软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(7):1937−1952 [doi: 10.13328/j.cnki.jos.005361]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

对三个多服务器环境下匿名认证协议的分析*

汪 定[1], 李文婷[2], 王 平[2,3,4]

[1](北京大学 信息科学技术学院,北京 100871)

[2](北京大学 软件与微电子学院,北京 100260)

[3](软件工程国家工程研究中心,北京 100871)

[4](高可信软件技术教育部重点实验室(北京大学),北京 100871)

通讯作者: 王平, E-mail: pwang@pku.edu.cn

摘 要: 设计安全、高效的多服务器环境下匿名身份认证协议是当前安全协议领域的研究热点.基于广泛接受的攻击者模型,对多服务器环境下的 3 个代表性匿名认证协议进行了安全性分析.指出:(1) Wan 等人的协议无法实现所声称的离线口令猜测攻击,且未实现用户匿名性和前向安全性;(2) Amin 等人的协议同样不能抵抗离线口令猜测攻击,且不能提供匿名性,对两种破坏前向安全性的攻击是脆弱的;(3) Reedy 等人的协议不能抵抗所声称的用户仿冒攻击和离线口令猜测攻击,且无法实现用户不可追踪性.突出强调这些协议失败的根本原因在于,违反协议设计的 3 个基本原则:公钥原则、用户匿名性原则和前向安全性原则.明确协议的具体失误之处,并提出相应修正方法.

关键词: 多服务器环境;认证协议;匿名性;离线口令猜测攻击;前向安全性

中图法分类号: TP309

中文引用格式: 汪定,李文婷,王平.对三个多服务器环境下匿名认证协议的分析.软件学报,2018,29(7):1937−1952. http.//www.jos.org.cn/1000-9825/5361.htm

英文引用格式: Wang D, Li WT, Wang P. Crytanalysis of three anonymous authentication schemes for multi-server environment. Ruan Jian Xue Bao/Journal of Software, 2018,29(7):1937−1952 (in Chinese). http.//www.jos.org.cn/1000-9825/5361.htm

Crytanalysis of Three Anonymous Authentication Schemes for Multi-Server Environment

WANG Ding[1], LI Wen-Ting[2], WANG Ping[2,3,4]

[1](School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China)

[2](School of Software and Microelectronics, Peking University, Beijing 100871, China)

[3](National Engineering Research Center for Software Engineering, Beijing 100871, China)

[4](Key Laboratory of High Confidence Software Technologies, Ministry of Education (Peking University), Beijing 100871, China)

Abstract. The design of secure and efficient user authentication protocols for multi-server environment is becoming a hot research topic in the cryptographic protocol community. Based on the widely accepted adversary model, this paper analyzes three representative, recently proposed user authentication schemes for multi-server environment. The paper reveals that: (1) Wan, *et al*.'s scheme is subject to offline password guessing attack as opposed to the authors' claim, and it also cannot provide user anonymity and forward secrecy; (2) Amin, *et al*.'s scheme cannot withstand offline password guessing attack, cannot preserve user anonymity and is vulnerable to two kinds of forward secrecy issues; (3) Reedy, *et al*.'s scheme cannot resist against user impersonation attack and offline password guessing attack, and also falls short of user un-traceability. The paper highlights three principles for designing more robust anonymous multi-factor

* 基金项目: 国家自然科学基金(61472016); 国家重点研发计划(2016YFB0800603, 2017YFB1200700)

Foundation item: National Natural Science Foundation of China (61472016); National Key Research and Development Plan (2016YFB0800603, 2017YFB1200700)

本文由"面向隐私保护的新型技术与密码算法"专题特约编辑黄欣沂教授推荐.

收稿时间: 2017-05-30; 修改时间: 2017-07-13; 采用时间: 2017-08-22; jos 在线出版时间: 2017-10-17

CNKI 网络优先出版: 2017-10-17 13:38:05, http://kns.cnki.net/kcms/detail/11.2560.TP.20171017.1338.008.html

authentication schemes: Public key principle, user anonymity principle and forward secrecy principle, explaining the essential reasons for the security flaws of the above protocols. It further proposes some amendments for the identified security flaws.

Key words. multi-server environment; authentication protocol; user anonymity; offline password guessing attack; forward secrecy

1 引 言

随着互联网应用需求的快速增长,多服务器网络逐渐在商业、军事、交通、娱乐、医疗等领域显现出广泛的应用前景.这种网络以多个服务器提供多种服务的方式组网,允许用户访问同一服务提供商提供的不同网络服务.由于分布式计算架构具有移动性、开放性、设备异构性等特点,如何保证通信实体的真实性,防止服务的滥用和资源的非法访问,同时不降低系统可用性,是当前多服务器网络环境面临的严峻挑战.

1.1 相关工作

为实现对远程用户的身份认证,1981 年,Lamport[1]首次提出适于客户端/服务器架构的基于口令身份认证协议,随后大量此类适于单服务器环境的口令认证协议被提出,典型的如文献[2,3].但这些协议要求用户单独在每个服务器注册,并记忆每个服务器的登录口令.对于一个有 n 个服务器的分布式系统来说,用户需要记忆 n 个口令.随着网络服务的不断增多,这造成用户的口令数量快速增长,大大增加了记忆负担.

为解决单服务器环境下身份认证协议的可用性问题,2001 年 Tsaur[4]首次提出一个基于“口令+智能卡”的适于多服务器环境的认证协议,用户只需要记忆一个口令,便可登录同一管理域下的多个服务.这一工作得到了众多学者的跟踪,提出了一系列新的适于多服务器环境下的认证协议,如文献[4−14].这些协议,依据协议涉及的认证因子的数目,可分为单因子协议(如基于用户口令)[4]、双因子协议(如基于用户口令+智能卡)[5]、三因子或称为多因子协议(如基于用户口令+智能卡+生物特征)[6];依据是否考虑用户隐私,可分为匿名协议[3]和非匿名协议[4];依据使用的基本密码技术的不同,可分为基于对称密码技术的认证协议[5]和基于公钥的认证协议[6,7].其中,基于公钥的认证协议,又可细分为基于大因子分解困难性问题的协议[7]、基于有限域上离散对数困难性问题的协议[8,9]、基于椭圆曲线上离散对数困难性问题的协议[10]以及基于 Chebyshev 混沌映射的认证协议[6,11]等.

2011 年,Yoon 等人[15]提出一个基于椭圆曲线的多服务器环境下匿名三因子认证协议.但是,在该协议提出不久,Kim 等人[16]指出 Yoon 等人的协议[15]不能抵抗仿冒攻击、内部攻击、智能卡丢失攻击和离线口令猜测攻击,并进一步提出了一个基于生物特征的改进协议.但该协议随后被发现,在登录阶段和口令更新阶段不能实验用户匿名性,且存在可用性较差等问题.2014 年,Chuang 等人[12]提出一个多服务器环境下匿名三因子密钥协商协议,该协议仅使用 Hash 运算,适用于实际应用.但是,2014 年 Mishra 等人[17]和 2015 年 Lin 等人[18]均指出 Chuang 等人[12]提出的协议存在安全问题,不能实现用户匿名性和前向安全性,对服务器仿冒攻击、智能卡丢失攻击、拒绝服务攻击是脆弱的.然后,他们分别给出改进协议,然而,Lu 等人[19]和 Wang 等人[20]指出 Mishra 等人的协议[17]易遭受用户仿冒攻击、服务器仿冒攻击、重放攻击、拒绝服务攻击,并且不能提供前向安全性和用户匿名性.Lu 等人[19]和 Wang 等人[20]分别提出改进协议.

2015 年,He 等人[21]、Jiang 等人[22]和 Odelu 等人[23]分别均针对多服务器应用,提出基于“口令+智能卡+生物特征”的密钥协商协议.在这 3 个协议中,注册中心 RC 参与认证阶段,注册中心负载过高,易造成单点故障,不适于实际应用.此外, Odelu 等人[23]指出 He 等人的协议[21]在认证阶段和口令更新阶段存在安全问题,对仿冒攻击是脆弱的.Jiang 等人的协议[22]可抵抗各种攻击,但未实现用户匿名性.近期,Reedy 等人[24]指出 Lu 等人的协议[19]易遭受仿冒攻击、中间人攻击,且存在时钟同步问题、用户匿名性问题,不能提供完善的前向安全性,于是提出改进方案.2016 年,Wan 等人[25]指出 Chuang 等人[12]的协议无法抵抗用户仿冒攻击,未实现用户匿名性,并进一步提出了一个改进协议.与此同时,Amin 等人[26]也指出前述这些方案存在各种各样的缺陷,并给出改进的适于多服务器环境的匿名认证协议.

1.2 本文贡献

本文深入分析 Wan 等人的协议、Amin 等人的协议及 Reedy 等人的协议,发现这 3 种多服务器环境下的匿

名身份认证协议都无法实现所声称的多因子安全性和用户匿名性,并且对离线口令猜测攻击是脆弱的,存在前向安全性问题和用户仿冒攻击威胁.

基于我们对 200 余个协议进行分析所得经验,本文对破坏前向安全性的攻击场景进行分类,突出被长期忽视的用户端口令泄漏所引起的前向安全性问题以及智能卡安全参数泄露引起的前向安全性问题.以 Wan 等人的协议和 Amin 等人的协议为例,分析两种常见的破坏前向安全性的攻击场景.

