

基于数字证书认证的电力安全拨号认证系统

秦超, 张涛, 林为民

(国网电力科学研究院/南京南瑞集团公司, 江苏省南京市 210003)

摘要: 针对电力远程拨号系统的安全防护需求, 对其相关安全隐患进行了分析, 并设计和实现了基于数字证书认证的电力安全拨号认证系统, 分析了其技术特点。该系统可对拨号客户端和拨号网关进行数字证书互验及客户端可信接入, 对传输数据进行加密、签名, 避免敏感信息泄漏及篡改, 并可进行细粒度访问控制和用户行为审计, 有效地解决了电力远程拨号系统相关安全隐患, 对电力二次系统安全防护具有重要意义。

关键词: 挑战握手验证协议; 公钥基础设施; 证书权威认证机构; 加密隧道; 智能卡双因素认证

中图分类号: TM73

0 引言

电力系统远程拨号应用非常广泛, 如能量管理系统(EMS)、相角测量系统、电能计量系统实时和准实时系统的远程维护, 以及调度生产管理系统厂站操作票应用、电厂数据传输等。基于广域网组成部分之一的公共交换电话网(PSTN)和电力内网的拨号通信, 客观上存在一定的安全风险。广域网上用户复杂, 黑客、间谍、病毒等非常猖獗, 对电力控制系统的数据传输安全性、可靠性、实时性等影响较大, 中国电力数据网络必须对广域网用户授权管理, 并进行边界安全设备部署防护^[1-2]。虽然电力系统对这些安全问题已开始逐步重视, 但还没有完善细致的远程拨号安全解决方案。因此, 本文针对电力远程拨号可能存在的所有安全问题进行了详细分析, 并对此进行电力安全拨号认证系统的系统部署、逻辑设计、功能框架结构设计等, 以实现完善的电力远程拨号应用的安全防护。

1 传统远程拨号系统安全性分析

长久以来, 传统远程拨号系统的结构都是采用拨号服务器进行远程拨号接入, 并使用基于挑战握手身份验证协议(CHAP)/微软挑战握手身份验证协议(MS-CHAP)的身份验证方式^[3], 电力系统 I 区 EMS/广域测量系统(WAMS)等的远程拨号维护应用的部署如图 1 所示。

传统的电力系统拨号应用接入方式存在很多安全隐患:

1) 拨号客户端主机安全性。在用户名、口令正

确的前提下, 任何客户端主机都可进行拨号连接, 包括未及时安装、升级系统补丁、防火墙软件、防病毒软件的主机。这些主机存在一定安全风险, 可能作为黑客进攻的跳板。

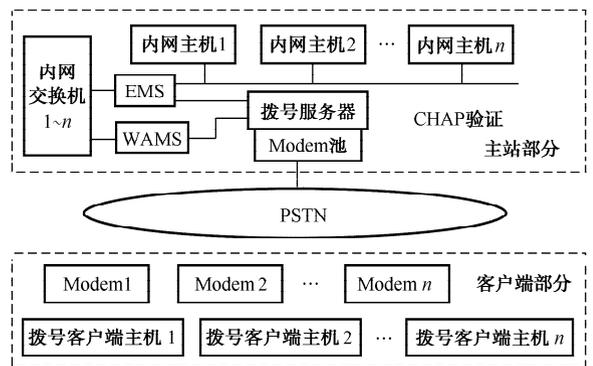


图 1 电力系统传统远程拨号应用部署
Fig. 1 Traditional remote dialing structure diagram of power system

2) CHAP/MS-CHAP 身份认证机制的局限性。目前拨号系统大多基于 CHAP/MS-CHAP, 通过单向哈希算法等进行用户身份鉴别, 但协议本身存在重大安全缺陷, 如易受字典攻击、重放攻击^[3]等。更突出的问题是, 在拨号系统实际运行中, 口令的强度、安全性、授权使用难以保证, 大多数口令易猜测获取, 并长久不变; 为使用方便, 共用账户登录现象非常普遍, 难以进行有效的身份鉴别, 而通过建立多账户管理并定期修改口令, 虽可提高安全性, 但由于拨号客户端较多, 造成管理复杂、成本较高。

3) 拨号过程数据安全传输问题。在拨号过程中, 大量业务数据包括敏感数据都经由 PSTN 明文传输, 无任何保密措施, 很容易被窃听和篡改。

4) 网络层协议访问控制问题。受系统软件限

制、管理成本等影响,对用户拨号访问基本没有协议、地址、端口等访问控制,或控制粒度较粗,用户通过认证后经交换机基本可访问所有内网主机。

5)应用层协议访问控制问题。几乎所有拨号系统对用户拨号访问都没有应用层协议访问控制,对常见应用协议,如 Telnet、rlogin、文件传输协议(FTP)、超文本传输协议(HTTP)、远程桌面协议(RDP)等没有安全监控、过滤,用户可执行任何命令操作。

