安全数据网的构建及其在河南电力调度数据网应用

罗汉武[1,2],李 昉[1,2],张 栋[3]
(1.天津大学 管理学院,天津 300072;2.河南省电力公司,河南 郑州 450052;
3.郑州市供电公司,河南 郑州 450052)

摘要:随着网络安全问题的日益突出,虚拟专用网 VPN(Virtual Private Networks)技术将被广泛应用,VPN 的基础安全协议——互联网协议安全 IPSec(Internet Protocol Security)能为任何 Internet 通信提供安全保护协议。详细分析了 IPSec 协议的体系结构、工作模式和关键技术,并结合 IPSec 采用鉴别报头、封装安全有效负荷等加密技术特点,提出了实现安全电力调度数据网的方案和建议,给出了一种利用 IPSec 协议构造电力数据网安全 VPN 的模型,该模型既能保证数据在网络层的保密传送,同时也能对真实通信主机的 IP 地址进行屏蔽和保护。最后,详细介绍了 IPSec 在河南电力调度数据网的应用。

关键词:IPSec 协议;网络安全;数据网
中图分类号:TM 734 **文献标识码**:A **文章编号**:1006-6047(2007)01-0065-03

电力调度数据网络是电力生产实时信息传输的网络,网络传输的主要信息是电力调度实时数据、生产管理数据、通信监测数据等,是电力指挥安全生产和调度自动化的重要基础,在协调电力系统发、送、变、配、用电等组成部分的联合运转及保证电网安全、经济、稳定、可靠的运行方面发挥关键的作用[1]。因此,如何有效地保障重要信息在调度数据网中安全传输,成为一个重要的课题。

1 IPSec 概述

IPSec(Internet Protocol Security)是一个开放式协议的基本框架,用以保证 IP 网络数据通信的安全性[2],IPSec 是一系列基于 IP 网络(包括 Intranet、Extranet 和 Internet)的,由 Internet 工程任务组 IETF(Internet Engineering Task Force)正式定制的开放性 IP 安全标准,是虚拟专网的基础,已相当成熟可靠。这个安全协议是虚拟专用网 VPN(Virtual Private Networks)的基本加密协议,它为数据在通过公用网络(如因特网)在网络层进行传输时提供安全保障[3-4]。

IPSec 可以保证局域网、专用或公用的广域网及 Internet 上信息传输的机密性、完整性和真实性,提供了全网范围内可用的灵活的安全策略解决方案[5-7]。

1.1 IPSec 实现机制

IPSec 通过提供下列服务来保护通过公共 IP 网络传送的私有数据。

a. 访问控制。访问控制是指防止未经授权对资源进行访问。IPSec 中,需要进行访问控制的资源通常指主机中的数据和计算能力、安全网关内的本地网及其带宽。IPSec 使用身份认证机制进行访问控制。

b. 数据源认证。数据源认证对数据来源所声明的身份进行验证,通常与无连接数据完整性相结合。IPSec 使用消息鉴别机制实现数据源认证服务。

c. 机密性和有限传输流量的机密性。相应的接收者能获取发送的真正内容,而无意获取数据的接收者无法获知数据的真正内容。有限传输流量的机密性服务是指防止对通信的外部属性(源地址、目的地址、消息长度和通信频率等)的泄露,从而使攻击者无法对网络流量进行分析,推导其中的传输频率、通信者身份、数据包大小、数据流标识符等信息。

d. 无连接完整性和抗重播。无连接完整性服务对单份数据包是否被修改进行检查,而对数据包的到达顺序不作要求。IPSec 使用数据源认证机制实现无连接完整性服务。IPSec 的抗重播服务,也称为部分序号完整性服务,是指防止攻击者截取和复制 IP包,然后发送到目的地。IPSec 根据 IPSec 头中的序号字段,使用滑动窗口原理,实现抗重播服务。

