

无须重注册的单向通信动态口令认证

鲁迁迁, 朱友文, 蒋炎

(南京航空航天大学计算机科学与技术学院, 江苏 南京 211100)

摘要: 动态口令是在系统中或设备上仅对一次会话有效的口令。目前存在的无须重注册的动态口令方案虽然不受认证次数的限制, 但仅支持在线认证, 不能离线认证。针对以上问题, 提出一种无须重注册的单向通信动态口令认证方案。该方案基于无须重注册的方式结合基于时间动态口令方案, 在实现离线认证的同时满足认证次数无限和口令有时效, 最后证明该方案的安全性。

关键词: 动态口令; 无须重注册; 口令有时效; 支持离线认证

中图分类号: TP301.6

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020038

One-time password authentication for one-way communication without re-registration

LU Qianqian, ZHU Youwen, JIANG Yan

School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211100, China

Abstract: One-time password is a password that is valid for only one session on a system or device. The existing one-time password scheme without re-registration which is not limited by the number of authentication only supports online authentication, but can not support offline authentication. To solve the above problems, a one-time password authentication scheme for one-way communication without re-registration was proposed. The scheme combined the time-based one-time password scheme with the way of no re-registration. It can realize the offline authentication while satisfying the infinite authentication times and the password time-effective. Finally, the security of the scheme is proved.

Key words: one-time password, no re-registration, timeliness password, offline authentication

收稿日期: 2020-01-15; 修回日期: 2020-05-11

通信作者: 鲁迁迁, 2293520373@qq.com

基金项目: 国家重点研发计划 (2017YFB0802300)

Foundation Item: The National Key R & D Program (2017YFB0802300)

论文引用格式: 鲁迁迁, 朱友文, 蒋炎. 无须重注册的单向通信动态口令认证[J]. 网络与信息安全学报, 2020, 6(3): 99-107.

LU Q Q, ZHU Y W, JIANG Y. One-time password authentication for one-way communication without re-registration [J]. Chinese Journal of Network and Information Security, 2020, 6(3): 99-107.

1 引言

身份认证是保障信息系统安全的第一道防线, 口令是应用最为广泛的身份认证方法。常见的口令认证机制大多是基于静态口令的, 认证服务器根据用户输入的口令和自身维护的口令表进行匹配来判断用户身份的合法性, 但容易受到重放、网络窃听以及猜测攻击。针对静态口令机制在安全方面的脆弱性, 研究口令认证的学者提出了动态口令认证技术以保护重要的网络系统资源。动态口令认证机制是在产生验证信息时加入不定因素(如用户登录的时间、用户登录的次数等), 使每次登录过程中网络传送的数据包不同, 从而提高登录的安全性。

目前已有的(或者常用的)身份认证方式(如令牌认证、手机应用程序等认证方式)非常烦琐, 无法满足人们的需求。令牌认证虽然很安全, 但用户必须随身携带令牌, 丢失或忘记令牌会造成不必要的麻烦。而目前存在的手机 App 大多采用挑战/应答机制认证, 导致用户和服务器之间需要双向通信, 即服务器随机生成挑战发送给用户, 用户利用挑战计算相应的应答并上传给服务器。然而, 该挑战需要用户手机始终保持连接状态, 一旦欠费或无信号, 通信立即中断。在这种情形下, 身份认证系统可采用基于时间的动态口令(TOTP, time-based one-time password)^[1], 仅需要从用户到服务器的单向通信。然而, TOTP 需要服务器以明文形式存储用户的私钥, 一旦服务器被攻破, 用户的私钥将立即泄露。一种可行的方法是将服务器上用户私钥替换为私钥哈希值。该方法采用无限后退哈希链的方式, 导致用户需要每隔一定时间重新注册。如何实现在用户不需要重新注册的基础上使手机支持离线认证, 是一个亟待解决的问题。

1981 年, Lamport 首次提出基于哈希链的动态口令(OTP, one-time password)认证方案, 后被改进为 S/KEY 方案^[2], 已被广泛地应用于各种认证机制^[3-4]。目前应用较广的有: 基于时间的 OTP^[1]、基于哈希链的 OTP(HOTP, HMAC-based one-time password)^[5]以及基于计数器的 OTP(COTP, count-based one-time password)^[6]。Lamport

