DOI:10.12158/j.2096-3203.2020.06.005

电能质量终端信息安全设计及应用

程立，徐东方，曾凯，刘中泽，朱何荣
（南京南瑞继保电气有限公司，江苏 南京 211102）

摘　要：随着现代计算机技术和互联网的发展，信息安全问题越来越突出。由于早期网络环境单一，传统的电能质量终端没有考虑信息安全问题，在抵御非法访问、网络攻击等方面能力偏弱。针对传统电能质量终端的设计缺陷，文中提出基于信息安全的终端设计及实现方案。方案在访问授权、审计记录、数据完整及防篡改性、网络攻击、备份与恢复以及源码安全等方面给出了切实的解决措施，有效提升了终端本体的信息安全强度。安全测试结果表明，该方案有效增强了终端信息安全能力，可有效抵御网络攻击等风险。文中提出的实现方案也可应用于保护、测控、PMU、录波器等间隔层终端设备。

关键词：电能质量；信息安全；数字签名；授权；加密
中图分类号：TM769　　**文献标志码**：A　　**文章编号**：2096-3203(2020)06-0026-08

0　引言

随着计算机技术和互联网行业的发展，各个行业与系统面临的网络攻击和威胁越来越多。原先处于封闭状态的电力系统网络也成为了被攻击的对象[1]，国内外网络安全问题逐渐突出[2]。为保证电力系统二次设备的防护安全，国家能源局依据发布的《电力监控系统安全防护规定》（国家发展和改革委员会 14 号令）[3]制定了《电力监控系统安全防护总体方案》（36 号文）[4]，防护措施升级速度加快。

在电弧炉等冲击性非线性负荷场合，常常会产生电压波动等电能质量问题[5—8]，需要安装电能质量监测终端进行监视；而风电、光伏等新能源与传统电源相比，具有出力不稳定、易受气候条件影响等特点[9]，由于要满足接入主电网的技术要求，相关设计规范上要求配置电能质量监测终端。由于早期变电站应用环境的限制，传统的电能质量监测终端应用网络环境单一，甚至不接入调度数据网，设计上没有过多考虑安全问题，国内相关文献[10—13]虽然做过研究，但在实际应用中仍然在访问授权、审计记录、数据完整及防篡改性、网络攻击、备份与恢复以及源码安全方面缺乏系统性设计。2015 年国家电网公司提出“建立统一的公司级电网谐波监测平台”，旨在把存量及新上的电能质量监测终端纳入监测系统，实现统一的管理，因此存量的传统的电能质量终端由于先天设计上的缺陷，很容易遭受恶意攻击。

文中在分析传统电能质量终端安全防护薄弱的基础上，针对入网控制、访问授权与认证、审计、数据完整性与机密性、网络防御、备份与恢复及源码检测等方面，提出了电能质量终端信息安全体系架构设计方案。相比传统的电能质量终端方案，该方案极大地提高了终端的网络安全可靠性，有效抵御了网络攻击。

1　传统终端安全问题

传统的电能质量系统架构如图 1 所示，分为过程层、间隔层和主站层三部分。过程层主要是互感器一次设备，负责将一次电压电流转换为二次小信号。间隔层由电能质量监测终端组成，负责采集二次电压电流信号，计算电能质量各项指标，通过路由器和防火墙将数据上送给主站系统。主站层由服务器、工作站等组成，负责接收电能质量监测终端数据，对电网的电能质量进行分析评估和决策治理。从电能质量系统架构可以看到，电能质量监测终端属于间隔层设备。在纵向数据上，终端直接通过路由器和防火墙接入主站，网络划分上属于业务三区。纵向网络上只有防火墙予以网络保护，一旦防火墙被黑客破解，终端将直接暴露在黑客之下，轻则造成终端运行异常，重则造成存储数据删除、数据丢失等问题[14]。