6)用户行为安全审计问题。大多数拨号系统无安全审计或仅有网络层审计,对于上述第2、第4和第5个问题,目前大多数电力拨号系统安全审计粒度较粗,无法对用户具体操作行为审计,更无法追究用户真正身份。

以上的安全问题相互联系,反映了目前的拨号系统在安全架构设计方面存在着重大缺陷,本文将结合电力系统实际情况,引入一些关键技术进行电力安全拨号认证系统的安全架构设计来解决上述问题。

2 电力安全拨号认证系统设计

2.1 系统结构设计

电力安全拨号认证系统主要由客户端系统和服务器端系统组成。如图2所示。

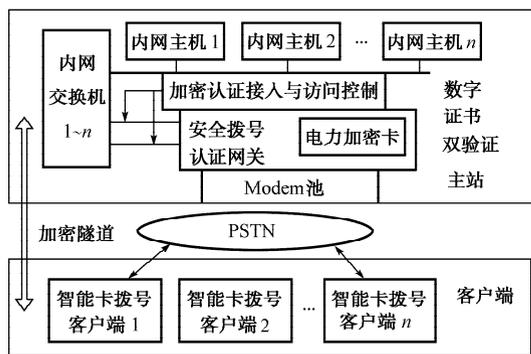


图2 电力安全拨号认证系统逻辑结构
Fig.2 Structure of electronic safely dialing and authentication system

1)客户端

拨号客户端通过内置数字证书智能卡进行本地身份验证,并部署专用安全拨号软件进行与服务器端的认证交互。

2)电力系统主机

部署内置电力加密卡的安全拨号认证网关。电力加密卡用于存放密钥及数字证书。拨号网关硬件结构采用 Motorola 公司 PowerPC 处理器架构及嵌入式 Linux 安全操作系统内核,以确保系统整体抗

攻击性和高性能。

通过客户端和拨号网关自身持有的数字证书进行双方强身份验证,建立安全加密隧道进行安全保密通信。在安全隧道中,通过客户端安全拨号软件和服务器端的安全认证接入软件进行可信认证接入和细粒度的访问控制及安全审计。

2.2 基于数字证书的身份认证机制

为克服传统用户名口令验证机制缺陷,考虑结合数字证书的身份验证方式,采用智能卡、电力加密卡作为密钥存储和硬件运算介质。

2.2.1 公钥基础设施与数字证书系统

公钥基础设施^[4-5](PKI)是用非对称密码算法原理和技术实现并提供安全服务的具有通用性的安全基础设施。用户可利用 PKI 平台提供的安全服务进行安全通信。使用基于公钥技术平台的用户建立安全通信信任机制的基础是:网络间进行的任何需要提供安全服务的通信都是建立在公钥的基础上的,而与公钥匹配的私钥只掌握于合法通信实体本身。数字证书为一个用户身份和公钥的结合,这种结合是证书权威认证机构^[4-5](CA)进行授权的,它是 PKI 的核心组成部分,是数字证书的签发机构。通过 CA 这一 PKI 应用中权威、可信任、公正的机构的签名授权以及对子 CA 授权形成的证书信任链,可唯一识别一个实体的身份并用于信息加解密、签名认证等。

目前电力系统普遍部署了基于 PKI 体系的 CA 系统,用于对电力生产及管理系统与数据网上的用户、关键网络设备、服务器提供数字证书服务。文献[6]就提出了一种基于 PKI 的变电站自动化系统访问安全管理的实现和应用结构。

2.2.2 基于数字证书的身份验证

系统实际通信前,客户端和拨号网关都必须申请数字证书。客户端智能卡证书由管理员直接调用硬件生成并置入,私钥由片上操作系统^[7]保护,不能出卡。拨号网关调用硬件加密单元,生成符合公钥加密第10项标准^[4-5](PKCS#10)格式的证书请求文件,由管理员将此请求文件提交 CA 进行签发。拨号网关私钥由加密芯片保护,双方申请都必须经过有关管理部门严格审核。

数字证书标准域信息主要含颁发者、被颁发者,含具体单位、部门、姓名等,以及有效时间、公开密钥值、CA 签名算法、授权签名(表明权威性)等。扩展域信息表明对该证书的密钥使用权限(数字签名、密钥协商等),以限制密钥使用范围。

2.2.3 数字证书的硬件载体

客户端数字证书存储介质为智能卡。智能卡^[7]