1.2 IPSec 运作模式

IPSec 可以在 2 种不同的模式下运作:传输模式和隧道模式。

a. 传输模式是指数据在网络中是如何发送和加密的。在此模式下,IPSec 的保护贯穿全程,从源头到目的地,被称为提供终端到终端的传输安全性[9-10]。

b. 隧道模式仅仅在隧道点或者网关之间加密数据。隧道模式提供了网关到网关的传输安全性。当数据在客户和服务器之间传输时,仅当数据到达网关时才得到加密,其余路径不受保护。一旦到达网关,就采用 IPSec 进行加密,等到达目的网关之后,

收稿日期:2006-02-14;修回日期:2006-06-26

数据包被解密和验证,之后数据发送到不受保护的目的主机。隧道模式通常适用于数据必须离开安全的局域网(LAN)或者广域网(WAN)的范围,且在诸如互联网这样的公共网络中传输的场合。

这2种模式下,鉴别报头AH(Authentication Header)和封装安全有效负荷ESP(Encapsulation Security Payload)都可以工作,但ESP具有不同的ESP模型,在传输模式下,只有IP数据被加密,而没有加密IP报头和选项,传输模式具有良好性能,因为编码通常具有较高的CPU开销。在隧道模式下,整个原始数据都被加密,成为一个新IP包,这时,路由器代表主机完成加密过程。源路由器加密数据包并沿着隧道转发,目的路由器解密数据包并转发到相应的目标系统。面对隧道模式,入侵者只能确定隧道的终端结点,而不是数据包的实际源和目的地址[11-12]。2种模式下受IPSec保护的IP包如图1所示。

原始IP包	IP头	TCP头	数据		
传输模式	IP头	IPSec头	TCP头	数据	
隧道模式	IP头	IPSec头	IP头	TCP头	数据

图1 2种模式下受IPSec保护的IP包

Fig.1 IP packages protected by IPSec under two modes

1.3 IPSec的优点

IPSec的主要特征在于它可以对所有IP级的通信进行加密和认证,正是这一点才使IPSec可以确保包括远程登录、客户/服务器、电子邮件、文件传输及Web访问在内多种应用程序的安全。

IPSec在传输层下,对应用程序是透明的。当在路由器或防火墙上安装IPSec时,无需更改用户或服务器系统中软件设置。即使在终端系统中执行IPSec,应用程序一类的上层软件也不会被影响;IPSec对终端用户也是透明的,因此不必对用户进行安全机制培训;如果需要,IPSec可为个体用户提供安全保障,这样做就可保护企业内部的敏感信息[13]。

2 IPSec在河南电力调度数据网的应用

2004年8月,河南电力调度数据专网开始建设,到目前为止,工程进入收尾阶段,该期工程所建设的网络共计103个站点,其中包括1个省调、18个地调及84个变电站。河南省电力系统调度数据专网拓扑结构分为3层,即核心层、汇聚层、接入层。

a. 核心层节点:河南省调、平顶山地调、洛阳地调和获嘉500 kV变电站。其中,省调节点采用双机配置,其他节点为单机配置。

b. 汇聚层节点:除核心节点外的其他16个地调节点。

c. 接入层节点:除获嘉变的其他83个变电站。

本工程建成投运后,将承载电量计费系统、电力市场技术支持系统、保护故障信息管理系统、调度自动化EMS系统、功角测量系统等业务,使河南电力调度数据更安全、可靠、实时地传送,以确保河南电网安全、可靠、稳定运行。

河南电力调度数据网络是电力生产实时信息传输的网络,网络传输的主要信息是电力调度实时数据、生产管理数据、通信监测数据等,是电力指挥安全生产和调度自动化的重要基础,在协调电力系统发、送、变、配、用电等组成部分的联合运转及保证电网安全、经济、稳定、可靠的运行方面发挥关键的作用。