在现场工程实际运行中，传统电能质量终端缺乏信息安全机制考虑，抵御侵入风险能力低，主要表现在以下几个方面。

（1）访问授权。客户端工具缺乏数字认证，往往简单的拷贝就能完成从计算机 A 到 B 的使用。

收稿日期：2020-05-28；修回日期：2020-07-03
基金项目：国家电网有限公司科技项目（SGLNJZ00YJJS180-0187）

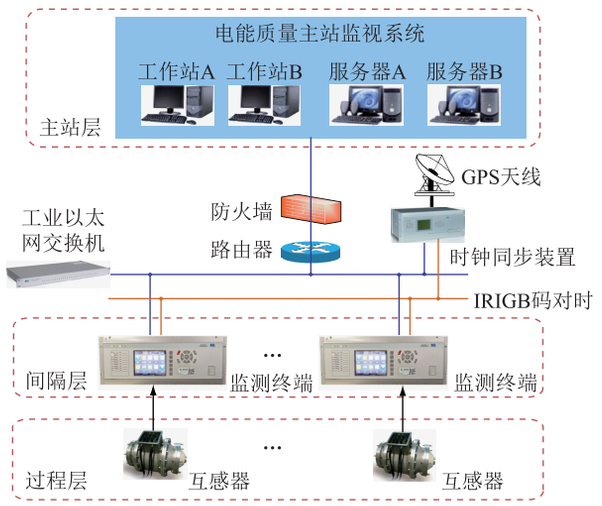


图 1 电能质量系统架构

Fig.1 Architecture of power quality system

客户端工具或液晶访问没有用户名密码校验,可以直接查看和修改数据。

(2) 审计记录。由于缺乏访问授权,造成的后果是更改完配置或定值后无法溯源,只知道修改了配置但无法知道具体哪个用户进行了哪些操作,是否存在越权行为。

(3) 完整性。程序和数据缺乏完整性保证,用户可随意修改配置和程序,若恶意下载无效配置可能导致终端无法启动。

(4) 保密性。重要配置及数据以明文传输和存储,缺乏加密体系支撑[15—16],容易暴露终端安全信息,如用户名和密码。

(5) 网络攻击。对泛洪攻击和模糊攻击容忍度差,容易造成终端死机和瘫痪。探测系统可侦测出明显的可利用的安全漏洞。

(6) 备份与恢复。程序和数据没有备份功能,当遭到破坏时缺乏恢复机制。

(7) 源码安全。使用不安全函数如 strlen、strcpy、sprintf 等容易引起栈缓冲区溢出导致黑客攻击。

2 终端安全原则

2.1 访问授权

从授权角度来看,主要考虑两点:一是软件本身的使用授权,即软件是否被允许使用;二是被授权用户的权限大小及范围。

(1) 软件授权。非授权软件不可访问终端,拒绝简单拷贝软件等非法使用操作。数字证书是一种较好的解决方案。数字证书是提供表明通信双方身份的一串数字码防止抵赖冒充行为,通常包含授权者信息、用户密钥及授权的数字签名。数字签名首先采用哈希(Hash)算法提取数据摘要,然后通过私钥签名后发送出去;接收侧公钥验签通过后,再对摘要报文进行哈希(Hash)算法确认完整性。数字证书是一种有效的授权方式,国内相关文献[17—20]做了很多相关研究,其具有信息保密性、身份确定性和不可抵赖性,原理见图 2。

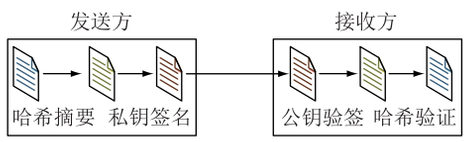


图 2 数字证书原理

Fig.2 Principle of digital certificate

(2) 用户权限。只允许身份验证通过的用户访问其授权的资源,授权应依据最小资源原则。设备应支持根据用户角色对设备功能进行授权,需要认证授权至少包括账户管理、查看数据、修改参数及审计日志功能。账户管理:可增加和删除包括管理员、普通用户及审计用户等用户角色,管理员可修改本身及普通用户密码,不可修改审计用户密码;审计用户只能修改自身密码,不能修改管理员及普通用户密码。查看数据与参数:能够查看终端的电压、电流、谐波以及闪变等运行数据;查看终端地址、IP 等参数。修改参数及配置:能够修改终端参数和配置并对其进行下载更新。审计日志:能够查看和上载审计日志。

根据以上权限的不同至少应该分配 3 个角色:管理员、普通用户和审计用户。管理员应具有管理普通用户的权限,包括添加、删除帐户,修改密码;查看运行数据、修改参数及配置等权限。普通用户具有察看运行数据、参数及配置等权限,但无修改配置权限。审计用户有且仅有察看审计日志功能,不能添加删除普通用户、修改密码及查看运行数据。

2.2 审计记录

审计记录是指设备应能够产生和存储安全性事件及重要业务事件的审计信息。只有审计用户可通过客户端工具或液晶查看,但不允许删除。审计记录是对设备产生和发生过的安全事件和重要业务事件做跟踪回溯。确保只有授权用户才能访问审计事件但不能删除,审计事件本身要加密,存储区域要同程序空间分离。审计事件至少包括以下内容。

(1) 帐户记录。增加和删除用户、修改用户密码操作。

(2) 修改记录。修改参数与定值操作,如修改 IP 地址,要形成“修改 IP 地址参数”记录。

（3）告警事件。审计过程中的告警事件，例如“连续输入错误密码超过设定次数”、“拒绝服务（denial of service，DOS）攻击”、“审计记录满”等事件。

