电力企业移动安全接入平台①

吴克河[1], 崔文超[1], 何健平[2]

[1](华北电力大学 控制与计算机工程学院, 北京 102206)
[2](上海市电力公司 信息通信公司, 上海 200122)

摘 要: 电力企业承担着为社会经济发展提供安全、可持续电力供应的重要使命, 因此, 电力企业信息系统的安全要求比普通企业要高. 随着电力企业信息化的快速推进, 各种远程移动终端与信息内网的数据交换需求日益增长. 如何保证移动终端远程接入的安全已成为电力企业信息化建设中的关键问题. 在分析传统 SSL VPN 技术的基础上, 针对电力企业信息安全建设的特点和特殊需求, 设计了一种适用于电力企业的新型移动安全接入平台. 该平台能够支持多种移动终端的多因素认证和访问控制, 同时实现了 SSL 高速协议栈、数据隔离等功能, 有效地解决了上面所提到的问题.

关键词: SSL VPN; 电力企业; 无线网络; 多类型终端认证; 双隧道模型; 协议栈

Wireless Security Access Platform in Power Utilities

WU Ke-He[1], CUI Wen-Chao[1], HE Jian-Ping[2]

[1](School of Computer and Control Engineering, North China Electric Power University, Beijing 102206, China)
[2](Information and Communications Company, SMEPC, Shanghai 200122 , China)

Abstract: Power utilities, whose crucial mission is to provide safe and sustainable power supply, have higher security requirements for the enterprise information system than ordinary enterprises. With the development of informatization for power utilities, the demand for data exchange between a variety of wireless remote terminals and Intranet is growing. How to guarantee the security of wireless remote access in power utilities has become a key problem. According to the characteristics and special needs of power utilities, this paper analyzes the traditional SSL VPN technology and designs a new secure wireless remote access platform based on SSL VPN for power utilities, which provides a new solution for secure wireless remote access in power utilities.

Key words: SSL VPN; power utilities; wireless network; multi-type terminals authentication; twin tunnel model; protocol stack

电力企业作为关系国家能源安全和国民经济命脉的重要企业, 其移动接入应用具有以下特点: (1)接入终端种类多, 数量大; (2)数据传输的安全性, 实时性要求高, 覆盖面广, 数据量大; (3)内网应用系统分区, 分级, 分域, 内、外网隔离. 随着电力企业内部网和中国电力数据网(SPDNet,原名 CEDnet)的建立[1], 各种数据与信息内网的数据交换日益增长. 如何实现移动终端的安全接入, 提高跨大区域数据交换的准确性和实时性, 实现生产运行状态和经营管理过程的能观能控, 对于电力企业来说, 是一个亟待解决的问题.

目前, 由 Netscape 公司制定的网络安全通信协议, 即安全套阶层协议 SSL 已成为保密通信的工业标准. 现行的各种浏览器普遍将 HTTP 和 SSL 协议相结合, 从而实现安全通信.

基于以上原因, 本文针对电力企业信息安全建设的特点和特殊需求, 设计了一种基于 SSL VPN 的移动安全接入平台. 该平台从终端接入, 数据传输及内网数据保护三个方面解决了电力企业移动终端接入的三

① 基金项目:中央高校基础科研专项基金(12QX16)
收稿时间:2013-11-22;收到修改稿时间:2014-01-10

个问题, 即移动终端存在安全漏洞且种类繁多, 数据传输使用的加密算法存在潜在风险, 内网服务直接面向外部接入终端, 从而为移动终端安全接入电力企业内网提供了一种可靠的解决方案.

1 相关研究

随着互联网应用的发展和企业信息化的发展, 企业信息安全问题日益严重, 如何保证企业的业务正常开展, 并能安全进行远程访问, 成为企业的迫切需求. 虚拟专用网络 (Virtual Private Network, 简称 VPN) 的提出就是来解决上述问题的, 它利用公共的网络通道 (通常是因特网), 采用安全加密措施, 建立起一个逻辑专用通道, 为客户提供一条安全加密的专用网络通道.