基于后退式哈希链, 设计了动态口令认证方案, 该方案哈希链链长固定, 受限于认证次数(即用户需要重注册), 并且不能抵抗小数目攻击^[7]。重注册是指哈希链长是固定的, 每当这个哈希链被用完以后, 用户必须重新生成条新的哈希链, 并将哈希链最初的验证值提交给服务器。Das 等^[8]提出基于身份(ID, identity)和 Hash 算法的动态口令鉴别方案, 该方案可防止用户 ID 被盗, 同时抵抗重放攻击、内部攻击以及猜测攻击。但是, AwaSthi^[7]指出如果智能卡被盗, Das 等^[8]提出的方案将不再安全, 攻击者可在智能卡中插入随机口令替换用户口令。Goyal^[9]提出了 N/R(N 代表哈希链总长, R 代表选取的子链长)动态口令方案, 减少了用户端的计算量, 但方案的安全性并没有提高。Gong 等^[10]提出的基于更新子链的动态口令虽然可以实现认证次数不受限制, 但仍然采用挑战/应答模式, 无法实现离线认证。Park 提出的不需要重注册的动态口令方案^[11], 虽然可以抵抗重放攻击、小数目攻击等多种攻击方式, 但依然无法实现离线认证。Kogan 将 Lamport 提出的 S/KEY 方案改进为 T/KEY 方案^[12], 可以实现离线认证, 但该方案和 S/KEY 方案一样需要重注册。Hwang^[13]提出了前向哈希链的动态口令方案, 虽无须重新注册, 但不能抵抗重放攻击^[7]。Chefranov^[14]在文献[13]方案的基础上, 提出了基于无限前进哈希链的动态口令认证方案, 该方案虽然避免了重注册的问题, 但受限于双向通信, 即仅支持在线认证。由于在实际应用中, 人们往往可能会遇到无网络或网络状态差的情况(如偏远的地区、电梯或地下停车场等), 因此, 研究和设计一种无须重注册的单向通信动态口令认证方案具有很重要的应用价值。

针对上述问题, 本文基于文献[14]所使用的无限前进哈希链结合 TOTP 算法, 提出一种无须重注册的单向通信动态口令认证方案。本文的主要贡献有: ① 提出了一种基于无限前进哈希链的动态口令方案, 该方案具有无须重注册与离线认证的特点; ② 运用 TOTP 算法, 限制动态口令的时效性, 即动态口令仅在短暂时间内有效(如 30 s); ③ 使用手机二维码产生动态口令的方式代替令牌, 提高了方案的可用性。

2 相关知识及方案

2.1 TOTP 算法

基于时间的动态口令算法是根据共享密钥和当前时间计算动态口令的算法,如图1所示,该算法是 HMAC 动态口令算法的扩展。 $TOTP = HMAC(K, (T - T_0 / X))$, 其中, K 表示共享密钥, T 表示当前的时间戳, T_0 表示开始的时间戳, X 表示时间步。

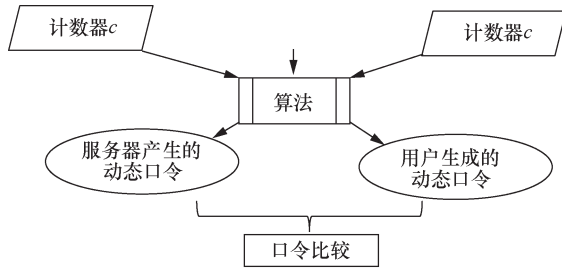


图1 TOTP 算法
Figure 1 TOTP algorithm

TOTP 算法可实现从用户到服务器的单向认证(即支持离线认证),并限制口令的时效性。

2.2 OTP 方案

Lamport^[15]采用后退式哈希链: $\{x_i = H(x_{i+1}), i \in [0, n-1]\}$ 其中 x_n 是用户随机选择的种子, n 是哈希链的链长(如 $n=1\ 000$)。Lamport 提出的方案后被改进为 S/KEY 方案,该方案包含用户注册和登录两个阶段,注册过程如图2所示。

注册时将用户的信息以及初始口令 x_0 (初始口令由用户随机选择的种子迭代哈希 n 次取得,即 $x_0 = H^{1000}(x_n)$) 发送给服务器。服务器将用户信息及初始口令存储在本地用于后续的登录验证。

第 $i+1$ 次登录时,登录过程如图3所示,用户登录的动态口令为 x_{i+1} ,当服务器接收到用户

第 $i+1$ 次发送过来的口令时,验证 $x_i = H(x_{i+1})$ 是否成立。如果成立,则用户登录成功,更新服务器的验证值为 x_{i+1} ,否则用户登录失败。

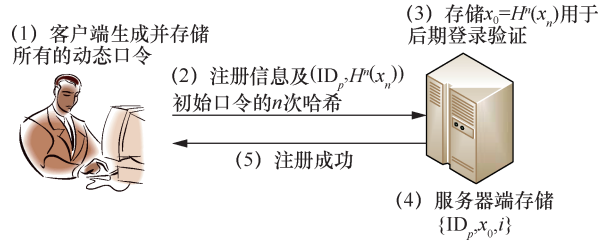


图2 OTP 方案的用户注册过程
Figure 2 The user registration process of OTP scheme

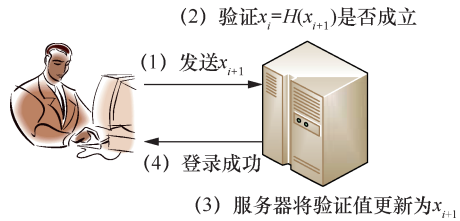


图3 OTP 方案的用户登录过程
Figure 3 The user login process of OTP scheme

Lamport 提出的 OTP 方案虽然产生了极大的反响,得到了广泛应用,但仍有许多方面有待改进,如哈希链的链长固定(n),当哈希链链长被使用完之后,用户必须重新选取一个新的种子 x'_n ,并将它迭代哈希 n 次的值作为新的验证值发送给服务器,这种类似重新注册的操作给用户带来了不太友好的体验感;如果攻击者模仿服务器,还会导致泄露用户尚未使用的动态口令。

