

Provable Secure Mobile User Authentication with Anonymity for the Global Mobility Network

Huizhi Li, Guangguo Han[†], Yi Wang

College of Science, Hangzhou Dianzi University, Hangzhou Zhejiang 310018, China

[†]Email: hangg@hdu.edu.cn

Abstract

Seamless roaming in the global mobility network (GLOMONET) is highly desirable for mobile users, although the proper authentication is challenging. This is because not only are wireless networks susceptible to be attacked, but also mobile terminals have limited computational power. Recently, some authentication schemes with anonymity for the GLOMONET have been proposed. The main contribution of this article is an improvement on the schemes before, it proposes a user authentication scheme based on smart cards, requires between user and two agents are four exchanges of information, and security analysis has proved that the scheme can resist various attacks. Compared with the schemes before, this scheme is simpler and has lower computation.

Keywords: Global Mobility Network; Security; Foreign Agent

全球移动网络中可证安全的匿名用户验证方案*

李慧智, 韩广国[†], 王沂

杭州电子科技大学 理学院, 浙江 杭州 310018

摘要: 在全球移动网络(GLOMONET)中, 无缝漫游对用户来说是非常可取的。但由于无线网路易被攻击及移动终端具有有限的计算能力, 所以对移动用户的安全认证是具有挑战的。近来, 一些基于安全认证的智能卡方案被提出。文章的主要贡献是通过对已有方案的改进, 提出了一个基于智能卡的身份验证方案。方案采用离散对数函数加密, 且只需要在用户、外地代理和家庭代理之间进行 4 次信息交换。最后证明了方案可以抵制多种攻击。相比已有方案, 本方案具有简便和计算量少的优点。

关键词: 全球移动网络; 安全; 外地代理

引言

作为信息安全关键技术密码学, 近年来空前活跃, 美、欧、亚各洲举行的密码学和信息安全学术会议频繁。1976 年美国学者提出的公开密钥密码体制, 克服了网络信息系统密钥管理的困难, 同时解决了数字签名问题, 它是当前研究的热点。安全协议可用于保障计算机网络信息系统中秘密信息的安全传递与处理, 确保网络用户能够安全、方便、透明地使用系统中的密码资源, 因此安全协议亦是当前研究的重点。随着全球移动网络 (GLOMONET) (比方说 4G 和 5G 移动通讯网络) 的迅猛发展, 安全协议在金融系统、商务系统、政务系统、军事系统和社会生活中的应用日益普遍。但是, 网络给人们生活、工作带来便捷的同时, 也增加了信息的不安全性。一些不法分子利用网络非法侵入他人的计算机系统窃取机密信息、篡改和破坏数据, 网络安全问题越来越引起人们的重视。众所周知, 移动用户漫游至外部代理管辖区域时可以获得由

*基金资助: 受国家自然科学基金(11471123), 浙江省自然科学基金(LY12A01004)支持资助。

外部代理提供的服务。显然，在提供服务之前，为了确保安全，必须验证用户的合法身份。近来，一些基于安全认证的智能卡方案被提出。但现有方案大都采用 RSA 加密或数字签名加密体制，轮换较多，且计算复杂。本文在总结其他学者安全协议的基础上，提出了一个改进的安全并匿名的用户认证方案。相比已有方案，本方案具有很多优点。首先，由于方案只采用离散对数加密和哈希函数，使得所有参与方容易执行。其次，它在用户和访问网络之间，访问网络和家庭网络之间采用简单的单次认证。最后，方案能抵制离线口令猜测攻击，已知密钥攻击，模仿攻击，重放攻击等，具有很强的安全性，能更好的运用于实际生活。

1 离散对数加密原理

第一个离散对数体制是 Diffie 和 Hellman 于 1976 年提出的。1984 年，ElGamal 提出了离散对数公钥加密方案和离散对数公钥签名方案。此后，人们相继提出了离散对数公钥密码的各种变体，下面我们将介绍基本 ElGamal 公钥加密方案。