是具有复杂安全体系和片上操作系统的智能卡片,具有高度安全性,通过特殊硬、软件设计使密钥产生、证书等文件存放达到很高安全级别,广泛应用于网银、税控等,是双因素认证^[5,7]的最普遍形式,即只有同时拥有智能卡硬件和掌握个人识别码(PIN)^[7]的人才具有证书使用权限,安全性很高,目前主流接口形式为 USB。

同时,服务器端拨号网关的密钥及证书等加密

存储于内嵌电力专用加密芯片的电力加密卡安全存储区内,密钥和证书等均受专用加密算法加密保护存放。加密芯片和加密卡均经过国家保密局审批,具有高度的安全性。

2.3 软件体系结构设计

2.3.1 软件体系设计及组成

电力安全拨号认证系统功能框架如图 3 所示。

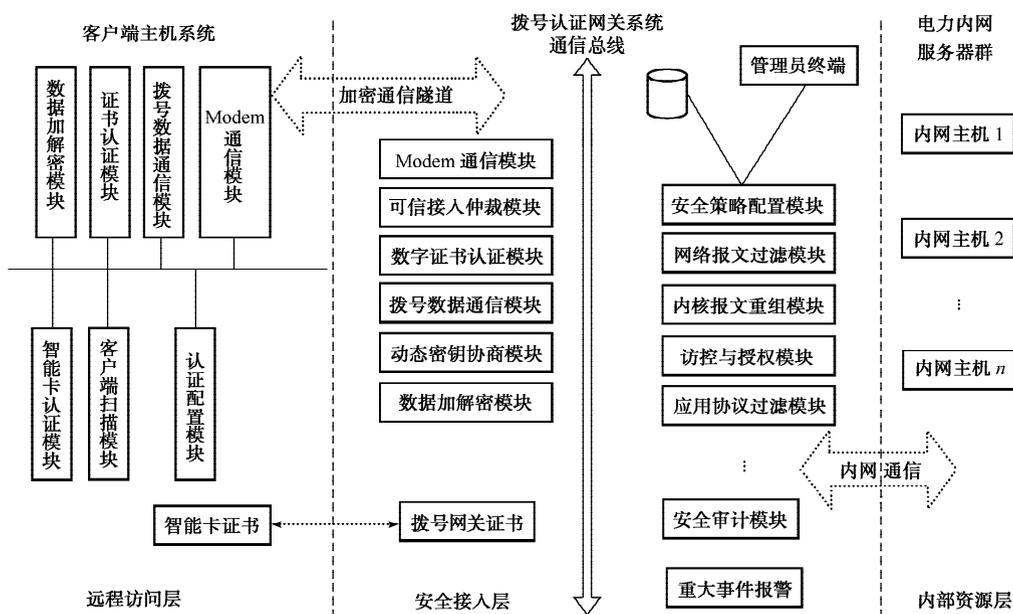


图 3 电力安全拨号认证系统功能框架

Fig. 3 Function architecture of electronic safely dialing and authentication system

客户端安全拨号软件主要包括 Modem 通信模块、智能卡认证模块、客户端扫描模块、数据通信模块等。服务器端安全接入软件主要包括 Modem 通信模块、证书认证模块、访问与授权模块及规则配置、安全审计模块等。双方交互的主要过程如下:

1) 管理员终端通过配置接口设置系统安全策略,对内网资源、用户组、用户、访问权限等设置,对客户端接入标准,如操作系统及内核、补丁版本、防火墙类型及开启状态、防病毒软件类型及开启状态、防病毒软件病毒库版本和风险服务及端口等进行定制,保存于安全策略数据库中。

2) 客户端软件及拨号网关侧同时配置正确的 CA 证书链^[4-5]和黑名单(CRL)^[4-5]列表,以进行后续证书双验证。

3) 两侧建立 Modem 通信信道连接,通过智能卡及数字证书认证模块等进行双方证书互验,双方必须通过以下认证步骤。①拨号客户端插入智能卡 PIN 码初验身份,3 次 PIN 码错误将锁死,必须重新提交直属电力 CA 进行重新签发,以确保禁止非法

用户尝试;②证书链合法性验证:按照由下而上方式尝试搜寻并依序验证 1 级 CA、2 级 CA、3 级 CA 等证书链的签名是否合法,能否顺利验签待验证证书合法性;③数字证书解析及有效性验证:按照 X.509 数字证书标准解析相关字段,检查待验证证书颁发者信息是否和直属 CA 证书一致,验证证书归属地、主题、组织、组织机构、密钥详细用途等字段的有效性等;④时效性验证:双方检查各自系统协调世界时间(UTC)时钟,并根据过程 2 中取得的起、止时间校验双方证书时效性,超过有效期的证书不能用于身份验证及后续密钥协商等过程;⑤CRL 验证:根据证书吊销列表,通过证书序列号等搜索匹配待验证证书,如已作废,则待验证证书非法。