（4）设置时间和日期。修改时间和日期的操作。

（5）常规事务。记录常规操作行为，例如“访问审计日志”、“用户登录及访问”、“终端断电”等事务。

2.3 完整性与保密性

数据传输和存储过程中应采用加密算法确保完整性，数据被破坏应能识别并丢弃。在升级过程中检验程序完整性，确保程序遭到破坏也能识别并拒绝下载。设备敏感数据要非明文存储，存储算法采用国密推荐算法。敏感数据在传输过程中也要采用非明文方式，确保被截获后也无法破解。

2.4 网络攻击

面对网络攻击，终端功能应不受网络攻击影响，必须运行正常，不误动，不误发报文，不死机，不重启。为此，终端必须采取以下措施提升本体网络防御能力。

（1）禁用端口。禁止使用易遭受恶意攻击的高危端口作为服务端口，如开启 21（ftp）、23（telnet）。禁止开启与业务无关的服务端口。

（2）防范协议攻击。防范 IEC 61850、IEC 103 的模糊攻击，制造报文规范（manufacture message specification，MMS）杂凑和 IEC 103 畸形包攻击。

（3）防范泛洪攻击。防范传输控制协议同步（transmission control protocol synchronization，TCP SYN）泛洪、用户数据报协议（user datagram protocol，UDP）泛洪、控制消息协议（internet control message protocol，ICMP）泛洪等网络攻击。

2.5 备份与恢复

终端应能提供备份与恢复功能，程序和数据下载过程中在特定存储区域形成备份，遭受破坏时能够予以恢复。

2.6 源码安全

避免使用不安全函数，防范栈缓冲区溢出导致的黑客攻击。避免源码中存在的内存泄露、句柄泄露、未初始化指针的应用。

3 安全设计与实现

3.1 访问授权

访问授权主要从工具软件授权及工具访问授权两方面来考虑，具体实施方法如下。

（1）工具软件授权。通过注册码、硬件看门狗等措施防止工具简单拷贝使用。注册码的算法采用硬件信息杂凑生成，硬件信息包括诸如中央处理器 ID（central processing unit ID，CPU ID），硬盘 ID，网卡媒体接入控制器（media access control，MAC）地址等。

（2）工具访问授权。首先初始化服务端监听套结字（SOCKET）、安全套结字协议层（secure sockets layer，SSL）会话等，通过加载客户端证书授权（certificate authority，CA）文件、本端证书和密钥。尝试连接服务器端，完成套接字连通后将安全套结字层/传输层安全（secure sockets layer/transport layer security，SSL/TLS）协议版本、密码算法及参数、超时时间等填充 SSL 配置，设置本端证书及私钥，利用 SSL 配置建立安全套结字协议层上下文（secure sockets layer context，SSL Context）尝试握手连接。握手过程中数字证书出错将中止会话，拒绝未授权非法访问。

3.2 用户权限

用户授权主要考虑权限的划分以及在权限划分的基础上进行角色的定义，具体实施方法如下。

（1）权限划分。权限设置具体划分为账户管理、信息察看、修改权限、配置权限以及审计权限等，详细划分见表 1。

表 1 权限划分

Table 1 Authority division

权限种类	权限细则
账户管理	增加删除用户 修改用户密码
信息察看	电压、电流、谐波、闪变 系统参数、间隔定值 终端信息 板卡信息 动作报告 自检报告 变位报告 波形文件
修改权限	修改系统参数 修改间隔定值 修改日期时间 在线调试
配置权限	修改终端配置 文件上载、下载 固件刷新
审计权限	察看审计日志 上载审计日志 保存审计日志

（2）用户定义。系统中应该配置独立的管理员角色、审计角色和普通操作员角色，且系统管理员、审计员必须为系统内置角色。管理员不能创建分

配审计员角色,管理员只能对普通操作员进行配置。

管理员具有普通用户帐号及权限管理、系统管理(如系统时间、调试工具的使用、查看系统信息、设置工作模式、系统升级、重启、关闭等)权限。审计员仅具有监控各类用户的操作轨迹及对审计数据进行管理、监视和运行维护的权限。普通用户只有普通操作权限,如数据查看、定值整定,不具有任何管理权限。

从用户管理来划分,可创立 3 个级别用户:管理员、普通用户和审计员,对应权限见表 2。

表 2 用户角色权限

Table 2 User role authority

用户权限	管理员	普通用户	审计用户
账户管理	√		
信息察看	√	√	
修改参数	√	√	
修改配置	√	√	
调试功能	√	√	
审计功能			√

(3) 设计实现。

第一步:配置工具默认提供一个管理员账户,用户名和密码均为 admin。该账户的角色是“管理员”角色,默认具有所有权限。用户第一次配置时使用 admin 账户进行登录,登录以后需要立即修改默认的用户名和密码。