本文突出了匿名多因子身份认证协议的3个基本设计原则:(1) 在非抗窜扰智能卡假设下,采用公钥技术是实现抗离线口令猜测攻击的必要条件;(2) 采用公钥技术是实现用户匿名性的必要条件;(3) 采用公钥技术是实现前向安全性的必要条件,且在服务器端至少进行两次模幂运算或椭圆曲线点乘运算.这些原则虽然最初针对单服务器构架的多因子协议而提出(见文献[8,27]),但本文突出了它们对多服务器环境下协议的普遍适用性.

1.3 组织架构

本文第 2 节描述多服务器系统架构、采用的攻击者模型,对破坏前向安全性问题的攻击场景进行总结.第 3 节回顾 Wan 等人提出的多服务器架构下的高效身份认证协议.在第 4 节中分析该协议的安全性.第 5 节描述 Amin 等人提出的基于动态 ID 技术的双因子协议.第 6 节指出该协议存在的安全问题.第 7 节和第 8 节分别回顾和分析 Reedy 等人提出的协议.第 9 节突出多因子认证协议的 3 个基本设计原则.最后第 10 节总结全文.

2 系统架构、攻击者模型及前向安全性攻击场景

2.1 多服务器系统架构

多服务器环境下远程用户认证协议通常涉及 3 个参与者:用户、服务提供商服务器和注册中心.如图 1 所示,在系统初始化阶段,服务提供商服务器需在注册中心注册.远程用户在注册中心完成一次注册后,得到包含安全参数信息的智能卡,然后可从多个服务器中获取不同服务[28].

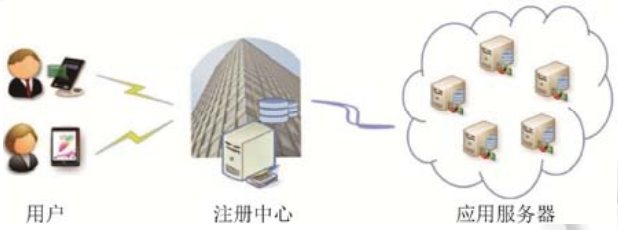

Fig. 1 Multi-Factor user authention in the multi-server architecture

图 1 多服务器环境下多因子认证系统架构

采用单服务器认证的协议,用户需多次注册、多次认证以获得同一服务提供商提供的不同应用服务.为提高访问效率,解决用户多服务器重复登记问题,多服务器环境的身份认证协议需实现一次注册、多次服务访问.此类协议广泛应用于交通卡、校园卡、智能银行卡、金融卡等高安全需求环境,一次注册通过,持卡人可在多个应用系统上消费(俗称“一卡通”),因而必须增强协议的强健性.

2.2 攻击者模型

远程用户口令认证协议的攻击者模型一直沿用经典的 Dolev-Yao 模型[29],即攻击者可任意侦听、截获、插入、删除或阻断流经公开信道中的消息.近年来,随着边信道攻击技术的发展[30](如功耗攻击、电磁攻击和计时攻击),攻击者可分析出智能卡内安全参数,攻击能力得到增强.本文采用 Wang 等人[3]和 Huang 等人[31]提出的迄今最严苛(但符合实际)的多因子协议攻击者模型,攻击者能力见表 1.

现实生活中,用户身份空间和口令空间十分有限($|\mathcal{D}_{id}| \leqslant |\mathcal{D}_{pw}| \leqslant 10^6$ [32,33]),故 C-01 是现实的.需要指出的是,

在分析协议安全性时,假设攻击者 $\mathcal{A}$ 可获取用户身份标识 ID,但在评估协议匿名性时,应假设用户身份标识 ID 为敏感信息.

需要注意的是,一个协议要实现 n-因子安全性(n=2 或 n=3),必须假设 $\mathcal{A}$ 可获得其中任意 n–1 个认证因子(口令、智能卡或生物因子),仍不能威胁到剩余的那个认证因子.现实中,攻击者有多种途径可获得会话密钥,比如会话密钥未及时有效擦除、协议主动公开过期会话密钥.因此,假设攻击者拥有能力 C-3 是合理的.

Table 1 Capabilites of the adversary

表 1 攻击者拥有的能力

能力	含义
C-00	$\mathcal{A}$ 可以离线穷举 $\|\mathcal{D}_{id}\|\times\|\mathcal{D}_{pw}\|$ 中所有元素
C-01	$\mathcal{A}$ (非评估隐私安全)可以获取用户身份标识 ID
C-1	$\mathcal{A}$ 任意侦听、截获、插入、删除或阻断流经公开信道中的消息
C-2	对于双因子协议, $\mathcal{A}$ 可以(1) 获取用户口令;(2) 提取智能卡内秘密信息,但二者不可兼得,否则为平凡攻击. 对于 3 因子协议, $\mathcal{A}$ 可以(1) 获取用户口令;(2) 提取智能卡内秘密信息;(3) 获取用户的生物特征信息.假设 $\mathcal{A}$ 可以同时获得 3 个认证因子中的两个,但不可假设 $\mathcal{A}$ 三者同时兼得,否则为平凡攻击
C-3	$\mathcal{A}$ 可以获取过期的会话密钥
C-4	$\mathcal{A}$ 可以获知服务器长期私钥,此能力仅用于评估系统终极失效时的强健性

2.3 前向安全性攻击场景

前向安全性是身份认证协议的重要安全目标之一.一个实现了前向安全性的协议所能保证的是,即使一个或多个协议参与方的长期私钥泄漏(对应于表 1 中的 C-4),它们之前建立的会话密钥的安全性不受影响[3].目前,绝大多数协议分析前向安全性时都假设服务器长期私钥泄漏[3,23,30,32].事实上,不同的应用环境包含多种不同的参与方,例如多服务器环境的参与方包括用户、控制服务器、应用服务器;无线传感器网络环境包括用户、服务器、传感器节点;移动网络环境包括用户、家乡服务器、漫游服务器.为便于分析且不失一般性,本文视各应用环境的参与方为用户和服务器两类.例如,多服务器环境下的控制服务器和应用服务器可被视作一个实体——服务器;无线传感器网络环境下的服务器和传感器节点也可被视作一个服务器实体.

本文在分析 100 余个近期提出的口令认证协议的基础上,根据不同的攻击场景,总结了 5 类前向安全性问题.其中,类型 I 受到的关注最多,比如文献[3,8,32,37–39]分析协议前向安全性时都只假设服务器长期私钥泄漏的情形.第 4.3 节和第 6.3 节中将给出类型 I 的实例分析.现实生活中,为方便记忆,用户通常选择低信息熵的口令,并且用户口令的这一脆弱性随着网络服务的增多而不断加剧,使攻击类型 II 比类型 I 更易实施.但是,据我们所知,攻击类型 II 长期缺乏应有的关注.第 6.4 节中将给出详细的攻击实例.与类型 II 的攻击方式相似但有明显不同,文献[40]中给出了一种针对 Yeh 等人的方案[35]的前向安全性攻击:攻击者首先通过猜测用户的 ID,然后可计算出先前建立的会话密钥.我们称这种攻击为类型 III.见表 2.

Table 2 Ataxonomy of forward secrecyissues

表 2 前向安全性攻击分类

类型	描述	攻击类型	典型失效协议
类型 I	服务器(注册中心、应用服务器)私钥泄漏	被动攻击	第 4.3 节,第 6.3 节,Tsai 等人[34]
类型 II	用户口令 PW 泄漏	被动攻击	第 6.4 节,Tsai 等人[34]
类型 III	用户身份标识 ID 泄露	被动攻击	Yeh 等人[35]
类型 IV	智能卡参数泄漏(未猜测 ID、PW)	被动攻击	Li 等人[36]
类型 V	服务器验证表项泄漏	被动攻击	Sood 等人[37]

文献[36]中,Li 等人提出了一个简单、高效的基于智能卡的远程用户口令认证协议,明确假设攻击者 $\mathcal{A}$ 可获取智能卡内秘密参数.由于用户智能卡内存储了一个所有用户共用的安全参数 $h(x)$,如果一个合法但恶意用户 $\mathcal{A}$ 分析出 $h(x)$, $\mathcal{A}$ 可计算出系统任意用户先前的会话密钥 $SK=h(D\oplus h(x)\oplus x_0\oplus y_0)$, 其中,$D$,$x_0$ 和 y_0 从传输的协议信息中截获而来.我们称此类攻击为类型 IV.为防止内部人员攻击和验证项窃取攻击,绝大多数协议在服

务器端都不保存用户相关敏感数据.Sood 等人的方案[37]遵守了这一推荐做法,但它在应用服务器中存储了每个用户 U_i 的身份标识 ID_i 及秘密参数 y_i,一旦 ID_i 及 y_i 泄漏,攻击者 $\mathcal{A}$ 可从截获的协议消息中推算出随机数 N_1,N_2 和 N_3,进而可成功计算出会话密钥 SK.我们称此类攻击为类型 V.

总之,现有研究多关注类型 I 的前向安全性攻击威胁,对类型 II~类型 V 研究极少,本文将弥补这一缺陷.需要指出的是,上述 5 类前向安全性攻击仅考虑了一方长期私钥泄露的情形,未关注两方或多方长期私钥同时泄露的情形,因为前者更为现实.还需注意的是,上述 5 类攻击是经验的总结,可能存在其他类型的攻击被遗漏,或者新型的攻击在未来被发现.尽管如此,这 5 类攻击可解释现有绝大多数协议的前向安全性失效之处,它们可作为检验一个协议是否可实现前向安全性的有效途径:仅当可抵抗这 5 类攻击时,协议才有可能实现前向安全性.

