软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(8):2375−2391 [doi: 10.13328/j.cnki.jos.005766]

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

无线传感器网络下多因素身份认证协议的内部人员攻击*

李文婷[1], 汪 定[2], 王 平[1,3]

[1](北京大学 软件与微电子学院,北京 102600)

[2](北京大学 信息科学技术学院,北京 100871)

[3](软件工程国家工程研究中心(北京大学),北京 100871)

通讯作者: 王平, E-mail: pwang@pku.edu.cn

摘 要: 无线传感器网络技术一经提出,迅速得到学术界、工业界的广泛关注,在国防军事、环境监测、智能家居、健康护理等领域发挥着重要作用.身份认证是保障无线传感器网络实时访问的关键安全技术.基于增强的攻击者模型,提出一种被长期忽略的内部攻击威胁,对无线传感器网络环境下的两个代表性认证协议进行了安全性分析.指出 Mir 等人的协议无法抵抗内部攻击和智能卡丢失攻击,且未实现前向安全性;指出 Fang 等人的协议同样无法实现所声称的前向安全性特性,且对内部攻击和智能卡丢失攻击是脆弱的.针对协议具体失误之处,提出相应的解决方案.总结了 7 类应对内部攻击的解决方案.指出了现有方法的不足,提出了合理的解决方案.

关键词: 无线传感器网络;认证协议;内部攻击;智能卡丢失攻击;前向安全性

中图法分类号: TP309

中文引用格式: 李文婷,汪定,王平.无线传感器网络下多因素身份认证协议的内部人员攻击.软件学报,2019,30(8):2375−2391. http://www.jos.org.cn/1000-9825/5766.htm

英文引用格式: Li WT, Wang D, Wang P. Insider attacks against multi-factor authentication protocols for wireless sensor networks. Ruan Jian Xue Bao/Journal of Software, 2019,30(8):2375−2391 (in Chinese). http://www.jos.org.cn/1000-9825/5766.htm

Insider Attacks Against Multi-factor Authentication Protocols for Wireless Sensor Networks

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

[1](School of Software and Microelectronics, Peking University, Beijing 102600, China)

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

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

Abstract: Once after the wireless sensor network technology was proposed, it quickly gained wide attention from the academic and industrial areas, and played a major role in the defense military, environmental monitoring, smart home, health care, and other fields. User authentication is becoming an essential mechanism for real-time access in wireless sensor networks. Based on the enhanced adversary model, a kind of insider attack is pointed out, of which it has been neglected for a long time. Then, two foremost authentication protocols are cryptanalyzed for wireless sensor networks environment. Two more things are point out as well. (1) Mir *et al*.'s protocol cannot resist against insider attack and smart card loss attack, and it also cannot provide forward secrecy; (2) Fang *et al*.'s protocol cannot achieve the claimed goal of forward secrecy and is vulnerable to insider attack and smart card loss attack. It is suggested that a reasonable solution according to the specific mistakes in their protocol and seven solutions in the existing literatures are summarized for dealing with insider attack. Furthermore, the deficiencies of existing methods are pointed out and a reasonable solution is given to resist insider attack.

* 基金项目: 国家重点研发计划(2016YFB0800603, 2017YFB1200700); 国家自然科学基金(61802006)

Foundation item: National Key Research and Development Program of China (2016YFB0800603, 2017YFB1200700); National Natural Science Foundation of China (61802006)

本文由"面向自主安全可控的可信计算"专题特约编辑贾春福教授推荐.

收稿时间: 2018-05-31; 修改时间: 2018-09-21; 采用时间: 2018-12-13; jos 在线出版时间: 2019-03-28

CNKI 网络优先出版: 2019-03-29 09:47:23, http://kns.cnki.net/kcms/detail/11.2560.TP.20190329.0947.017.html

Key words: wireless sensor network; authentication protocol; insider attack; smart card loss attack; forward secrecy

1 引 言

无线传感器网络(wireless sensor network,简称 WSN)历经智能传感器、无线智能传感器、无线传感器这 3 个阶段的发展,无线通信和信息交互能力日益增强,逐渐实现物与物的互联,感知触角深入世界各个角落[1−3].目前,无线传感器网络不仅是学术界关注的热点,在产业界的应用也遍布各个领域,如智慧城市[4]、环境监测[5]、医疗监测[6]等.这些应用往往要求较高的实时性,允许用户实时访问传感器节点.

此类应用环境通常包含 3 类参与者:1 个或多个网关节点(GWN,或称作基站)、分布式节点及外部用户.通常,外部用户要访问传感器节点的信息有两种方式:(1) 用户向 GWN 发送查询请求,GWN 查询相应节点,并回传用户请求的信息;(2) 用户直接登录传感器节点,与传感器节点建立实时通信.前者的安全性依赖 WSN 的安全策略,但时延长,仅适于信息轮询或实时性要求不高的应用场景;后者具备较高的实时性,但如何确保用户的合法性、防止传感器节点数据泄漏变得至关重要.

1.1 相关工作

用户身份认证是保证 WSN 环境安全和用户隐私的重要安全机制[7,8].相比于传统网络环境,由于无线传感器网络通常部署在无人监守的环境,但执行安全攸关的任务(如海洋大气监测[9]、精准农业温度监测[10]、健康状况监测[11]等),设计适于无线传感器网络的用户身份认证协议面临更严峻的挑战.

2006 年,基于 Lamport[12]的口令认证协议和 Das 等人[13]提出的“动态 ID”技术,Wong 等人[14]首次提出了适于无线传感器网络的单因子(因子,亦称为因素)口令身份认证协议.该协议仅基于轻量级密码算法,允许合法用户直接访问传感器节点的数据.然而,在该协议提出不久,Tseng 等人[15]和 Das 等人[16]分别指出 Wong 等人的协议[14]不能抵抗重放攻击、窃取验证项攻击、仿冒攻击和节点捕获攻击,并进一步提出了改进协议[17].其中,Das 等人[16]提出的新协议引入“智能卡”因子,开启了无线传感器网络环境下双因子认证的新篇章.

Das 等人的工作[14]得到了众多学者的跟踪(如图 1 所示,图 1 基于文献[18]中的图 2,下划线表示协议易遭受内部攻击),一系列新的适于无线传感器网络环境的双因子认证协议被提出来,如文献[19,20].

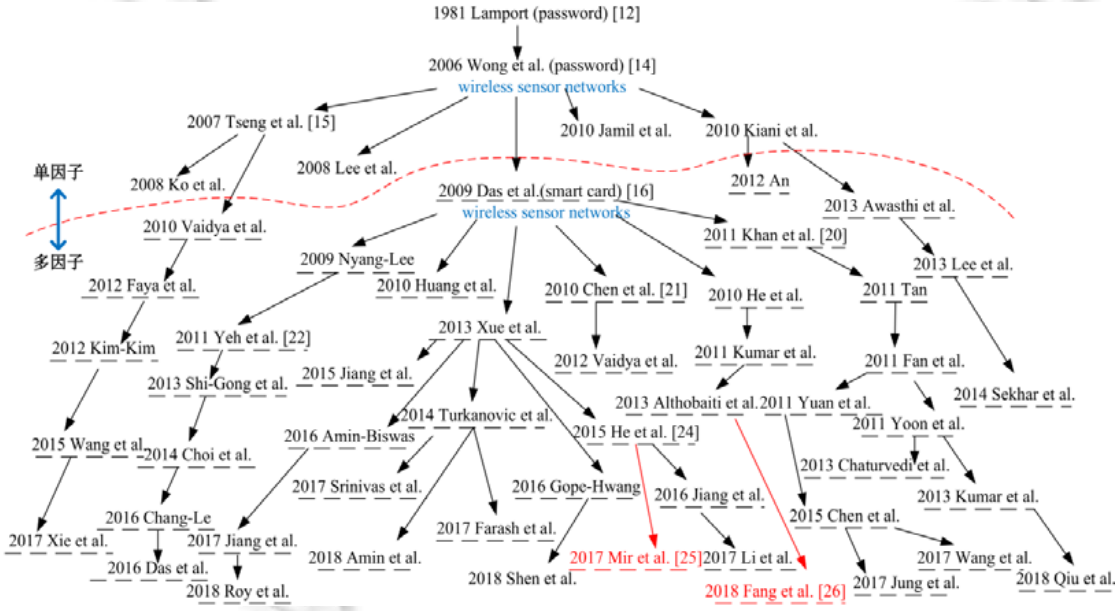

Fig.1 A history of user authentication protocol for wireless sensor networks

图 1 无线传感器网络环境下认证协议历史

然而不久之后,Khan 等人[21]、Chen 等人[22]和 Yeh 等人[23]指出 Das 等人的协议[14]存在一系列安全威胁,如易遭受仿冒攻击、离线口令猜测攻击、内部攻击和节点捕获攻击,且不能实现用户匿名性和前向安全性.随后,Khan 等人[21]、Chen 等人[22]和 Yeh 等人[23]分别在 Das 等人协议[14]的基础上提出改进协议.2012 年,鉴于传感器节点计算能力和存储容量有限,Kumar 等人[24]提出一个高效的适于远程医疗服务的无线传感器网络认证协议.2013 年,He 等人[25]指出 Kumar 等人[24]的协议不能实现用户匿名性,且对离线口令猜测攻击和内部攻击是脆弱的,并进一步提出一个改进协议.

近期,Mir 等人[26]指出 He 等人[25]的协议缺乏口令本地验证,且易遭受离线口令猜测攻击、用户仿冒攻击和违反匿名性攻击.与此同时,Fang 等人[27]指出,早期的 WSN 环境下的安全协议均存在或多或少的问题,以 Althobaiti 等人的协议[28]为例,分析协议中常见的节点捕获攻击、GWN 仿冒攻击、中间人攻击和内部攻击,并给出改进的适于无线传感器网络环境下的远程用户认证协议.