电网调度技术不断发展,电力调度数据网承载的业务也不断发展。监控和数据采集/能量管理系统(SCADA)仍是电力调度最基础、最关键的业务;传统上使用专用通道传输的电网事故信息和继电保护信息,开始向数据网络转移。此外,调度生产管理系统、水调自动化系统、电力市场技术支持系统都需要电力数据网承载。业务系统的不断发展对调度数据网络提出更高要求,多个关键系统在同一数据网络承载,保证不同业务系统间的有效隔离、保证业务系统安全,是调度数据网建设的重要要求。

电力调度数据网强调系统安全防护,不同业务系统间必须实现有效隔离,控制生产类实时业务与非控制生产业务隔离,关键业务系统间按照需要进行隔离。电力调度数据网必须实行有效的安全分区,进行有效的安全防护和管理。根据电力调度数据网中系统和数据的重要性、安全性的需要,通过构造不同的VPN将电力调度数据网进行划分,如图2所示。

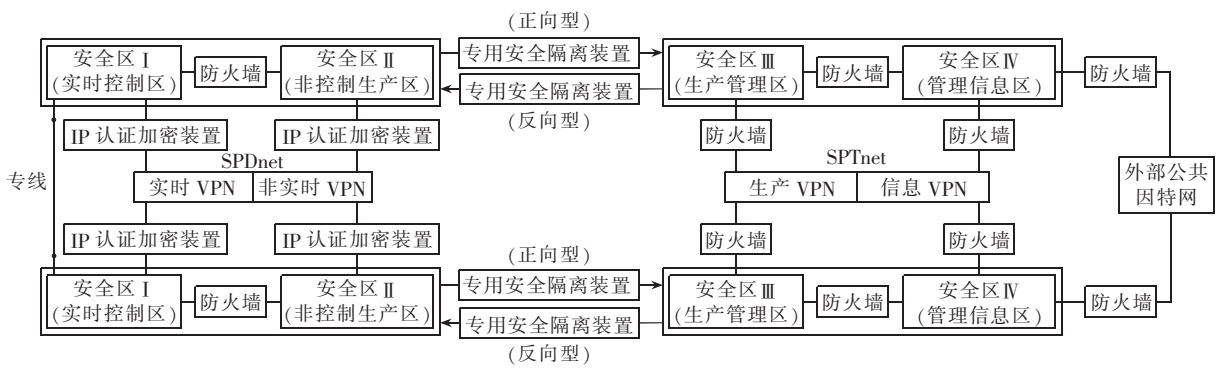

图2 电力调度数据网中VPN的划分

Fig.2 VPN partitions of power data network

安全区Ⅰ、Ⅱ连接的广域网为电力调度数据网SPDnet(State Power Data network)。其中,采用 IPSec VPN 技术构造的 SPDnet 为安全区Ⅰ、Ⅱ分别提供 2个逻辑隔离的 VPN1 和 VPN2,VPN 子网可提供 2 个逻辑隔离子网。安全区Ⅲ连接的广域网为电力数据通信网 SPTnet(State Power Telecommunication network)。

由于调度自动化系统有大量的控制信息,直接影响着电力系统的安全,其安全性是电网公司极其关注和重视的。在实际组网过程中采用了 IPSec 的隧道模式确保调度信息的安全传输,隧道模式的优点是 2 个隧道端点之间的数据是安全的,而不管最终的目的地如何。针对隧道模式配置的 IPSec 时,网络之间所有的通信是安全的,而不要求在各个计算机上配置 IPSec[14]。

3　结语

随着网络安全问题的日益突出,VPN 技术将不断发展和广泛应用。IPSec 作为目前一种能为任何 Internet 通信提供安全保护的协议,它将有很好的应用前途。特别对于电力行业,信息安全尤为重要,在目前的技术水平下,保障电力信息,特别是电力生产信息的安全,IPSec 是电力调度数据网的最优选择。

参考文献:

[1] 江红,余青松,顾君忠. VPN 安全技术的研究与分析[J]. 计算机工程,2002,28(4):130-132.
JIANG Hong,YU Qing-song,GU Jun-zhong. Research and analysis on security techniques in VPN[J]. Computer Engineering,2002,28(4):130-132.