3 Wan 等人的方案回顾

Wan 等人的协议[25]分为 4 个阶段:注册、登录、认证和口令修改.系统初始化时,注册中心 RC 选取秘密参数 x 和 y,为每个服务器 S_j ($j \in \{1,2,...,m\}$, m 为服务器个数)选取随机数 y_j,通过安全信道将 $h(SID_j \| y_j), h(y)$ 传递给 S_j.

3.1 注册阶段

1) 用户 U_i 选取身份标识 ID_i,口令 PW_i 并输入生物特征 BIO_i,计算 $P_i = h(PW_i \oplus BIO_i)$.

2) $U_i \Rightarrow RC: \{ID_i, P_i\}$.

3) RC 计算 $A_i = h(ID_i \| x), C_i = h(ID_i \| h(y) \| P_i), D_i = A_i \oplus h(ID_i) \oplus h(P_i), E_{ij} = h(A_i) \oplus h(h(SID_j \| y_j) \oplus h(A_i)), F_{ij} = E_{ij} \oplus h(ID_i \| P_i)$, 然后,将 $\{(F_{i1}, F_{i2}, ..., F_{ik}), C_i, D_i, h(y), h(\cdot)\}$ 写入智能卡.

4) $RC \Rightarrow U_i$: 智能卡.

3.2 登录阶段

当用户 U_i 要访问远程服务器的资源时,将进行如下操作.

1) 用户 U_i 将智能卡插入读卡器,输入 ID_i 和 PW_i, 扫描 BIO_i. 智能卡计算 $P_i = h(PW_i \oplus BIO_i), C_i^* = h(ID_i \| h(y) \| P_i)$, 并验证 C_i^* 与存储的 C_i 是否相等.如果不相等,则表明用户输入的 ID_i 和 PW_i 是不合法的,智能卡终止协议.

2) 智能卡计算 $A_i = D_i \oplus h(ID_i) \oplus h(P_i), G_{ij} = h(A_i) \oplus h(SID_j \| h(y)), E_{ij} = F_{ij} \oplus h(ID_i \| P_i)$. 智能卡 SC 生成随机数 N_1,计算 $H_{ij} = E_{ij} \oplus N_1, AID_i = h(N_1) \oplus h(ID_i), M_1 = h(h(A_i) \| h(ID_i) \| N_1)$.

3) $U_i \rightarrow S_j : \{SID_j, G_{ij}, H_{ij}, AID_i, M_1\}$.

3.3 认证阶段

此阶段实现用户和服务器的相互认证,并协商会话密钥.

1) 服务器 S_j 收到来自用户的登录请求后,计算 $h(A_i) = G_{ij} \oplus h(SID_j \| h(y)), E_{ij} = h(A_i) \oplus h(h(SID_j \| y_j) \oplus h(A_i)), N_1 = E_{ij} \oplus H_{ij}, h(ID_i) = AID_i \oplus h(N_1)$, 并验证 $h(h(A_i) \| h(ID_i) \| N_1)$ 是否等于接收到的 M_1.如果相等,则表明用户 U_i 是合法的;否则,终止协议.

2) S_j 选取随机数 N_2,计算 $M_2 = N_1 \oplus N_2 \oplus h(ID_i), M_3 = h(N_1 \| N_2 \| SID_j), SK_{ij} = h(N_1 \| N_2 \| h(ID_i) \| h(ID_i) \| SID_j)$.

3) $S_j \rightarrow U_i : \{SID_j, M_2, M_3\}$.

4) 智能卡接收到 S_j 返回的信息后,计算 $N_2 = N_1 \oplus M_2 \oplus h(ID_i)$, 并验证 $h(N_1 \| N_2 \| SID_j)$ 是否与收到的 M_3 相等.如果相等,则 U_i 计算会话密钥 $SK_{ij} = h(N_1 \| N_2 \| h(ID_i) \| SID_j)$.

5) $U_i \rightarrow S_j : \{SK_{ij} \oplus h(N_2)\}$.

6) S_j 恢复 $h(N_2)$ 进行重放攻击检查.

4 Wan 等人的方案的安全性分析

Wan 等人[25]发现文献[12]中提出的方案不能实现用户匿名性,且不能抵抗智能卡丢失攻击.因此,Wan 等人[25]提出了一个改进的多服务器架构下的匿名三因子认证协议,声称改进协议弥补了文献[12]的安全漏洞.但经仔细分析,我们发现 Wan 等人的方案[25]仍不能实现用户匿名性,无法确保前向安全性这一理想属性,且对离线口令猜测攻击是脆弱的.

4.1 匿名性失效

随着物联网、云计算、移动互联网的快速发展,用户隐私问题面临着巨大的挑战.为保护用户隐私(如登录位置、个人偏好、个人数据等[41,42]),匿名性成为远程用户认证协议中不可或缺的理想属性.匿名性有两个层次的含义[8,27]:(1) 基本层次要求攻击者无法获知用户的真实身份标识,即用户 ID 保护;(2) 高级层次要求攻击者无法分辨出两个会话是否由同一用户参与,即用户不可追踪性.在现有研究中,绝大多数协议所涉及的匿名性即为用户不可追踪性[43−45],因此除非另有说明,后文"匿名性"均指用户不可追踪性.尽管 Wan 等人的协议[25]实现了基本层次的匿名性,即用户 ID 保护,但攻击者仍可追踪用户行为,对用户的隐私构成威胁.

任意合法用户的智能卡中存有注册中心 RC 的秘密参数 $h(y)$.目前,绝大多数身份认证协议都基于智能卡非抗窜扰假设[3,8],即当攻击者在非监督环境下较长时间占有用户智能卡时,可以提取智能卡内秘密信息.这一假设在 Wan 等人的方案[25]中明确提出.如果存在恶意用户 U_k,通过边信道攻击技术[41,46−48]提取自己智能卡中的参数 $h(y)$,则可破解其他合法用户的不可追踪性.具体流程如下.

1) 从公开信道中侦听到 U_i 发送给服务器 S_j 的登录请求消息 $\{SID_j, G_{ij}, H_{ij}, AID_i, M_1\}$;

2) 计算 $h(A_i)=G_{ij}\oplus h(SID_j \| h(y))$, 其中, G_{ij} 和 SID_j 来自截获消息.

其中, $A_i=h(ID_i \| x)$, 则 $h(A_i)$ 是一个与用户 ID 直接相关的固定参数,可以唯一标识用户 U_i.因此恶意用户 U_k 依据 $h(A_i)$ 可以实现对 U_i 访问行为的追踪.值得注意的是,这一过程无需借助受害用户的智能卡,且攻击者一旦提取出参数 $h(y)$,就可以在用户完全未知的情况下多次实施攻击.故 Wan 等人的方案[25]无法实现用户匿名性.

事实上,文献[8]已从理论上严格证明,在无线传感器网络环境下,基于非抗窜扰智能卡假设,仅采用对称密码技术(如 Hash、异或运算)无法实现高级层次匿名性的多因子认证协议.不难发现,这一理论同样适用于多服务器环境.Wan 等人的方案[25]未采用任何公钥技术,因此无法实现用户不可追踪性.

4.2 离线口令猜测攻击

Huang 等人在文献[31]中指出,对三因子认证协议,攻击者 $\mathcal{A}$ 获取其中任何两个认证因子(口令、智能卡或生物因子),不能威胁到另外一个认证因子,即:

1) 当 $\mathcal{A}$ 获取用户口令、智能卡时,生物因子仍然安全;

2) 当 $\mathcal{A}$ 获取用户口令、生物因子时,智能卡内秘密参数仍然安全;

3) 当 $\mathcal{A}$ 获取用户智能卡、生物因子时,用户口令仍然安全.

其中,情况 1 和情况 2 下攻击者 $\mathcal{A}$ 成功的可能性极小,因为生物因子常基于模糊提取,极难恢复[31],而智能卡内通常存储高信息熵的安全参数[30];由于针对低信息熵口令的在线或离线字典攻击技术的快速进展,攻击者可以在极少猜测次数下,以不可忽略概率(甚至大概率)猜出用户口令.比如,允许 100 次猜测,攻击者可以 32%~73%的概率猜出用户口令[32,33].因此,情况 3 下协议面临严重威胁.

分析发现,Wan 等人[25]企图引入生物因子弥补 Chuang 等人的协议[12]的安全漏洞并不可取,一旦攻击者 $\mathcal{A}$ 获取用户智能卡和生物因子(如采用指纹膜提取用户指纹),那么, $\mathcal{A}$ 可离线猜测出用户口令.具体过程如下.

1) $\mathcal{A}$ 通过边信道攻击技术[46−48]分析出智能卡内敏感信息 $\{(F_{i1}, F_{i2}, ..., F_{ik}), C_i, D_i, h(y), h(\cdot)\}$;

2) $\mathcal{A}$ 从用户身份空间 $\mathcal{D}_{id}$ 和口令空间 $\mathcal{D}_{pw}$ 猜测 (ID^*, PW^*);

3) 计算 $P_i^*=h(PW^*_i \oplus BIO_i)$; $C_i^*=h(ID^*_i \| h(y) \| P_i^*)$, 其中, $h(y)$从智能卡中提取;

4) 验证 $C_i^*=C_i$ 是否成立.如果成立,则 (ID^*, PW^*) 猜测正确,否则,转 1).