在离散对数体制中，密钥对是与公开参数组 (p, q, g) 联系在一起的。其中 p 是素数， q 是 $p-1$ 的素因子， $g \in [1, p-1]$ ， g 的阶为 q ，即 $t=q$ 是满足 $g^t \equiv 1 \pmod p$ 的最小正整数。私钥 x 是从区间 $[1, q-1]$ 内随机选择一个整数，而相应的公钥是 $y = g^x \pmod p$ ，对于给定的参数组 (p, q, g) 和 y ，确定 x 是离散对数问题(DLP)。

(1) 加密：当实体 A 想要发送信息 m ，先选择 $k \in_R [1, q-1]$ ，计算 $C_1 = g^k \pmod p$ ， $C_2 = my^k \pmod p$ ，并把 C_1, C_2 发送给实体 B。

(2) 当实体 B 收到 C_1, C_2 时，根据私钥 x ，计算 $C_2 C_1^{-x} \pmod p = my^k g^{-kx} \pmod p = mg^{kx} g^{-kx} \pmod p = m$ ，得到信息 m 。

攻击者要恢复出信息 m ，必须计算 $y^k \pmod p$ 。根据参数组 (p, q, g) ， y 和 $C_1 = g^k \pmod p$ 计算 $y^k \pmod p$ 被称为 Diffie-Hellman 问题(DHP)。DHP 被认为与离散对数问题一样困难。

2 改进的方案

在这部分，我们将给出一个轻便又安全的用户认证方案。协议分为五个部分：注册阶段、登陆阶段、认证阶段、密钥更新阶段和口令改变阶段。在接下来的方案描述中，我们假设情境：有一个移动用户 MU 与他的家庭代理 HA 相连，正在访问外部网络 FA。假设每个外部代理都与 HA 共享长期密钥 K_{FH} ， FA_i 与 HA 之间的所有密钥 K_{FH_i} 是不同的，需要一个安全基站来储存这些密钥。

2.1 注册阶段

在这个阶段，移动用户 MU 自由地选择一个口令 PW_{MU} 和随机数 b ，计算 $h(PW_{MU} \oplus b)$ ，MU 通过安全信道把 ID_{MU} ， $h(PW_{MU} \oplus b)$ 发送给 HA，这里 ID_{MU} 的长度为 128 比特，接着 HA 执行以下操作：

(1) 计算 $V_1 = h(ID_{MU} // h(PW_{MU} \oplus b))$ 。

(2) 选择素数 p 和 q ， q 是 $p-1$ 的素因子， $g \in [1, p-1]$ ，其中 $g^q \equiv 1 \pmod p$ ，选择一个随机数 x ，且 $x \in_R [1, q-1]$ ， $y = g^x \pmod p$ 。

(3) 生成一张智能卡，里面包括 $\{h(\cdot), y, p, q, g, V_1\}$ ，并通过安全信道把智能卡发送给 MU。

接收到智能卡后，MU 在智能卡中输入 b ，最后智能卡中包括 $\{h(\cdot), y, p, q, g, V_1, b\}$ 。

2.2 登陆阶段

当 MU 漫游进外部网络时，FA 在提供服务前先通过 HA 验证 MU。认证过程中，MU 把智能卡插入设备，输入 ID_{MU} 和 PW_{MU} ，智能卡执行以下操作：

(1) 计算 $V_1^* = h(ID_{MU} // h(PW_{MU} \oplus b))$ ，验证 V_1^* 是否等于 V_1 。如果相等，用户的合法性得到验证，进行下一步操作；否则，拒绝登陆请求。

(2) 产生随机数 $x_0 \in [0, p-1]$ ，随机整数 k ，计算 $C_1 = g^k \pmod p, C_2 = x_0 y^k \pmod p$ ，

$PID_{MU} = (ID_{HA} \oplus ID_{MU})_{x_0}$, $V_2 = h(x_0 // ID_{MU} // ID_{FA} // T_{MU})$ 。

