变电站的计算机网络安全分析

陈文刚,张婷婷
(山西晋城供电公司,山西 晋城 048000)

摘 要:随着电力系统数据网络建设步伐的加快,变电站计算机网络安全问题日益突出。详细分析了变电站面临的网络安全威胁和网络安全需求,并结合变电站计算机网络的结构特点,提出了相应的系统安全策略和信息安全策略,重点介绍了应用于变电站的几种网络安全技术。

关键词:变电站;计算机网络安全;防火墙;移动代理;VPN

Abstract: Along with the fast construction progress of data network in power system, the problems of computer network security in the substation are becoming more and more prominent. The network security threats and demands faced by the substation are analyzed in detail. The corresponding system safety strategy and the information security strategy are proposed according to the structure characteristics of its computer network. Several kinds of network security technologies used in the substation are mainly introduced.

Key words: substation; computer network security; firewall; motion agent; VPN

中图分类号:TM645 **文献标识码**:B **文章编号**:1003-6954(2008)03-0075-04

作为电力自动化系统的数据和各种控制行为执行者的变电站自动化系统,一旦因网络的安全原因引起误动、拒动、整定参数的错误更改、上传数据紊乱等,将给电力系统的安全稳定运行带来严重威胁,甚至引发灾难性事故。将重点讨论在网络环境下变电站的安全需求、安全威胁及相应对策。

1 变电站计算机网络结构

变电站局域网基本是以太网设计,因电压等级及其在电力系统运行控制中的地位不同,网络主机从2~20台不等,通过路由器或交换机与远动网络或SPDnet连接。变电站网络结构有以下两种基本形式。

1.1 基于通信控制器的分层分布式网络

此为现代变电站计算机网络设计中比较流行的一种结构。所有的IED设备通过现场总线或其他总线网连接在一起,由通信控制器对它们统一进行访问和控制,通信控制器可以提供TCP/IP接口和站内以太网连接。该结构的缺点是由于协议和实时性的限制,TIED设备所能提供的很多维护和运行信息都不能被充分利用,只能选一些比较重要的信息通过远动协议送向远方调度。

1.2 基于嵌入式Internet技术(EMIT)的对等网络

利用EMIT,在多个IED设备组网时放弃使用代码较长的TCP/IP协议,而采用RS-232、RS-485、CAN、红外、射频等轻量级总线网络协议,然后通过嵌入式网关(可采用桌面计算机或者高性能的嵌入式处理器)与Internet连接,每一个IED设备的应用程序中都有一个独立的通信任务emMicro,仅占约1KB空间,与嵌入式网关一起提供基于Internet的远程数据采集、远程控制、自动报警、上传/下载数据文件等功能。在这种结构下,IED设备与其他网络主机都是变电站局域网中的对等实体,这是一种理想的变电站组网方式,无须自己设计通信协议以及配套的软硬件,也不必使用专用信道,只要连上Internet,就可非常方便地实现变电站IED设备的远程通信。目前国际上很多IED的生产厂家已经开始提供具有网络接口的IED设备,不久这种网络结构可以在变电站中得以实现。

2 变电站计算机网络安全需求

变电站的计算机网络安全需求包括网络系统安全和网络信息安全两方面。其中,网络系统安全表现为:系统对外来破坏具有健壮性,对操作人员不规范操作具有预防性,以及系统自身信息具有封闭性;网络信息安全表现为:数据的完整性、合法性、访问安全

性、可控性及不可否认性。

3 变电站计算机网络安全威胁

变电站网络安全威胁主要来自变电站所连接的外部网络。不管变电站内部的组网方式如何，通过网络化的远动通道对变电站构成的安全威胁始终存在。这些威胁主要包括：

3.1 截获

非法获取变电站与其他系统之间传输的信息，非法获取变电站网络中存储的信息。信息截获尽管不会影响信息的传输，但往往是变电站网络系统遭受安全侵害的第一步。特别是在电力市场运营环境下，避免信息截获十分重要。

3.2 中断

使变电站内部或与其他系统之间的通信中断，使调度主站无法了解变电站的运行工况，主站的控制命令也无法正确执行。对无人值班变电站危害较大。

3.3 篡改

更改变电站与其它系统之间传输的信息，使调度主站得到错误的运行工况，威胁电网的安全运行。如果篡改的是遥控命令、修改定值命令等，更有可能造成严重的后果。

3.4 伪造

伪造“合法”信息发往变电站或主站，可能造成与篡改信息类似的后果。

3.5 恶意程序

包括计算机里蠕虫、特洛伊木马、逻辑炸弹等计算机病毒，将严重影响变电站自动化系统运行的正确性、实时性和可靠性，并且可能使运行程序瘫痪。

3.6 权限管理不当

包括权限的级别设置不当、权限处理上的不合理等。这些看似“细小”的因素，可能使完备的网络安全机制形同虚设，整个系统将从内部遭受严重破坏。

3.7 Internet 的安全漏洞

Internet 在发展之初就以数据高度共享和网络互联为目的，缺乏必要的安全防范，所以导致很多安全漏洞，其中最为突出的三大问题是网络安全质量失控、不具备实时服务的性能以及系统管控“弱智”。