4) 两侧数据加解密及通信模块调用硬件算法如 RSA, 3DES, AES, SHA1 等按照 IPsec(IP security protocol)或其他协议进行 IKE(Internet key exchange protocol)密钥协商^[4-5,8],建立基于对称算法的加密隧道,对后续通信全程加密、签名认证。原始 IP 报文经过加密、签名后可以消除报文传输过程

中被窃听、被篡改的风险,而且动态密钥协商模块定时协商、更换加密密钥,增加了黑客破解、攻击的难度,有效地保证了数据的完整性、保密性、不可抵赖性。

5)对不同类型客户端,依据预定义接入标准,由客户端扫描模块进行系统动态安全检查(一般定时周期为 30 s~60 s),及时判断客户端主机系统当前的健康状态并传递给服务器端进行仲裁,对存在安全风险的主机如未及时升级系统补丁、防病毒库版本太低、存在风险端口服务等情况均进行警告并拒绝接入。

6)拨号网关系统模块依靠通信总线进行消息通信,依据全局策略进行安全控制。Modem 通信模块进行拨入号码、物理端口限制;数据包过滤模块、访控与授权模块通过用户层接口和内核报文重组模块通信,对报文的协议、端口、地址进行过滤,阻止畸形、碎片的攻击以及其他非法报文通过,并进行详细的日志记录。

7)除进行上述网络层控制外,通过应用协议过滤模块,可同时对接入用户越权、危险动作进行过滤,如针对 telnet 协议命令 shutdown、kill、rm 等进行正则表达式匹配过滤,确保可能的操作不会危及内网主机安全,并通过 Syslog 日志系统进行日志审计。

8)所有模块日志信息包括非法报文丢弃信息、攻击信息和会话通信信息(包括真实用户身份、连接建立与终止时间、分配 IP、通信持续时间、数据流量、通信协议、地址、端口、操作命令及参数)等都通过 Syslog 日志接口发送给安全审计模块进行详细记录审计,并在重大事件发生时通过硬件接口进行声光报警。管理员对远程拨号访问发生的全部事件一目了然,便于事后追查和修补漏洞。

2.3.2 系统技术特点

与电力传统拨号系统相比,该系统具有以下显著特点:

1)身份验证强度高。客户端和拨号网关双方通过数字证书体系的数字证书及硬件密码算法进行彼此身份验证,验证强度高、安全性好,并且管理简捷、安全,管理成本低。

2)可信安全接入与有效访问控制。客户端和服务器端分别部署专用安全软件进行安全扫描、加密隧道协商、数据加密签名、数据过滤、安全监控、网络及应用层访问控制、安全审计等,既保证了通信过程中数据的保密性、完整性、不可抵赖性,又可进行细粒度访问控制,并可对用户具体操作进行详细审计;对客户端主机安全性进行的监控和评估,避免了风险接入可能对内网造成的侵害。

3)系统可扩展性好。凡是符合 ISO 7816^[7]、微软 CSP(cryptographic service provider)^[4-5,7]标准的智能卡都可以作为客户端数字证书载体。针对电力用户需求,可定制开发新的应用协议过滤模块,以进行细粒度访问控制及用户行为安全审计。

4)密码运算安全、高速。客户端和服务端的安全软件底层基于硬件智能卡、电力专用加密芯片进行硬件算法运算,加密保护通信过程的全部数据,全部运算在硬件中进行,安全性、稳定性、实时性高。实测 RSA 非对称算法可实现 1 024 bit 公钥运算 2 000 次/s、私钥运算 800 次/s。

5)实际通信速率良好。文献[9]提出了一种用于发电竞价信息的加密系统开发方法,直接调用 RSA 非对称算法加密,而 RSA 非对称算法速度较慢^[8],其系统运算开销比 3DES 等对称算法大,不适合长时间、大数据量数据加密传送。而本系统通过动态协商的对称密钥加密,既保证数据报文保密传送,又在拨号网络的低速通道中加快了系统传输速度。拨号过程实测加密通信速率平均为上行 27.4 kbit/s(下行 30 kbit/s)和 56 kbit/s Modem 正常明文平均通信速率上行 33.6 kbit/s(下行 40 kbit/s)比较下降了 18.45%(25%),根据用户现场对 ANSI 类 Telnet/SSH 的命令行终端、WTS(windows terminal service)等远程桌面类图形界面终端的测试,操作响应时间在可接受范围内,可进行正常的远程维护和数据传输。