(3) 把消息 $M_1 = \{C_1, C_2, PID_{MU}, V_2, T_{MU}\}$ 发送给 FA。

2.3 认证阶段

当收到消息 M_1 时, FA 执行以下操作:

(1) 检验 T_{MU} 。

(2) 计算 $V_3 = h(K_{FH} // ID_{FA} // T_{FA} // T_{MU})$, 发送 $M_2 = \{M_1, V_3, ID_{FA}, T_{FA}, T_{MU}\}$ 给 HA。

当收到消息 M_2 时, HA 执行以下操作:

(1) 检验 T_{FA} 。

(2) 计算 $V_3^* = h(K_{FH} // ID_{FA} // T_{FA} // T_{MU})$, 检验 V_3^* 是否等于 V_3 。如果相等, FA 的合法性得到确认, 继续下一步操作; 否则停止操作。

(3) 计算 $x_0 = C_2 C_1^{-x} \bmod p$ 。

(4) 用 x_0 解密 PID_{MU} 得到 ID_{MU} , 接着计算 $V_2^* = h(x_0 // ID_{MU} // ID_{FA} // T_{MU})$, 并检验 V_2^* 是否等于 V_2 。如果相等, 则执行下一步操作; 否则, 停止。

(5) 计算 $V_4 = (x_0 // h(ID_{MU} // ID_{FA}) // T_{HA})_{K_{FH}}$ 。

(6) 把 $M_3 = \{V_4, T_{HA}\}$ 发送给 FA。

当收到消息 M_3 时, FA 执行以下操作:

(1) 检验 T_{HA} , 用密钥 K_{FH} 解密 V_4 , 得到 $x_0, h(ID_{MU} // ID_{FA}), T_{HA}$ 。

(2) 计算 $SK = h(h(x_0) // h(ID_{MU} // ID_{FA})), V_5 = (h(x_0) // ID_{FA})_{SK}$ 。

(3) 把 $M_4 = V_5$ 发送给 MU。

收到 M_4 时, MU 执行以下操作:

(1) 计算 $SK = h(h(x_0) // h(ID_{MU} // ID_{FA}))$ 。

(2) 解密 V_5 得到 $h^*(x_0)$, ID_{FA} 。检验 $h^*(x_0)$ 是否等于 $h(x_0)$ 。如果相等, 则 FA 的身份得到验证, MU 以 SK 作为合法的会话密钥。

2.4 密钥更新阶段

为了保证高效性和强安全性, 当 MU 经常访问 FA 时, 密钥需要进行周期性更新, 过程如下:

在认证阶段和密钥建立之后, FA 通过发送 $(Tcert_{MU})_{SK}$ 传递 MU 的临时证书 $Tcert_{MU}$ 。当 MU 和 FA 进行第 i 次会话时, MU 发送 $\{Tcert_{MU}, (n_i // Tcert_{MU} // other\ information)_{SK_i}\}$ 给 FA, 这里 $SK_i = h(n_{i-1} // h(ID_{MU} // ID_{FA})), (i = 1, 2, 3, \dots, n_0 = h(x_0))$ 。当收到从 MU 发送的消息时, FA 检验 $Tcert_{MU}$ 是否有效。如果有效, FA 解密

$(n_i // Tcert_{MU} // other\ information)_{SK_i}$

得到 n_i , 并保存 n_i 以待下一次通信。

2.5 口令改变阶段

这个阶段只有在 MU 需要改变他的口令时才启动, 描述如下:

(1) MU 把智能卡插入设备, 输入 $\{ID_{MU}, PW_{MU}\}$, 然后请求更改口令。

(2) 收到更改口令请求和 $\{ID_{MU}, PW_{MU}\}$ 后, MU 的智能卡计算

$V_1^* = h(ID_{MU} // h(PW_{MU} \oplus b))$

检验是否等于 V_1 。如果相等, MU 的合法性得到确认, 执行下一步; 否则, 拒绝更改口令请求。

(3) MU 选择新口令 PW_{new} 和随机数 b_{new} , 计算 $h(PW_{new} \oplus b_{new})$, 接着计算

$V_1^* = h(ID_{MU} // h(PW_{new} \oplus b_{new}))$

MU 用 V_1^* 取代 V_1 。最后，MU 的智能卡里包括 $\{h(\cdot), y, p, q, g, V_1^*, b_{new}\}$ 。

3 安全性分析

3.1 抵抗可能的攻击

3.1.1 离线口令猜测攻击

任何密钥协商协议中，口令猜测攻击都是非常重大的问题。但是我们的方案没有口令表，用户的口令在登陆和认证阶段也不传送。此外，用户的口令也只在 $V_1 = h(ID_{MU} // h(PW_{MU} \oplus b))$ 中存在。显然，敌手在不知道 ID_{MU}, b 的情况下不可能猜测出口令 PW_{MU} 。因此，我们的方案能抵制口令猜测攻击。

3.1.2 已知密钥攻击

能够抵制已知密钥攻击是指即使敌手知道了其他会话密钥，协议依然能够实现。我们的方案在每次会话时使用短暂的随机数 x_i ，而随机数在每次会话中都是随机和独立的。因此，会话密钥 $SK = h(h(x_0) // h(ID_{MU} // ID_{FA}))$ 也是独立的。所以，以前的会话密钥并不能帮助取得新的会话密钥。因此，方案能抵抗已知密钥。

3.1.3 模仿攻击

1 敌手无法模仿 HA 来欺骗 FA，因为敌手不知道 K_{FH} ，它也不可能产生有效的回应 M_3 给 FA。2 敌手无法模仿 FA 来欺骗 MU，敌手不知道 x_0 ，不可能产生 $SK = h(h(x_0) // h(ID_{MU} // ID_{FA}))$ ，然后发送有效信息给 MU。3 敌手无法模仿 MU 欺骗 FA，因为 MU 的口令通过 $h(pw_{MU} \oplus b)$ 发送，所以敌手不可能获得 MU 的口令，无法通过验证。

3.1.4 重放攻击

重放攻击是指敌手得到以前的通讯信息，再重新发送给认证服务器。敌手能收集 MU 和 FA 间传递的消息 $\{M_1, M_2, M_3, M_4\}$ ，也可以重新发送 $M_1 = \{C_1, C_2, ID_{MU}, V_2, T_{MU}\}$ ，然后收到回复信息 $\{M_2^*, M_3^*, M_4^*\}$ 。然而敌手不知道 $h(x_0)$ ，不能计算出会话密钥 $SK = h(h(x_0) // h(ID_{FA} // ID_{MU}))$ ，所以敌手不能取得 FA 的服务。况且，我们设置了时间戳，假如敌手修改了时间戳 T_{MU} 后重放，由于 $V_2 = h(x_0 // ID_{MU} // ID_{FA} // T_{MU})$ ，敌手还是无法通过 FA 的验证。所以，我们的协议能抵制重放攻击。

3.1.5 内部攻击

内部攻击是指任何系统的管理层故意泄露秘密信息导致了协议的安全漏洞。在我们的方案中，如果家庭代理 HA 的内部人员获得了 MU 的口令 PW_{MU} ，他就能模仿用户登录外部代理。但是，在协议的注册阶段，MU 仅仅发送了 ID_{MU} 和 $h(PW_{MU} \oplus b)$ 给 HA，也就是说， PW_{MU} 没有暴露给 HA。此外，在口令更改阶段需要定时更改口令。既然内部人员不能得到用户的口令，所以方案能抵制内部攻击。

3.2 一些其它的安全性能

3.2.1 用户匿名性

在我们的方案中，只有 HA 能得到 MU 真正的身份 ID_{MU} 。HA 通过解密得到 x_0 ，接着解密 $PID_{MU} (= (ID_{HA} \oplus ID_{MU})_{x_0})$ 得到 ID_{MU} 。由于敌手不可能得到 x_0 ，所以无法得到 ID_{MU} 。因此，我们的方案能保证用户匿名性。