1.2 研究动机

尽管用户认证协议已经过 30 多年的发展,设计安全高效的用户身份认证协议仍面临巨大挑战[3,26].众多安全威胁(如智能卡丢失攻击、仿冒攻击等)和设计难题(如安全性-可用性平衡等)被学者们揭示出来,但关注内部人员攻击的研究却很少.为实现实时访问,常见的无线传感器网络(WSN)应用(如智慧交通、智慧医疗等)允许用户一次登录多次访问,在此类应用环境中,避免内部人员威胁尤为重要.下文分析中,我们将网关节点 GWN 视作传统 C/S 架构下的服务器端.

在早期的单因子口令认证协议中,为实现用户认证,服务器端势必要存储口令相关的验证表项,则内部攻击不可避免.1991 年,Chang 等人[29]首次提出了基于智能卡的口令认证协议,用户的智能卡中需存储私密认证参数.2004 年以前,协议均基于智能卡抗窜扰假设,即智能卡内秘密参数不能被攻击者获取,因此,大多数协议(如文献[29,30])在智能卡中直接存储口令验证项.随着攻击技术的进展,智能卡内的参数可以被分析出来.2004 年,Ku 等人[31]首次提出了基于非抗窜扰假设的“口令+智能卡”双因子认证协议.此后,协议设计者逐渐加强智能卡中存储数据的安全性和认证过程中服务器端存储数据的安全性,同时避免用户直接将口令明文发送给服务器,但却假设注册阶段的通信完全安全.而现实中往往存在内部攻击威胁,注册阶段,服务器并不完全可信,内部人员可通过窃取注册阶段的消息和用户智能卡中的数据猜测出用户口令.但这一类型的内部攻击被长期忽略,即使有协议设计者意识到此类内部攻击的威胁,也并未给出合理的解决方案.

1.3 本文贡献

本文深入分析了 Mir 等人及 Fang 等人的协议,发现这两个无线传感器网络环境下的身份认证协议都存在内部攻击威胁和前向安全性问题,并且对智能卡丢失攻击是脆弱的.

结合现实安全情况,提出了新的增强攻击者模型,指出了一种被长期忽略的内部攻击场景.本文以无线传感器网络为例对此类攻击进行说明,传统的 C/S 网络、移动互联网等均存在此类攻击.需要指出的是:此类攻击场景要求攻击者首先在注册阶段监听用户和服务器的注册信息,当用户注册后,攻击者利用窃取的用户智能卡分析出智能卡内参数信息实施攻击;以 Mir 等人和 Fang 等人的协议为例,分析两种失效的解决方案.

基于我们对 300 余个协议的分析经验,本文对文献中已有的解决方案进行分类总结,指出现有解决方案的不足,说明在用户注册阶段采用“加盐 Hash”技术传输用户口令并且在智能卡中以某种方式保存用户选择的随机数的协议,无法抵抗内部攻击.最后,本文提出合理的解决方案抵抗内部攻击.

1.4 组织架构

第 2 节描述本文采用的攻击者模型,指出一种被长期忽略的内部攻击场景.第 3 节回顾 Mir 等人提出的无线传感器网络环境下的高效身份认证协议.第 4 节分析 Mir 等人协议的安全性.第 5 节描述 Fang 等人提出的基于生物特征的三因子用户认证协议.第 6 节指出该协议存在的安全问题.第 7 节对现有文献中解决内部攻击的策略进行总结,并指出现有方案存在的问题,提出新的解决方案.最后,第 9 节总结全文.

2 增强的攻击者模型及内部攻击场景

设计安全高效的远程用户口令认证协议离不开所基于的攻击者模型.1983 年,Dolev-Yao[32]提出了一个经典的敌手威胁模型,即攻击者可以任意侦听、截获、插入、删除或阻断流经公开信道中的消息.该模型细致地刻画了攻击者的行为能力,被广泛应用于安全协议的设计和分析中.然而,随着近几年边信道攻击技术的发展(如时间攻击、功耗攻击和软件漏洞攻击)[33,34],智能卡内秘密参数信息可以被攻击者分析出来,攻击能力显著增强,早期的模型已不足以刻画攻击者的现实能力.

2016 年,Wang 等人[35]提出一个严格(但实际)的多因素协议攻击者模型,如表 1 中的 C-1~C-4 所示.为评估系统终极失效时的强健性,该模型假设攻击者可以获知服务器长期私钥.该模型充分考虑了攻击者的现实能力,是迄今最严苛的攻击者模型之一.例如,用户口令服从 Zipf 分布,且身份标识空间和口令空间有限,约为$|\mathcal{D}_{id}|\leqslant|\mathcal{D}_{pw}|\leqslant10^6$[36];攻击者可能通过多种途径获得未及时擦除的,或协议公开的过期会话密钥等.Wang 等人[35]的模型全面揭示了敌手的攻击能力,其中,C-1 用以描述重放攻击、中间人攻击、平行会话攻击、异步攻击等,并辅助完成其他各类攻击;C-2 和 C-3 刻画了口令猜测攻击和智能卡丢失攻击;C-4 用以分析前向安全性.该模型几乎涵盖所有攻击方式,在文献[7,17,18,37]中被广泛应用.

Table 1 Capabilites of the adversary

表 1 攻击者拥有的能力

能力	含义
C-1	$\mathcal{A}$可以任意侦听、插入、删除、截获或阻断流经公开信道中的消息[3,19,35]
C-2	$\mathcal{A}$可以离线穷举用户身份标识空间和口令空间$|\mathcal{D}_{id}|\times|\mathcal{D}_{pw}|$的所有元素; 且在评估非隐私安全性时,$\mathcal{A}$可以获知用户身份标识 ID[3,19,35]
C-3	在评估 n-因子安全性时(n=2 或 3),$\mathcal{A}$可以获得以下任意 n−1 个因子:(1) 用户口令;(2) 智能卡内秘密信息;(3) 用户的生物特征信息.但 n 因子不可同时兼得,否则为平凡攻击[19]
C-4	$\mathcal{A}$可以获取过期的会话密钥[3,19]
C-5	$\mathcal{A}$可以腐化服务器 S,侦听、窃取 S 在任意操作中接收的消息,但不能获知服务器长期私钥,仅评估系统终极失效的强健性时可假设$\mathcal{A}$获知服务器长期私钥

然而现实生活中,服务器不应被视作可信实体.近年来,因配置错误、内存泄漏、恶意程序等问题,服务器数据泄漏事件及未授权端口被监听事件层出不穷.2018 年,安全研究人员 Giovanni Collazo 通过 Shodan 搜索引擎发现了 2 284 个暴露在互联网上的 etcd 服务器[38].2016 年,韩国著名购物网站 Interpark 的服务器遭黑客攻击,1 000 万以上客户的个人信息被泄漏[39].文献[40–42]也明确假设服务器中存储的关键数据已经泄漏.在上述安全事件中,攻击者已经腐化服务器,该能力被 Wang 等人[35]提出的攻击者模型所忽略.因此,为刻画此类威胁,我们增加 C-5 攻击者能力:假设$\mathcal{A}$可以腐化服务器 S,侦听、窃取 S 在任意操作(注册、登录、认证阶段)中接收的消息是现实的.

为防止服务器获取口令明文,多数用户认证协议采用“加盐 Hash”技术[43]辅助完成用户注册过程,即在注册阶段,用户向服务器提交使用随机数加盐的随机口令.随后,用户将该随机数写入智能卡中.在 Dolev-Yao 模型和 Wang 等人模型的假设下,由于服务器在注册阶段完全可信,此种注册方式是安全的.但在 C-5 假设下,可能引起潜在的内部人员攻击.我们以 2017 年 Farash 等人[44]在 Adhoc Networks 上提出的协议为例进行说明.该协议方便高效、简单易用,能抵御各种潜在攻击,如重放攻击、平行会话攻击、仿冒攻击等.我们选用 Farash 等人的协议主要因为该协议的用户请求注册过程具备典型性和代表性.

在用户注册阶段,用户 U_i 选取身份标识 ID_i,口令 PW_i 和随机数 b,并计算 $RPW_i=h(PW_i\oplus b)$.用户将$\{ID_i,RPW_i\}$发送给服务器,服务器完成基本的安全检查,比如 ID_i 是否是已经注册过的用户等.然后,服务器计算特定安全参数,将包含安全参数的智能卡发送给用户.最终,U_i 将 b 写入智能卡.根据攻击者能力 C-5,$\mathcal{A}$侦听通信信道,并获得用户随机口令 RPW_i,同时根据 C-3,攻击者$\mathcal{A}$可能无意中(拾取/窃取)获得用户 U_i 的智能卡,则$\mathcal{A}$可以借助边信道攻击技术[33,34]提取智能卡内存储的随机数 b.攻击者$\mathcal{A}$可实施离线口令猜测,具体流程如下:

1) $\mathcal{A}$从用户口令空间$\mathcal{D}_{pw}$猜测可能的口令PW_i^*.

2) 计算$RPW_i^* = h(PW_i^* \oplus b)$.

3) 验证$RPW_i^* = RPW_i$是否成立:如果成立,则PW_i^*猜测正确;否则,转步骤 1).

