

智能电网 PDA 终端的密钥管理和认证研究

喻潇¹, 田里¹, 刘喆^{2,3}, 王捷¹

(1. 国网湖北省电力有限公司电力科学研究院, 武汉 430077;

2. 武汉大学国家网络安全学院, 湖北 武汉 430072;

3. 武汉大学空天信息安全与可信计算教育部重点实验室, 湖北 武汉 430072)

摘要: 针对智能电网 PDA 终端缺乏合理的密钥管理与认证协议的安全问题, 提出了一种基于加扰 PUF 的智能电网 PDA 终端密钥管理机制和认证协议, 利用可信硬件模块和 PDA 终端构造移动可信平台, 设计了一种可以唯一代表硬件设备身份且可由用户的密钥管理机制, 保证密钥安全的同时建立安全有效的密钥备份和恢复机制。以可信硬件模块作为基础, 联合上述密钥管理策略中生成的公私钥等, 利用改进的基于公钥密码学的接入认证协议, 实现智能电网 PDA 终端的安全接入。

关键词: 智能电网; PDA 终端; 可信计算; 密钥管理; 认证协议

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018026

Research on key management and authentication protocol of PDA in smart grid

YU Xiao¹, TIAN Li¹, LIU Zhe^{2,3}, WANG Jie¹

1. State Grid Hubei Electric Power Research Institute, Wuhan 430077, China

2. School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

3. Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan 430072, China

Abstract: According to PDA in smart grid, which faced with security issues, key management and authentication protocol for PDA in smart grid based on scrambling PUF were presented. With the construction of mobile trusted platform by trusted hardware module and PDA, a key management mechanism was designed which presented for the indentify of hardware and controlled by user, to guarantee the security of key management and build a safe and effective mechanism of key backup and recovery. Based on trusted hardware module, security access for PDA in smart grid was realized, with the public and private key of key management strategy and improved access authentication protocol based on public key cryptography.

Key words: smart grid, PDA, trusted computing, key management, authentication protocol

1 引言

近年来, 随着计算、通信、控制等技术的发展, 电力系统和信息技术的结合成了必然的趋势,

正是因为两者的有机结合产生了智能电网的概念。智能电网是指在电力设备的基础上, 将通信技术、传感技术、测量技术和控制技术 etc 与电网高度集成形成的新型电力系统^[1]。在智能电网的

收稿日期: 2017-10-31; 修回日期: 2018-01-23

通信作者: 喻潇, 183796616@qq.com

基金项目: 可信计算在智能变电站的应用研究基金资助项目

Foundation Item: Research on the Application of Trusted Computing in Intelligent Substation Foundation

未来发展中,把无线通信技术作为下一步的重点研究目标,利用无线网络随时随地获取服务、信息等,一大批支持无线通信技术的电力移动作业终端应运而生,利用这些移动终端可以满足更加多样化的功能需求,其中最典型的的就是智能电网 PDA (personal digital assistant) 终端, PDA 是一种小型的具有无线通信功能的嵌入式设备,在电力线巡检和电能表的现场校验等环节发挥了重要作用,能够减轻操作人员繁重的工作负担。

然而, PDA 终端在为电力移动作业带来便利的同时,由于安全机制的不完善也暴露了较多的安全问题,为此国家电网公司专门制定了相关标准来保证 PDA 的安全,并制定了《智能电网移动作业 PDA 终端安全防护规范》来保障智能电网 PDA 终端的应用安全,总体要求中提出 PDA 终端要通过无线专网 APN,经安全接入平台接入相应业务系统的信息内网;安全技术要求中提出安全 TF 卡要支持相应的加密算法,用于加密传输和身份认证且使用公司统一数字证书系统颁发的证书,在密钥管理上,提出利用安全 TF 卡提供措施确保密钥产生、协商、存储、使用、更换以及销毁整个生命周期的安全^[2]。通过对相关标准和文件的分析可知,目前提出的安全技术主要是在 PDA 终端中建立基于安全 TF 卡的密钥管理方案,利用数字证书、私钥签名技术基于公钥密码学的身份认证接入协议,但是,仅利用安全 TF 卡无法保证密钥管理的全过程安全,一旦密钥泄露将对接入、通信造成严重的安全威胁。

