

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 泄露,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 亿用户信息泄露,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,用户口令泄露的可能性远高于服务器私钥泄露的可能性,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 $K_j = h(SID_j \parallel ASK)$, 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 $PID_i = h(ID_i \parallel r_i)$, $PWD_i = h(PW_i \parallel r_i)$.
- 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 $Q_j = h(PID_i \parallel K_j)$, $R_j = Q_j \oplus PWD_i$, 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 $W_j = h(PID_i \parallel USK)$, 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 $X_j = W_j \oplus PWD_i$, $C_i = h(ID_i \parallel W_j)$, $(\sigma_i, \theta_i) = Gen(BIO_i)$, $V_i = r_i \oplus h(\sigma_i)$, 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 $\sigma'_i = Rep(BIO'_i, \theta_i)$, $r_i = V_i \oplus h(\sigma'_i)$, $PID_i = h(ID_i \parallel r_i)$, $PWD_i = h(PW_i \parallel r_i)$, $W_j = X_j \oplus PWD_i$, 验证 $C_i \stackrel{?}{=} h(ID_i \parallel W_j)$, 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 $\alpha = N_1 P$, $B_{ij} = PID_i \oplus h(SID_j \parallel \alpha \parallel h(ASK))$, $D_{ij} = h(PID_i \parallel Q_j \parallel \alpha)$.
- 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 $PID_i = B_{ij} \oplus h(SID_j \parallel \alpha \parallel h(ASK))$, $Q_j = h(PID_i \parallel K_j)$, 并验证 $D_{ij} \stackrel{?}{=} h(PID_i \parallel Q_j \parallel \alpha)$ 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 $\beta = N_2 P$, $K_{ij} = N_2 \alpha$, $SK = h(Q_j \parallel K_{ij} \parallel PID_i)$, $E_{ij} = h(SK \parallel SID_j \parallel \beta \parallel \alpha \parallel Q_j)$.
- 3) $S_j \rightarrow U_i : \{E_{ij}, \beta\}$.
- 4) U_i 计算 $K_{ij} = N_1 \beta$, $SK = h(Q_j \parallel K_{ij} \parallel PID_i)$, 并验证 $E_{ij} \stackrel{?}{=} h(SK \parallel SID_j \parallel \beta \parallel \alpha \parallel Q_j)$ 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 $F_{ij} = h(SID_j \parallel \alpha \parallel \beta \parallel SK \parallel Q_j)$.
- 5) $U_i \rightarrow S_j : \{F_{ij}\}$.
- 6) S_j 验证 $F_{ij} \stackrel{?}{=} h(SID_j \parallel \alpha \parallel \beta \parallel SK \parallel Q_j)$ 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 $\sigma_r = Rep(BIO_r, \theta_r)$; $r_i = V_i \oplus h(\sigma_r)$, 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 $O((2T_h + T_{xor}) \cdot |\mathcal{D}_{id}| \cdot |\mathcal{D}_{pw}|)$, 实际身份空间和口令空间十分有限 ($|\mathcal{D}_{id}| \leq |\mathcal{D}_{pw}| \leq 10^6$ [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 $U_i \rightarrow S_j : \{B_{ij}, D_{ij}, \alpha\}$;
- 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) $\mathcal{A} \rightarrow S_j : \{B_{ij}^*, D_{ij}^*, \alpha^*\}$.

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露的情况下,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 and 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] Tsauro 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 map 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 (ICCD). 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 using 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, Aloian 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.



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.



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