由于用户口令空间$|\mathcal{D}_{pw}|$十分有限($|\mathcal{D}_{pw}| \leqslant 10^6$ [36]),上述攻击可以在多项式时间内完成.近期,Github[45]和Twitter[46]发现:由于口令重置功能中的系统漏洞,导致用户口令以明文格式记录在公司的内部日志中,少量特权内部员工有权访问记录用户口令的日志文件.Github 和 Twitter 公司均采用"加盐 Hash"技术存储和传输用户口令.这说明:即使在资本雄厚、以技术见长的组织中,针对认证系统的内部人员攻击也有潜在可能,需要纵深防御.但本文提到的内部攻击并未引起重视,鲜有文献明确描述此类攻击过程.需要指出的是,此类攻击场景需要攻击者首先在注册阶段监听到用户和服务器的交互信息;当用户注册后,窃取并分析出用户智能卡内参数信息.因此,这一攻击场景具有一定的局限性.不过,本攻击场景具有普适性,除无线传感器网络,也适于传统的 C/S 架构、多服务器架构、移动互联网等.接下来,我们以 Mir 等人的方案[26]和 Fang 等人的方案[27]为例,分析被长期忽略的内部攻击问题以及协议设计中的常见安全问题.

3 Mir 等人的方案回顾

Mir 等人的方案[26]分为 5 个阶段:用户注册、传感器节点注册、登录、认证和口令修改.系统初始化阶段,网关节点 GWN 生成并安全存储主密钥 d.方案中所使用的符号缩写及其含义见表 2.

Table 2 Notations and abbreviations

表 2 符号及缩写

符号	描述	符号	描述
U_i	第 ith 用户	GWN	网关节点
S_j	第 jth 传感器节点	SID_j	传感器节点 S_j 的身份标识
ID_i	用户 U_i 的身份标识	d,X_{GWN},x	GWN 的主密钥
PW_i	用户 U_i 的口令	$E_{key}(\cdot)$,$D_{key}(\cdot)$	对称密钥加解密函数
SC	智能卡	$h(\cdot)$	安全的无碰撞单向散列函数
$\Rightarrow$	安全通信信道	$\|$	字符串级联操作
$\rightarrow$	公共通信信道	$\oplus$	异或操作

3.1 用户注册阶段

外部用户若要登录系统,则首先执行如下过程.

1) 用户 U_i 选取身份标识 ID_i、口令 PW_i,生成随机数 r_i,计算 $RPW_i=h(PW_i||r_i)$.

2) $U_i \Rightarrow$GWN:$\{PW_i, ID_i\}$.

3) GWN 随机生成安全参数 b,计算 $X_i=h(ID_i||d)$,$TC_i=X_i \oplus RPW_i$,$Q_i=h(RPW_i||X_i||ID_i)$.GWN 在数据库中存储 $\{ID_i \oplus h(d||b)\}$,同时,将$\{TC_i, h(\cdot), h(Q_i)\}$写入智能卡.其中,$d$ 为系统主密钥.

4) GWN$\Rightarrow U_i$:智能卡.

5) U_i 接收到智能卡,计算 $F=r_i \oplus h(ID_i||PW_i)$,将 F 写入智能卡.则此时,智能卡中包含参数$\{TC_i, h(\cdot), h(Q_i), F\}$.

3.2 传感器注册阶段

首先,任意传感器节点 S_j 选择 SID_j 和随机数 y,计算 $V_j=h(SID_j||y)$,将$\{V_j, SID_j\}$通过安全信道发送给 GWN,完成以下注册过程.

1) GWN 计算 $TC_j=h(d||SID_j) \oplus V_j$,将$\{SID_j, V_j \oplus h(SID_j||b)\}$存入数据库.

2) GWN$\Rightarrow S_j$:$\{TC_j\}$.

3) S_j 接收到 GWN 的返回信息后,计算 $G=TC_j \oplus V_j=h(d||SID_j)$,$J=h(h(d||SID_j)||V_j)$,将 J 安全地写入内存中.

3.3 登录阶段

若用户 U_i 要直接访问传感器节点的资源,需进行如下操作.

1) 用户 U_i 在读卡器中插入智能卡,输入 ID_i 和 PW_i.智能卡计算 $r_i=F\oplus h(ID_i||PW_i),RPW_i=h(ID_i||PW_i||r_i),X_i=TC_i\oplus RPW_i=h(ID_i||d),Q_i^*=h(RPW_i\|X_i\|ID_i)$,并验证 $h(Q_i^*)$ 与存储的 $h(Q_i)$是否相等:如果不相等,则说明用户输入的 ID_i 和 PW_i 不正确,智能卡终止执行.
2) 智能卡生成随机数 K_i,计算 $H_i=h(T_1\|K_i\|ID_i),M=E_{X_i}(ID_i\|K_i\|T_1\|H_i)$.其中,$T_1$ 为当前时间戳.
3) $U_i\rightarrow$GWN:$\{M\}$.

3.4 认证阶段

此阶段实现用户、网关节点、传感器节点的相互认证,并建立会话密钥.

1) GWN 收到来自用户的登录请求后,计算 $X_i=h(ID_i||d),M=D_{X_i}(ID_i\|K_i\|T_1\|H_i)$,验证$(T_2-T_1)>\Delta T$ 是否成立(其中,T_2 表示当前时间戳).
   - 如果成立,则表明收到的消息$\{M\}$超出最大时间间隔,GWN 终止用户的登录请求;
   - 反之,GWN 计算 $H_i^*=h(T_1\|K_i\|ID_i)$,并验证 $H_i^*=H_i$ 是否相等:如果不相等,GWN 终止协议.
2) GWN 计算 $J=h(h(d||SID_j)||V_j),H_j=h(K_i||SID_j||ID_i||T_3||T_1),A_j=E_J(ID_i||SID_j||K_i||T_1||H_j)$.其中,$T_3$ 表示当前时间戳.
3) GWN$\rightarrow S_j$:$\{A_j,T_3\}$.
4) S_j 接收到 GWN 的信息后,首先验证$(T_4-T_3)>\Delta T$ 是否在合理的时间间隔内:
   - 如果成立,则终止协议;
   - 反之,S_j 用存储的主密钥 J 解密 $A_j=D_J(ID_i||SID_j||K_i||T_1||H_j)$,计算 $H_j^*=h(K_i\|SID_j\|ID_i\|T_3\|T_1)$,验证 $H_j^*=H_j$ 是否相等:如果不相等,S_j 终止协议;反之,S_j 生成随机数 K_j,计算 $SK=h(K_i||K_j||ID_i||SID_j||T_1)$, $PKS_j=K_j\oplus h(K_i||T_1)$, $SID_j^*=SID_j\oplus h(K_i\|K_j)$, $C_j=h(SID_j||ID_i||K_j||T_5)$.
5) $S_j\rightarrow U_i:\{SID_j^*,T_5,C_j,PKS_j\}$.
6) U_i 收到 S_j 的返回消息后,首先检查$(T_6-T_5)>\Delta T$ 是否成立:
   - 如果成立,则终止连接;
   - 反之,U_i 计算 $K_j=PKS_j\oplus h(K_i\|T_1),SID_j=SID_j^*\oplus h(K_i\|K_j),C_i^*=h(SID_j\|ID_i\|K_j\|T_5)$,并验证 $C_i^*=C_i$ 是否相等:如果不相等,U_i 终止会话;反之,U_i 认证 S_j 和 GWN,且 U_i 和 S_j 之间建立新的通信,协商会话密钥 $SK=h(K_i||K_j||ID_i||SID_j||T_1)$.

4 Mir 等人的方案安全性分析

Mir 等人[26]发现:文献[25]中提出的无线传感器网络环境下的匿名用户认证方案不能实现前向安全性,且不能抵抗离线口令猜测攻击和仿冒攻击.因此,Mir 等人[26]给出了一个高效的适于 WSN 环境的匿名双因子协议,声称该方案弥补了文献[25]的安全缺陷,且使用 BAN 逻辑证明了改进协议的正确性.但经仔细分析,我们发现 Mir 等人的方案[26]仍无法实现前向安全性这一理想属性,且对内部攻击和智能卡丢失攻击是脆弱的.

4.1 内部攻击

分析发现,文献[25]的方案无法抵抗内部攻击,但 Mir 等人没有意识到该安全缺陷.尽管用户注册阶段略有改进,Mir 等人所提出的方案[26]仍继承了这一缺陷.根据第 2 节的攻击者能力 C-5,假设恶意的内部特权用户 $\mathcal{A}$ 侦听并截获用户注册阶段发送给 GWN 的消息$\{RPW_i,ID_i\}$.同时,$\mathcal{A}$可能以某种方式长期占有(窃取/拾取)用户 U_i 的智能卡,并(借助专业机构)通过边信道攻击[33,34]分析出智能卡内秘密参数信息$\{TC_i,h(\cdot),h(Q_i),F\}$,然后,$\mathcal{A}$可通过以下方式离线猜测出用户口令.

1) $\mathcal{A}$从用户口令空间$\mathcal{D}_{pw}$猜测可能的口令 PW_i^*.
2) $\mathcal{A}$计算 $r_i=F\oplus h(ID_i\|PW_i^*)$,其中,$ID_i$ 来自截获的消息,F 从智能卡中提取.

3) $\mathcal{A}$计算 $RPW_i^* = h(ID_i \| PW_i^* \| r_i)$.

4) $\mathcal{A}$验证 $RPW_i^* = RPW$ 是否成立:如果成立,则表明猜测的 PW_i^* 是正确的;否则,转步骤 1).

由于系统缺陷、代码漏洞等,用户提交的注册请求可能泄漏给有权访问系统日志的少数内部员工,故上述假设是合理的.当然,有些学者可能会建议采用更安全的信道执行注册阶段,例如面对面注册.这对安全性要求较高的服务是合理的,例如政府机关、军事机要组织等.但随着云计算、物联网、移动互联网的快速发展,普通大众成为网络服务的主要参与方,用户要访问的资源量明显增多,实时性要求进一步增强.为实现多用户远程实时访问,大多数系统允许用户远程注册,则上述内部攻击过程就不可避免.