本文通过引入可信计算技术的思想,利用可信硬件模块和 PDA 终端构造移动可信平台,设计了一种可唯一代表硬件设备身份且由用户管理控制的密钥管理机制,建立安全有效的密钥备份和恢复机制,同时,为了确保接入身份的真实性和安全性,以可信硬件模块作为基础,联合上述的密钥管理策略中生成的公私钥等,利用改进的基于公钥密码学的接入认证协议,实现智能电网 PDA 终端的安全接入。

2 背景介绍

众所周知,人类手指上的指纹信息可以作为唯一性的标识信息代表个人身份,物理不可克隆

函数(PUF, physical uncloneable function)技术正是仿照并根据人类指纹的这一特点,利用硬件内在的物理特性生成唯一性的标识,即输入激励后可输出一个唯一且无法预测的响应,该信息既可作为根密钥,也可作为唯一性的身份信息实现接入控制。目前,关于 PUF 的生成技术主要包括非电子 PUF、模拟电路 PUF 和数字电路 PUF 这 3 类^[3],其中,非电子类 PUF 主要依靠的是光学特性,在其实现过程中对所选的激光束和滤波器具有非常高的精度要求且需要投入使用较多的物理设备;以涂层 PUF 为代表的模拟电路 PUF 需要在电路板表面涂抹一层特殊材料用于特征提取,相对于光学 PUF,该方式虽然降低了复杂程度,但仍需要精密度较高的仪器对电容等进行精确测量^[4];相较于以上 2 种 PUF,数字电路 PUF 仅利用现有的存储器即可完成生成过程,大大减少了整个实现过程的难度和成本,因此,数字 PUF,尤其是 SRAM PUF 已成为目前 PUF 研究和应用的主流方向。

3 基于加扰 PUF 的密钥管理机制

在智能电网移动作业应用中, PDA 终端将密钥存储在 TF 卡中,虽然这在一定程度上增加了密钥泄露的难度,但还不能从根本上保证密钥的安全,攻击者还是可以利用侵入式攻击、逆向分析等物理攻击方法获取存储在安全 TF 卡中的密钥。对于该安全问题,越来越多的专家和学者提出可以利用物理不可克隆函数的方法抵抗物理攻击以提高密钥的安全性,但由于 PUF 的唯一性和顽健性,任意获得 PUF 提取方式的攻击者都能得到相同的秘密值,因此直接利用 PUF 产生的物理特征码无法对用户敏感数据形成有效保护,用户数据与隐私仍面临着被泄露的风险。

针对在密钥保护上的安全威胁,本文提出一种基于加扰 PUF 的密钥管理方法,利用物理不可克隆函数、密钥加扰协商技术确保密钥基于物理特性唯一相关的机制由用户掌控,通过在安全区域存储帮助数据、在卡内执行加密或签名等的安全手段,确保密钥的生成安全和使用安全,进而保证私钥和身份证书的安全,同时,利用密钥