第二步:配置工具进行权限配置,首先设置需要密码校验的权限,其次设置超时时间。用户登录以后,在超时时间内执行具有权限的操作,不需要校验密码。若在超时时间内用户没有执行任何操作,则到达超时时间时,用户会被自动退出。

第三步:创建角色,给角色分配权限,并且创建用户,将用户添加到角色组中。

第四步:配置完成后保存到权限(authority)文件中,再下载到终端,最终生效。若工程文件中没有打包 authority 文件,可从终端中上召 authority 文件进行配置。

完整的权限配置流程见图 3。

3.3 完整性与保密性

加密方案可划分为两大类:单钥方案和双钥方案。前者采用单一秘钥,客户端与服务器端共用一把钥匙,因此秘钥一旦被窃取很容易造成信息被破解。后者采用一对秘钥,一个是公开的公钥,另一个是保密的私钥。在数据传输中,一端通过公钥加密,另外一端通过私钥解密,想通过公钥破解得到私钥的可能性很低或者理论上根本行不通,因此双

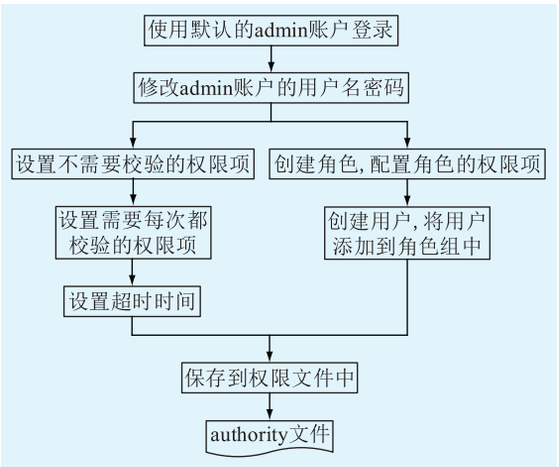


图 3 权限配置流程

Fig.3 Authority configuration process

钥系统安全性较高。文中采用双钥方案。

工具和终端之间通信使用非对称的双钥加密方案,工具有一对公钥和私钥,终端也有一对公钥和私钥。工具中存储自己的私钥和终端的公钥,终端中存储自己的私钥和工具的公钥。

工具给装置发送数据时,使用装置的公钥进行加密,装置接收到数据后,使用自己的私钥解密数据。装置给工具发送数据时,使用工具的公钥进行加密,工具接收到数据后,使用自己的私钥解密数据。即使其他客户端从网络中抓取到数据,也无法破解,只有工具或装置有对应的私钥才可解密数据。

具体实现上,首先工具生成 proj 文件后,先使用一个 Hash 算法计算得到 proj 文件的摘要,然后工具使用自己的私钥对于摘要进行加密,形成数字签名,最后再用装置的公钥对 proj 和签名进行加密,流程如图 4 所示。

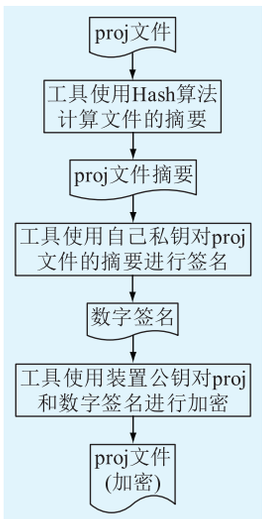


图 4 数字签名及加密流程

Fig.4 Digital signature and encryption process

工具下载加密 proj 文件给装置，首先装置接收到数据后使用自己的私钥进行解密，然后装置再使用工具的公钥对数字签名进行验签，如果验签成功，则可证明数字签名是工具生成。最后装置使用相同的 Hash 算法计算接收到的 proj 文件的摘要。如果摘要与验签数字签名得到的摘要相同，那么可以验证 proj 文件传输成功，没有被篡改过，流程如图 5 所示。