VPN 是一种综合的网络安全方案, 包含了包括身份认证、信息加解密、密钥管理和隧道技术在内的多种重要技术, 其中加密和隧道技术是 VPN 的核心技术. 隧道技术可以分为第二层隧道技术、第三层隧道技术. 第二层隧道技术通过 PPP 包封装各种网络协议在数据链路层实现的隧道技术. 常见的第二层隧道技术有 L2F (RFC 2341, Layer 2 Forwarding)、L2TP (RFC 2661, Layer Two Tunneling Protocol) 、PPTP (RFC 2637, Point-to-Point Tunneling Protocol). 目前, L2F 已经过时; PPTP 则成为目前工业标准, 并被广泛实现和使用; L2TP 是 PPTP 和 L2F 隧道功能的集合, 目前应用也比较多. 第二层隧道技术简单易行, 支持多重连接特性, 但其可扩展性差, 且没有提供内在的安全机制, 所以存在很大的安全隐患. 第三层隧道技术直接把各种网络协议装入隧道协议中, 从而在网络层实现隧道技术. 常见的第三层隧道技术有 GRE (RFC 2784, General Routing Encapsulation)和 IPSec (IP Security). GRE 协议提出较早, 有很强的封装能力, 但其缺点也是不提供任何的安全机制. IPSec 协议定义了应用于 IP 层上网络数据安全的一整套体系结构, 是一组协议簇, 从而充分实现了 VPN 的安全通信要求, 保证了数据来源的可靠性、数据内容的完整性、数据传输的机密性, 是目前主要的 VPN 隧道协议之一. 但是它的主要不足是: 通信兼容性较差, 需要定制的客户端软件, 并且安装和维护困难. 最新一代的 VPN 解决技术是采用 SSL 协议来实现的[2]. 它以 HTTPS 为基础或采用支持 SSL 的应用程序来实现通过网页访问企业内网的网络资源[3], 无需安装特定的客户端软件, 因此具有很高的扩展性和安全性, 是当前最流行的 VPN 解决技术.

从 VPN 的应用角度来看, 早期的 VPN 主要是用于 PC 终端或者移动笔记本电脑的接入, 并且利用的网络环境是公用共享网络, 如 Internet. 到目前为止, 国内外大的运营商如 AT&T、Sprint、Verizon、BellSouth、NTT 都已经开始应用 VPN 构建企业级 VPN 网络系统[4]. 美国的 Array Networks 公司为银行办公网提供的 SSL VPN 解决方案, 有效的解决了银行部门的安全接入问题.

但是在电力行业, 《国家电网公司信息化“SG186”工程安全防护建设方案》指出, 电力企业信息系统安全建设必须坚持以 “分区、分级、分域”为基础, 以“二级系统统一成域, 三级系统独立分域”为指导. 因此, 由于电力企业信息安全建设的自身特点和特殊要求, 上述安全接入解决方案已不能满足电力企业远程接入的需求.

基于上述调查研究, 本文设计了一种新型的移动安全接入平台, 从体系结构, 接入流程等各个方面有效地加强了远程接入的安全性, 具有鲜明的行业特色和其他 VPN 接入方案不可比拟的优越的安全性.

2 平台设计

2.1 逻辑架构

根据相关研究的分析, SSL VPN 是当前最新的安全接入解决技术, 因此平台采用最新的 SSL VPN. 为了保证信息交换的秘密性、完整性和合法性, 本平台对移动终端和安全接入网关之间的数据进行加密处理, 并提取传输信息的特征值, 以保证信息交换的秘密性和完整性. 通过使用证书技术和可信的第三方认证, 平台可以保证移动终端身份的合法性. 依据电力企业 “分区、分级、分域”的防护原则, 平台逻辑架构设计为四个 “安全区”和三个 “专用网络”. 逻辑架构如图 1 所示.