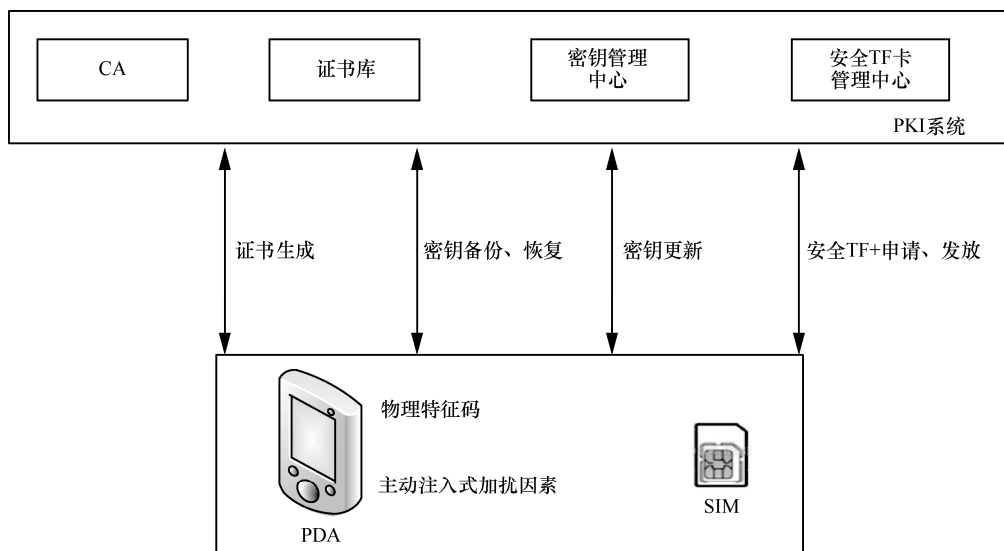


图 1 密钥管理机制

多层次分隔的原则备份密钥信息，建立高效的密钥恢复和再生成的机制，保证密钥在备份过程中的安全，以上管理机制如图 1 所示。

3.1 密钥生成

智能电网移动作业 PDA 作为典型的嵌入式系统，具备 SRAM PUF 生成所需的所有必要条件，可利用 SRAM PUF 的方式生成代表硬件特征的物理特征码，同时，为解决上述所提的关于传统 PUF 在生成物理特征码上存在安全隐患的问题，本文设计了可由用户掌握安全的基于加扰物理特征码的密钥生成方法，以物理特征码和 Pin 码为基础生成加扰物理特征码（PFC，Pin and feature code），在 PFC 的生成过程中包含提取物理特征码阶段和密钥加扰阶段，以下就这 2 个阶段进行详细描述。

3.1.1 Pin 码与密钥更新

该阶段主要通过 SRAM PUF 技术提取出代表硬件特征信息的物理特征码。在物理特征码的提取过程中，因为受温度、湿度等环境因素的噪声影响，每次在同一芯片之间的 SRAM PUF 的提取结果都可能存在较大的差异，对此需要引入模糊提取器的概念，以便将每次的提取结果都纠错并恢复成与注册时得到的相同特征值。在该 PUF 生成中所需的模糊提取器主要分为注册阶段和认证阶段 2 部分，在注册阶段需要用到的是 BCH 编码模块，在认证阶段需要用到的是 BCH 解码模块，如图 2 所示。

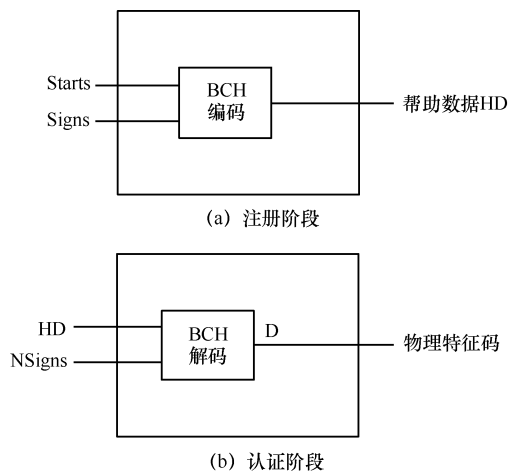


图 2 模糊提取器

在注册阶段，将输入数据（SRAM 身份识别码 Signs、基始值 Starts）发送至模糊提取器并生成帮助数据（HD, help data），帮助数据 HD 需要保存在安全 TF 卡中作为认证阶段其一的输入数据，用于帮助将带有噪声的识别码恢复。

在认证阶段，把带有噪声的识别码数据 NSigns 以及帮助数据 HD 作为输入数据发送给模糊提取器，模糊提取器利用帮助数据将 NSigns 恢复成注册阶段时输入的 Signs，该 Signs 即为提取所得的可以代表物理身份特征的物理特征码。

3.1.2 注入式加扰

在物理特征码生成后，使用 Pin 码作为主动的加扰手段，分别利用物理特征码和 Pin 码生成

相应的密钥种子 s_1 、 s_2 ，此外还要生成密钥协商所需的一些参数信息，通过密钥种子和必要参数根据 ECDH 算法协商出由用户主动管理控制的加扰物理特征码 (PFC)。具体过程如下。