2.3 Chefranov 方案

Chefranov^[14]构建无限向前的哈希链,避免了用户需要重注册的问题。方案分为注册和登录两个阶段,注册过程如图4所示。

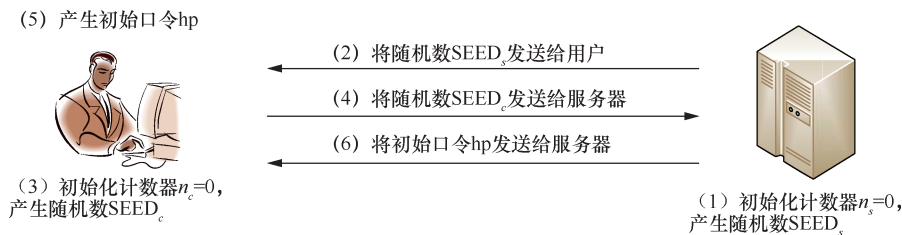


图4 Chefranov 方案的用户注册过程
Figure 4 The user registration process of Chefranov scheme

注册时, 用户和服务器各自有一个计数器, 初始值都为 0。用户和服务器各自随机选择一个初始种子 $SEED_c$ (用户)、 $SEED_s$ (服务器), 并在一个安全的通道中将各自的种子发送给对方; 然后根据用户注册时提交的静态口令以及种子生成初始的动态口令, 并将初始口令 hp 发送给服务器 $\{p = H(K \oplus SEED_s), p_1 = H(p), hp = H(p_1)\}$, 服务器将 hp 存储在本地。

登录过程如图 5 所示, 用户首先产生一个噪声 D_c , 用于加密发送的动态口令 p_1 , 然后发送消息 $M1$, $M1$ 的计算式为 $M1 = (M_{11}, M_{12}, M_{13}, M_{14})$, 其中 $\{M_{11} = p_1 \oplus H(D_c), M_{12} = H(p \oplus H(p_1))H(D_c), M_{13} = H^2(p \oplus H(p_1))D_c, M_{14} = SEED_c \oplus D_c\}$ 。服务器接收到 $M1$, 首先用存储在本地的 $SEED_c$ 取得用户随机产生的噪声 $D_c (D_c = SEED_c \oplus M_{14})$, 随后验证 $hp = H(M_{11} \oplus H(D_c))$ 和 $M_{13} \oplus D_c = H(M_{12} \oplus H(D_c))$ 是否成立, 如果不成立, 则验证失败; 如果成立, 则服务器计数器加 1, 同时更新服务器验证值 $hp = M_{12} \oplus H(D_c)$ 。认证成功后, 服务器将 $M2$ 返回给用户: $M2 = (M_{21}, M_{22}) = \{(D_c + 1) \oplus SEED_s, (D_c + 1) \oplus SEED_c\}$ 。用户收到 $M2$, 验证 $M_{21} \oplus SEED_s = M_{22} \oplus SEED_c = D_c + 1$ 是否成立。如果成立, 用户认证服务器成功, 用户计数器加 1, 同时更新下一次登录的动态口令 $p_1 = p \oplus H(p_1)$; 否则, 用户认证服务器失败, 认证结束。

Chefranov 方案采用前向哈希链取代后退式哈希链, 避免了重注册的过程, 同时可以抵抗重放攻击以及小数目攻击等多种方式的攻击。但是, Chefranov 方案仍采用用户和服务器双向认证的

模式, 一旦用户由于某些原因处于没有网络的状态时, 认证将无法继续; 另外, 目前提出的大多数动态口令方案和 Chefranov 方案存在同样的弊端: 动态口令时效性的问题, 动态口令在一个不确定的时间内有效, 有效时间由用户两次登录间隙决定, 如果用户登录的并不是很频繁, 足够的登录间歇时间给了攻击者可乘之机。

3 无须重注册的单向通信动态口令认证方案

3.1 无须重注册的单向通信动态口令认证过程

无须重注册的单向通信动态口令认证方案基于 Chefranov 方案无须重注册的优点结合 TOTP 算法, 实现用户到服务器的单向通信, 并用手机 App 产生动态口令, 确保用户在没有网络的情况下认证仍然可以完成。该方案利用 TOTP 算法限制口令实效的优点, 使动态口令每隔很短的时间便会更换, 但使用 TOTP 算法需要在用户和服务器两端同时设置时钟。方案分为用户注册和登录认证两个阶段, 如图 6 所示。

3.1.1 注册阶段

用户提交注册信息如用户名 ID、静态口令 K 、邮箱、手机号码等, 同时产生两个随机数 $SEED_p$ 、 $SEED_c$, 其中, $SEED_c$ 将被发送到服务器用于后期验证, $SEED_p$ 和用户提交的静态口令 K 一起生成动态口令, 注册过程如图 7 所示。