上述攻击的时间复杂度为$\mathcal{O}((2T_h+T_{xor})\cdot|\mathcal{D}_{id}|\cdot|\mathcal{D}_{pw}|)$, 其中,$T_h$为 Hash 操作时间,$T_{xor}$为异或操作时间.文献[44]指出,用户口令遵循 Zipf 分布,实际空间大小十分有限(如$|\mathcal{D}_{id}|\leqslant|\mathcal{D}_{pw}|\leqslant 10^6$),且用户 ID 通常满足特定格式,分析协议安全性时可视作公开信息.故上述攻击可在多项式时间内完成.不难发现,为实现“口令本地自由更新”,Wan 等人的协议在智能卡内设置安全参数C_i以检测用户输入口令的正确性,但C_i为攻击者提供了验证猜测口令正确性的预言机服务,这一过程引入了新的安全缺陷.Wang 等人在文献[39]中提出将“模糊验证因子”技术和“Honeywords”技术相结合,以合理地平衡这一安全性和可用性问题.因此,为解决 Wan 等人的协议[25]的离线口令猜测攻击,建议引入“模糊验证因子”和“Honeywords”技术,修改C_i的计算方式为$C_i=h(ID_i\|h(y)\|P_i) \bmod n$, 其中,$n$表示(*ID*,*PW*)池容量的整数, $2^4\leqslant n\leqslant 2^8$. 同时,在服务器端维护一个 Honeywords 列表,一旦 Honeywords 的登录数量达到预先定义的阈值,则锁定帐号.

4.3 前向安全性问题I

实现前向安全性的协议要保证,即使一方或多方的长期私钥泄露,此前建立的会话密钥仍然安全[49,50].在 Wan 等人的方案[25]中,如果任意服务器S_j被攻击者$\mathcal{A}$捕获或偶然泄露长期私钥y_j,则$\mathcal{A}$可截获用户U_i发往S_j的登录请求信息$\{SID_j,G_{ij},H_{ij},AID_i,M_1\}$, 推导出之前的会话密钥,具体过程如下.

1) $\mathcal{A}$计算$E_{ij}=h(A_i)\oplus h(h(SID_j\|y_j)\oplus h(A_i));N_1=E_{ij}\oplus H_{ij};h(ID_i)=AID_i\oplus h(N_1)$;

2) $\mathcal{A}$截获S_j的回送消息$\{SID_j,M_2,M_3\}$, 并计算$N_2=N_1\oplus M_2\oplus h(ID_i)$;

3) $\mathcal{A}$推导出会话密钥$SK_{ij}=h(N_1\|N_2\|h(ID_i)\|SID_j)$, 其中,$N_1$,$N_2$,$h(ID_i)$从计算所得,$SID_j$为截获信息.

可以看出,任意服务器S_j的长期私钥y_j泄露后,攻击者$\mathcal{A}$可获得访问过该服务器的所有用户的会话密钥.事实上,Ma 等人在文献[27]中证明了在服务器端无验证表项情况下,服务器至少进行两次模幂运算或椭圆曲线点乘运算才能实现前向安全性.在 Wan 等人的方案[25]中,为实现前向安全性,可引入传统的 Diffie-Hellman 密钥交换技术(如文献[51]),使用临时值g^x和g^y分别替换随机数N_1和N_2.新型的技术(如 Chaotic-Maps)也可达到目的.

5 Amin 等人的方案回顾

本节回顾 Amin 等人[26]在 2016 年提出的基于动态 ID 技术的多服务器环境下远程用户认证协议.Amin 等人的方案[26]包含 4 个阶段:注册、登录、认证、口令更新.

5.1 注册阶段

注册阶段分为用户注册阶段和服务器注册阶段.首先,服务器S_j选取身份标识SID_j发送给注册中心 RC,RC 使用长期私钥x计算$P_j=h(SID_j\|x)$, 并通过安全信道发送给S_j.用户注册过程如下.

1) 用户U_i选取身份标识ID_i、口令PW_i和随机数b,并计算$PWR_i=h(PW_i\oplus b)$.

2) $U_i\Rightarrow RC:\{ID_i,PWR_i\}$.

3) RC 收到来自U_i的注册请求后,选取随机数y_i,计算$CID_i=h(ID_i\oplus y_i\oplus x)$.RC 检查数据库中是否存有$CID_i$,若没有,则认为$U_i$是新注册的用户,计算$REG_i=h(ID_i\|PWR_i\|CID_i),T_i=h(CID_i\oplus x)\oplus PWR_i$; 反之,RC 选取新的随机数$y_i^*$, 计算$CID_i=h(ID_i\oplus y^*{}_i\oplus x)$, RC 将$\{CID_i,REG_i,T_i,y_i,h(\cdot)\}$写入智能卡.

4) $RC\Rightarrow U_i$: 智能卡.

5) U_i将b写入智能卡.

5.2 登录阶段

1) 用户U_i将智能卡插入读卡器,输入ID_i和PW_i, SC 计算$PWR_i=h(PW_i\oplus b),REG^*{}_i=h(ID_i\|PWR_i\|CID_i)$, 并比较$REG^*{}_i$是否等于存储的$REG_i$.如果相等,表明用户输入的$ID_i$和$PW_i$合法,SC 计算$L_1=T_i\oplus PWR_i$, 生成随机数$N_1$,$N_2$,计算$N_3=N_1\oplus N_2,L_2=N_2\oplus PWR_i,L_3=h(L_1\|SID_j\|N_1\|L_2\|N_3)$.

2) $U_i \to RC:\{CID_i, SID_j, T_i, L_3, L_2, N_3\}$.

5.3 认证阶段

1) RC 收到来自用户的登录消息后,先检查 CID_i 和 SID_j 的格式是否正确,如果不正确,RC 拒绝登录请求;否则,计算 $A_1 = h(CID_i \| x), PWR_i = T_i \oplus A_1, N_2 = L_2 \oplus PWR_i, N_1 = N_3 \oplus N_2$, 然后,比较计算的 $L_3^* = h(L_1 \| SID_j \| N_1 \| L_2 \| N_3)$ 是否等于接收到的 L_3.如果不相等,则 RC 终止会话;否则,RC 生成随机数 N_4,计算 $A_2 = h(SID_j \| x)$, $A_3 = A_2 \oplus N_4, N_5 = N_1 \oplus N_4, A_4 = h(P_j \| N_4 \| N_1 \| CID_i)$.

2) $RC \to S_j:\{CID_i, A_3, A_4, N_5\}$.

3) S_j 接收到来自 RC 的消息后,计算 $N_4 = P_j \oplus A_3, N_1 = N_5 \oplus N_4, A^*_4 = h(P_j \| N_4 \| N_1 \| CID_i)$, 并比较是否等于 A_4.如果相等,则 S_j 认为 RC 和 U_i 是合法的.S_j 生成随机数 N_6,计算 $N_7 = N_1 \oplus N_6, SK_s = h(SID_j \| CID_i \| N_6 \| N_1)$, $A_5 = h(SK_s \| N_6)$.

4) $S_j \to U_i:\{SID_j, A_5, N_7\}$.

5) U_i 接收到来自 S_j 的消息后,计算 $N_6 = N_1 \oplus N_7, SK_u = h(SID_j \| CID_i \| N_6 \| N_1), A_5^* = h(SK_s \| N_6)$, 并比较 A_5^* 是否等于 A_5.如果相等,则用户确认 S_j 的合法性.U_i 和 S_j 之间协商会话密钥 $SK_u = SK_s$.

6 Amin 等人的方案的安全性分析

Amin 等人在文献[26]中指出,Sood 等人的方案[37]和 Li 等人的方案[52]皆无法抵抗离线口令猜测攻击、用户仿冒攻击,并且对内部攻击是脆弱的,故提出改进方案.分析发现,Amin 等人提出的改进方案[26]仍无法实现所声称的目标,且存在用户匿名性问题和前向安全性问题.

6.1 匿名性失效

为实现用户匿名性,常见的方法是采用 Das 等人[43]提出的“动态 ID 技术”,将真实用户名隐藏在会话可变的伪 ID 中,仅认证服务器可获知用户真实 ID,而传输信道中的其他实体无法获取任何有用的个人信息.采用这种技术的协议被称为隐私保护协议,尽管 Amin 等人的方案采用了“动态 ID 技术”,但并未完全实现用户匿名性.

用户 U_i 向注册中心 RC 发送登录请求消息 $\{CID_i, SID_j, T_i, L_3, L_2, N_3\}$, 其中, CID_i 表示隐藏用户真实 ID 的假用户名. $CID_i = h(ID_i \oplus y_i \oplus x)$ 由 RC 选取随机数 y_i 计算所得,长期保存在 RC 数据库及用户智能卡中,并不具备会话可变性.此外, T_i 也与用户 U_i 直接相关且固定不变.因而攻击者 $\mathcal{A}$ 可通过跟踪固定参数 CID_i 或 T_i 获得用户 U_i 的访问行为.为解决这一问题, CID_i 的计算参数 y_i 应为会话变量,使用随机数 N_1, N_2 伪装固定参数 T_i.

6.2 离线口令猜测攻击

由于人类记忆力受限,用户往往会选择低信息熵的口令[32,33].进而,攻击者可借助:(1) 在线字典攻击;(2) 离线字典攻击方式来确认正确的口令.而后者不需要与服务器交互,可在本地进行,不受服务器端安全机制的限制,是基于口令的认证协议面临的最大安全威胁[53].