[2] BROWN S. 构建 VPN 网络[M]. 董晓宇,译. 北京:人民邮电出版社,2001.

[3] WILSON W. 虚拟专用网的创建与实现[M]. 钟鸣,译. 北京:机械工业出版社,2000.

[4] HUITEMA C. IPv6—the new Internet protocol[M]. 2 版. 北京:清华大学出版社,1999.

[5] 何宝宏. IP 虚拟专用网技术[M]. 北京:人民邮电出版社,2002.

[6] 申锟铠. 虚拟专用网 VPN 研究与实现[D]. 长沙:湖南师范大学,2002.
SHEN Kun-kai. Research and implemention on the VPN[D]. Changsha:Hunan Normal University,2002.

[7] PEPELNJAK I,GUICHARD J. MPLS 和 VPN 体系结构[M]. 卢泽新,朱培栋,齐宁,译. 北京:人民邮电出版社,2001.

[8] 王达. 虚拟专用网(VPN)精解[M]. 北京:清华大学出版社,2004.

[9] DORASWAMY N,HARKINS D. IPSec——新一代因特网安全标准[M]. 京京工作室,译. 北京:机械工业出版社,2000.

[10] STALLINGS W. 密码编码学与网络安全:原理与实践[M]. 2 版. 刘玉珍,王丽娜,傅建明,等,译. 北京:电子工业出版社,2001.

[11] SCHNEIER B. 应用密码学——协议、算法与 C 源程序[M]. 吴世忠,祝世雄,张文政,等. 译. 北京:机械工业出版社,2000.

[12] 洪帆,陈卓. IPSec 安全机制的体系结构与应用研究[J]. 小型微型计算机系统,2002,23(8):946-949.
HONG Fan,CHEN Zhuo. Research of architecture and application for the Internet protocol security[J]. Mini-Micro Systems,2002,23(8):946-949.

[13] 秦磊华,余胜生. IPSec 密钥交换(IKE)协议的分析与改进[J]. 计算机工程,2002,28(3):130-132.
QIN Lei-hua,YU Sheng-sheng. Analysis of the Internet key exchange protocol[J]. Computer Engineering,2002,28(3):130-132.

[14] DAVIS C R. IPSec:securing VPNs[M]. 北京:清华大学出版社,2002.

(**责任编辑**: 康鲁豫)

作者简介:

罗汉武(1975-),男,湖北黄石人,工程师,博士研究生,主要从事电力二次系统规划建设和管理工作(**E-mail**:highwoo@sohu.com);

李　昉(1976-),女,河南郑州人,博士研究生,主要从事电力信息系统的建设管理工作;

张　栋(1975-),男,河南郑州人,工程师,主要从事电力二次系统的运行维护工作。

Construction of secure power data network and its application in Henan power data network

LUO Han-wu[1,2],LI Fang[1,2],ZHANG Dong[3]

(1. School of Management,Tianjin University,Tianjin 300072,China;
2. Electric Power of Henan,Zhengzhou 450052,China;
3. Electric Power of Zhengzhou,Zhengzhou 450052,China)

Abstract: Along with network security becoming more and more serious, VPN (Virtual Private Networks) technology will be adopted more widely and IPSec(Internet Protocol Security) will become more popular,which could provide secure protection for any Internet communication. The system structure,working mode and key technology of IPSec are analyzed. With the encryption techniques of AH(Authentication Header) and ESP(Encapsulation Security Payload) applied in IPSec,a solution of secure power data network is proposed and a model for constructing power data secure VPN using IPSec is given,which ensures secure data transfer in network and amasks the IP address of real communication host. Its application in Henan power data network is introduced in detail.

Key words: IPSec; network security; data network