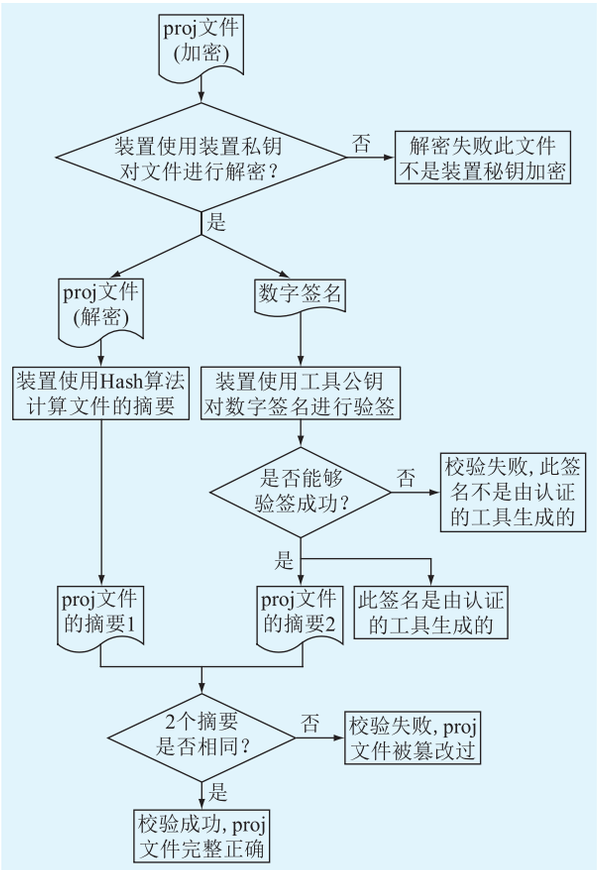


图 5　解密、验签与哈希流程

Fig.5　Decryption, signature verification and hash process

3.4　网络攻击

为有效防范网络攻击，提升终端网络攻击抵御能力，具体实施方法如下。

（1）不安全端口。采用 nmap 软件扫描端口，根据据扫描结果关闭不安全的端口如 21（ftp）、23（telnet）等。在 Linux 等操作系统启动脚本 profile 中去掉 vsftpd、telnetd 等启动命令。

（2）协议攻击。针对 MMS 等特定协议发起协议攻击，如模拟 COTP、OSI-SPDU、Init Grammar、Init Damage 包进行攻击。若发现协议异常要直接修改 MMS 源代码。

（3）模糊攻击。采用 FUZZ 工具发起畸形包对诸如调试等端口进行攻击，尤其发起 TCP 连接进行持续攻击。该攻击可能会引起终端服务器端性能下降，可采取包括多线程方案：每个线程专门处理一个客户端，不影响主服务线程。静态加载：证书加载采用静态方式，即初始化加载一次，避免客户端多次加载。静态内存分配：采用内存预分配方案，避免多客户端频繁分配/释放内存保证效率。

（4）泛洪攻击。对于 TCP SYN 泛洪、UDP 泛洪、ICMP 泛洪等网络攻击，主要依赖于操作系统协议栈健壮性。采用协议栈健壮的操作系统，如 Linux、Unix 等都能抵抗泛洪攻击。

3.5　备份与恢复

采用独立分区备份程序与配置，终端 flash 划分 2 个区：mtd1 和 mtd2。mtd1 备份程序，mtd2 备份配置。采用守护进程定时对运行程序和配置进行 MD5 有效性校验，若校验出错，则表明运行程序和配置被破坏，守护进程对破坏程序进行还原恢复，配置流程见图 6。

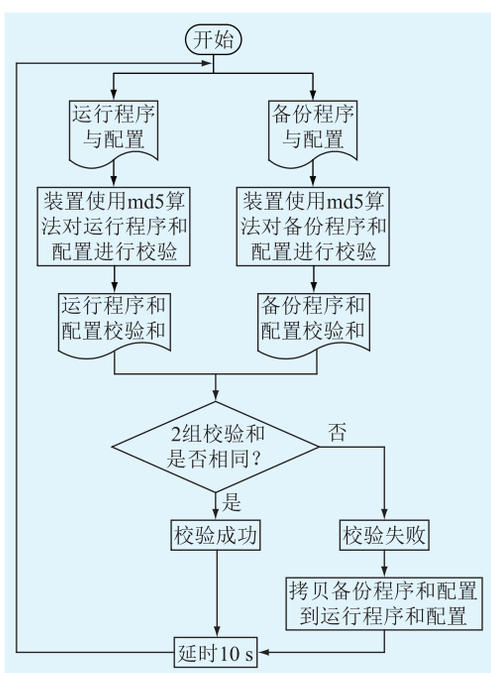


图 6　备份与恢复流程

Fig.6　Backup and recovery process

3.6　源码安全

常见的源码安全包括内存泄露：内存分配函数调用结束后不予释放，即有 malloc 而没有 free，造成系统内存耗尽。初始化错误：使用未初始化指针或变量，内存指向错误或初始迭代条件错误，造成程序异常终止或者输出错误结果，使得终端功能崩溃或者误动作。内存越界：内存访问超出使用者界定范围溢出到其他数据空间，造成正常数据破坏或者访问非法内存引发程序崩溃终端异常。使用非安