此外,文献[25]中构造随机口令的方式与第 2 节描述的经典方案相同,即 $RPW_i=h(PW_i||r_i)$,且在智能卡中明文存储随机数 r_i.攻击者对此方法发起攻击的时间复杂度为 $\mathcal{O}((T_h+T_{xor})\times|\mathcal{D}_{pw}|)$,其中,$T_h$ 为 Hash 操作时间,T_{xor} 为异或操作时间,$|\mathcal{D}_{pw}|$表示用户口令空间.文献[35,36]指出,实际用户口令服从 Zipf 分布,空间大小十分有限,约 $|\mathcal{D}_{pw}|\leqslant 10^6$,故此攻击过程可在多项式时间内完成.Mir 等人[26]似乎意识到文献[25]的注册过程并不安全,但未明确指出.新提出的方案略有改进,其中,随机口令包含用户身份 ID,在智能卡中以 ID_i 和 PW_i 的 Hash 值保护随机数,即存储 $F=r_i\oplus h(ID_i||PW_i)$.但实际仅增加了一次 Hash 操作的难度,攻击的时间复杂度为 $\mathcal{O}((2T_h+T_{xor})\times|\mathcal{D}_{pw}|)$,并没有实质性地增加攻击难度.除此之外,攻击者利用截获的 RPW_i 和智能卡中提取的 TC_i,可直接计算出 X_i,以此仿冒用户登录系统.故 Mir 等人的方案仍易遭受内部攻击.

4.2 智能卡丢失攻击

在 Mir 等人的方案[26]中,存在另一种获取用户口令的方法,即利用用户智能卡内存储的安全参数进行离线口令猜测.统计数据显示:近年来,智能卡丢失是带动智能卡销售的关键因素之一[47].在日常生活中,用户极易将智能卡遗落在读卡器上.一旦攻击者获得用户智能卡,就能通过(自行或求助专业机构)实施边信道攻击分析出智能卡内秘密参数信息 $\{TC_i,h(\cdot),h(Q_i),F\}$.值得一提的是:Mir 等人[26]在攻击文献[25]的方案及分析新方案的安全性时,明确假设“攻击者可能窃取或找到用户丢失的智能卡,并提取卡内秘密参数”.故而,攻击者 $\mathcal{A}$ 可通过以下方法离线猜测出用户口令 PW_i.

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

2) $\mathcal{A}$ 计算 $r_i^* = F \oplus h(ID_i^* \| PW_i^*), RPW_i^* = h(ID_i^* \| PW_i^* \| r_i^*), X_i^* = TC_i \oplus RPW_i^* = h(ID_i^* \| d), Q_i^* = h(RPW_i^* \| X_i^* \| ID_i^*)$,其中,$F$ 和 TC_i 从智能卡中提取.

3) $\mathcal{A}$验证 $h(Q_i^*) = h(Q_i)$ 是否成立:如果成立,则表明猜测的 (ID_i^*,PW_i^*) 是正确的;否则,转步骤 1).

上述口令猜测攻击的时间复杂度为 $\mathcal{O}((4T_h+2T_{xor})\times|\mathcal{D}_{id}|\times|\mathcal{D}_{pw}|)$,其中,$T_{xor}$ 为异或操作时间.现实中,异或运算的时间相对较短,可忽略不计.文献[39,48]皆指出,用户身份 ID 通常遵循特定格式,评估非隐私安全时可视作公开信息.另一方面,第 4.1 节提出的内部攻击中,用户 ID 在注册阶段以明文传输,并保存在 GWN 的验证表项里,可能由于管理员的疏忽或系统漏洞泄漏用户身份 ID.则上述攻击的时间复杂度弱化为 $\mathcal{O}((4T_h+T_{xor})\times|\mathcal{D}_{pw}|)$,故攻击者可通过丢失的智能卡在多项式时间内猜测出用户口令.

不难发现,Mir 等人的协议存在内部攻击的本质原因是在智能卡内存储安全参数 $h(Q_i)$,以验证用户输入的口令,实现“口令本地自由更新”,但此参数同时为攻击者提供了验证口令的预言机服务.为解决上述安全性和可用性平衡问题,可采用文献[35]中提出的“模糊验证因子”+“Honeywords”技术,即将 Q_i 的计算方式修改为 $Q_i=h(RPW_i||X_i||ID_i) \bmod n$,且 GWN 维护用户尝试登录的 Honeywords 列表.其中,n 表示用户身份和口令 (ID,PW) 池容量的整数,一般满足 $2^4\leqslant n\leqslant 2^8$.若用户尝试登录次数达到阈值,则锁定该账号.

4.3 前向安全性问题

通常情况下,无线传感器网络均部署在无人监管的环境,且执行高安全性的任务,如战场环境监测、健康状况检测和交通监管等[3,4].一方面,传感器中存有敏感数据,易引起攻击者的注意;另一方面,相比于网关节点 GWN,传感器节点的安全保护措施明显不足.因传感器节点内存容量和电池容量限制等因素,一般不配备防篡

改硬件,这使得敌手更可能在物理上捕获传感器节点.一旦攻击者$\mathcal{A}$捕获传感器节点 S_j,则$\mathcal{A}$可获得 S_j 的长期私钥 J.同时,根据第 2 节的攻击者能力 C-1,$\mathcal{A}$可侦听、截获任意合法用户 U_i,GWN 和 S_j 之间的通信消息,则$\mathcal{A}$可利用截获的通信消息和 S_j 的长期私钥推导出先前的会话密钥,具体过程如下.

1) $\mathcal{A}$截获 GWN 发送给 S_j 的消息$\{A_j,T_3\}$.
2) $\mathcal{A}$使用 S_j 存储的秘密参数 J 解密 $A_j=D_J(ID_i||SID_j||K_i||T_1||H_j)$,获得 ID_i,SID_j,K_i,T_1,H_j.
3) $\mathcal{A}$截获 S_j 回送给用户的消息 $\{SID_j^*,T_5,C_j,PKS_j\}$.
4) $\mathcal{A}$计算 $K_j = PKS_j \oplus h(K_i \| T_1), SID_j = SID_j^* \oplus h(K_i \| K_j)$,其中,$K_i$ 和 T_1 从步骤 2)中获得.
5) $\mathcal{A}$推导出会话密钥 $SK=h(K_i||K_j||ID_i||SID_j||T_1)$.

可以看出:K_i,K_j,ID_i,SID_j 和 T_1 均为截获或推导出的正确数值,攻击者可获得合法的会话密钥 SK.除此之外,$\mathcal{A}$能够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[49]中证明了:为实现前向安全性,公钥密码技术不可或缺.此外,在服务器端至少进行两次模幂运算或椭圆曲线点乘运算[17].Mir 等人的方案[26]中未采用公钥密码技术,本质上无法实现前向安全性.故建议在 Mir 等人的方案中引入 Diffie-Hellman 密钥交换技术、椭圆曲线技术[50]、Chaotic Maps 技术[51]等轻量级公钥密码技术,以实现前向安全性.

5 Fang 等方案回顾

2018 年,Fang 等人[27]提出一个高效、实用的基于生物特征的三因子用户认证协议.该协议能抵抗各种潜在攻击,如仿冒攻击、重放攻击等,有效实现用户匿名性、口令和生物特征自由更新.Fang 等人的方案[27]包含 4 个阶段:注册、登录、认证、口令和生物特征更新.

5.1 注册阶段

当用户 U_i 访问传感器网络时,需向 GWN 完成如下注册过程.

1) U_i 选择身份标识 ID_i 和口令 PW_i,扫描生物特征 B_i,生成随机数 K,利用生物特征模糊提取函数 $Gen(\cdot)$ 计算 $Gen(B_i)=(\sigma_i,\tau_i)$,生成 B_i 对应的密钥σ_i 和公共参数τ_i,其中,σ_i 仅为 U_i 所知.U_i 进一步计算 $RPW_i=h(PW_i||K)$,选取 key_i 作为 U_i 与 GWN 的共享密钥.
2) $U_i \Rightarrow$GWN:$\{RPW_i,ID_i,key_i\}$.
3) GWN 在数据库中存储 key_i,利用主密钥 X_{GWN} 计算 $r_i=h(ID_i||X_{GWN})$,将$\{r_i,h(\cdot)\}$写入智能卡.
4) GWN$\Rightarrow U_i$:智能卡.
5) U_i 收到 GWN 返回的智能卡后,计算 $e_i=h(ID_i||\sigma_i)\oplus K, f_i=h(ID_i||RPW_i||\sigma_i)\oplus K, g_i=h(ID_i||\sigma_i)\oplus key_i, l_i=r_i\oplus h(ID_i||K)=h(ID_i||X_{GWN})\oplus h(ID_i||K)$,并用 l_i 替换 r_i,同时在智能卡中存储参数$\{e_i,f_i,g_i,Gen(\cdot),Rep(\cdot),\tau_i\}$.

5.2 登录阶段

当用户 U_i 要登录传感器网络时,将进行以下操作.