根据安全防护的作用对象不同, 逻辑架构分为四个安全区, 其中包括: 安全终端区、安全传输区、安全接入区、安全访问区. 这四个安全区功能独立, 相互协调, 按照信息流向, 从终端到内部应用系统全面保证移动接入的安全性. 安全终端区包含各种移动终端, 如笔记本电脑、PDA、智能手机、智能电表等. 通过在移动终端中嵌入数字证书、加密芯片、安全软件和安全通信模块, 保证接入终端自身的安全性. 安全传

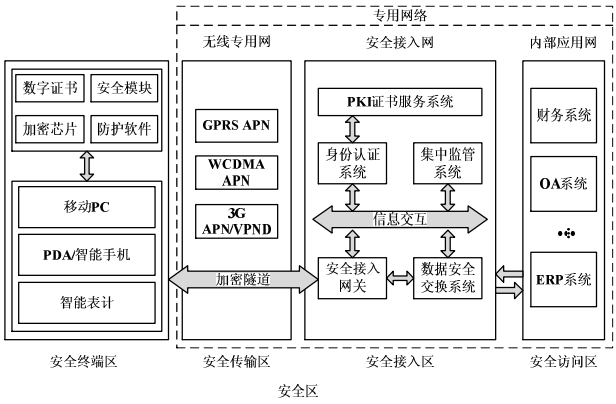


图 1 移动安全接入平台逻辑架构

输区指建立加密传输隧道的无线网络区域. 该区域由私有的高速的网络组成. 它包括 GPRS APN、WCDMA APN 和 3G APN/VPND. 因为无线网络是私有的, 所以企业外部人员无法接入和使用该网络, 降低了无关信息的干扰性, 保证了无线传输环境的安全性. 安全接入区由 PKI 证书服务系统、身份认证系统、集中监管系统、安全接入网关、数据安全交换系统组成. PKI 证书服务系统和身份认证系统用于保证移动终端身份的合法性; 安全接入网关用于转发接入、访问请求以及访问数据, 同时平衡负载; 数据安全交换系统用于数据过滤, 保证内网应用系统数据的安全性; 集中监管系统, 则是对所有接入终端的行为进行集中监控和管理, 同时记录并审核其对内部应用的访问. 安全访问区由企业内部的各种应用系统组成, 如 OA 系统, 财务系统, ERP 系统等. 移动终端的访问最终到达该区相应的应用系统. 各个应用系统根据不同的访问请求给予相应的响应. 该区的主要作用是保证企业内网各种应用系统运行的稳定性和安全性, 并处理最终的请求.

根据信息传输关系的不同, 平台设计了三个专用网络, 其中包括无线专用网、安全接入网、内部应用网. 这三个网络均与公网隔离, 各网络内部数据一致性高, 网络之间耦合度低. 这样设计易于管理和维护, 同时可以防止侵害的扩散. 其中, 无线专用网是指移动接入终端和安全接入点之间的通信网络. 该网络属于安全传输区. 它采用前面介绍的三种私有网络之一搭建, 负责移动终端到安全接入点之间的信息传输. 传输的信息包括应用请求信息和由应用系统返回的响应信息组成, 是最原始和最终的信息. 通过使用私有网络, 该网络即保证了内部应用系统获得准确完整的应用请求, 又保证了移动终端获得正确的请求信息. 安全接入网是指安全接入点和安全接入平台各个子系统之间的通信网络. 该网络属于安全接入区. 它是一个企业内部的局域网络, 负责移动终端的认证和信息的审核. 当移动终端将接入请求及相应的认证信息传送到该网络, 该网络将这些信息传送给相应的子系统, 以完成移动终端的安全检查和认证. 内部应用网指安全接入层对企业内网接口和各应用系统之间的通信网络. 该网络属于安全访问区. 它也是一个企业内部的局域网络, 负责将请求信息传送给应用系统, 同时返回响应信息. 因为该网络与外界没有直接连接, 所以对安全性要求较前两个网络较低.

2.2 物理拓扑

根据逻辑架构设计, 平台的物理拓扑如图 2 所示, 其中主要的物理组成部分有安全移动接入终端、安全接入网关、应用前置机、安全认证系统、单向传输装置、访问控制器.