3.2.2 后向保密

后向保密性保证了被动的敌手在掌握了组密钥的一个子集之后不能发现前组密钥。在我们的方案中

$h(ID_{MU} // ID_{FA})$ 在每次会话中都是固定的。如果敌手知道了 SK_i, SK_{i+1} , 敌手能用 SK_i 解密 $(n_i // TCert_{MU} // other\ information)_{SK_i}$ 得到 n_i 。然而 SK_{i+1} 是哈希函数的输出值, 因此获得 $h(ID_{MU} // ID_{FA})$ 是困难的。所以, 即使敌手知道了 $\{n_i, n_{i+1}\}$, 敌手也不可能得到 $h(ID_{MU} // ID_{FA})$ 。然而, 得不到 $h(ID_{MU} // ID_{FA})$, 敌手就不可能得出 $SK_{i-1}(= h(n_{i-2} // h(ID_{MU} // ID_{FA})))$ 。因此, 我们的方案能达到后向保密性。

3.2.3 前向保密

前向保密是指敌手在获得一组旧的密钥子集却不能发现后续组密钥。在本方案中, 对于每一个会话密钥中 $h(ID_{FA} // ID_{MU})$ 是固定的, 如果敌手知道了 SK_{i-1}, SK_i , 敌手通过用已知的 SK_{i-1} 解密传送的消息 $(n_{i-1} // TCert_{MU} // Other\ infomation)_{SK_{i-1}}$ 而获得 n_{i-1} 。然而, SK_i 是一个哈希函数的输出值, 因此, 想要获得 $h(ID_{FA} // ID_{MU})$ 是困难的, 也就是说, 即使掌握了 n_{i-1} , 敌手也将无法获得 $h(ID_{FA} // ID_{MU})$ 。因此敌手在不了解 $h(ID_{FA} // ID_{MU})$ 的情况下不能计算出后续的会话密钥 $SK_{i+1}(= h(n_i // h(ID_{MU} // ID_{FA})))$ 。故本方案能够达到前向保密性。

4 结语

文章提出了一个基于智能卡的用户验证方案, 它只需要在用户、外地代理和家庭代理之间进行 4 次信息的交换, 因此, 更适合想节能的移动用户使用。方案采用离散对数函数加密, 减少了计算量, 并已证明了可以抵制多种攻击。相比[1]中方案, 本方案具有简便和计算量少的优点。

致谢

非常感谢导师在写作过程中对我的悉心指导, 感谢编辑和审稿人对论文早期版本的建设性意见, 使我受益很大。最后, 感谢国家自然科学基金(11471123), 浙江省自然科学基金(LY12A01004)支持资助。

REFERENCES

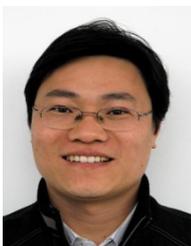
- [1] Chun chen, Daojing He, Sammy Chan, et al. Lightweight and provably secure user authentication with anonymity for the global mobility network[J]. Commun. Syst, 2011, 16(6): 347-362
- [2] Chenchi Lee, Minshiang Hwang, Ien Liao. Security enhancement on a new authentication scheme with anonymity for wireless environments[J]. IEEE Transactions on Consumer Electronics, 2006, 53(5): 1683-1687
- [3] Peng Zeng, Zhenfu Cao, Kimkwang Choo. On the anonymity of some authentication schemes for wireless communications[J]. IEEE Communications Letters, 2009, 13(3): 170-171
- [4] Daojing He, Chun Chen, Sammy Chan, et al. Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions[J]. IEEE Transactions on Consumer Electronics, 2012, 11(1): 48-53
- [5] Daojing He, Yi Gao, Sammy Chan, et al. An enhanced two-factor user authentication scheme in wireless sensor networks[J]. OCP Science, 2010, 31(7): 1-11
- [6] Chiachun Wu, Weibin Lee. A secure authentication scheme with anonymity for wireless communications[J]. IEE Communications Letters, 2008, 12(10): 722-723
- [7] Daojing He, sammy Chan, Chun Chen, et al. Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks[J]. Springer science, 2010, 25(5): 465-476
- [8] Daojing He, Sammy Chan. A Secure and Lightweight User Authentication Scheme with Anonymity for the Global Mobility Network[J]. Network-Based Information Systems. 2010, 9(10): 305-312
- [9] Huixian Li, Yafang Yang, Liaojun Pang. An Efficient Authentication Protocol with user anonymity for mobile networks[J]. IEEE Wireless Communications and Networking Conference, 2013, 13(9): 1842-1847
- [10] Arshad R, Ikram N. Elliptic curve cryptography based mutual authentication scheme for session initiation protocol. Multimed