全函数:使用 strlen、strcpy 等非安全函数,引发堆栈溢出,容易被黑客获取系统控制权进而破坏系统,造成终端死机、重启或丢失重要数据。

要保证源码安全,除了采用严格的代码规范流程,采用统一代码编写规则,开发人员代码相互 review 外,还可采用成熟的代码检测产品,如 Coverity。Coverity 的静态分析引擎能够帮助开发者找出代码缺陷和安全漏洞,提供精确、可行的修复指导,支持包括 C/C++, Java, C#, Javascript, Objective-C,Python, 超文本预处理(PHP: hypertext preprocessor,PHP)等语言。

4 测试及应用

文中选取传统模式设计的电能质量监测终端和考虑信息安全设计的电能质量监测终端进行测试对比。两者监测终端的硬件相同,CPU 采用精简指令集架构的中央处理器(performance optimization with enhanced RISC-performance computing,PPC),主频 800 MHz,通信网口 100 Mbps。针对信息安全进行如下测试,测试结果见表 3。

表 3 信息安全测试

Table 3 Information security test

测试项	传统终端	信息安全终端
DOS 攻击(80 Mbps)	通信中断 无法连接	运行正常
协议 FUZZER 测试	CPU 负载加重 液晶响应慢	运行正常
重放攻击	允许登录	拒绝登录
端口扫描测试	ftp/telnet 等 不安全端口	无风险及未用端口
明文测试	用户名密 码为明文	无明文
DLL 注入攻击	允许非法 DLL 调用	拒绝非法 DLL
敏感信息泄露	用户名、密码暴露	未发现
越权访问	无权限分级 权限都为 root 用户	未发现
文件白名单	非法文件允许下载	未授权拒绝下载
逆向分析	存在非安全 函数等漏洞	未发现漏洞

(1) DOS 攻击。施加 SYN flood、UDP flood 和 ICMP flood 流量 80 Mbps,测试终端正常业务是否正常。

(2) FUZZ 攻击。模拟 MMS、调试端口畸形数据报,采用 UDP/TCP 方式发送,测试终端业务是否正常。

(3) 重放攻击。抓取登录报文进行重放攻击,查看终端是否允许登录。

(4) 端口扫描。采用 nmap 工具扫描端口,对非法及未用端口进行扫描查看终端是否仅开启合法端口。

(5) 明文测试。抓取客户端登录报文查看用户名、密码是否采用明文传输。

(6) 动态库(dynamic link library,DLL)注入攻击。对客户端工具进行 DLL 注入,监测客户端工具是否拒绝非法 DLL。

(7) 敏感信息泄露。检测是否存在用户名、密码、开发路径以及关键文件名等敏感信息泄露。

(8) 越权访问。检测普通用户是否存在越权行为,如分配用户、查看审计日志;审计用户是否存在查看数据等越权行为。

(9) 文件白名单。检测是否存在非法文件下载功能,如未授权文件上载和下载功能。

(10) 逆向分析。对程序进行反汇编,检测是否存在拒绝服务漏洞、缓冲区溢出漏洞、整型漏洞、释放再利用等漏洞。

与传统的电能质量终端相比,通过访问授权的控制策略禁止非授权软件非法访问;通过角色控制策略细分用户权限,避免无权限划分造成的非法及越权访问;通过对数据进行签名和加密算法,保证了程序和数据的完整性与机密性;通过关闭系统漏洞和未用端口,使用健壮的操作系统和协议栈,优化应用程序避免了网络攻击;通过独立监护进程进行程序和配置完整性校验,建立了程序备份与恢复机制;通过源码检测机制,从源代码层面避免了拒绝服务漏洞、缓冲区溢出漏洞、整型漏洞、释放再利用等漏洞。传统终端与文中终端对比结果见表 4。

表 4 终端对比测试

Table 4 Terminal comparison test

对比项	传统终端	文中终端
访问授权	无	强
角色控制	无	强
完整性与机密性	无	强
网络攻击	弱	强
备份与恢复	无	强
源码安全	无	强

文中设计的电能质量终端从授权访问、角色控制、完整性与机密性、网络攻击、备份与恢复、源码安全等方面进行了全方位考虑,有效地预防可能出现的网络安全问题。该终端广泛适用于各电压等级的发电厂、常规及智能变电站、直流换流站、新能源、钢铁化工、精密仪器制造等应用场景,可有效抵御针对终端本体的网络攻击,降低信息丢失及死机