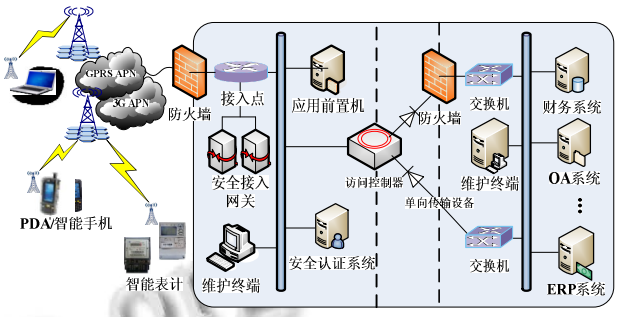


图 2 移动安全接入平台物理拓扑

安全移动接入终端是能够接收多种信号的移动智能设备. 本平台可以支持多种移动终端的接入, 其中包括: 笔记本终端、PDA、智能手机和智能表计等. 为了保证这些移动终端的安全性, 它们均经过改造, 添加了相应的安全模块, 以保证接入终端的安全性. 它们和应用系统前置机进行通信以完成应用请求. 传输数据可以使用国产商密算法(SM1 算法)进行加密, 进一步提高了通信的安全性. 安全接入网关是该平台的核心部分之一. 它是企业内网与移动专网的唯一接口. 它既用于转发接入、访问请求, 又用于将应用系统的返回的信息传回相应的接入终端, 并且负责保证负载均衡. 应用前置机暂存应用系统的最新一段时期的数据, 同时具有相应内部应用系统的一部分功能. 它接

收并处理接入终端的数据包, 同时提供与内部应用系统通信, 数据转发和存储的功能. 当接入终端数量增长时, 可以设置更多的应用前置机, 以保证内部相应的应用系统的稳定运行. 安全认证系统包含证书服务器、公钥/私钥服务器、目录服务器. 它采用基于角色的多因素认证策略, 实现多种移动终端的多因素认证及身份绑定. 单向传输设备用于约束数据流的方向. 它只允许数据从其指定的一端传递到另一端, 不允许反向传输数据. 采用这种装置来实现相互独立的单向数据传输机制有利于分离请求和响应过程, 有效保证了数据的秘密性. 访问控制器将安全接入网关转发来的访问请求经过审核, 过滤后经发送端单向传输设备传递给安全访问区中相应的应用系统, 同时接收由接收端单向传输装置传来的响应数据包, 经处理后转发回安全接入网关.

2.3 接入流程

因为在同一时间可能同时存在请求接入和正在访问应用系统的两种移动终端, 所以为了防止请求接入终端的认证过程对其它正在稳定通信的终端的影响, 平台采用双隧道模型将控制信息和应用数据相互分离, 保证平台的稳定运行. 移动终端的接入过程如图 3 所述.

移动终端的接入过程如下:

(1) 安全移动接入终端向安全接入网关发送接入请求.

(2) 终端和接入网关握手协商, 建立控制通道. 在此过程中, 通信双方交换协议版本、加密算法类型等. 如果控制通道建立成功, 则执行步骤(3). 否则, 返回握手失败错误, 并重连或退出.

(3) 通过控制通道交换认证参数. 不同的终端类型具有不同的认证参数. 然后, 进行多因素认证. 如果认证成功, 则执行步骤(4). 否则, 返回认证失败错误, 并重新认证或退出.

(4) 通过控制通道交换用于数据加密的预共享主密钥, 建立数据通道. 如果数据通道建立成功, 则执行步骤(5). 否则, 返回数据通道建立失败错误, 并且重连或退出.

(5) 安全接入网关收到 SSL 数据包后, 对其进行解密, 然后转发给接入控制器.

(6) 接入控制器对包进行过滤, 并选择合适的发送端的单向传输装置将包传输给相应的内网应用系统.

(7) 应用系统接收并处理请求, 将处理结果再经接收端的单向传输装置传输回安全接入网关.

(8) 安全接入网关接收到应用系统的响应信息后, 将其封装成 SSL 数据包, 然后发送给移动终端.

(9) 通信结束后, 移动终端发送 FIN 消息断开连接, 并清空缓存. 安全接入网关在接收到 FIN 消息后, 等待一段时间, 然后清空此次会话, 并向内部其它模块发送 FIN 消息. 平台其它模块以相同机制结束会话.