1) 用户输入安全 TF 卡内置的 Pin 码，启动 TF 卡。

2) 提取出存储在安全 TF 卡中的 Pin 码散列值，利用种子生成算法生成密钥种子 s_1 。

3) 利用帮助数据和带噪声的识别码恢复出物理特征码，对物理特征码进行散列运行，并利用种子生成算法生成密钥种子 s_2 。

4) 假定目前已有椭圆曲线 E 、阶 N 、基点 G ，判断 s_1 与 N 的大小，若 $s_1 > N$ ，则使 $s_1 = s_1 \% N$ ，之后计算参数 C 的大小。

$$C = aG$$

5) 判断 s_2 与 N 的大小，若 $s_2 > N$ ，则使 $s_2 = s_2 \% N$ ，之后计算参数 D 的大小。

$$D = bG$$

6) 嵌入式系统和安全 TF 卡交换参数 C 和参数 D ， C 和 D 两参数可以直接明文传输，即便攻击者获取了 C 和 D 的值，但由于椭圆曲线上离散对数问题的难破解性，攻击者无法通过 C 、 G 推导出 a 的值，同理也无法通过 D 、 G 推导出 b 的值。

7) 安全 TF 卡通过获取的参数 C ，计算 $Q = bC$ 。

8) 嵌入式系统通过获取的参数 D ，计算 $Q = aD$ 。

通过计算可知

$$\begin{aligned} Q &= bC = b(aG) = (ba)G = (ab)G \\ &= a(bG) = aD = Q = \text{PFC} \end{aligned}$$

由此得到加扰的物理特征码 PFC，即为嵌入式系统的根密钥，在得到加扰的物理特征码后，通过公私钥生成算法即可生成 PDA 设备的公钥 Pub 和私钥 Pri，同时，也可以通过公私钥生成上层应用所需的加密密钥 S_u 。

3.2 密钥的备份与恢复

PDA 终端中最终生成的密钥 (PFC) 是由从 SRAM 的初始状态中提取得到的物理特征码和用户主动注入式的 Pin 码通过一系列的协商计算得到，为了保证密钥备份时的安全，本文将 PFC 拆

分成 3 个部分，根据物理特征码的生成原理将物理特征码拆分成带噪声的识别码和帮助数据 2 个独立的特征实体，这样即使数据丢失，也无法利用以上数据恢复出用户的密钥信息，同时将 Pin 码作为单独的一部分，将上述 3 部分信息分别利用单独存储的方式保存在密钥管理中心。在密钥管理中心备份的用户信息如表 1 所示。为防止 USBKEY 被盗用，每次使用 USBKEY 时需验证用户身份，验证方式采用 Pin 码，验证通过后方可使用 USBKEY 的功能，具体认证流程所表 1 所示。

表 1 密钥管理中心-密钥备份

用户名	序列号	带噪声的识别码	帮助数据	Pin 码
User ₁	SN ₁	NSigns ₁	HD ₁	Pin ₁
User ₂	SN ₂	NSigns ₂	HD ₂	Pin ₂
User ₃	SN ₃	NSigns ₃	HD ₃	Pin ₃

对于密钥恢复，存在安全 TF 卡丢失、嵌入式终端损坏以及嵌入式终端丢失 3 种情况。

表 2 密钥恢复存在的 3 种情况

对象	情况 1	情况 2	情况 3
Pin	丢失	未丢失	丢失
HD	丢失	未丢失	丢失
NSigns	未丢失	丢失	丢失
Generate New Key	不需要	需要	需要

3.3 密钥管理中的 2 个关键问题

在基于移动可信平台的密钥管理方法中，安全 TF 卡是最重要的组成部分之一，如何安全地获取可信硬件芯片是一个关键问题。同时，在密钥管理的要求中，任何密钥都有一定的期限，为了防止密钥长时间使用带来的安全隐患，本文还提出了适用于该机制的密钥更新方法，下面详细介绍提出的 2 个关键问题。

3.3.1 可信硬件模块获取

在使用智能电网 PDA 终端进行移动作业之前，用户需要先向密钥管理中心注册并申请获得安全 TF 卡。用户向密钥管理中心的注册模块提交 PDA 的序列号 ID 和口令 Pin 码，在注册模块分别验证短信验证码和身份，验证通过后将 Pin 码写入安全 TF 卡中，再由分发中心通过安全的