风险,弥补了安全防护体系缺失的一环,有效提升了电能质量监测系统网络的健壮性。

5 结语

文中针对传统电能质量存在的安全体系结构缺陷,从授权访问、角色控制、完整性与机密性、网络攻击、备份与恢复、源码安全等方面提出了设计方案。授权访问避免软件非法授权访问;角色控制禁止非法用户访问和越权访问;完整性和机密性保证了程序、数据完整和防止非法篡改;网络攻击避免终端死机、业务停止;备份与恢复提供程序和配置遭受破坏后恢复机制;源码安全保证源码层面的溢出漏洞。设计方案有效地提高了终端运行和维护的安全性。

文中提出的方案还能被应用于变电站间隔层保护、测控、PMU、录波器等嵌入式终端,从授权访问、角色控制、完整性与机密性、网络攻击、备份与恢复、源码安全等方面考虑都是适用的,对提升变电站间隔层设备本体安全能力有很大的参考意义和实用价值。

参考文献:

[1] 倪明,颜诘,柏瑞,等. 电力系统防恶意信息攻击的思考[J]. 电力系统自动化,2016,40(5):148-151.
NI Ming,YAN Jie,BO Rui,et al. Power system cyber attack and its defense[J]. Automation of Electric Power Systems,2016,40(5):148-151.

[2] 童晓阳,王晓茹. 乌克兰停电事件引起的网络攻击与电网信息安全防范思考[J]. 电力系统自动化,2016,40(7):144-148.
TONG Xiaoyang,WANG Xiaoru. Inference and countermeasure presuppostion of network attack in incident on Ukrainian power grid[J]. Automation of Electric Power Systems,2016,40(7):144-148.

[3] 国家发展改革委员会. 电力监控系统安全防护评估规定(国家发展和改革委员会14号令)[S]. 2014.
National Development and Reform Commission. Regulations on security protection evaluation of power monitoring system (No. 14 of national development and Reform Commission)[S]. 2014.

[4] 国家能源局. 电力监控系统安全防护总体方案(国能安全36号)[S]. 2015.
National Energy Administration. Overall security protection scheme for power monitoring system (National Energy Security No.36)[S]. 2015.

[5] 彭卉,邹舒,付永生,等. 冲击负荷接入电网的电能质量分析与治理方案研究[J]. 电力系统保护与控制,2014,42(1):54-61.
PENG Hui,ZOU Shu,FU Yongsheng,et al. Research of the power quality problem and treatment scheme for impact loads connected into Chongqing power system[J]. Power System Protection and Control,2014,42(1):54-61.

[6] 刘书铭,李琼林,陈栋新,等. 中高压配电网非线性用户的电能质量特性研究[J]. 电力系统保护与控制,2012,40(15):150-155.
LIU Shuming,LI Qionglin,CHEN Dongxin,et al. Study of power quality characteristics of nonlinear electric user in medium-high voltage distribution networks[J]. Power System Protection and Control,2012,40(15):150-155.

[7] 丁思奇,曼苏乐,崔灿,等. 静止同步补偿器在电弧炉治理中的应用仿真[J]. 电力系统及其自动化学报,2013,25(1):155-160.
DING Siqi,MAN Sule,CUI Can,et al. Simulation of STATCOM for electric arc furnace governance[J]. Proceedings of the CSU-EPSA,2013,25(1):155-160.

[8] 秦贞良,贾春娟,张卫星,等. 实测冲击负荷建模新方法[J]. 电力系统及其自动化学报,2015,27(9):80-84.
QIN Zhenliang,JIA Chunjuan,ZHANG Weixing,et al. New modeling method for measuring impact load[J]. Proceedings of the CSU-EPSA,2015,27(9):80-84.

[9] 吕志盛,闫立伟,罗艾青,等. 新能源发电并网对电网电能质量的影响研究[J]. 华东电力,2012,40(2):251-256.
LYU Zhisheng,YAN Liwei,LUO Aiqing,et al. Impact of new energy power grid-integration on grid power quality[J]. East China Electric Power,2012,40(2):251-256.

[10] 高昆仑,辛耀中,李钊,等. 智能电网调度控制系统安全防护技术及发展[J]. 电力系统自动化,2015,39(1):48-52.
GAO Kunlun,XIN Yaozhong,LI Zhao,et al. Development and process of cybersecurity protection architecture for smart grid dispatching and control systems[J]. Automation of Electric Power Systems,2015,39(1):48-52.

[11] 邹春明,郑志千,刘智勇,等. 电力二次安全防护技术在工业控制系统中的应用[J]. 电网技术,2013,37(11):3227-3232.
ZOU Chunming,ZHENG Zhiqian,LIU Zhiyong,et al. Application of cyber security in industrial control systems based on security protection technology for electrical secondary system[J]. Power System Technology,2013,37(11):3227-3232.

