u，并对T_s进行检验.如果T_s无效，$T_s = T_u$或是$|T_s - T'_u| > \Delta T$，则停止当前会话.否则U计算$R'_s = C_4 \oplus h(\mathrm{ID} \| P)$和$C'_3 = h_P((h(r \oplus b) \oplus T_s) \| P \| R'_s)$，并将$C'_3$与接收到的$C_3$比较.如果$C'_3 = C_3$，则S的身份得到验证.U计算$W_u = (R'_s)^{r_u} \bmod p$和$K_u = h(W_u \| h(r \oplus b))$作为共享密钥.

4.4 口令更改阶段

当U需要更改口令时，口令更改阶段被调用.该阶段包括以下步骤：

①执行节4.2和4.3的登录阶段和验证阶段，完成双向身份认证.

②U输入新口令$\mathrm{PW}_{\mathrm{new}}$，要求更改口令.

③U的智能卡计算$R_{\mathrm{new}} = R \oplus h(b \oplus \mathrm{PW}) \oplus h(b \oplus \mathrm{PW}_{\mathrm{new}})$，并用$R_{\mathrm{new}}$替换$R$存储在智能卡中.

5 所提出方案的安全分析

因为所提出的安全性增强方案基于对Chen等的方案[1]的安全分析，其继承了Chen等的方案所具有的安全性，例如对抗重放攻击、伪装攻击、并行

会话攻击等. 在这一部分我们仅针对 Chen 等的方案存在的问题进行分析. 我们首先分析在敌手获取用户丢失智能卡的情况下，所提出的方案能够抵抗离线口令猜测攻击；然后我们论证所提出的方案具有完备前向安全性.

5.1　抵抗离线口令猜测攻击

当敌手获取 U 所丢失的智能卡时，敌手通过功率分析获得智能卡中所存储的信息，包括 $\{p, q, g, R, b\}$，其中 p, q, g 是可公开的参数，敌手从其中不能获取关于用户口令的信息. 另外，$R = h(\mathrm{ID} \oplus x) \oplus h(b \oplus \mathrm{PW})$，因为 $h(\mathrm{ID} \oplus x)$ 对敌手是机密的，因此敌手无法通过 R 和 b 实行离线口令猜测攻击.

5.2　完备前向安全性

在敌手窃听 U 和 S 之间登录过程和验证过程的情况下，敌手能够获取的信息包括 $\{\mathrm{ID}, C_0, C_1, C_2, T_u, T_s, C_3, C_4\}$. 其中，

$$C_0 = h(\mathrm{ID} \oplus h(\mathrm{ID} \oplus x)) \oplus R_u,$$

$$C_1 = h(\mathrm{ID} \oplus x) \oplus h(r \oplus b),$$

$$C_2 = h_{h(\mathrm{ID} \oplus x)}(h(r \oplus b) \| T_u \| R_u),$$

$$C_3 = h_{h(\mathrm{ID} \oplus x)}((h(r \oplus b) \oplus T_s) \| h(\mathrm{ID} \oplus x) \| R_s),$$

$$C_4 = h(\mathrm{ID} \| h(\mathrm{ID} \oplus x)) \oplus R_s.$$

如果服务器长期密钥 x 被敌手获取，他可以通过窃听到的 C_0 和 ID 得到 R_u，通过 C_1 得到 $h(r \oplus b)$，通过 C_4 得到 R_s. 因为 $R_u = g^{r_u} \bmod p$，$R_s = g^{r_s} \bmod p$，$W_u = W_s = g^{r_u r_s} \bmod p$，$K_u = K_s = h(W_u \| h(r \oplus b))$. 根据群 G_q 上的计算 Diffie-Hellman 假设(参见节 1.2)，敌手无法从 R_u 和 R_s 得到 W_u，从而无法得到 U 和 S 的共享密钥. 另外，如果敌手获取到用户口令 PW，则因为敌手所获取到的上述信息与 PW 无关，敌手也不能得到 U 和 S 以前的共享密钥. 由此可见，所提出的方案具有完备的前向安全性.

6　结论

基于口令的远程认证密钥协商在基于网络的服务中被广泛用于为用户和服务器提供身份认证和会话密钥生成. 本文针对 Chen 等的方案[1]提出安全性分析，指出其不能抵抗离线口令猜测攻击，并且不具有完备前向安全性. 这两个安全缺陷使得 Chen 等的方案易受敌手的攻击，不能适用于网络服务中. 针对 Chen 等的方案的安全缺陷，我们提出了一个安全性增强的方案. 所提出方案的安全性基于单向哈希函数的性质和计算 Diffie-Hellman 假设. 所提出的方案继承了 Chen 等的方案的优点，能够防止离线口令猜测攻击，并具有完备的前向安全性.

参考文献(References)

[1] Chen T H, Hsiang H C, Shih W K. Security enhancement on an improvement on two remote user authentication schemes using smart cards [J]. Future Generation Computer Systems, 2011, 27(4): 337-380.

[2] Kocher P C, Jaffe J, Jun B. Differential power analysis [C]// Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer-Verlag, 1999: 388-397.

[3] Messerges T, Dabbish E, Sloan R. Examining smart-card security under the threat of power analysis attacks [J]. IEEE Transactions on Computers, 2002, 51(5): 541-552.

[4] Boneh D. The decision Diffie-Hellman problem [C]// Proceedings of the Third Algorithmic Number Theory Symposium. London, UK: Springer-Verlag, 1998: 48-63.

[5] Diffie W, Oorschot P C, Wiener M J. Authentication and authenticated key exchanges [J]. Designs, Codes and Cryptography, 1992, 2(2): 107-125.

[6] NIST. FIPS-PUB-180-2: Secure Hash Standard [S/OL]. (2002) [2011-03-17]. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf.

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

[8] Wang X M, Zhang W F, Zhang J S, et al. Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards [J]. Computer Standards & Interfaces, 2007, 29(5): 507-512.

[9] Yang G, Wong D S, Wang H, et al. Two-factor mutual authentication based on smart cards and passwords [J]. Journal of Computer and System Sciences, 2008, 74(7): 1 160-1 172.

[10] Xu J, Zhu W T, Feng D G. An improved smart card based password authentication scheme with provable security [J]. Computer Standards & Interfaces, 2009, 31(4): 723-728.

[11] Hsiang H C, Shih W K. Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards [J]. Computer Communications, 2009, 32(4): 649-652.

[12] Chung H R, Ku W C, Tsaur M J. Weaknesses and improvement of Wang et al.'s remote user password authentication scheme for resource-limited environments [J]. Computer Standards & Interfaces, 2009, 31(4): 863-868.