3 结语

本文设计的电力安全拨号认证系统,针对传统拨号应用中存在的安全问题,通过采用多种安全技术,如基于数字证书验证、安全扫描、隧道加密、网络层和应用层访控技术、细粒度安全审计技术等,进行了新的系统结构及软件体系设计,较大地增强了电力远程拨号应用的安全性及防护能力。

目前,该系统的软、硬件设备已广泛应用于全国各级电力调度中心和电厂、变电站等,对电力远程拨号应用的安全防护起到了重要作用,对落实《电力二次系统安全防护总体方案》的有关规定有重大的现实意义,并有力地保障了电力系统安全监控、生产的进行。

参考文献

- [1] 辛耀中,胡红升,卢长燕,等.中国电力数据网络建设和运行中应注意的四个关系.电力系统自动化,1998,22(1):1-5.
XIN Yaozhong, HU Hongshen, LU Changyan, et al. The four relationships having to be considered in the construction and operation of China electric power data network. Automation of Electric Power Systems, 1998, 22(1): 1-5.

(下转第 100 页 continued on page 100)

- [2] 辛耀中. 电力信息化几个问题的探讨. 电力信息化, 2003, 1(3): 20-23.
XIN Yaozhong. Discussion on electric power information technology. Electric Power Information Technology, 2003, 1(3): 20-23.
- [3] 李焕洲, 林宏刚, 戴宗坤, 等. MS-CHAP 鉴别协议安全性分析. 四川大学学报: 工程科学版, 2005, 37(6): 12-15.
LI Huanzhou, LIN Honggang, DAI Zongkun, et al. Analysis on the security of MS-CHAP. Journal of Sichuan University: Engineering Science Edition, 2005, 37(6): 12-15.
- [4] NASH A, DUANE W, JOSEPH C, et al. PKI: implementing and managing E-security. New York, NY, USA: Osborne/McGraw-Hill, 2001.
- [5] ADAMS C, LLOYD S. Understanding PKI: concepts, standards, and deployment considerations. 2nd ed. Upper Saddle River, NJ, USA: Addison-Wesley Pub Co, 2002.
- [6] 段斌, 刘念, 王健, 等. 基于 PKI/PMI 的变电站自动化系统访问安全管理. 电力系统自动化, 2005, 29(23): 58-63.
DUAN Bin, LIU Nian, WANG Jian, et al. Access security of substation automation systems based on PKI/PMI. Automation

- of Electric Power Systems, 2005, 29(23): 58-63.
- [7] 李祥. 智能卡研发技术与工程实践. 北京: 人民邮电出版社, 2003.
- [8] STALLINGS W. 密码编码学与网络安全. 孟庆树, 王丽娜, 傅建明, 等译. 北京: 电子工业出版社, 2006.
- [9] 姚建刚, 罗滇生, 陈亮, 等. 湖南电网发电竞价信息加密系统的开发. 电力系统自动化, 2001, 25(15): 12-14.
YAO Jiangan, LUO Diansheng, CHEN Liang, et al. Development of information encryption system for Hunan electricity bidding market. Automation of Electric Power Systems, 2001, 25(15): 12-14.

秦 超(1978—), 男, 通信作者, 硕士, 工程师, 主要研究方向: 电力系统信息网络安全。E-mail: qinchao@sgepri.com
张 涛(1976—), 男, 硕士, 高级工程师, 主要研究方向: 电力系统信息网络安全。E-mail: zhangtao@sgepri.com
林为民(1964—), 男, 硕士, 研究员级高级工程师, 主要研究方向: 电力系统信息网络安全的研究及管理。E-mail: linweimin@sgepri.com

A Digital Certificate Authentication-based Electric Power Safe Dialing Authentication System

QIN Chao, ZHANG Tao, LIN Weimin

(State Grid Electric Power Research Institute, Nanjing 210003, China)

Abstract: In view of the demand for security and protection of the electric power remote dialing system, an in-depth analysis is made of the possible hidden dangers to the system. An electric power safe dialing authentication system based on digital certificate authentication is designed and implemented. The technical characteristics of the system are dealt with such as its capability of certificate verification of both the dialing client end and the dialing grid and client end creditable access, data encryption and signature to avoid sensitive information leakage and distortion, while performing fine grained access control and user behavior auditing, effectively solving possible security problems with the electric power remote dialing system.

Key words: challenge handshake authentication protocol; public key infrastructure; certificate authority; encrypted tunnel; smartcard dual factor