方式将卡交到用户手中, 以上前提是要保证用户名和口令值的传输信道是安全的, 具体过程如图3所示。

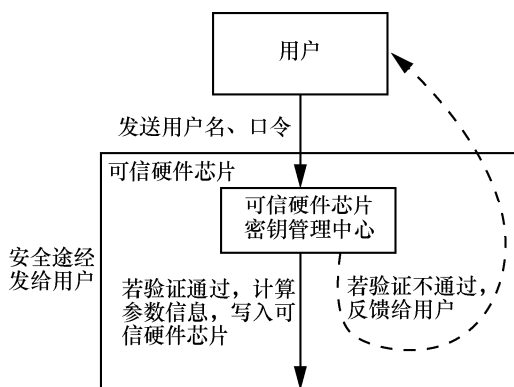


图3 可信硬件模块获取过程

3.3.2 密钥更新

在密钥管理的要求中, 密钥要有一定的有效期, 即不能无限使用, 因为密钥的使用时间越长, 它泄露的可能就越大, 而且一旦泄露, 造成的损失就越大。本文所介绍的密钥是由物理特征码和用户主动注入式的 Pin 码结合生成, 因此对于密钥的更新可以通过更新身份识别信息 Pin 码完成^[5]。对于 Pin 码的修改, 可以利用现有的 SIM 卡采取动态身份验证机制。用户向密钥管理中心发出申请, 服务器验证身份后, 发送随机的数字验证码给用户, 通过动态的身份验证机制确定用户的身份。之后将新 Pin 码提交给密钥管理表, 将原有 Pin 码替换并在 PDA 终端中重新得到一系列全新的密钥。

3.4 Pin 码修改与管理

在传统的接入认证中, 主要通过基于公开密钥密码学的双向认证协议证明双方的身份, 利用用户名与口令、数字证书和私钥信息保证接入设备的身份合法性。但是在 PDA 终端中, 因为无法在硬件架构中直接增加新的安全硬件, 这在包括密钥在内的多种隐私数据的保护上存在较大的安全问题, 对此, 本文在 3.3 节介绍的基于可信计算技术的可由用户管理控制的密钥管理方案的基础上, 提出了一种改进的基于公钥密码学的认证协议, 将用户的身份特征、相关的密钥信息等都由可信硬件模块进行保护, 实现基于硬件保护的通信双方的身份认证。另外, 在原有协议基于

用户层面的身份认证基础上, 根据可信计算对平台进行身份认证的思想, 新加入了可以唯一代表设备信息的物理特征码, 进行对于指定设备特有的终端身份认证, 实现了从用户到移动终端的双因子认证。为了更好地在实际中应用, 本文还通过 PKI 系统, 把利用加扰物理特征码作为种子值生成的 PDA 公钥做成证书。最后, 利用可信硬件模块中的散列操作实现对关键模块的配置信息的摘要, 并将标准值事先在接入服务器中预存, 接入时判断 PDA 终端的摘要值和服务器中的预存值是否匹配, 只有匹配时才准许接入, 否则拒绝接入, 保证了 PDA 终端接入时的完整性, 即终端安全性。整体架构如图4所示。