1) U_i 在读卡装置中插入 SC_i,输入 ID_i,PW_i 和生物特征 B_i^*.SC_i 计算 $\sigma_i^* = Rep(B_i^*,\tau_i), K^* = h(ID_i \| \sigma_i^*) \oplus e_i$, $RPW_i^* = h(PW_i \| K^*), f_i^* = h(ID_i \| RPW_i^* \| \sigma_i^*)$,并验证 $f_i^* = f_i$ 是否相等:如果不相等,则终止操作.
2) SC_i 进一步计算 $key_i=g_i\oplus h(ID_i||\sigma_i), C_1=l_i\oplus h(ID_i||K)=h(ID_i||X_{GWN})$,生成随机数 RN_i,选择将要访问的节点 S_j,计算 $C_2=C_1+RN_i=h(ID_i||X_{GWN})\oplus RN_i, C_3=h(ID_i||SID_j||C_1||RN_i||T_1)$.其中,$T_1$ 表示当前时间戳.
3) $U_i \rightarrow GWN:\{E_{key_i}(SID_j,C_2,C_3,T_1)\}$.

5.3 认证阶段

GWN 收到来自用户登陆请求后,利用 key_i 解密 $D_{key_i}(SID_j,C_2,C_3,T_1)$,得到参数$(SID_j,C_2,C_3,T_1)$,继续执行以下操作.

1) 验证$|T_2-T_1|\leq\Delta T$ 是否成立:

- 如果不成立,则终止协议;
- 反之,GWN 计算 $C_4=h(ID_i||X_{GWN}),C_5=C_2\oplus h(ID_i||X_{GWN})=h(ID_i||X_{GWN})\oplus RN_i\oplus h(ID_i||X_{GWN})=RN_i,C_6=h(ID_i||SID_j||C_4||C_5||T_1)$,并验证 $C_6=C_3$ 是否成立:若成立,表明 U_i 是合法用户;否则,GWN 终止操作.

接下来,GWN 提取 S_j 的主密钥 MK_j,计算 $C_7=E_{MK_j}(ID_i,SID_j,C_5,h(C_4),T_1,T_3)$.其中,$T_3$ 表示当前时间戳.

2) GWN$\Rightarrow S_j$:$\{SID_j,C_7\}$.

3) S_j 接收到来自 GWN 的消息后,解密 C_7 得到 ID_i, SID_j^* ,C_5,$h(C_4)$,T_1 和 T_3,验证 $SID_j^*=SID_j$ 和$|T_4-T_3|\leqslant\Delta T$ 是否成立.其中, SID_j^* 是解密所得,而 SID_j 是接收到的消息.如果上述两项均成立,则 S_j 成功认证 U_i;若任意一项不成立,则终止操作.进一步,S_j 生成随机数 RN_j,计算会话密钥 $SK=h(ID_i||SID_j||h(C_4)||C_5||RN_i||T_1||T_5),C_8=h(SK),C_9=C_5\oplus RN_j\oplus ID_i=RN_i\oplus RN_j\oplus ID_i$.其中,$T_5$ 表示当前时间戳.

4) $S_j\rightarrow U_i$:$\{C_8,C_9,T_5\}$.

5) U_i 接收到 S_j 的返回消息后,首先检验$|T_6-T_5|\leqslant\Delta T$ 是否成立.
   - 如果不成立,则终止连接;
   - 反之,SC_i 计算 $C_{10}=C_9\oplus RN_i\oplus ID_i=RN_j,SK=h(ID_i||SID_j||h(C_4)||RN_i||C_{10}||T_1||T_5),C_{11}=h(SK)$,并验证 $C_{11}=C_8$ 是否相等:如果相等,则 U_i 成功认证 S_j;否则,U_i 终止操作.U_i 和 S_j 实现相互认证,并建立共享会话密钥 SK.

6 Fang 等人方案安全性分析

近期,Fang 等人[27]指出,Althobaibi 等人的方案[28]无法抵抗节点捕获攻击,GWN 仿冒攻击和中间人攻击,并且对内部攻击是脆弱的,故提出改进方案.Fang 等人提出的改进方案[27]仅采用对称密码技术,简单高效,适于资源受限的无线传感器网络.然而经分析,Fang 等人的方案[27]仍无法实现所宣称的抗内部特权攻击和智能卡丢失攻击,且存在前向安全性问题.

6.1 内部攻击

分析发现,Fang 等人[27]企图引入生物因子弥补内部攻击的安全漏洞并不可取.

- 一方面,生物特征具有唯一性和稳定性,一旦丢失将不可挽回[52,53].近几年,生物信息泄漏时有发生.2016 年,美国人事管理办公室(OPM)和国防部发现在最近的 OPM 数据泄露事故中,2 150 万人的敏感信息被盗,其中约 560 万人的指纹记录被泄漏[54].
- 另一方面,指纹等生物信息易于伪造.现实生活中,简单使用透明胶带或指纹膜即可伪造指纹.

因此,假设攻击者通过某种途径(系统泄漏、伪造或窃取)获取用户生物信息是现实的.

值得一提的是,多因子安全性是多因素认证协议最基本的安全目标,即假设攻击者获取多因子中的 $n-1$ 个因子,仍不能推测出另一因子或仿冒用户.在 Fang 等人[27]的三因子认证协议中,假设攻击者$\mathcal{A}$获得:1) 用户口令;2) 智能卡内秘密参数;3) 用户生物特征.其中任意两因子,仍不能得到最后一个因子,即攻击者能力 C-3.根据以上推断及第 2 节中攻击者能力 C-1,我们假设攻击者$\mathcal{A}$通过侦听用户注册阶段,截获用户注册请求消息$\{RPW_i,ID_i,key_i\}$,并以某种方式(如拾到智能卡和用指纹膜提取指纹信息)获得了用户智能卡和生物信息,$\mathcal{A}$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[33]提取智能卡内敏感信息$\{l_i,e_i,f_i,g_i,h(\cdot),Gen(\cdot),Rep(\cdot),\tau_i\}$;

2) $\mathcal{A}$从用户口令空间$\mathcal{D}_{pw}$中猜测 PW_i^*;

3) $\mathcal{A}$计算 $K^*=h(ID_i||\sigma_i)\oplus e_i$, $RPW_i^*=h(PW_i^*\|K^*)$,其中,e_i 从智能卡中提取,ID_i 从传输信道中获得;

4) $\mathcal{A}$验证 $RPW_i^*=RPW_i$ 是否相等:如果相等,则 PW_i^* 猜测正确;否则,转步骤 2).

事实上,很多协议(如文献[48])允许用户在注册阶段直接将生物因子传输给服务器,恶意管理员可在远程传输的过程中截获或内部提取用户生物信息.故假设攻击者获得用户生物信息是合理的.在这一假设下,上述攻击方式与第 4.1 节中提出的攻击方式一致,攻击者可在多项式时间内离线猜测出用户口令.

6.2 智能卡丢失攻击

用户会选择便于记忆的低熵口令,而且用户可能利用个人信息构造口令,或重用口令,这些用户行为都会显著降低攻击者猜测口令的难度.近期,Wang 等人在文献[53]中指出,对安全的三因子认证协议,假设攻击者获取了用户智能卡和生物特征,仍能保证用户口令的安全性.事实上,由于在线或离线字典攻击技术的发展,确保三因子安全性并非易事.在 Fang 等人的协议[27]中,假设攻击者通过边信道攻击技术(如差分能耗分析[33]、逆向工程技术[34]等)获得受害者智能卡内敏感信息[17],并通过 PC 或支付设备的恶意扫描器获得用户生物信息 B_i,则可以发起离线口令猜测攻击.

1) $\mathcal{A}$通过边信道攻击技术提取智能卡内敏感信息$\{l_i,e_i,f_i,g_i,h(\cdot),Gen(\cdot),Rep(\cdot),\tau_i\}$.
2) $\mathcal{A}$计算$\sigma_i=Rep(B_i,\tau_i)$,其中,B_i通过其他途径获得,例如从 PC 或者刷脸支付设备中窃取.
3) $\mathcal{A}$从用户身份空间$\mathcal{D}_{id}$和口令空间$\mathcal{D}_{pw}$猜测(ID_i^*,PW_i^*).
4) $\mathcal{A}$计算$K^*=h(ID_i^*\|\sigma_i)\oplus e_i, RPW_i^*=h(PW_i^*\|K^*), f_i^*=h(ID_i^*\|RPW_i^*\|\sigma_i)$,其中,$e_i$从智能卡中提取.
5) $\mathcal{A}$验证$f_i^*=f_i$是否相等:如果相等,则(ID_i^*,PW_i^*)猜测正确;否则,转步骤 3).

一旦攻击者猜测出正确的(ID_i^*,PW_i^*),可利用智能卡内存储的参数 l_i 和 g_i,选择随机数 RN_i,进一步仿冒用户 U_i 与任意服务器 S_j 通信.值得一提的是:上述攻击的时间复杂度为$\mathcal{O}((3T_h+T_{xor})\times|\mathcal{D}_{id}|\times|\mathcal{D}_{pw}|+T_b)$,其中,$T_b$ 表示生物特征模糊提取技术的操作时间,T_h 表示 Hash 操作时间,T_{xor} 为异或操作时间.文献[35,51]中的测试结果表明,类似的攻击可在两周内在单台 PC 上完成(其中,T_h(SHA-1)≈0.598μs,T_{xor}≈0.006μs,T_b 只执行 1 次,可忽略不计).如果借助亚马逊 AWS 云服务或微软 Azure 云服务,上述攻击可在几小时内完成.

不难发现,存在上述攻击的根本原因是用户智能卡中存储了口令验证项 f_i.为实现用户口令本地自由更新,同时防止离线口令猜测攻击,仍建议采用 Wang 等人[35]提出的"模糊验证因子"技术,修改 f_i 的计算方式为 $f_i=h(ID_i\|RPW_i\|\sigma_i) \bmod n$.假设$|\mathcal{D}_{id}|\leqslant|\mathcal{D}_{pw}|\leqslant10^6$ [36],$2^4\leqslant n\leqslant2^8$,则至少存在 2^{32} 个候选(ID,PW)阻碍攻击者猜测出正确的口令.