用户注册成功以后, 无论用户是否登录, 动态口令均会在很短的时间间隔内更新一次 (本文为叙述方便, 设置口令每隔 1 min 更新一次), 更新公式为 $p_i = p_{i-1} \oplus H(p_{i-1})$, 具体注册过程如下。

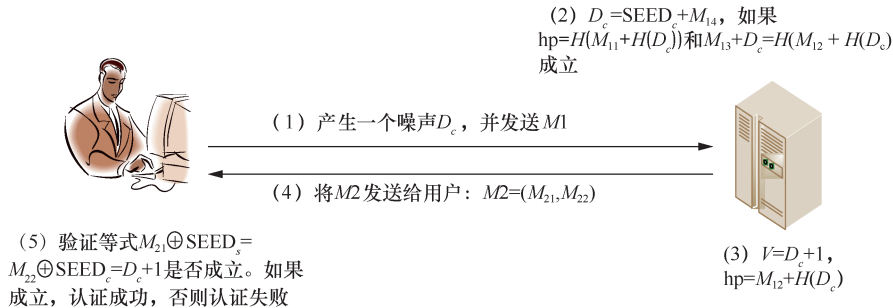


图 5 Chefranov 方案的用户登录认证过程
Figure 5 The user login authentication process of Chefranov scheme

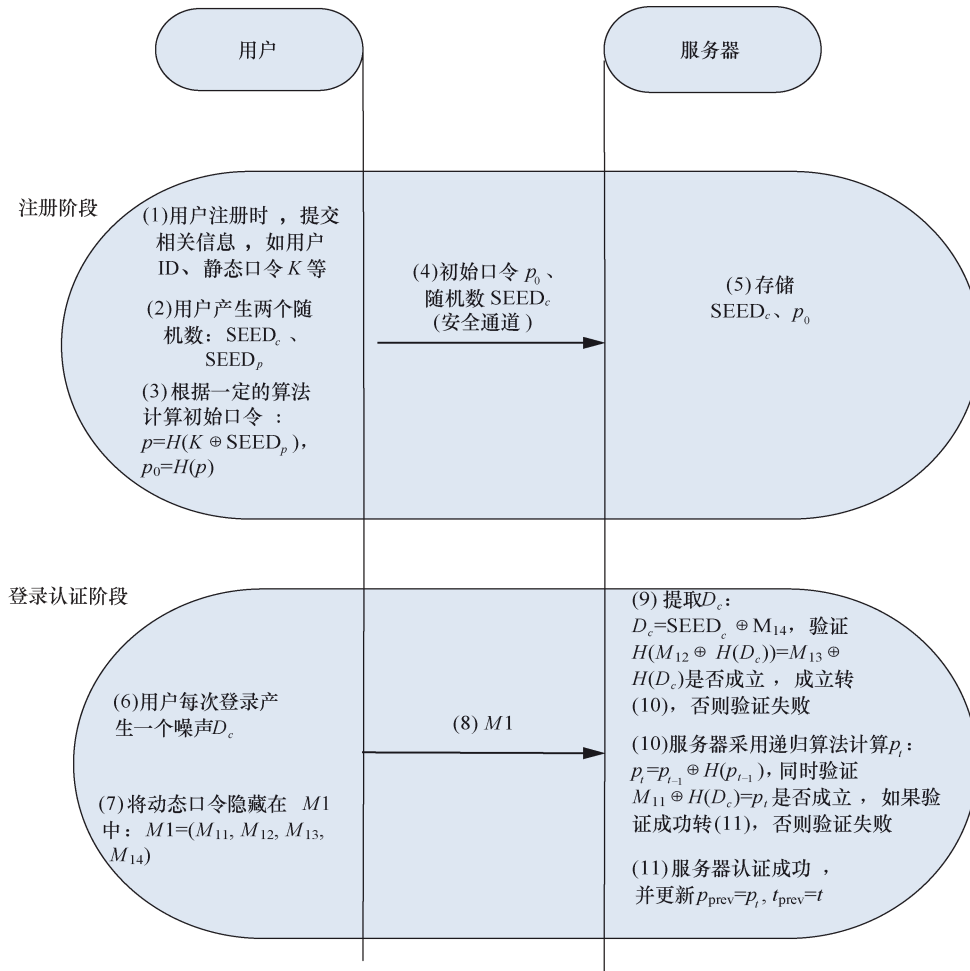


图6 用户注册和登录认证

Figure 6 The user registration and login authentication

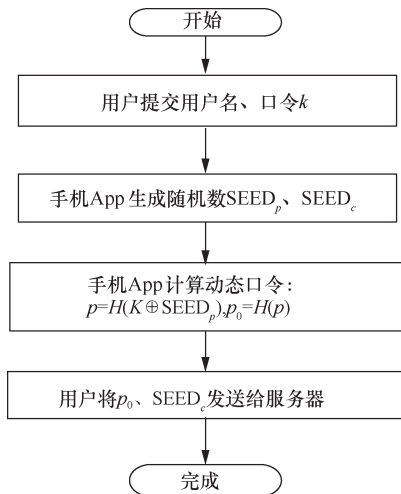


图7 用户注册流程

Figure 7 The flow chart of user registration

1) 用户提交相关信息，如用户 ID、静态口令 K 等。

2) 用户产生两个随机数 $SEED_p$ 、 $SEED_c$ ，其中，随机函数的生成方式为均匀随机地选择 $S_1, S_2 \leftarrow (0,1)^n$ ，计算 $SEED_p = H(S_1, k)$ ， $SEED_c = H(S_2, k)$ ，之后安全删除 S_1, S_2 。