在非窜扰智能卡假设情况下,攻击者 $\mathcal{A}$ 可通过边信道技术(如逆向工程技术[47]、差分能耗分析[30,48])获得智能卡内敏感信息 $\{CID_i, REG_i, T_i, y_i, b, h(\cdot)\}$, $\mathcal{A}$ 可发起如下口令猜测攻击.

1) $\mathcal{A}$ 从用户身份空间 $\mathcal{D}_{id}$ 和口令空间 $\mathcal{D}_{pw}$ 猜测 (ID^*, PW^*);

2) $\mathcal{A}$ 计算 $PWR^*_i = h(PW^*_i \oplus b); REG^*_i = h(ID^*_i \| PWR^*_i \| CID_i)$, 其中, CID_i 和 b 从智能卡中提取;

3) 验证 $REG_i^* = REG_i$ 是否成立.如果成立,则 (ID^*, PW^*) 猜测正确,否则,转 1).

上述攻击的时间复杂度为 $\mathcal{O}((2T_h + T_{xor}) \cdot |\mathcal{D}_{id}| \cdot |\mathcal{D}_{pw}|)$, 其中, T_h 为 Hash 操作时间, T_{xor} 为异或操作时间.文献[32,33]表明,用户身份空间和口令空间十分受限 $|\mathcal{D}_{id}| \leqslant |\mathcal{D}_{pw}| \leqslant 10^6$ [43,44].根据文献[50]在 Intel i7-4790 3.6GHZ 的 PC 上的测试结果, T_h (SHA-1)平均运行时间为 0.591μs, T_{xor} 平均运行时间为 0.006μs,则上述攻击可在两周内完成.如果借助亚马逊等云计算平台,可在几小时内完成.

需要指出的是,本节的“离线口令猜测攻击”本质上是“智能卡丢失攻击”,因为发起这一攻击的前提条件是 $\mathcal{A}$ 已经获得了用户的智能卡,更详细的信息可参见文献[50].一旦攻击者 $\mathcal{A}$ 猜测出正确的 (ID^*, PW^*), 利用智能卡内参数 CID_i 和 b,选取随机数 N_1,N_2,便可计算参数 L_3,L_2,N_3,仿冒用户 U_i 访问任意服务器 S_j.

事实上,1999 年,文献[53]证明采用公钥技术是实现单因子口令认证协议抗离线口令猜测攻击的必要条件;2014 年,文献[27]证明采用公钥技术是实现“口令+智能卡”双因子认证协议抗离线口令猜测攻击的必要条件.由于 Amin 等人的方案[26]仅采用了对称密码技术(即 Hash 函数),本质上不能抵抗该攻击.

6.3 前向安全性问题I

在开放网络环境中,所有参与通信会话的实体(如用户和服务器)都应被视为不可信实体.尤其是在多服务器环境下,恶意管理员的存在或攻击者腐化控制服务器,都会导致(应用)服务器长期私钥泄露,因此应确保会话密钥与(应用)服务器私钥之间的独立性.

假设攻击者 $\mathcal{A}$ 获取了服务器 S_j 的长期私钥 P_j,并截获 RC 发往 S_j 的消息 $\{CID_i, A_3, A_4, N_5\}$ 及 S_j 回送 U_i 的消息 $\{SID_j, A_5, N_7\}$, 则可获取 U_i 和 S_j 的会话密钥,具体流程如下.

1) $\mathcal{A}$ 计算 $N_4 = P_j \oplus A_3; N_1 = N_5 \oplus N_4$;

2) $\mathcal{A}$ 计算 $N_6 = N_1 \oplus N_7$, 获得会话密钥 $SK = h(SID_j \| CID_i \| N_6 \| N_1)$.

为实现上述攻击,攻击者只需侦听通信信道中的消息,无需与服务器交互,则攻击者 $\mathcal{A}$ 可获得所有登录过服务器 S_j 的用户的会话密钥.此外,前向安全性是评价系统终极失效后的强健性的安全属性.在 Amin 等人的方案[26]中,服务器 S_j 的长期私钥 $P_j = h(SID_j \| x)$ 与注册中心 RC 的私钥 x 唯一相关,一旦秘密参数 x 泄漏,攻击者可获得所有服务器上登录用户的会话密钥,威胁整个系统安全性.协议实际运行时,为避免单点故障,降低系统通信负载,注册中心 RC 应只负责系统参数的选取及用户、服务器注册,而不应直接参与用户认证过程.

6.4 前向安全性问题II

在上节给出的前向安全性问题中,假设攻击者 $\mathcal{A}$ 可以获得服务器长期私钥 P_j.下面给出另一种攻击方式.依据第 6.2 节,攻击者可分析出智能卡内安全参数,并通过离线口令猜测攻击获得用户 U_i 的口令 PW_i,则 $\mathcal{A}$ 计算 $PWR_i = h(PW_i \oplus b)$ 可以获取 U_i 和 S_j 的会话密钥,具体流程如下.

1) $\mathcal{A}$ 截获 U_i 发往 S_j 的登录请求消息 $\{CID_i, SID_j, T_i, L_3, L_2, N_3\}$, 并计算 $N_2 = L_2 \oplus PWR_i, N_1 = N_2 \oplus N_3$;

2) $\mathcal{A}$ 截获 S_j 回送 U_i 的消息 $\{SID_j, A_5, N_7\}$, 并计算 $N_6 = N_1 \oplus N_7$;

3) $\mathcal{A}$ 获得会话密钥 $SK = h(SID_j \| CID_i \| N_6 \| N_1)$.

为方便记忆,用户构造口令具有偏好性,如使用国民口令和基于个人信息,故而用户口令被视作低熵信息,易被攻击者猜测出来[33].并且,用户口令重用现象十分常见,近年来不断发生的口令泄露事件,产生“多米诺骨牌”效应,大大增加了用户口令泄露的风险[32].2013 年,Yahoo 公司 10 亿用户信息泄漏,包括姓名、口令、生日、邮箱、地址等.2016 年,京东、Myspace、Linkedin、Twitter、Tumblr、VK. Com 等知名网站的数十亿口令被黑客窃取[54].因此,用户口令泄漏的可能性远高于服务器私钥泄漏的可能性,在评估系统终极失效的强健性时,假设攻击者 $\mathcal{A}$ 可获取用户口令是现实且可取的.

7 Reedy 等人的方案回顾

2017 年,Reedy 等人[24]提出一个抗仿冒攻击的多服务器环境下的密钥协商协议,该协议包含初始化阶段、用户和服务器注册阶段、登录阶段、相互认证阶段、口令和生物因子更新阶段、服务器动态增加阶段、用户撤销/重新注册阶段.在初始化阶段,注册中心 RC 选取椭圆曲线 $E_p: y^2 = x^3 + ax + b$ 上一点 P,选取私钥 USK,ASK, 公开参数 $\{E_p, P, h(\cdot)\}$.

7.1 服务器注册阶段

1) $S_j \Rightarrow RC: \{SID_j\}$.

2) RC 计算 $K_j = h(SID_j \| ASK)$, 在后台数据库中存储 $\{SID_j, K_j\}$.

3) $RC \Rightarrow S_j : \{K_j, h(ASK), P\}$.

7.2 用户注册阶段

1) 用户 U_i 选取 ID_i、PW_i, 生成随机数 $r_i \in Z_p^*$, 计算 $PID_i = h(ID_i \| r_i), PWD_i = h(PW_i \| r_i)$.

2) $U_i \Rightarrow RC : \{PID_i, PWD_i\}$.

3) RC 检查 PID_i 是否是已经注册的用户,为所有注册的 SID_j 计算 $Q_j = h(PID_i \| K_j), R_j = Q_j \oplus PWD_i$, 在表 T_i 中存储 $\{SID_j, R_j\}$, 表 T_C 中存储 $\{PID_i, C_i, T_R = 1\}$. 其中,T_R=1 表明 U_i 初次注册.RC 计算 $W_j = h(PID_i \| USK)$, 将 $\{W_j, T_i, h(ASK)\}$写入智能卡中.

4) $RC \Rightarrow U_i$: 智能卡.

5) U_i 扫描生物特征 BIO_i,计算 $X_j = W_j \oplus PWD_i, C_i = h(ID_i \| W_j), (\sigma_i, \theta_i) = Gen(BIO_i), V_i = r_i \oplus h(\sigma_i)$, X_j 替换 W_j, 将 $\{C_i, V_i, \theta_i\}$ 写入智能卡,则智能卡包含参数 $\{X_j, V_i, C_i, T_i, \theta_i, P, h(\cdot), h(ASK)\}$.

7.3 登录阶段

U_i 插入智能卡,输入 ID_i、PW_i, 扫描 BIO_i'.

1) SC 计算 $\sigma_i' = Rep(BIO_i', \theta_i), r_i = V_i \oplus h(\sigma_i'), PID_i = h(ID_i \| r_i), PWD_i = h(PW_i \| r_i), W_j = X_j \oplus PWD_i$, 验证 $C_i \stackrel{?}{=} h(ID_i \| W_j)$, 如果不相等,则拒绝登录请求.

2) U_i 选取将要访问的 S_j,从表 T_i 中提取 R_j,计算 $Q_j = R_j \oplus PWD_i$, 生成随机数 $N_1 \in Z_p^*$, 计算 $\alpha = N_1 P$, $B_{ij} = PID_i \oplus h(SID_j \| \alpha \| h(ASK)), D_{ij} = h(PID_i \| Q_j \| \alpha)$.