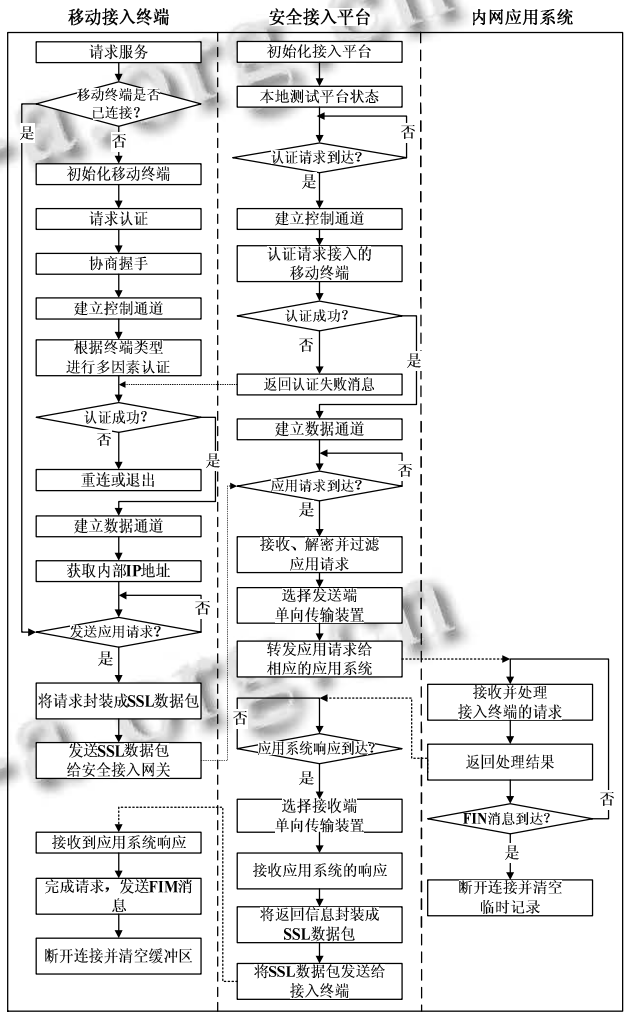


图 3　移动接入终端接入流程

3　平台实现关键技术

3.1 双隧道模型

该模型由四个部分组成: 移动终端、安全接入网关、控制通道、数据通道, 其模型结构如图 4 所示. 它将接入控制信息和通信数据信息相分离, 提高平台的稳定性, 便于统一监管.

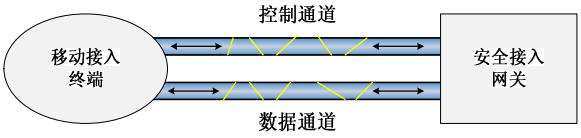


图 4 双隧道模型

由图 4 可知, 该模型的核心部分是两个通信通道, 即控制通道和数据通道. 控制通道的作用是在移动终端和安全接入网关之间交换证书、认证参数, 共享预主密钥等控制信息. 数据通道的作用是加密与内部应用系统通信的数据. 通信双方首先建立控制通道, 然后通过控制通道交换用于数据加密的对称密钥, 用于建立数据通道. 控制通道的建立过程如图 5 所示; 数据通道的建立过程如图 6 所示.