3) 用户根据静态口令 K 和随机生成的 $SEED_p$ ，生成初始口令 p_0 ： $p = H(K \oplus SEED_p)$ ， $p_0 = H(p)$ 。

4) 用户将 $SEED_c$ 和 p_0 在一个安全的通道中发送给服务器。

5) 服务器接收并存储用户发送过来的初始口令 p_0 和随机数 $SEED_c$ ，并把 p_0 记作 p_{prev} 。

3.1.2 登录认证阶段

用户登录过程如图 8 所示，用户随机产生一个噪声，用于加密发送的动态口令；服务器接收用户发送过来的消息，使用存储在本地

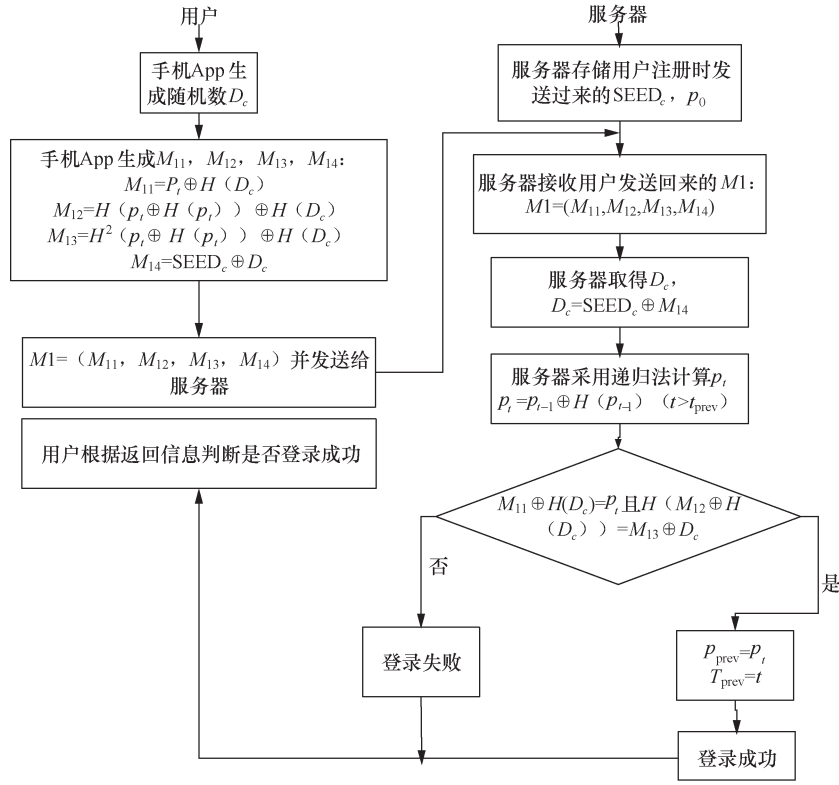


图8 用户登录过程

Figure 8 The login process of user

提取用户产生的噪声, 然后检验消息在传输过程中是否被攻击者篡改。如果验证通过, 服务器将从消息中提取出的动态口令和服务器本地采用与时间相关的算法计算出来的动态口令进行比较, 口令一致则服务器认证成功, 否则认证失败。图9显示了动态口令的验证过程和服务器验证值的更新

新过程。具体登录认证过程如下。

1) 用户每次登录都会随机产生一个噪声 D_c , 噪声 D_c 产生的公式为均匀随机地选择 $r \leftarrow (0,1)^n$, 计算 $D_c = H^2(i, r)$, 其中 i 是用户登录的次数。

2) 用户使用哈希函数、异或操作和噪声 D_c

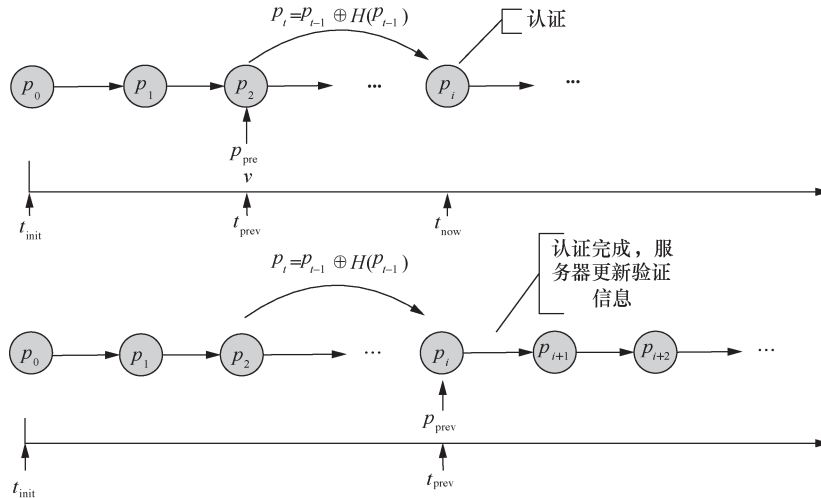


图9 动态口令的验证过程和服务器验证值的更新

Figure 9 Verification process of one-time password and update of server authentication value