- [11] Dawei Zhao, Haipeng Peng, Lixiang Li, Yixian Yang. A secure and effective anonymous authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications*, 2014, 78(1), 247-269
- [12] Minsu park, Hyunsung Kim, Sung Woon Lee. Privacy preserving biometric-based user authentication protocol using smart cards[J]. *IEEE International Conference on Computational Science and Engineering*, 2014, 14(3): 1541-1544

【作者简介】



¹ 李慧智 (1989-), 女, 汉族, 在读研究生, 代数及其应用, 学习经历: 2009年9月到2013年7月在衡阳师范学院数学系学习, 并获得学士学位; 2013年9月至今, 在杭州电子科技大学理学院攻读硕士。Email: 1296525554@qq.com



² 韩广国 (1972-), 男, 汉族, 博士, 教授, 研究方向: 群与组合结构、代数几何和密码学。学习经历: 1989年9月到1993年7月在山东师范大学数学系

学习, 并获得学士学位; 1993年9月到1996年7月在曲阜师范大学数学系攻读硕士, 并获得硕士学位; 2000年2月到2003年4月在浙江大学数学系攻读博士, 并获得博士学位。

Email: hangg@hdu.edu.cn



³ 王沂 (1991-), 女, 汉族, 在读研究生, 代数及其应用, 学习经历: 2009年9月到2013年7月在咸阳师范学院数学系学习, 并获得学士学位; 2013年9月至今, 在杭州电子科技大学理学院攻读硕士。Email: 909573612@qq.com

Appendix

MU	FA	HA
Generate $x_0 \in_R [0, p-1], k$	Check T_{MU}	Check T_{FA}
$C_1 = g^k \bmod p, C_2 = x_0 y^k \bmod p$	$V_3 = h(K_{FH} // ID_{FA} // T_{FA} // T_{MU})$	
	$V_3^* = h(K_{FH} // ID_{FA} // T_{FA} // T_{MU}) = V_3$	
$PID_{MU} = (ID_{HA} \oplus ID_{MU})_{x_0}$	$M_2 = \{M_1, V_3, ID_{FA}, T_{FA}, T_{MU}\}$	$x_0 = C_2 C_1^{-x} \bmod p$
$V_2 = h(x_0 // ID_{MU} // ID_{FA} // T_{MU})$		Decrypt $PID_{MU} \Rightarrow ID_{MU}$
$M_1 = \{C_1, C_2, PID_{MU}, V_2, T_{MU}\}$	Check T_{HA}	$V_2^* = h(x_0 // ID_{MU} // ID_{FA} // T_{MU}) = V_2$
	Decrypt V_4	$V_4 = (x_0 // h(ID_{MU} // ID_{FA}) // T_{HA})_{K_{FH}}$
	$\Rightarrow \{x_0, h(ID_{MU} // ID_{FA}), T_{HA}\}$	$M_3 = \{V_4, T_{HA}\}$
$SK = h(h(x_0) // h(ID_{MU} // ID_{FA}))$	$SK = h(h(x_0) // h(ID_{MU} // ID_{FA})), V_5 = (h(x_0) // ID_{FA})_{SK}$	
Decrypt V_5	$M_4 = V_5$	
	$h^*(x_0) = h(x_0)$	