3) $SC \rightarrow S_j : \{B_{ij}, D_{ij}, \alpha\}$.

7.4 认证阶段

1) S_j 接收到 U_i 的登录请求后,计算 $PID_i = B_{ij} \oplus h(SID_j \| \alpha \| h(ASK)), Q_j = h(PID_i \| K_j)$, 并验证 $D_{ij} \stackrel{?}{=} h(PID_i \| Q_j \| \alpha)$ 是否成立.如果成立,则 S_j 认证 U_i 为合法用户;否则,S_j 终止会话.

2) S_j 生成随机数 $N_2 \in Z_p^*$, 计算 $\beta = N_2 P, K_{ij} = N_2 \alpha, SK = h(Q_j \| K_{ij} \| PID_i), E_{ij} = h(SK \| SID_j \| \beta \| \alpha \| Q_j)$.

3) $S_j \rightarrow U_i : \{E_{ij}, \beta\}$.

4) U_i 计算 $K_{ij} = N_1 \beta, SK = h(Q_j \| K_{ij} \| PID_i)$, 并验证 $E_{ij} \stackrel{?}{=} h(SK \| SID_j \| \beta \| \alpha \| Q_j)$ 是否成立.如果成立,则 U_i 认证 S_j;否则,终止会话.U_i 计算 $F_{ij} = h(SID_j \| \alpha \| \beta \| SK \| Q_j)$.

5) $U_i \rightarrow S_j : \{F_{ij}\}$.

6) S_j 验证 $F_{ij} \stackrel{?}{=} h(SID_i \| \alpha \| \beta \| SK \| Q_j)$ 是否成立.如果成立,则 U_i 和 S_j 完成相互认证,建立会话密钥 SK.

8 Reedy 等人的方案的安全性分析

Reedy 等人[24]宣称所提出的方案可以抵抗各类已知攻击,但本文分析发现,该方案不能抵抗离线口令猜测攻击、仿冒攻击,且不能实现用户匿名性.

8.1 离线猜测攻击

与第 4.1 节类似,在分析三因子协议安全性时,假设攻击者 $\mathcal{A}$ 获得其中两个认证因子(口令、智能卡或生物因子),判断能否威胁第 3 个认证因子.由于用户自主选择的口令 PW_i 往往是弱口令,离线口令猜测攻击对此类协议构成极大威胁.假设攻击者 $\mathcal{A}$ 通过边信道攻击技术(如逆向工程技术[47]、差分能耗分析[48])获得智能卡内敏感信息 $\{X_j, V_i, C_i, T_i, \theta_i, P, h(\cdot), h(ASK)\}$, 并通过恶意扫描器获得用户生物信息 $BIO_{i'}$, 则可以发起口令猜测攻击.

1) $\mathcal{A}$ 计算 $\sigma_{i'} = Rep(BIO_{i'}, \theta_i); r_i = V_i \oplus h(\sigma_{i'})$, 其中,$V_i$ 和 θ_i 从智能卡中获得.

2) 从用户身份空间 $\mathcal{D}_{id}$ 和口令空间 $\mathcal{D}_{pw}$ 猜测 (ID^*, PW^*).

3) $\mathcal{A}$ 计算 $PWD^*_i = h(PW^*_i \| r_i); W^*_j = X_j \oplus PWD^*_i; C^*_i = h(ID^*_i \| W^*_j)$, 其中, X_j 从智能卡中获得.

4) 验证 $C^*_i = C_i$ 是否成立.如果成立,则 (ID^*, PW^*) 猜测正确,否则,转 2).

由于随机数 r_i 只需计算一次,可忽略,则上述攻击的时间复杂度为 $\mathcal{O}((2T_h + T_{xor}) \cdot |\mathcal{D}_{id}| \cdot |\mathcal{D}_{pw}|)$, 实际身份空间和口令空间十分有限($|\mathcal{D}_{id}| \leqslant |\mathcal{D}_{pw}| \leqslant 10^6$ [32,33]),攻击可在多项式时间内完成.不难发现,上述猜测攻击能够成功的根本原因在于,用户智能卡内的参数 C_i 为攻击者提供了验证猜测口令正确性的验证项.一旦攻击者获得参数 PW_i,便可选择随机数 α,计算参数 B_{ij}, D_{ij} 仿冒 U_i 登录任意服务器 S_j.

8.2 仿冒攻击

上一节给出的仿冒攻击中,攻击者 $\mathcal{A}$ 需获得受害用户 U_i 的智能卡.下面给出另一种攻击方式.在 Reedy 等人的方案[24]中,任意用户智能卡中存储注册中心 RC 的长期私钥 Hash 值 $h(ASK)$.如果攻击者 $\mathcal{A}$ 是恶意用户 U_k,可从自己的智能卡中提取参数 $h(ASK)$,发起用户仿冒攻击.

1) $\mathcal{A}$ 截获 $U_i \to S_j : \{B_{ij}, D_{ij}, \alpha\}$;

2) $\mathcal{A}$ 计算 $PID_i = B_{ij} \oplus h(SID_j \| \alpha \| h(ASK))$;

3) $\mathcal{A}$ 从智能卡表 T_k 中提取 R_j,计算 $Q_j = R_j \oplus PWD_k$;

4) $\mathcal{A}$ 生成随机数 $N^*_1 \in Z^*_p$, 计算 $\alpha^* = N^*_1 P; B^*_{ij} = PID_i \oplus h(SID_j \| \alpha^* \| h(ASK)); D^*_{ij} = h(PID_i \| Q_j \| \alpha^*)$;

5) $\mathcal{A} \to S_j : \{B^*_{ij}, D^*_{ij}, \alpha^*\}$.

由于 PID_i 从通信消息中计算所得, D^*_{ij} 可被 S_j 验证通过.攻击者和服务器 S_j 协商新的会话密钥 SK^*. 上述攻击中,攻击者只需侦听通信信道中的消息,可在受害用户完全未知的情况下发起攻击.任意用户的登录请求都成为攻击的有效数据,攻击者利用自己智能卡中存储的 $h(ASK)$推导 PID_i,使用表 T_k 的信息计算服务器 S_j 的安全参数 Q_j,对任意用户实施仿冒攻击.

不难发现,上述攻击的根本原因在于所有用户智能卡中都存储了相同的来自 RC 和 S_j 的安全参数.Reedy 等人在智能卡内放置这些参数的目的是实现“注册中心离线”,即注册中心不参与认证过程,以减少通信各方的通信量,同时避免注册中心成为通信瓶颈[55].除上述安全性问题以外,这一方法引入新的可扩展性问题.随着网络应用的快速发展,在线视频点播、在线游戏等服务需求的增长,多服务器环境的可扩展性成为不可或缺的属性[28].在 Reedy 等人的方案中,如果有新服务器加入系统,用户只有通过重新注册,更新智能卡中的参数才能访问新服务器,这大大增加了用户负担,在大规模系统中是不现实的.

8.3 匿名性失效

我们在上一节中已指出,用户 U_i 提交给任意应用服务器 S_j 的登录请求信息中都携带 PID_i.恶意但合法的用户 U_k 可通过自己智能卡中存储的 $h(ASK)$推算出 PID_i,详见第 8.2 节中的步骤 1 和步骤 2.其中, $PID_i = h(ID_i \| r_i), r_i$ 为注册阶段选取的常数,则 PID_i 是与用户身份标识直接相关的固定参数.攻击者可以依据 PID_i 时刻追踪用户 U_i 的访问过程.故 Reedy 等人的方案[24]不能实现用户匿名性.

事实上,第 4.1 节中已指出,在非抗窜扰智能卡假设情况下,仅采用对称密码技术(如 Hash、异或等)无法实现用户匿名性,因而在 Reedy 等人提出的基于椭圆曲线的远程用户认证方案[24]中可使用椭圆曲线点乘的方法以隐藏真实用户身份标识 ID.

9 协议设计原则的强调

自 1993 年 Chang 等人[56]首次提出基于智能卡的身份认证协议以来,大量“增强型”协议被提出.在这些工作中,他们首先提出对先前方案的攻击,然后再设计新协议,并展示新协议的优势,往往忽略了其不足之处.这就导致总体上,多因子认证协议研究进入一个不理想的“怪圈”.

攻击→改进→攻击→改进...

尽管有大量工作研究现有协议的安全缺陷(如文献[9−11,26,57−59]),但从协议设计原则的视角来分析现有协议缺陷的研究相对较少,故而同样的共性错误一再重复.实际上,本文指出的 Wan 等人的协议[25]、Amin 等人的协议[26]和 Reedy 等人的协议[24]的众多安全缺陷,都是因为违反了下述多因子协议的基本设计原则(见表 3).

Table 3 A summary of the violation of three protocol design principles in recent multi-factor schemes

表 3 现有方案对本节 3 个协议设计基本原则的违反情况

协议设计原则	原则的内涵	典型失效协议
公钥技术原则	在非抗窜扰智能卡假设下,公钥密码技术是实现多因子安全性的必要条件	[5,12,15,20,37,46,52,60−64]
用户匿名性原则	在非抗窜扰智能卡假设下,公钥密码技术是实现用户匿名性的基本组件	[12,17,20,52,59,61−64]
前向安全性原则	公钥密码技术是实现前向安全性的必要条件,且服务器端至少两次公钥运算	[5,12,17,20,34,37,59,60−64]

(1) 公钥技术原则

文献[53]中,Halevi-Krawczyk 提出一个基于口令的单因子身份认证协议,并证明在分布式计算安全模型下(即 Dolev-Yao 模型[29]),仅采用对称密码原语(如 Hash 运算、异或运算)的口令认证协议无法抵抗离线口令猜测攻击.基于这一结果,Ma 等人[27]证明在非抗窜扰智能卡假设情况下,未采用公钥密码技术的双因子认证协议同样无法抵抗离线口令猜测攻击.