隐藏动态口令 p_t , 加密方法为 $M1=(M_{11}, M_{12}, M_{13}, M_{14})$, 其中 $\{M_{11}=p_t \oplus H(D_c), M_{12}=H(p_t \oplus H(p_t)) \oplus H(D_c), M_{13}=H^2(p_t \oplus H(p_t)) \oplus H(D_c)\}, M_{14}=\text{SEED}_c \oplus (D_c)$ 。

3) 用户将 $M1$ 发送给服务器。

4) 服务器接收用户发送过来的 $M1$, 首先使用存储在本地的 SEED_c 获取用户产生的噪声 D_c : ($D_c=\text{SEED}_c \oplus M_{14}$), 同时验证 $H(M_{12} \oplus H(D_c))=M_{13} \oplus H(D_c)$ 是否成立, 如果等式不成立, 则认为该消息在传送中已遭受攻击者恶意更改, 停止认证; 否则继续认证。

5) 服务器使用递归算法计算 p_t : $p_t = p_{t-1} \oplus H(p_{t-1}), t > t_{\text{prev}}$, 验证 $M_{11} \oplus H(D_c) = p_t$ 是否成立, 如果成立, 认证成功, 并更新服务器验证信息 $p_{\text{prev}} = p_t, t_{\text{prev}} = t$, 否则认证失败。

3.2 安全性分析

3.2.1 重放攻击

OTP 方案的实施需要满足两个安全要求。首先, 传送消息的双方之间需要建立一个安全可靠的通道, 因此 OTP 方案通常使用 SSL/TLS 通道。SSL/TLS (secure socket layer /transport layer security) 的使用意味着用户和服务器之间交换消息的完整性得到了保证, 在服务器接收到发送过来的消息时, 服务器可以确定这个消息来自用户, 即在消息传递的过程中攻击者不能篡改消息, 反之亦然。如果不满足这个安全要求, 攻击者可以对 Lamport 的 OTP 发起中间人攻击。其次, 服务器在验证动态口令时, 需要保证 OTP 的完整性。因此, 可以假设服务器从用户接收到的 OTP 在服务器的防篡改模块 (TRM) 中处理。在该模块中, 它保证了在服务器认证用户过程中 OTP 的值不会被篡改。

重放攻击是指攻击者为了欺骗用户让其接受自己的请求, 发送给目的主机一个已经被目的主机接受过的包。OTP 的两个安全要求中的第一个要求, 仅保证消息在用户和服务器之间不会被篡改, 但可以偷窥到用户发送给服务器的动态口令, 在满足上述两个安全要求的基础之上, 本文提出的 OTP 攻击模型是这样的: 攻击者可以偷窥到用户和服务器所交换的消息, 但不能通过正常认证的信道传递来修改它们的值。

定理 1 在上述攻击模型条件下, 攻击者不可能发送一个已发送的动态口令来欺骗服务器。

证明 假设攻击者偷窥到的第 i 次用户向服务器发送的动态口令 OTP 为 $M1=(M_{11}, M_{12}, M_{13}, M_{14})=\{p_t \oplus H(D_c), H(p_t \oplus H(p_t)) \oplus H(D_c), H^2(p_t \oplus H(p_t)) \oplus H(D_c), \text{SEED}_c \oplus D_c\}$, 攻击者记录此次的动态口令并模仿用户, 再次将 $M1$ 发送给服务器, 当服务器接收到攻击者假扮用户给予的动态口令时, 首先用存储在本地的 SEED_c 获取随机数 D_c , 同时验证 $H(M_{12} \oplus H(D_c))=M_{13} \oplus H(D_c)$ 是否成立, 因为攻击者是将刚刚发送过的动态口令再一次发送给服务器, 因此 $H(M_{12} \oplus H(D_c))=M_{13} \oplus H(D_c)$ 一定成立; 接着, 服务器使用递归算法计算 $p'_t=p_{t-1} \oplus H(p_{t-1})$, 由于攻击者是在用户发送动态口令 $M1$ 以后偷窥到 $M1$, 进而假扮用户再一次发送 $M1$ 给服务器, 所以此时的时间 $t' \neq t$, 那么 p'_t 也一定和 p_t 不一样, 所以经受得住重放攻击。

3.2.2 伪造攻击

OTP 方案实施的两个安全要求中的第一个要求: 双方之间需要具备一个安全可靠的通道, 该通道满足即使攻击者有机会偷窥到用户发送给服务器的动态口令, 也无法修改动态口令的值。通常使用 SSL/TLS 通道来满足这个要求。但在现实生活中, SSL/TLS 已经不再是安全可靠的, 2013 年, Meyer^[17]提出了针对 SSL/TLS 的攻击模型, 可以成功地拦截用户发送的动态口令并且修改拦截的动态口令, 然后模仿用户发送给服务器以达到伪造一个可以被服务器接受的动态口令的目的。此时, 本文提出的 OTP 攻击模型是这样的: 攻击者可以访问用户和服务器所交换的消息, 并且能通过正常认证的信道传递来拦截并修改它们。假设在攻击者偷窥到许多个动态口令后, 发现了一些动态口令的规律, 在这些规律的前提下, 攻击者是否可以伪造出被用户接受的下一个 OTP?