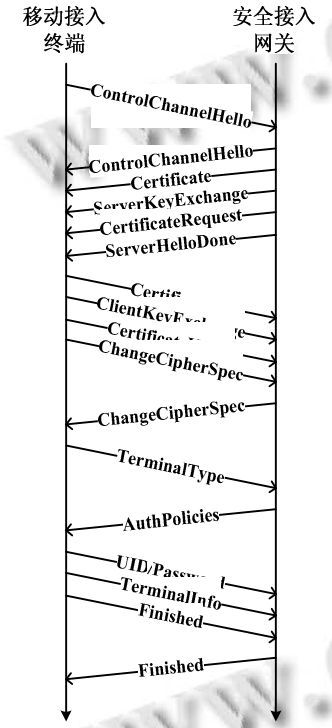


图 5 控制通道的建立过程

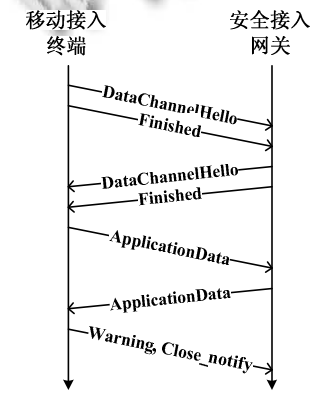


图 6 数据通道的建立过程

3.2 高速协议栈结构

平台改进了传统的 TCP/IP 协议栈, 添加了 SSL 协议处理层, 提高了数据包的解析速率, 从而大幅度地提高了平台的性能. 图 7(a)中说明了传统的 TCP/IP 协议栈的结构[5] [6]. 它需要对数据包进行反复拆包或封包, 频繁在用户态和内核态间接换, 严重影响了系统性能[7]. 而高速协议栈采用了将整个 TCP/IP 协议族整合为一体的设计思路, 整个数据包的处理过程完全在操作系统内核部分完成. 它针对 SSLVPN 的通信特点定制, TCP 层与 IP 层不做明显分层, 数据入栈后 IP 头和 TCP 头一并剥去后直接交由应用数据处理模块处理, 数据出栈时也是直接封装 TCP 头与 IP 头后直接交由数据链路层处理.

如图 7(b)所示.

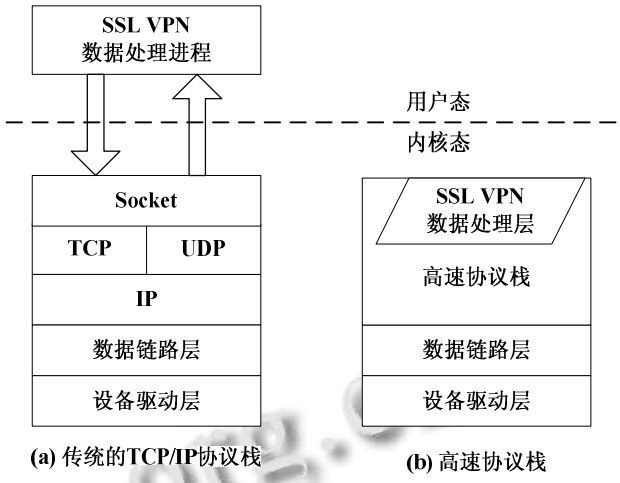


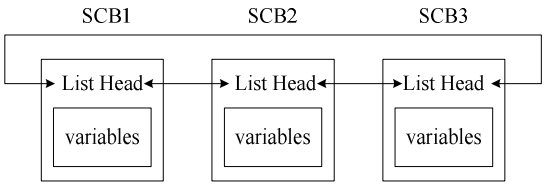
图 7 两种 TCP/IP 协议栈的比较

高速协议栈使用了一种关键的数据结构, 称为 SSL 控制块(SCB). 在图 8(a)中, 三个 SSL 控制块在双向链表中彼此连接, 每个控制块代表一个 SSL 连接. 在每个控制块中有 SSL,TCP,UDP,IP 协议变量的各参数, 以及指向有效载荷的指针 WX_data 和 RX_data, SSL VPN 数据包处理过程通过参考 SSL 控制块中的参数来封包和拆包. 图 8(b)阐述了使用 SSL 控制块创建数据包的原理.

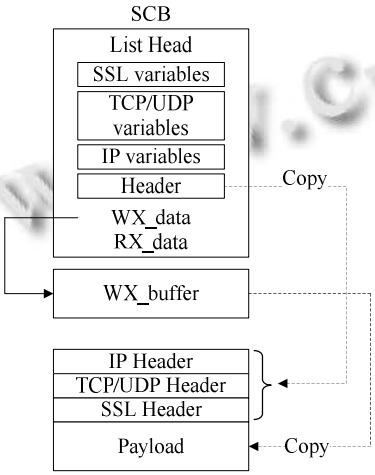
3.3 多类型终端认证方式

多类型终端认证方式是为了满足多种类型移动终端的接入认证需求而设计的. 它是基于多因素认证技术[8]. 它结合了动态口令/动态密码技术、数字证书技术及多因素人机绑定技术[9]. 该技术基于角色, 将不