根据第 2.2 节中的攻击者模型,在分析三因子协议安全性时,应假设攻击者可获得其中任何两个认证因子(口令、智能卡或生物因子),判断能否威胁第 3 个认证因子.因此,在分析离线口令猜测攻击时,假设攻击者可获得智能卡内秘密参数和生物特征,则三因子安全问题退化为传统的基于“口令+智能卡”的双因子协议的安全问题.不难发现,Wang 等人证明的双因子领域的公钥技术原则同样适用于三因子或更多因子的认证协议.此外,需强调的是,该原则具有普适性,除传统的 C/S 架构外,也适于多服务器架构、无线传感器网络、移动互联网等.

本文分析的 3 个协议,为实现“口令本地安全更新”,在智能卡中均存储口令验证表项,因此无法抵抗离线口令猜测攻击,即存在 Huang 等人提出的“安全性 vs.可用性”平衡问题[2].幸运的是,文献[49]将“模糊验证因子”技术[3]和系统安全领域的 Honeywords 技术相结合,成功地解决了文献[2]中遗留的问题,可实现较好的平衡“安全性 vs.可用性”,并实现超越传统上限的安全性.

(2) 用户匿名性原则

文献[8]中,Wang 等人针对无线传感器网络环境下的“口令+智能卡”双因子协议,提出了匿名性公钥原则:在非抗窜扰智能卡假设情况下,仅采用对称密钥技术来实现用户匿名性的策略本质上是不可行的.文献[8]基于 Havelli-Crawczyk 工作[53]和 Impagliazzo-Rudich 工作[65]严格证明了该原则的有效性.文献[8]还指出,这一原则具有普适性,不仅适用于无线传感器网络环境,同样适用于多服务器环境.故 Wan 等人的协议[25]、Amin 等人的协议[26]仅采用 Hash 函数和异或操作等对称密码原语,在本质上无法实现用户匿名性.尽管 Reedy 等人的协议采用了椭圆曲线密码技术,但该技术仅用于会话密钥的计算,没有对认证消息采用公钥密码运算,忽略了对动态 ID 的保护,因此,Reedy 等人的协议从根本上无法实现匿名性.

(3) 前向安全性原则

协议能够实现前向安全性,即要确保在一方或多方的长期私钥泄漏的情况下,先前建立的会话密钥仍然安全.文献[66]首次研究了密钥协商协议中实现前向安全性的原则,提出前向安全性只能由两种方法来实现.(1) 基于传统的 Diffie-Hellman 密钥交换技术;(2) 基于服务器所选随机数的机密性.文献[27]进一步指出,为实现前向安全性,基于口令的多因子协议必须满足基本条件:(1) 采用公钥密码技术;(2) 服务器端至少需要两次模幂运算或椭圆曲线点乘运算.这很好地解释了文献[25,26]失效的原因.

除了采用传统的Diffie-Hellman密钥交换技术[67,68]以外,基于Chebyshev混沌映射的密钥交换技术[6,11]和动态大整数素因子分解困难性问题[69],也可有效实现前向安全性.其中,基于后者的加密指数一般较小,解密密钥较大(如 RSA、Rabin 等非对称加密算法),从而导致加密端和解密端计算量存在非对称性,设计协议时也可利用这一特性.因此,RSA 或 Rabin 等算法的加密运算更适于存储空间、运算能力和电池能量受限的用户端设备,解

密运算适于资源相对丰富的服务器端.

10 结 语

确保身份认证协议的安全性是一个公开难题,一方面因为实用的密码协议越来越复杂,另一方面在于密码协议的优劣严重依赖于协议设计者的经验:只有知道攻击者如何攻击,协议才能进行更有针对性的防御.本文对多服务器网络环境下的 3 个代表性匿名认证协议进行了安全性分析,突出针对此类协议的一些严重安全威胁,并给出了攻击者可能采取的具体攻击手段,将为此类协议的分析和设计提供更好的参考和借鉴.

具体来说,本文首先回顾 Wan 等人的协议,指出其不能抵抗离线口令猜测攻击,且不能实现用户匿名性和前向安全性;然后分析了 Amin 等人的协议,指出其同样不能抵抗离线口令猜测攻击,且不能提供匿名性,对两种破坏前向安全性的攻击是脆弱的;最后分析了 Reedy 等人的协议,指出其对离线口令猜测攻击和仿冒攻击是脆弱的,且不能实现匿名性.基于 100 余个此类协议分析经验,对破坏前向安全性的攻击场景进行分类,突出被广泛忽略的用户端口令泄漏所及智能卡不安全参数引起的前向安全性问题.

指出前述协议不能抵抗离线口令猜测攻击,无法实现匿名性和前向安全的根本原因在于,违反了 3 个相应的多因子认证协议设计基本原则:公钥技术原则、用户匿名性原则和前向安全性原则.在明确现有协议的根本失误之处后,进一步给出了协议的相应修正方法.根据这些协议设计基本原则,设计高效的、可证明安全匿名多因子认证协议是下一步值得研究的方向.

References:

[1] Lamport L. Password authentication with insecure communication. Communications of the ACM, 1981,24(11):770–772.

[2] Huang X, Chen X, Li J, *et al*. Further observations on smart-card-based password-authenticated key agreement in distributed systems. IEEE Trans. on Parallel and Distributed Systems, 2014,25(7):1767–1775.

[3] Wang D, He D, Wang P, *et al*. Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. IEEE Trans. on Dependable and Secure Computing, 2015,12(4):428–442.

[4] Tsaur WJ. A flexible user authentication scheme for multi-server internet services. In: Proc. of the Int'l Conf. on Networking (ICN 2001). LNCS 2093, 2001. 174–183.

[5] Yi X, Rao F Y, Tari Z, *et al*. ID2S password-authenticated key exchange protocols. IEEE Trans. on Computers, 2016,65(12): 3687–3701.

[6] Jangirala S, Mukhopadhyay S, Das AK. A multi-server environment with secure and efficient remote user authentication scheme based on dynamic ID using smart cards. Wireless Personal Communications, 2017. [doi: 10.1007/s11277-017-3956-2]

[7] Chatterjee S, Roy S, Das AK, *et al*. Secure biometric-based authentication scheme using chebyshev chaotic cap for multi-server environment. IEEE Trans. on Dependable and Secure Computing, 2016. [doi: 10.1109/TDSC.2016.2616876]

[8] Wang D, Wang P. On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions. Computer Networks, 2014,73:41–57.

[9] Wei FS, Zhang G, Ma JF, Ma CG. Privacy-Preserving multi-factor authenticated key exchange protocol in the standard model. Ruan Jian Xue Bao/Journal of Software, 2016,27(6):1511–1522 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5001.htm [doi: 10.13328/j.cnki.jos.005001]

[10] He D, Wang D. Robust biometrics-based authentication scheme for multiserver environment. IEEE Systems Journal, 2015,9(3): 816–823.

[11] Jiang Q, Wei F, Fu S, *et al*. Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy. Nonlinear Dynamics, 2016,83(4):2085–2101.

[12] Chuang MC, Chen MC. An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. Expert Systems with Applications, 2014,41(4):1411–1418.

[13] Liao YP, Wang SS. A secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards & Interfaces, 2009,31(1):24–29.

[14] Yang D, Yang B. A biometric password-based multi-server authentication scheme with smart card. In: Proc. of the 2010 Int'l Conf. on Computer Design and Applications (ICCDA). IEEE, 2010. 554–559.

[15] Yoon EJ, Yoo KY. Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. The Journal of Supercomputing, 2013,63(1):235–255.

[16] Kim H, Jeon W, Lee K, *et al*. Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme. In: Proc. of the 12th Int'l Conf. on Computational Science and Its Applications (ICCSA 2012). IEEE, 2012. 391–406.

[17] Mishra D, Das AK, Mukhopadhyay S. A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. Expert Systems with Applications, 2014,41(18):8129–8143.

[18] Lin H, Wen F, Du C. An improved anonymous multi-server authenticated key agreement scheme using smart cards and biometrics. Wireless Personal Communications, 2015,84(4):2351–2362.

[19] Lu Y, Li L, Yang X, *et al*. Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards. PLOS One, 2015,10(5):e0126323.

[20] Wang C, Zhang X, Zheng Z. Cryptanalysis and improvement of a biometric-based multi-server authentication and key agreement scheme. PLOS One, 2016,11(2):e0149173.

[21] He D. Security flaws in a biometrics-based multi-server authentication with key agreement scheme. IACR Cryptology ePrint Archive, 2011,2011:365.

[22] Jiang P, Wen Q, Li W, *et al*. An anonymous and efficient remote biometrics user authentication scheme in a multi server environment. Frontiers of Computer Science, 2015,9(1):142–156.

[23] Odelu V, Das AK, Goswami A. A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Trans. on Information Forensics and Security, 2015,10(9):1953–1966.

[24] Reddy AG, Yoon EJ, Das AK, *et al*. Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment. IEEE Access, 2017,5:3622–3639.