定理 2 在上述攻击模型条件下, 攻击者不可能伪造出被服务器接受的 OTP 的值。

证明 假设攻击者可以多次偷窥到用户和服务器所交换的消息, 并且通过多次对比动态口令发现, 用户每次发送的 $M1=(M_{11}, M_{12}, M_{13}, M_{14})$ 中的 M_{12}, M_{13} 仅用来验证消息传送中是否有攻击

者对消息进行拦截并做出修改,只要 OTP 满足 $H(M_{12} \oplus H(D_c)) = M_{13} \oplus H(D_c)$, 服务器就认为动态口令在传送的过程中没有被攻击者篡改,所以攻击者可以反复使用 M_{12}, M_{13} 。同理, M_{14} 用来获取用户发送的随机数,由于服务器也不知道用户每次发送的随机数是什么,所以 M_{14} 可以重复使用,接下来攻击者将 M_1 修改为 $M'_1 = (M'_{11}, M_{12}, M_{13}, M_{14}) = \{p_i \oplus H(D'_c), H(p_i \oplus H(p_i)) \oplus H(D_c), H^2(p_i \oplus H(p_i)) \oplus H(D_c), SEED_c + D_c\}$, 当攻击者将 M'_1 成功地发送给服务器后,服务器首先用存储在本地的 $SEED_c$ 获取随机数 D_c , 同时验证 $H(M_{12} \oplus H(D_c)) = M_{13} \oplus H(D_c)$ 是否成立,因为攻击者仅将 M_{11} 修改为 M'_{11} , 因此 $H(M_{12} \oplus H(D_c)) = M_{13} \oplus H(D_c)$ 一定成立;接着,服务器使用递归算法计算 $p'_i = p_{i-1} \oplus H(p_{i-1})$, 如果想要让服务器验证通过,则 $p_i \oplus H(D'_c) = p'_i$, 即 $H(D'_c) = p'_i \oplus p_i$, 如果攻击者想要让服务器接收自己伪造的动态口令,则必须找到这样的 D'_c , 使 $H(D'_c) = p'_i \oplus p_i$ 成立。但是,根据哈希函数的不可逆性可知,即使在已知哈希函数 H 以及哈希函数映射的哈希值 y 的情况下,也无法找到其中的 x , 使 $H(x)=y$ 成立。因此,想要找到这样的 D'_c 使 $H(D'_c) = p'_i \oplus p_i$ 成立是不现实的。

3.2.3 小数目攻击

小数目攻击通常发生在后退式哈希链中。攻击者假扮服务器向用户发送一个小数字,如 10, 用户向攻击者发送 $H^{10}(x)$ 。这样,攻击者就可以轻松地计算出没有使用过的一系列动态口令,从而伪装成用户。本文使用前向哈希链,不需要服务器向用户发送挑战,所以不存在小数目攻击。

4 方案的实施

本文使用用户到服务器的单向通信取代用户到服务器的双向通信方式,使用户即使处于不在线状态,认证依然可以完成。根据本文提出的方案,使用手机 App 以二维码的方式产生动态口令,手机 App 每隔 1 min 就会随机产生一个动态口令二维码。本文使用 Windows10 系统作为软件的开发环境,使用 Android Studio 作为软件的开发工具,使用具有摄像功能的台式机作为服务器来实现所提方案。服务器通过摄像头扫描手机 App 产

生的二维码,获得用户的动态口令;同时,服务器使用递归算法计算动态口令,如果服务器使用递归算法计算出来的动态口令和用户发送过来的动态口令一致,则认证成功,否则认证失败。

本文仅需要用户到服务器的单向交流,不要用户返回任何消息,手机 App 仅需提供动态口令的二维码。由于二维码不需要在网络上传播,因此,用户的手机是可以没有网络的。手机二维码每隔 1 min 更新一次,这意味着每个动态口令的使用寿命仅有 1 min, 1 min 之后动态口令便会失效。生活中已经使用了和此类功能相似的软件,如微信支付的二维码是可以实现离线付款的,并且付款的二维码只在比较短的时间内有效。所以,本文方案在技术实施上具有可行性。

本文提出的动态口令方案在用户和服务器双方都设置了时钟,关于时钟同步性的问题,本文允许一个合理的滑动窗口的存在,只要在窗口值范围内,就认为动态口令是合法的。目前正在流行的支付宝离线支付,同步用户和服务器双方的方法就是通过设置一个合理的滑动窗口值来实现的,支付宝离线支付功能的使用验证了同步双方不再是难题。因此,关于具体的同步用户和服务器双方的问题,具体实现细节不加以细述。