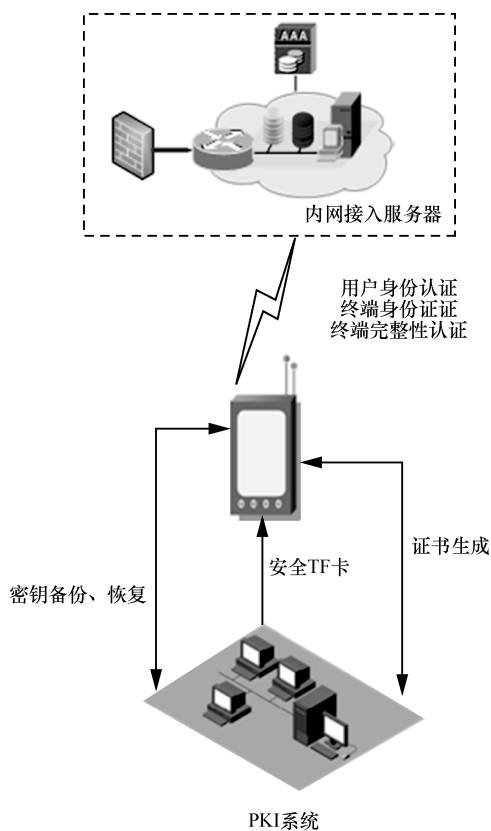


图4 整体架构

具体流程如下。

- 1) 用户输入密码 PW , 将输入的密码进行散列操作并与安全 TF 卡中存储的数据进行对比, 若一致, 则输入正确, 否则重新输入, 该阶段得到数据 $\alpha = \text{SHA}(PW)$ 。
- 2) 调用安全 TF 卡中基于硬件的加密引擎, 对设备的序列号进行 SHA-1 散列操作, 该阶段得

到数据 $\beta = \text{SHA}(ID)$ ，并将接入请求标识、 $\text{SHA}(PW)$ 和 $\text{SHA}(ID)$ 一同发送至接入服务器。

3) 接入服务器收到该请求后，验证 $\text{SHA}(ID)$ 和 $\text{SHA}(PW)$ 与数据库中内容是否匹配，若匹配成功，则随机生成动态的短信验证码并发送回 PDA 终端，否则返回错误信息。

4) PDA 终端输入短信验证码并发送至接入服务器，输入成功后返回成功信息，否则执行步骤 3)并重新输入验证码。

5) PDA 终端利用安全 TF 卡中的硬件随机数发生器生成随机数 R1,将 R1 发送至接入服务器。

6) 接入服务器收到 R1，调用接入服务器的私钥签名 R1，得到 $\gamma = \text{Ser_Sig}(R1)$ ，服务端利用当前时间作为种子值生成随机数 R2。将 $\text{Ser_Sig}(R1)$ 、R2 发送到 PDA 终端。

7) PDA 终端接收到信息后，利用接入服务器的公钥验签 $\gamma' = \text{Ser_Dec}(\gamma)$ ，得到 γ' ，若 $\gamma' = \gamma$ ，则证明了接入服务器端的真实性，即服务端平台身份验证通过。调用接入服务端公钥加密随机数 R2 和物理特征码 $\varepsilon = \text{Ser_Enc}(R2, \text{PFC})$ ，并将 ε 发送至接入服务器。如果 $\gamma' \neq \gamma$ ，则表明对接入服务器的身份认证失败，断开连接。

8) 接入服务器用私钥将接收到的 ε 解密，得到 $(R2, \text{PFC}) = \text{Ser_Dec}(R2, \text{PFC})$ ，利用接收到的 R2' 和 PFC' 与接入服务器中的数据比对，如果 $R2' = R2$ 且 $\text{PFC} = \text{PFC}'$ ，则对客户端的平台身份认证通过，并将验证成功的标识发送给客户端，否则发送消息验证失败。

9) 客户端收到反馈消息后，如果标识为失败，则断开连接；如果标识为成功，则客户端开始进行完整性收集。利用安全 TF 卡中内置的基于硬件的散列算法，对包括版本号、端口开关情况、通信模块的关键配置文件、数据传输模块关键配置文件进行散列运算，得到完整性度量值 $\xi = \text{SHA}(\text{ver}, \text{por}, \text{com}_{\text{ver}}, \text{dat}_{\text{ver}})$ 。PDA 终端将 ξ 发送至接入服务器。

10) 接入服务器验证 ξ 的值是否符合准入接入的策略，如果 ξ 值不在安全范围内，则可认为该 PDA 终端存在安全威胁，阻止其接入。如果 ξ 值在安全范围内，服务端利用当前时间作为种子值生成用于通信信道中加密的会话密钥 K ，利用

PDA 终端数字证书中的公钥加密会话密钥 K 得到 $\delta = \text{Pda_Enc}(K)$ ，将 δ 发送至 PDA 终端中。

11) PDA 终端接收到信息后将该信息发送至通信模块，通信模块调用安全 TF 卡内的私钥解密功能。首先利用帮助数据以及带有噪声的识别码生成根密钥从而得到私钥，之后在安全 TF 卡内利用私钥解密得到 $K' = \text{Pda_Dec}(\delta)$ ，该 K' 即为后续通信所用的会话密钥^[6]。