[25] Wan T, Liu ZX, Ma JF. Authentication and key agreement protocol for multi-server architecture. Journal of Computer Research and Development, 2016,53(11):2446–2453 (in Chinese with English abstract).

[26] Amin R. Cryptanalysis and efficient dynamic ID based remote user authentication scheme in multi-server environment ssing smart card. Int'l Journal of Network Security, 2016,18(1):172–181.

[27] Ma CG, Wang D, Zhao SD. Security flaws in two improved remote user authentication schemes using smart cards. Int'l Journal of Communication Systems, 2014,27(10):2215–2227.

[28] He D, Zeadally S, Kumar N, *et al*. Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures. IEEE Trans. on Information Forensics and Security, 2016,11(9):2052–2064.

[29] Dolev D, Yao A. On the security of public key protocols. IEEE Trans. on Information Theory, 1983,29(2):198–208.

[30] Veyrat-Charvillon N, Standaert FX. Generic side-channel distinguishers: Improvements and limitations. In: Proc. of the Annual Cryptology Conf. Berlin, Heidelberg: Springer-Verlag, 2011. 354–372.

[31] Huang X, Xiang Y, Chonka A, *et al*. A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. IEEE Trans. on Parallel and Distributed Systems, 2011,22(8):1390–1397.

[32] Wang D, Zhang Z, Wang P, *et al*. Targeted online password guessing: An underestimated threat. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security (ACM CCS 2016). ACM, 2016. 1242–1254.

[33] Wang D, Wang P. On the implications of Zipf's law in passwords. In: Proc. of the 21st European Symp. on Research in Computer Security (ESORICS 2016). Springer Int'l Publishing, 2016. 111–131.

[34] Tsai JL. Efficient multi-server authentication scheme based on one-way hash function without verification table. Computers & Security, 2008,27(3):115–121.

[35] Yeh KH, Su C, Lo NW, *et al*. Two robust remote user authentication protocols using smart cards. Journal of Systems and Software, 2010,83(12):2556–2565.

[36] Li H, Yang Y, Pang L. An efficient authentication protocol with user anonymity for mobile networks. In: Proc. of the IEEE Wireless Communications and Networking Conf. (WCNC 2013). IEEE, 2013. 1842–1847.

[37] Sood SK. Dynamic identity based authentication protocol for two-server architecture. Journal of Information Security, 2012,3(4): 326.

[38] Turkanović M, Brumen B, Hölbl M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. Ad Hoc Networks, 2014,20:96–112.

[39] Li X, Niu J, Khan MK, *et al*. An enhanced smart card based remote user password authentication scheme. Journal of Network and Computer Applications, 2013,36(5):1365–1371.

[40] Wang D, Ma C, Zhao S, *et al*. Breaking a robust remote user authentication scheme using smart cards. In: Proc. of the IFIP Int'l Conf. on Network and Parallel Computing (NPC 2012). Berlin, Heidelberg: Springer-Verlag, 2012. 110–118.

[41] Liu B, Jiang Y, Sha F, *et al*. Cloud-Enabled privacy-preserving collaborative learning for mobile sensing. In: Proc. of the 10th ACM Conf. on Embedded Network Sensor Systems. ACM, 2012. 57–70.

[42] Zhu F, Carpenter S, Kulkarni A. Understanding identity exposure in pervasive computing environments. Pervasive and Mobile Computing, 2012,8(5):777–794.

[43] Das ML, Saxena A, Gulati VP. A dynamic ID-based remote user authentication scheme. IEEE Trans. on Consumer Electronics, 2004,50(2):629–631.

[44] Das ML. Two-Factor user authentication in wireless sensor networks. IEEE Trans. on Wireless Communications, 2009,8(3): 1086–1090.

[45] Xue K, Hong P, Ma C. A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. Journal of Computer and System Sciences, 2014,80(1):195–206.

[46] Zhou Y, Yu Y, Standaert FX, *et al*. On the need of physical security for small embedded devices: a case study with COMP128-1 implementations in SIM cards. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer-Verlag, 2013. 230–238.

[47] Duchêne J, Le Guernic C, Alata E, *et al*. State of the art of network protocol reverse engineering tools. Journal of Computer Virology and Hacking Techniques, 2017, 1–16.

[48] Messerges TS, Dabbish EA, Aloan RH. Examining smart-card security under the threat of power analysis attacks. IEEE Trans. on Computers, 2002,51(5):541–552.

[49] Wang D, Wang P. Two birds with one stone: Two-Factor authentication with security beyond conventional bound. IEEE Trans. on Dependable and Secure Computing, 2016. [doi: 10.1109/TDSC.2016.2605087]

[50] Wang D, Gu Q, Cheng H, *et al*. The request for better measurement: A comparative evaluation of two-factor authentication schemes. In: Proc. of the 11th ACM Asia Conf. on Computer and Communications Security (ASIACCS 2016). ACM, 2016. 475–486.

[51] Krawczyk H. HMQV: A high-performance secure Diffie-Hellman protocol. In: Proc. of the Annual Int'l Cryptology Conf. (CRYPTO 2005). Berlin, Heidelberg: Springer-Verlag, 2005. 546–566.

[52] Li CT, Weng CY, Fan CI. Two-Factor user authentication in multi-server networks. Int'l Journal of Security and Its Applications, 2012,6(2):261–267.

[53] Halevi S, Krawczyk H. Public-Key cryptography and password protocols. ACM Trans. on Information and System Security, 1999, 2(3):230–268.

[54] Goodin D. Twitch resets user passwords following breach. 2015. http://arstechnica.com/security/2015/03/twitch-resets-user-passwords-following-breach/

[55] Wang G, Yu J, Xie Q. Security analysis of a single sign-on mechanism for distributed computer networks. IEEE Trans. on Industrial Informatics, 2013,9(1):294–302.

[56] Chang CC, Wu TC. Remote password authentication with smart cards. IEE Proc. E-Computers and Digital Techniques, 1991, 138(3):165–168.

[57] Sun DZ, Li JX, Feng ZY, *et al*. On the security and improvement of a two-factor user authentication scheme in wireless sensor networks. Personal and Ubiquitous Computing, 2013,17(5):895–905.

[58] He D, Gao Y, Chan S, *et al*. An enhanced two-factor user authentication scheme in wireless sensor networks. Ad Hoc & Wireless Sensor Networks, 2010,10(4):361–371.

[59] Amin R, Kumar N, Biswas GP, *et al*. A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment. Future Generation Computer Systems, 2016. [doi: 10.1016/j.future.2016.12.028]

[60] Yeh KH, Tsai KY, Hou JL. Analysis and design of a smart card based authentication protocol. Journal of Zhejiang University (Science C), 2013,14(12):909–917.

[61] Lu Y, Li L, Peng H, *et al*. A lightweight ID based authentication and key agreement protocol for multiserver architecture. Int'l Journal of Distributed Sensor Networks, 2015, Article ID 635890:1–9.

[62] Banerjee S, Dutta MP, Bhunia CT. A perfect dynamic-id and biometric based remote user authentication scheme under multi-server environments using smart cards. In: Proc. of the 8th ACM Int'l Conf. on Security and Information and Networks (SIN 2015). ACM, 2015. 58–64.

[63] Gope P. Enhanced secure mutual authentication and key agreement scheme with user anonymity in ubiquitous global mobility networks. Journal of Information Security and Applications, 2017,35:160–167.

[64] Maitra T, Islam SK, Amin R, *et al*. An enhanced multi-server authentication protocol using password and smart-card: Cryptanalysis and design. Security and Communication Networks, 2016,9(17):4615–4638.

[65] Impagliazzo R, Rudich S. Limits on the provable consequences of one-way permutations. In: Proc. of the 21st Annual ACM Symp on Theory of Computing (STOC 1989). ACM, 1989. 44–61.

[66] Park DG, Boyd C, Moon SJ. Forward secrecy and its application to future mobile communications security. In: Proc. of the Int'l Workshop on Public Key Cryptography (PKC 2000). Berlin, Heidelberg: Springer-Verlag, 2000. 433–445.

[67] Wang C, Xu G, Guo Y. Cryptanalysis of three password-based remote user authentication schemes with non-tamper resistant smart card. Security and Communication Networks, 2017. [doi: 10.1155/2017/1619741]

[68] Xie Q, Wong DS, Wang G, *et al*. Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model. IEEE Trans. on Information Forensics and Security, 2017,12(6):1382–1392.

[69] Wang C, Wang D, Xu G, *et al*. A lightweight password-based authentication protocol using smart card. Int'l Journal of Communication Systems, 2017. [doi: 10.1002/dac.3336]

附中文参考文献:

[9] 魏福山,张刚,马建峰,马传贵.标准模型下隐私保护的多因素密钥交换协议.软件学报,2016,27(6):1511–1522.http://www.jos.org.cn/1000-9825/5001.htm [dio: 10.13328/j.cnki.jos.005001]

[25] 万涛,刘遵雄,马建峰.多服务器架构下认证与密钥协商协议.计算机研究与发展,2016,53(11):2446–2453.

汪定(1985－),男,湖北十堰人,博士,讲师,CCF 专业会员,主要研究领域为公钥密码学,信息安全.

李文婷(1990－),女,博士生,CCF 学生会员,主要研究领域为公钥密码学,信息安全.

王平(1961－),男,博士,教授,博士生导师,CCF 专业会员,主要研究领域为信息安全,系统软件,物联网.