5 相关方案比较

本节对 Lamport 提议的 OTP、Chefranov 提议的 OTP 以及本文提议的 OTP 在通信方式、是否需要用户重新注册等方面进行了比较,相关方案的比较结果如表 1 所示。其中,关于通信方式, Lamport 方案和 Chefranov 方案都采用用户到服务器的双向通信模式,无法实现离线认证;本文采用用户到服务器的单向通信模式,不需要服务器给予用户应答,同时,采用手机二维码方式产生动态口令,仅需要使用带有扫码功能的服务器扫描手机二维码即可完成登录功能,无须用户时刻保持在线状态,即使用户因为各种原因造成手机无法联网,如地处偏僻、手机停机等,认证仍然可以完成。关于无须重注册, Lamport 方案采用后退式哈希链,哈希链长度固定,产生的动态口令个数有限,一旦动态口令使用完毕,则需要用户重新注册; Chefranov 方案和本文方案采用前向哈希链取代后退式哈希链,认证次数不受限制,因此无

须用户重新注册。关于口令具有时效性，Lamport 方案和 Chefranov 方案的动态口令的有效时长取决于用户两次登录的时间间隔，本文方案无论用户是否登录，动态口令的有效时长都仅有 1 min。

表 1 相关方案比较
Table 1 Comparison of relevant schemes

方案	单向通信	无须重注册	口令具有时效性
Lamport	×	×	×
Chefranov	×	✓	×
本文方案	✓	✓	✓

6 结束语

本文基于前向哈希链结合 TOTP 算法设计了一种无须重注册的单向通信动态口令认证方案，利用手机 App 以二维码的方式生成动态口令，提高了可用性，给出了安全性分析。但是，如何尽可能地减少由于用户两次登录的时间间隔过长而导致的用户和服务器哈希值的计算量有待进一步地研究。

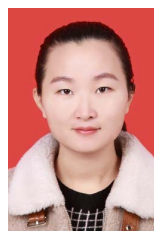
参考文献：

- [1] M'RAIHI D, MACHANI S, PEI M, et al. TOTP: time-based one-time password algorithm[R]. 2011.
- [2] HALLER N. The s/key one-time password system[C]//Proceedings of the Internet Society Symposium on Network and Distributed Systems. 1995: 151-157.
- [3] ZHOU Z C, LI L X, GUO S. Biometric and password two-factor cross domain authentication scheme based on blockchain technology[J]. Journal of Computer Applications, 2018, (6).
- [4] PRAKASH S, NITESH S. Listening watch: wearable two-factor authentication using speech signals resilient to near-far attacks[R]. 2018.
- [5] RAIHI D M, BELLARE M, HOORNAERT F, et al. HOTP: an HMAC-based one-time password algorithm[S]. 2005
- [6] 刘知贵, 臧爱军, 陆荣杰, 等. 基于事件同步及异步的动态口令身份认证技术研究[J]. 计算机应用研究, 2006, 23(6): 133-134.
- [7] LIU Z G, ZANG A J, LU R J, et al. Dynamic password authentication based on event-synchronous and challenge/response technology[J]. Application Research of Computers, 2006, 23(6): 133-134.
- [8] AWASTHI A K. Comment on a dynamic d-based remote user authentication scheme[J]. Transaction on Cryptology, 2004, 1(2): 15-16
- [9] DAS M L, SAXENA A, GULATI V P. A dynamic ID-based remote user authentication scheme[J]. IEEE Transactions on Con-

sumer Electronics, 2004, 50(2): 629-631.

- [9] GOYAL V, ABRAHAM A, SANYAL S, et al. The N/R one time password system[C]//International Conference on Information Technology: Coding and Computing. 2005: 733-738.
- [10] GONG L, PAN J, LIU B, et al. A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords[J]. Journal of Computer and System Sciences, 2013, 79(1): 122-130.
- [11] PARK C S. One-time password based on hash chain without shared secret and re-registration[J]. Computers & Security, 2018, 75.
- [12] KOGAN D, MANOHAR N, DAN B. T/Key: second-factor authentication from secure Hash chains[R]. 2017.
- [13] HWANG, SHEN H Y, HWANG J J. A secure one-time password authentication scheme using smart cards[J]. IEICE Trans Commun, 2002, 85(11): 2515-2518.
- [14] CHEFRANOV A G. One-time password authentication with infinite Hash chains[M]. Berlin: Springer Netherlands, 2008.
- [15] LAMPORT L. Password authentication with insecure communication[J]. Communications of the ACM, 1981, 24(24): 770-772.
- [16] MEYER C, SCHWENK J. Lessons learned from previous SSL/TLS attacks – a brief chronology of attacks and weaknesses[J]. IACR Cryptology ePrint Archive, 2013.

[作者简介]



鲁迁迁（1993—），女，江苏徐州人，南京航空航天大学硕士生，主要研究方向为信息安全。



朱友文（1986—），男，安徽阜南人，南京航空航天大学副教授，主要研究方向为信息安全。



蒋炎（1992—），男，湖北仙桃人，南京航空航天大学博士生，主要研究方向为信息安全。