4 原型系统实现与分析

本文研究的原型系统所采用的配置包括：作为后台接入服务器的 Intel NUC，作为移动智能终端的迅为（TOPEET）ITOP-4412，三未信安 microSD（TF）密码卡，无线接入点 TP-LINK TL-WR941N。

4.1 加密的处理

本文所述关于智能电网 PDA 终端的安全接入方法在可行性测试方面，主要涉及 3 方面的内容：基于加扰物理特征码的密钥生成方法，改进的基于公钥密码学的认证协议，移动终端或安全 TF 卡丢失后的密钥恢复、再生成和密钥的更新方法。第一，基于加扰物理特征码的密钥生成方法，主要测试用户在申请并获得安全 TF 卡硬件后，能否在 PDA 终端中利用物理不可克隆函数生成物理特征码，并让用户的注入式因素参与密钥的生成过程中，在安全 TF 卡中执行加扰算法生成根密钥，并在安全区域中存储少量的帮助数据，同时利用得到的根密钥生成公私钥和加密密钥，实现主要密钥都可由用户掌握且能保证密钥的生成安全和存储安全；第二，在改进的基于公钥密码学的认证协议中，主要测试能否利用安全的公私钥和代表硬件身份的物理特征码保证接入时身份的真实性，以及能否以可信硬件模块为基础，实现对终端完整性状态的收集，保证接入终端的安全性；第三，测试在安全 TF 卡内的密钥恢复、再生成、更新操作，测试内容包括在用户丢失智能终端导致的设备和 TF 卡同时丢失或安全 TF 卡或智能终端损坏后对于包括密钥恢复如初或重新生成一个全新密钥的不同密钥处理方法，以及在有效期过后，能否利用密钥更新机制生成一个全新密钥。

4.2 安全性

4.2.1 可信硬件模块安全性分析

对于不法份子窃取用户的安全 TF 卡的安全风险,通过利用 Pin 码的安全访问控制技术,将安全 TF 卡和用户的主动因素绑定,当用户丢失可信硬件时,因为攻击者不知道 Pin 码,无法访问到芯片内部的数据。而且利用在安全 TF 卡中固化的访问控制技术,将安全 TF 卡和终端设备绑定,保证只有安全 TF 卡和指定的 PDA 终端结合,在通过双因子认证后才可以进行之后的操作,这也防止了 PDA 设备在丢失时某些数据泄露的安全威胁。

4.2.2 密钥生成及存储安全性分析

为了抵抗物理攻击,提高密钥的安全性,保证 PDA 终端在密钥生成上的安全,提出利用加扰 PUF 的方式生成根密钥。针对目前大多数嵌入式设备中的密钥需要存储的问题,本文提出了使用 SRAM PUF 根据物理特性生成物理特征码的方式。通过 SRAM PUF 得到的物理特征码不需要存储在系统中,解决了密钥存储所带来的安全性难题。然而,随着黑客技术的进一步发展,未来可能会出现对于 PUF 的克隆攻击,对此本文提出在物理特征码生成后增加用户主动的干扰因素,保证最终生成的密钥是由用户掌控的而不仅由物理特性决定。攻击者即使复制了物理特征码或者窃取了 Pin 码,也无法计算出最终密钥,在生成算法上实现了密钥生成过程中的安全。此外,在与密钥相关信息的存储上,只需要存储与最终密钥相关性较低的帮助数据即可,在信息存储的层面也加强了密钥生成的安全。

在硬件层面上,安全 TF 卡实现了硬件的可信,在安全 TF 卡的芯片中具有强身份认证功能和基于硬件的逻辑保护,无法通过常规的攻击手段得到内部所执行的指令,以硬件层面为基础实现了在芯片中执行环境的安全。同时,在安全 TF 卡中具有安全的存储区域,将与生成密钥相关的信息存储在安全区域中,可以有效提高相关信息保护的强度。