6.3 前向安全性问题

Fang 等人在文献[27]中指出,基于 Dolev-Yao 攻击者拓展模型,Althobaiti 等人的协议[28]不能抵抗节点捕获攻击,故 Althobaiti 等人的协议未实现前向安全性.Fang 等人[27]明确假设:一旦攻击者$\mathcal{A}$捕获传感器节点 S_j,即可获取 S_j 的长期私钥 MK_j,这与第 2 节中攻击者能力 C-5 一致.在此假设下,攻击者$\mathcal{A}$可通过侦听、截获任意用户 U_i 和 S_j 通信的公开信道的消息,获取 U_i 和 S_j 的会话密钥,具体流程如下.

1) $\mathcal{A}$侦听并截获 GWN 发往 S_j 的消息$\{SID_j,C_7\}$.
2) $\mathcal{A}$利用 S_j 的主密钥解密 C_7 得到 $ID_i,SID_j,C_5,h(C_4),T_1$ 和 T_3.
3) $\mathcal{A}$侦听并截获 S_j 回送给 U_i 的消息$\{C_8,C_9,T_5\}$,提取 T_5,并计算 $RN_j=C_9\oplus C_5\oplus ID_i$.
4) $\mathcal{A}$计算会话密钥 $SK=h(ID_i\|SID_j\|h(C_4)\|C_5\|RN_j\|T_1\|T_5)$.

最终,攻击者计算 $C_8=h(SK)$,验证计算的 C_8 是否与截获的 C_8 相等:如果相等,则说明攻击者$\mathcal{A}$获得了 U_i 和 S_j 先前的会话密钥,则$\mathcal{A}$可利用该会话密钥和截获的通信消息,解密 U_i 和 S_j 的通信.可见,一旦传感器节点 S_j 被攻击者捕获,任意用户与 S_j 的通信将会完全暴露给攻击者.值得一提的是,为了实现上述攻击,$\mathcal{A}$只需侦听通信信道中的消息,无需与 GWN 交互,$\mathcal{A}$实施攻击后,可在 GWN 未察觉的情况下,重启节点 S_j.

在 Fang 等人的协议[27]中,会话密钥的安全性与传感器节点的主密钥唯一相关.而在开放的网络环境中,恶意管理员或外部攻击者可能腐化或控制传感器节点,因此应确保会话密钥与传感器节点主密钥之间的独立性.为此,可采用 Diffie-Hellman 密钥交换技术将 Fang 等人协议中的随机数 RN_i 和 RN_j 修改为 g^{RN_i} 和 g^{RN_j},在会话密钥 SK 的计算中级联 $g^{RN_i\cdot RN_j}$,且 RN_i 和 RN_j 无需传输.由于仅用户 U_i 和与之通信的传感器节点 S_j 知道随机数 RN_i 和 RN_j,攻击者无法从通信消息中计算出会话密钥,则可确保会话密钥的安全性.

综上,我们根据文献[18]中提出的标准对 Mir 等人的协议[26]和 Fang 等人的协议[27]进行了综合性的评估,见

表 3.基于本文增强的攻击者能力假设,目前已有的多因素认证协议均未能实现 C3,即服务器管理人员可能通过内部攻击获得用户口令.上文中已分析,Mir 等人的协议和 Fang 等人的协议均无法实现标准 C4,C5,C12.此外,两个协议中未提及智能卡撤销操作,即无法实现 C6;且采用时间戳机制,则无法实现 C8.

Table 3 A systematic evaluation of Mir, *et al*.'s protocol and Fang, *et al*.'s protocol

表 3 Mir 等人的协议和 Fang 等人的协议综合性评估

方案	标准											
	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12
Mir 等人的协议	✓	✓	×	×	×	×	✓	×	✓	✓	✓	×
Fang 等人的协议	✓	✓	×	×	×	×	✓	×	✓	✓	✓	×

注:C1:无口令验证表项;C2:口令友好性;C3:无口令泄露;C4:抗智能卡丢失攻击;
C5:抗各种已知攻击;C6:可修复性;C7:密钥协商;C8:无时钟同步;
C9:检测错误口令输入;C10:双向认证;C11:用户匿名性;C12:前向安全性

7 改进策略

自 1981 年 Lamport[12]首次提出口令认证密钥交换协议(PAKE)以来,基于口令的认证协议获得长足发展.然而早期的仅口令认证的协议,由于服务器负责验证用户输入口令的正确性,服务器不可避免地要存储口令相关的验证表项,势必存在内部攻击问题.1991 年,Chang 等人[29]首次将智能卡引入用户身份认证协议,智能卡的出现,极大地缓解了内部攻击问题.智能卡代替服务器验证用户口令,尽管并未从根本上解决离线口令猜测攻击,但却有效缓解了服务器端口令泄漏风险.本节将分析现有研究中针对内部攻击的增强策略的不足之处,并提出合理的解决方案.

7.1 已有增强策略

文献[55–57]中提出了一种常见的内部攻击场景,即用户在注册阶段将明文口令 PW 发送给服务器(如文献[58–60],服务器内部人员可能尝试利用窃取的用户口令访问其他网站的服务.文献[35]中指出,由于用户需要管理大量帐号信息,而用户记忆力有限,口令重用现象十分明显,因此上述内部攻击是现实的.近几年,协议设计者意识到存在内部人员威胁,协议设计中已基本避免此种类型的攻击发生.然而,本文第 2 节中提到的攻击场景并未引起广泛重视.

Amin 等人在文献[61]中指出,Xue 等人的协议[62]存在第 2 节指出的内部攻击,即用户将随机数加盐的口令发送给服务器,内部人员可能通过窃听服务器的通信、窃取用户智能卡的方式离线猜测出用户口令.但在随后提出的新协议中,Amin 等人并未给出合理的解决方法.同样的攻击在文献[63]中也明确提及,但仍未给出解决策略.文献[64–69]中虽未明确说明,但作者考虑到可能存在这一攻击,故在设计新协议时采取了适当的修正措施.分析发现:存在此类型内部攻击的关键在于随机数的保存,由于攻击者能够通过边信道攻击等技术[33,34]从窃取的智能卡中获得随机数,才使得上述内部攻击得以实现.

基于 300 余个用户身份认证协议的分析经验,本文将现有协议中抵抗第 2 节提出的内部攻击的改进策略分为 7 类,见表 4.其中,方案 I 应用最为广泛,如文献[61,64–66].其注册过程不变,即用户向服务器发送用随机数加盐的随机口令,但在智能卡中不存储随机数明文 r_i,而保存 $r_i \oplus h(ID_i||PW_i)$.从第 4.1 节的分析中可以看出,此种方案仅给攻击者增加了一次 Hash 的难度,并未阻止攻击者离线猜测用户口令.第 6.1 节中给出了方案 II 的实例分析.现实生活中,用户生物特征信息泄漏现象时有发生,且生物信息一旦泄漏将无法挽回.遗憾的是,就我们所知,大量文献(如[67–69])均基于生物信息安全可靠的假设,生物信息安全性缺乏应有的关注.根据第 6.1 节的攻击实例可得,方案 II 的攻击与方案 I 的攻击难度相当,但涉及用户隐私泄漏,方案 II 存在更大的安全威胁.

文献[70]中,Namasudra 等人提出一个基于 Chebyshev 多项式的简单、高效的用户口令认证协议.该协议注册阶段允许任意用户 U_i 将身份标识 ID_i 和随机口令 $RPW_i=h(PW_i||ID_i)\oplus r_i$ 发送给服务器.服务器计算 $A_i=h(ID_i||x)$, $C_i=A_i\oplus RPW_i$,将 C_i 写入智能卡并传送给用户.其中,r_i 为用户选择的随机数,x 为服务器主密钥.用户接收到智能卡后,计算 $d_1=C_i\oplus r_i$,$d_2=h(PW_i||ID_i)$,以 d_1,d_2 替换智能卡中的 C_i.可以看出:随机数 r_i 包含在 d_1 中,而计算出 d_1 的关键

在于服务器的主密钥 x,我们称这种保护随机数的方法为方案 III.事实上,方案 III 易遭受智能卡丢失攻击.假设攻击者$\mathcal{A}$已获得智能卡内秘密参数信息,则$\mathcal{A}$可以直接猜测合理的 (ID_i^*,PW_i^*),计算 $d_2^*=h(PW_i^*\|ID_i^*)$,并验证计算的 d_2^* 是否等于提取的 d_2:如果相等,则表明$\mathcal{A}$猜测的 (ID_i^*,PW_i^*) 是正确的.攻击过程无需侦听通信信道,针对方案 III 的离线口令猜测攻击更易实施.