[12] 王栋,陈传鹏,颜佳,等. 新一代电力信息网络安全架构的思考[J]. 电力系统自动化,2016,40(2):6-11.
WANG Dong,CHEN Chuanpeng,YAN Jia,et al. Pondering a new-generation security architecture model for power information network[J]. Automation of Electric Power Systems,2016,40(2):6-11.

[13] 李田,苏盛,杨洪明,等. 电力信息物理系统的攻击行为与安全防护[J]. 电力系统自动化,2017,41(22):162-167.
LI Tian,SU Sheng,YANG Hongming,et al. Attacks and cyber security defense in cyber-physical power system[J]. Automation of Electric Power Systems,2017,41(22):162-167.

[14] 苏盛,吴长江,马钧,等. 基于攻击方视角的电力CPS网络攻击模式分析[J]. 电网技术,2014,38(11):3118-3125.
SU Sheng,WU Changjiang,MA Jun,et al. Attacker's perspective based analysis on cyber attack mode to cyber-physical sys-

tem[J]. Power System Technology,2014,38(11):3118-3125.

[15] 骆钊,谢吉华,顾伟,等. SM2 加密体系在智能变电站站内通信中的应用[J]. 电力系统自动化,2015,39(13):116-123.
LUO Zhao,XIE Jihua,GU Wei,et al. Application of SM2 encrypted system in smart substation inner communication[J]. Automation of Electric Power Systems,2015,39(13):116-123.

[16] 骆钊,谢吉华,顾伟,等. 基于 SM2 密码体系的电网信息安全支撑平台开发[J]. 电力系统自动化,2014,38(6):68-74.
LUO Zhao,XIE Jihua,GU Wei,et al. SM2-cryptosystem based information security supporting platform in power grid[J]. Automation of Electric Power Systems,2014,38(6):68-74.

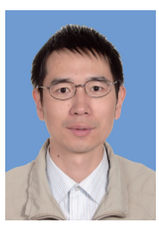
[17] 赵兵,高欣,郜盼盼,等. 适用于用电信息采集的轻量级认证密钥协商协议[J]. 电力系统自动化,2013,37(12):81-86.
ZHAO Bing,GAO Xin,GAO Panpan,et al. A lightweight authenticated protocol with key agreement for power utilization information collecting[J]. Automation of Electric Power Systems,2013,37(12):81-86.

[18] 樊爱宛,杨照峰,常强,等. 电力调度系统无证书数字签名技术[J]. 电力系统自动化,2013,37(19):105-109.
FAN Aiwan,YANG Zhaofeng,CHANG Qiang,et al. Application of certificateless signature scheme in electric power dispatching system[J]. Automation of Electric Power Systems,2013,37(19):105-109.

[19] 徐茹枝,郭健,李衍辉. 智能电网中电力调度数字证书系统[J]. 中国电力,2011,44(1):37-40.
XU Ruzhi, GUO Jian, LI Yanhui. Power dispatching digital certificate system in smart grid[J]. Electric Power,2011,44(1):37-40.

[20] 樊爱宛,刘玉坤,赵伟艇. 数字签密技术在智能电网中的应用[J]. 智能电网,2014,47(7):128-133.
FAN Aiwan,LIU Yukun,ZHAO Weiting. Application of certificateless signcryption scheme to smart grids[J]. Smart Grid,2014,47(7):128-133.

作者简介:


程立

程立(1977),男,硕士,高级工程师,从事智能数字化变电站、电能质量等相关工作(E-mail:chengl@nrec.com);

徐东方(1979),男,硕士,高级工程师,从事嵌入式平台软件开发等相关工作;

曾凯(1988),男,硕士,高级工程师,从事工具软件开发等相关工作。

Design and application of power quality terminal information security

CHENG Li, XU Dongfang, ZENG Kai, LIU Zhongze, ZHU Herong

(NR Electric Co.,Ltd.,Nanjing 211102,China)

Abstract:With the development of modern computer technology and internet,the problem of information security has become more and more obvious. Because of the simple network environment in the early times,the traditional power quality terminal is not considered the information security issues,and is weak in resisting illegal access and network attacks. In view of the design defects of traditional power quality terminals,a terminal design and implementation scheme based on information security is proposed. Also,a practical solutions in access authorization,audit record,data integrity and tamper-proof modification,network attack,backup and recovery,and source code security are provided in the scheme. The information security strength of terminal is enhanced effectively. The security test results show that the scheme effectively enhances the terminal information security capability and resists network attack and other risks. The implementation scheme proposed can also be applied to protection relay,bay control unit,PMU,wave recorder and bay layer terminals.

Keywords:power quality;information security;digital signature;authorization;encryption

(编辑 钱悦)