4.2.3 改进的接入认证协议的安全性分析

本协议以可信计算的密钥保护方案为基础,通过改进的接入认证方案保证了 PDA 终端接入

时的真实性和安全性。首先,双方的密钥都受到强安全保护,其中 PDA 终端中的公私钥等由物理不可克隆函数的特性和安全 TF 卡共同保障。即使攻击者重放关于终端申请接入服务端的消息,因为无法获得双方的私钥,则无法解密随机数和会话密钥,从而无法通过验证,连接断开。另外,在认证过程中,需要用户提供正确的口令以及与硬件特性强相关的物理特征码,属于强双因子身份认证。而且在协议中用到的 ID、口令和随机数等都是在安全 TF 卡内部实现的,由根密钥生成的密钥进行加密保护,具有不可迁移性,保证了认证过程中的真实性。最后,在该协议中还增加了完整性认证,利用可信硬件芯片模块的硬件引擎度量终端的完整性并将其发送至接入服务器,只有完整性度量值符合接入策略才准许其接入,保证了接入的安全性。

5 结束语

本文针对智能电网 PDA 终端中接入过程缺乏对密钥保护的现状,提出了一种基于加扰 PUF 的密码管理机制,根据国家“十三五”提出的将可信计算技术与电网安全结合的思想,在电力系统中引入可信计算技术,利用安全 TF 卡和 PDA 终端构建移动可信平台,同时制定了基于物理不可克隆函数和用户加扰因素的密钥管理方案。此外,为了实现基于移动可信平台的 PDA 终端的安全接入,本文改进了基于公钥密码学的双向认证协议,保证了终端接入的安全。最后,搭建演示系统,对该机制的可行性和安全性进行详细的分析。实验表明,该方案具有较好的安全性和可行性,对智能电网 PDA 终端的安全接入具有一定的实际意义和理论价值。

参考文献:

- [1] 刘伟强,崔益军,王成华.一种低成本物理不可克隆函数结构的设计实现及其 RFID 应用[J]. 电子学报,2016,(7),1772-1776.
LIU W Q, CUI Y J, WANG C H. Design and implementation of a low-cost physical unclonable function and its application in RFID[J]. Chinese Journal of Electronics, 2016,(7),1772-1776.
- [2] 焦芳. 基于 Lustre 的集群存储系统的安全性研究[D]. 青岛: 中国石油大学. 2012.
JIAO F. Research on the safety of a cluster storage system based on

Lustre [D]. Qingdao: China University of Petroleum. 2012.

- [3] 李少娟. 基于需求侧管理理念的电力市场营销方案的制定及实例分析[D]. 广州: 华南理工大学, 2012.

LI S J. Development and case analysis of power marketing plan based on demand side management concept[D]. Guangzhou: South China University Of Technology, 2012.

- [4] 贺章擎, 郑朝霞, 戴葵, 等. 基于 PUF 的高效低成本 RFID 认证协议[J]. 计算机应用, 2012,(3): 683-685.

HE Z Q, ZHENG Z X, DAI K, et al. Low-cost RFID authentication protocol based on PUF[J]. Journal of Computer Applications, 2012,(3): 683-685.

- [5] 赵波, 李逸帆, 米兰·黑娜亚提, 等. 基于可信模块的云存储用户密钥管理机制研究[J]. 四川大学学报(工程科学版), 2014,(6): 25-31.

ZHAO B, LI Y F, MI-LAN Heinayati, et al. Research of key management based on trusted module for cloud storage user[J]. Journal of Sichuan University(Engineering Science Edition), 2014,(6): 25-31.

- [6] 张俊, 周正, 李建, 等. 基于 MLS 策略的机密性和完整性动态统一模型[J]. 计算机工程与应用, 2008,44(12),19-21.

ZHANG J, ZHOU Z, LI J, et al. Confidentiality and integrity dynamic union model based on MLS policy[J]. Computer Engineering and Applications, 2008, 44(12):19-21.

[作者简介]



喻潇 (1984-), 男, 湖北红安人, 国网湖北省电力有限公司电力科学研究院工程师, 主要研究方向为信息安全。



田里 (1984-), 男, 湖北十堰人, 国网湖北省电力有限公司电力科学研究院工程师, 主要研究方向为信息安全。

刘喆 (1989-), 男, 山东青岛人, 武汉大学博士生, 主要研究方向为信息安全。

王捷 (1987-), 男, 湖北黄冈人, 博士, 国网湖北省电力有限公司电力科学研究院工程师, 主要研究方向为信息安全。