Table 4 A taxonomy of improvement strategies

表 4 改进策略分类

方案	描述	可能存在的问题	典型失效协议
方案 I	*ID*,*PW* 保护随机数	内部攻击	第 4.1 节,Wu 等人[64]
方案 II	用户的生物特征保护随机数	内部攻击、隐私泄露	第 6.1 节,Odelu 等人[67]
方案 III	服务器主密钥保护随机数	无本地验证、智能卡丢失攻击	Namasudra 等人[70]
方案 IV	服务器无 *PW*,注册阶段仅发送 *ID*	无本地验证、用户不能自选口令	Wang 等人[71]、Amin 等人[72]
方案 V	不选随机数,使用 *ID* 保护 *PW*	智能卡丢失攻击、内部攻击	Amin 等人[73]
方案 VI	不选随机数,使用生物特征信息保护 *PW*	隐私泄漏、内部攻击	Farash 等人[69]
方案 VII	不选随机数,服务器公钥保护 *PW*	内部攻击	Sood 等人[55]

为防止智能卡丢失攻击和内部人员攻击,Wu 等人[74]给出另一种以服务器主密钥保护随机数的方案 III.在注册阶段,用户向服务器发送$\{ID_i,RPW_i\}$.服务器选择随机数 e_i,计算 $T_1^*=h(ID_S\|x\|e_i)\oplus RPW_i\oplus h(ID_i\|e_i),T_2^*=h(ID_i\|e_i)\oplus RPW_i$,服务器将 $\{T_1^*,T_2^*,e_i\}$ 写入智能卡并发送给用户.用户收到智能卡后计算 $T_1=T_1^*\oplus r_i,T_2=T_2^*\oplus r_i$,并用 T_1,T_2 替换 T_1^*,T_2^*.然而在 Wu 等人的[74]方案中,由于智能卡无法获知服务器主密钥 x,因此不能验证用户输入的口令是否正确.口令验证过程由服务器实现,则不能实现“口令本地自由更新”.

方案 IV 也存在两种实现方法.

- 文献[71]中,Wang 等人提出一个高效的基于动态 ID 的远程用户口令认证协议.该协议注册阶段仅将用户身份标识 ID_i 发送给服务器,由服务器选择用户口令,并将口令 PW_i 以明文发送给用户.可见,Wang 等人的协议[71]不支持用户自由选择口令,仍然存在内部攻击威胁.
- 文献[72]中,Amin 等人对方案 IV 的实现方法略有改进.用户在注册阶段发送身份标识 ID_i,服务器返回智能卡后,用户再输入选择的 PW_i.经分析,Amin 等人的方案[72]缓解了上述内部攻击,但存在两种类型的智能卡丢失攻击:一是直接利用智能卡内存储的秘密参数进行口令猜测;另一种是借助智能卡内信息和公开信道中的消息进行口令猜测.因此,方案 IV 也不可取.

与上述方案不同,文献[73]在注册阶段未选择随机数,用户计算 $HPW_i=h(PW_i\|ID_i)$,将 ID_i 和 HPW_i 发送给服务器.我们称此类方法为方案 V.不难看出,内部攻击者可直接通过截获的通信消息猜测出用户口令,故方案 V 未解决内部攻击问题.方案 VI 与方案 V 如出一辙,以用户生物特征替换 ID_i 来计算 HPW_i.依据第 6.1 节的实例分析,方案 VI 仍存在内部攻击威胁.此外,由于用户将生物特征发送给服务器,还可能存在隐私泄露风险.

文献[55]中,Sood 等人提出一种基于公钥密码技术的口令认证协议.在系统初始化阶段,服务器选择公私钥对,并公开公钥 *PK*.用户注册过程先选择会话密钥 *SS*,以会话密钥加密用户自主选择的身份标识和口令,再以服务器公钥 *PK* 加密会话密钥 *SS*,即用户将$\{(SS)_{PK},(ID_i)_{SS},(PW_i)_{SS}\}$发送给服务器.

此类方案有效解决了传输消息的安全性,但假设恶意内部管理员有权解密用户注册请求或监听到服务器解密及计算过程,则依然能获得用户口令.

总之,第 2 节中提到的内部攻击威胁并未引起广泛关注,文献[17,35,75]仍建议将随机数以明文保存在智能卡中.上述 7 类解决方案对内部攻击威胁有适当的缓解作用,但可能引入新的安全问题,并未从根本上解决内部攻击问题.本文将弥补这一缺陷,提出合理的解决方案抵抗内部攻击.

7.2 内部攻击解决方案

为避免服务器获得口令明文和用户隐私泄漏,采用“加盐 Hash”技术传输口令相比其他几种方式更简单、安全、高效[35].基于对 300 余个用户认证协议的分析经验,我们发现大多数采用“加盐 Hash”技术实现用户注册的

协议均无法抵抗内部攻击,这是因为这些协议均有以下两条性质.

1. RPW_i 由 ID_i,PW_i 和 r_i 确定;
2. r_i 可由用户 ID_i,PW_i 或 SC 计算出来.

其中,r_i 表示用户在注册过程中选择的随机数,SC 表示用户智能卡.以下我们将会说明,具有这两条性质的协议无法抵抗内部攻击.因此,我们称其为内部攻击的简易判断标准.

说明 1. 常见的口令存储形式有 3 种:明文、加密、哈希值.明文不可取,而加密和直接 Hash 均易被服务器还原,因此,增加一个随机盐可以有效增加口令的安全性.近年来,“加盐 Hash”技术广泛应用于现有的身份认证协议(如文献 17,19,20,35,71,75]),用户在注册阶段选择随机数 r_i,计算 $RPW_i=h(PW_i||r_i)$,将 $\{ID_i,RPW_i\}$ 发送给服务器,此类方法有助于确保服务器不能获得口令明文,且不能直接猜测用户口令.

说明 2. 假设用户登录阶段使用 RPW_i 进行验证,即智能卡无需计算出随机数 r_i,则可能存在内部攻击者仿冒用户攻击.否则,智能卡需计算出 r_i,以验证用户口令 PW_i 的正确性.此外,假设随机口令 RPW_i 与用户 ID_i,PW_i 无关,则只能与服务器主密钥相关,而服务器的目标是验证用户的合法性,若以服务器主密钥推算随机数 r_i,则服务器相当于一个预言机,将为攻击者提供仿冒用户或验证猜测口令正确性的预言机服务.

综上所述,任意协议在用户注册阶段采用了“加盐 Hash”技术传输用户口令,并且在智能卡中以某种方式保存了用户选择的随机数,该协议将无法抵抗内部攻击.针对此问题,本文提出一种新的解决方案,在此只简述用户注册过程的基本思路,协议登录、认证过程可兼容现有的用户身份认证协议.

1) 用户 U_i 选取身份标识 ID_i,口令 PW_i,生成随机数 r_i,计算 $RPW_i=h(PW_i||r_i)$.
2) $U_i\Rightarrow S$:$\{ID_i,RPW_i\}$.
3) 服务器 S 随机生成安全参数 a_i,计算 $X_i=h(h(ID_i||x)\oplus a_i)$,$F_i=h((h(ID_i)\oplus RPW_i) \bmod n)$,$D_i=X_i\oplus RPW_i$.在数据库中存储 $\{ID_i,a_i\}$;同时,将 $\{D_i,F_i,n\}$ 写入智能卡.其中,x 为系统主密钥,n 表示 (ID,PW) 池容量的整数,$2^4\leqslant n\leqslant 2^8$.
4) $S\Rightarrow U_i$:智能卡.
5) U_i 接收到智能卡,计算 $X_i=D_i\oplus RPW_i$,重新生成随机数 r_i',计算 $RPW_i'=h(PW_i\,\|\,r_i')$,$F_i'=h((h(ID_i)\oplus RPW_i') \bmod n)$,$D_i'=X_i\oplus RPW_i'$,以 D_i',F_i' 替换智能卡中的 D_i,F_i,并将 r_i' 写入智能卡.

需要指出的是:服务器接收到的 RPW_i 与智能卡中参与计算的 RPW_i' 并不相同,即使攻击者截获了注册过程中的 RPW_i,提取用户智能卡中的安全参数,也无法借助随机数 r_i' 猜测出用户口令.此外,通过引入“模糊验证因子”技术[35],如第 4.2 节和第 6.2 节所示,增加了攻击者猜测出正确口令的难度.因此,本文提出的方案可以有效解决第 2 节的内部攻击,同时允许用户自主选择口令,保护用户隐私,实现口令本地自由更新.

8 结 语

无线传感器网络的身份认证面临严峻挑战:一方面由于传感器节点计算能力和存储容量有限,无法支撑复杂密码协议;另一方面,攻击者的攻击能力不断增强,先前安全的协议在新的攻击场景下将不再安全.本文以无线传感器网络环境下的两个代表性认证协议为例,分析一种实际存在的、但未引起广泛关注的内部攻击威胁,并且给出攻击者的具体攻击过程.

具体来说,本文首先回顾 Mir 等人的协议,指出其不能抵抗内部攻击和智能卡丢失攻击,且不能实现前向安全性;然后分析 Fang 等人的协议,指出其同样不能抵抗内部攻击和智能卡丢失攻击,且未实现所宣称的前向安全性属性.针对 Mir 等人的协议和 Fang 等人的协议的具体失误之处,提出相应解决方案.本文指出一种被长期忽略的内部攻击,基于 300 余个协议分析经验,对现有尝试抵抗内部攻击的方案进行分类,指出现有解决方案的不足之处,进一步提出合理的解决方案.根据本文提出的抗内部攻击方法,设计更安全高效的用户身份认证协议,是下一步值得研究的方向.

References:

[1] Shim KA. BASIS: A practical multi-user broadcast authentication scheme in wireless sensor networks. IEEE Trans. on Information Forensics and Security, 2017,12(7):1545−1554.

[2] He D, Zeadally S, Wu L, *et al*. Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography. Computer Networks, 2017,128:154−163.

[3] 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.

[4] Tan R, Phillips DE, Moazzami MM, *et al*. Unsupervised residential power usage monitoring using a wireless sensor network. ACM Trans. on Sensor Networks, 2017,13(3):Article No.20.

[5] Decker CJ, Reed C. The National Oceanographic Partnership Program: A Decade of Impacts on Oceanography. Oceanography, 2009,22(2):208−227.

[6] Huang H, Gong T, Ye N, *et al*. Private and secured medical data transmission and analysis for wireless sensing healthcare system. IEEE Trans. on Industrial Informatics, 2017,13(3):1227−1237.