同类型的移动终端分为不同的角色. 每一种角色具有可制定的认证和绑定策略, 如PDA/智能手机终端可以绑定手机号码、手机序列号等, 验证用户名/口令及证书; 智能表计可以绑定机器 ID 号, 只验证证书. 移动终端使用 USB KEY、SIM 卡、TF 卡存储终端的密钥及数字证书. 图 9 描述了多终端认证流程.



(a) SSL控制块循环双向队列



(b) 利用SCB创建数据包的机制

图 8　高速协议栈结构

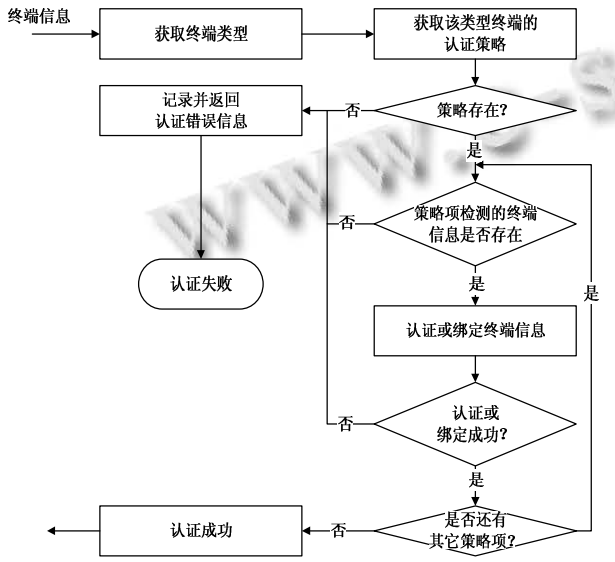


图 9　多类型终端认证方式流程图

4　总结

本文首先对 VPN 的相关研究进行了概述, 并在此基础上针对电力企业信息安全建设的特点和特殊需求, 设计了一种适用于电力企业的新型移动安全接入平台, 详细阐述了该平台的逻辑架构、物理拓扑和接入流程. 然后, 本文分析了实现该平台的关键技术. 现阶段, 主流的安全接入解决方案大部分是针对 PC 终端, 并且利用公用网络接入, 终端接入后直接访问应用. 而本平台则根据电力企业信息安全建设的自身特点和特殊需求, 解决了多种移动终端的安全接入问题. 平台还采用了无线专用网络作为网络通信环境, 提高了系统整体的安全性. 同时, 终端在接入后并不直接访问内网核心应用, 而是通过数据安全交换系统间接访问, 进一步保证了内部系统的安全性. 因此, 本平台具有显著的行业特色和优越的安全性, 是其他安全接入方案不可比拟的. 本平台已经在具体项目中实施部署, 并取得良好成效.

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.
2　Freier K. The SSL protocol Version 3.0. http://www .netscape.com/newsref/SSL 3.0. [1996-11].
3　张岚.SSL VPN 技术在电力企业移动办公中的应用.电力系统通信,2008,29(183):53–56.
4　Resorla E.崔凯(译).SSL 与 TLS.北京:中国电力出版社, 2002.
5　Yoon IS, Chung SH, Kim JS. Implementation of lightweight TCP/IP for small, wireless embedded system. IEEE. Proc. of International Conference on Advanced Information Networking and Applications, 2009.
6　Stevens WR.范建华,译.TCP/IP 详解(卷1:协议).北京:机械工业出版社,2007.
7　Dunkels T, Voigt J, Alonso H. Connecting wireless sensor nets with TCP/IP networks. IEEE. Proc. of the 2nd Int. Conf. on Wired/Wireless Internet Communications, 2004.
8　金斌,周凯波,冯珊.多因素认证系统设计与实现.武汉理工大学学报,2006,28(7):101–104.
9　Schneier B. Applied Cryptography.北京:机械工业出版社,2000.