[7] Li X, Niu J, Kumari S, *et al*. A three-factor anonymous authentication scheme for wireless sensor networks in Internet of things environments. Journal of Network and Computer Applications, 2018,103:194−204.

[8] Shen J, Chang S, Shen J, *et al*. A lightweight multi-layer authentication protocol for wireless body area networks. Future Generation Computer Systems, 2018,78:956−963.

[9] United States Environmental Protection Agency. Remote sensing information gateway. 2018. http://www.epa.gov/rsig

[10] Askraba S, Paap A, Alameh K, *et al*. Laser-Stabilized real-time plant discrimination sensor for precision agriculture. IEEE Sensors Journal, 2016,16(17):6680−6686.

[11] Habib C, Makhoul A, Darazi R, *et al*. Self-adaptive data collection and fusion for health monitoring based on body sensor networks. IEEE Trans. on Industrial Informatics, 2016,12(6):2342−2352.

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

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

[14] Wong KHM, Zheng Y, Cao J, *et al*. A dynamic user authentication scheme for wireless sensor networks. In: Proc. of the IEEE Int'l Conf. on Sensor Networks, Ubiquitous, and Trustworthy Computing. 2006. 1−8.

[15] Tseng HR, Jan RH, Yang W. An improved dynamic user authentication scheme for wireless sensor networks. In: Proc. of the IEEEGlobal Telecommunications Conf. 2007. 986−990.

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

[17] 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 with English abstract). http.//www.jos.org.cn/1000-9825/5361.htm [doi: 10.13328/j.cnki.jos.005361]

[18] Wang D, Li WT, Wang P. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Trans. on Industrial Informatics, 2018,14(9):4081−4092.

[19] 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.

[20] Wu F, Xu L, Kumari S, *et al*. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. Journal of Network and Computer Applications, 2017,89:72−85.

[21] Khan MK, Kim SK, Alghathbar K. Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'. Computer Communications, 2011,34(3):305−309.

[22] Chen TH, Shih WK. A robust mutual authentication protocol for wireless sensor networks. ETRI Journal, 2010,32(5):704−712.

[23] Yeh HL, Chen TH, Liu PC, *et al*. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors, 2011,11(5):4767−4779.

[24] Kumar P, Lee SG, Lee HJ. E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. Sensors, 2012,12(2):1625−1647.

[25] He D, Kumar N, Chen J, *et al*. Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimedia Systems, 2015,21(1):49−60.

[26] Mir O, Munilla J, Kumari S. Efficient anonymous authentication with key agreement protocol for wireless medical sensor networks. Peer-to-Peer Networking and Applications, 2017,10(1):79−91.

[27] Fang WD, Zhang WX, Yang Y, *et al*. Biometric-based three-factor user authentication protocol for wireless sensor network. Acta Electronica Sinica, 2018,46(3):702−713 (in Chinese with English abstract).

[28] Awasthi AK, Srivastava K. A biometric authentication scheme for telecare medicine information systems with nonce. Journal of Medical Systems, 2013,37(5):Article No.9964.

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

[30] Hsu CL. Security of two remote user authentication schemes using smart cards. IEEE Trans. on Consumer Electronics, 2003,49(4): 1196−1198.

[31] Ku WC, Chen SM. Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards. IEEE Trans. on Consumer Electronics, 2004,50(1):204−207.

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

[33] Kim TH, Kim C, Park I. Side channel analysis attacks using AM demodulation on commercial smart cards with SEED. Journal of Systems and Software, 2012,85(12):2899−2908.

[34] Barenghi A, Breveglieri L, Koren I, *et al*. Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. Proc. of the IEEE, 2012,100(11):3056−3076.

[35] Wang D, Wang P. Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE Trans. on Dependable and Secure Computing, 2018,15(4):708−722.

[36] Wang D, Cheng H, Wang P, *et al*. Zipf's law in passwords. IEEE Trans. on Information Forensics and Security, 2017,12(11): 2776−2791.

[37] 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]

[38] Thousands of servers password and sensitive information. 2018. https://www.solidot.org/story?sid=55915

[39] The Korean shopping website server was hacked and tens of millions of users' information was leaked. 2016. http://news.fznews.com.cn/fuzhou/20160726/5796c55702ef9.shtml

[40] Wang D, Cheng H, Wang P, *et al*. A security analysis of honeywords. In: Proc. of the 25th Network and Distributed System Security Symp. (NDSS 2018). ISOC, 2018. 1−16.

[41] Golla M, Beuscher B, Dürmuth M. On the security of cracking-resistant password vaults. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. ACM Press, 2016. 1230−1241.

[42] Juels A, Rivest RL. Honeywords: Making password-cracking detectable. In: Proc. of the 2013 ACM SIGSAC Conf. on Computer & Communications Security. ACM Press, 2013. 145−160.

[43] Morris R, Thompson K. Password security: A case history. Communications of the ACM, 1979,22(11):594−597.

[44] Farash MS, Turkanović M, Kumari S, *et al*. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of things environment. Ad Hoc Networks, 2016,36:152−176.

[45] Phillip T. Github security flaw leaks user passwords to employees. 2018. https://www.dailydot.com/debug/github-bug-passwords/

[46] Agrawal P. Keeping your account secure. 2018. https://blog.twitter.com/official/en_us/topics/company/2018/keeping-your-account-secure.html

[47] The demand of smart card, financial IC card market and industrial chain analysis in China 2017. 2018. http://www.chinaidr.com/tradenews/2018-01/117551.html

[48] Li X, Niu J, Kumari S, *et al*. A three-factor anonymous authentication scheme for wireless sensor networks in Internet of things environments. Journal of Network and Computer Applications, 2018,103:194−204.

[49] 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.

[50] Yang JH, Chang CC. An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Computers & Security, 2009,28(3-4):138−143.

[51] Xiao D, Liao X, Deng S. A novel key agreement protocol based on chaotic maps. Information Sciences, 2007,177(4):1136−1142.

[52] 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.

[53] 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 Press, 2016. 475−486.

[54] Michael C. OPM OPM breach: What's the risk of exposed fingerprint data? 2016. https://searchsecurity.techtarget.com/answer/OPM-breach-Whats-the-risk-of-exposed-fingerprint-data

[55] Sood SK. Secure dynamic identity-based authentication scheme using smart cards. Information Security Journal: A Global Perspective, 2011,20(2):67−77.

[56] Li X, Niu J, Liao J, *et al*. Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update. Int'l Journal of Communication Systems, 2015,28(2):374−382.

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

[58] Chang YF, Tai WL, Chang HC. Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update. Int'l Journal of Communication Systems, 2014,27(11):3430−3440.

[59] Yeh KH. A lightweight authentication scheme with user untraceability. Frontiers of Information Technology & Electronic Engineering, 2015,16(4):259−271.

[60] 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.

[61] 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, 2018,78:1005−1019.

[62] 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.

[63] Madhusudhan R, Hegde M. Security bound enhancement of remote user authentication using smart card. Journal of Information Security and Applications, 2017,36:59−68.

[64] Wu F, Xu L, Kumari S, *et al*. An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. Multimedia Systems, 2017,23(2):195−205.

[65] Srinivas J, Mishra D, Mukhopadhyay S. A mutual authentication framework for wireless medical sensor networks. Journal of Medical Systems, 2017,41(5):Article No.80.

[66] Xiong H, Tao J, Yuan C. Enabling telecare medical information systems with strong authentication and anonymity. IEEE Access, 2017,5:5648−5661.

[67] 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.

[68] Srinivas J, Mukhopadhyay S, Mishra D. Secure and efficient user authentication scheme for multi-gateway wireless sensor networks. Ad Hoc Networks, 2017,54:147−169.

[69] Farash MS, Attari MA. An anonymous and untraceable password-based authentication scheme for session initiation protocol using smart cards. Int'l Journal of Communication Systems, 2016,29(13):1956−1967.

[70] Namasudra S, Roy P. A new secure authentication scheme for cloud computing environment. Concurrency and Computation: Practice and Experience, 2017,29(20):Article No.e3864.

[71] Wang Y, Liu J, Xiao F, *et al*. A more efficient and secure dynamic ID-based remote user authentication scheme. Computer Communications, 2009,32(4):583−585.

[72] Amin R, Islam SKH, Biswas GP, *et al*. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. Computer Networks, 2016,101:42−62.

[73] Amin R, Islam SKH, Biswas GP, *et al*. A robust and anonymous patient monitoring system using wireless medical sensor networks. Future Generation Computer Systems, 2018,80:483−495.

[74] Wu F, Xu L, Kumari S, *et al*. A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client—Server networks. Computers & Electrical Engineering, 2015,45:274−285.

[75] 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.

附中文参考文献:

[17] 汪定,李文婷,王平.对 3 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 [doi: 10.13328/j.cnki.jos.005361]

[27] 房卫东,张武雄,杨旸,等.基于生物特征标识的无线传感器网络三因素用户认证协议.电子学报,2018,46(3):702−713.

[37] 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 [doi: 10.13328/j.cnki.jos.005001]

[38] 数千服务器泄漏密码密钥等敏感信息.2018. https://www.solidot.org/story?sid=55915

[39] 韩购物网站服务器遭黑客攻击 千万用户信息被泄.2016. http://news.fznews.com.cn/fuzhou/20160726/5796c55702ef9.shtml

[47] 2017 年中国智能卡、金融 IC 卡市场需求及产业链分析.2018. http://www.chinaidr.com/tradenews/2018-01/117551.html

[54] Michael C.OPM 数据泄露:生物识别可以信任吗?2016. https://searchsecurity.techtarget.com.cn/11-24678/

李文婷(1990－),女,山东青岛人,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,物联网软件.

汪定(1985－),男,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.