应该注意到，当变电站网络安全受到威胁时，往往存在着上述多种情况的组合。网络的安全问题必须从多方面进行综合考虑，不能强调某一方面而忽视另一方面。

4 变电站计算机网络安全策略

不少电力工作者都有这样一种观点，认为只要不把 SPDnet 同 Internet 连接，保持独立，就可以保证系统的网络安全。实际上，由于 SPDnet 基本采用 Internet 技术构建，和 Internet 有着同样的安全漏洞，而黑客出现的时间和地点都具有不确定性，因此，不管是否与 Internet 连接，网络安全的威胁同样存在。从严格意义上讲，不存在绝对安全的网络，系统的安全和开放本身就是互相矛盾的，因为网络的安全问题而放弃系统的开放性是不明智的，只能采取一系列的网络安全防护措施，增强内部工作人员的安全意识，尽最大努力保证网络的安全运行。

安全性的保证和变电站的网络结构是密不可分的，不同的网络结构设计，可以考虑采用不同的安全对策。

原则上，其他应用网络所采用的安全策略都适用于变电站计算机网络。但是由于变电站计算机网络要考虑信息传输的实时性，因而必须对其安全策略进行具体分析。

4.1 系统安全策略

4.1.1 健壮的网络操作系统

操作系统是计算机和网络的工作平台，应选用软件工具齐全、丰富、缩放性强的操作系统。如果有很多版本可供选择，应选用用户群最少的版本，这样可减少入侵者用各种方法攻击计算机的可能性。另外，还要有较完善的访问控制和系统设计等安全功能。

在最近的黑客行动中，美国被攻陷的网站几乎有 90% 是 Windows NT 和 Windows 2000 操作系统。而且，有报道称，微软也承认 Windows 2000 远种服务中存在七大漏洞。因此，变电站的网络系统管理员应及时测试系统的安全漏洞；为使用的软件安装最新版本的安全补丁程序，包括操作系统和日常应用程序；为系统设备进入许可密码以及定期更换默认密码。

4.1.2 容错技术

容错技术包括软件容错和硬件容错两方面。软

件容错是指软件系统对操作人员误操作具有一定的预防性;硬件容错是指系统具有组件冗余、无单点硬件失效、动态重组、错误校正等功能。在重要的变电站,也可以采取双机备份同步校验方式,或者采用双网冗余备份或信息分流的组网方式,建立一套可靠、高效的运行机制,当一个系统由于意外而崩溃时,计算机自动切换,以确保整个网络系统正常运转,保证各项数据信息的完整性和一致性。

4.2 信息安全策略

4.2.1 加密技术

加密技术是最基本、最常用而又最有效的信息安全技术,可以有效地限制截获、中断、篡改。伪造的概率,从而达到保证信息安全的目的。针对变电站计算机网络,选用一些最常用的加密算法(international data enctyption algorithm,缩写为IDEA),例如国际数据加密算法就可满足要求,密钥长度在56～128位比较合适。

由于加密算法比较简单,明文X通过加密算法E和加密密钥K即可得到密文$Y=E_k(X)$。有时E或K可能是公开的,因此,安全性的保证主要依赖于密钥管理。加密和解密的过程耗时很小,可以认为基本不影响变电站信息(音、视频信息除外)传输的实时性。

4.2.2 防火墙技术

防火墙为不同网络或网络安全域之间构建了一道安全屏障,它通过有选择地拒绝非法端口,允许合法的TCP/IP数据流通过,以保证内部网络的数据和资源不会流向非法地点。

目前防火墙技术已经比较成熟,通常使用包过滤、应用级网关、电路级网关和规则检查防火墙等安全控制手段实现其安全防护功能。防火墙的工作一般都非常有效,可以说,好的防火墙系统,配以恰当的维护,将非常有助于预防有问题的Internet访问。但值得注意的是,防火墙不能有效控制来自网络内部的非法访问,而且防火墙的设置将导致信息传输的明显延时。考虑到电力远动信息的实时性要求,建议开发变电站网络专用的防火墙组件,以降低通用防火墙软件的延时带来的不利影响。

4.2.3 移动代理(mobile agent)技术

一旦外部的非法入侵者突破防火墙,进一步的网络安全防护工作变更要由本地入侵监测系统负责。此时需要一个智能系统对非法入侵实时检测并迅速采取相应的对策,移动代理技术则为其实现提供了一条便捷途径。

移动代理技术是目前安全领域的研究热点,尤其适用于分布式系统,一般利用Java的安全机制实现。变电站自动化正在朝着分布式应用发展,因此,可将该技术应用于变电站局域网的安全管理中。

图1是一种基于移动代理技术的自适应网络安全模型,其特点是每一个被监视的设备都对应一个移动代理,这些移动代理作为系统的安全警察存在,当检测到被监视设备遭到攻击时,就立刻向代理管理机请求并执行相应对策,如果该移动代理不能解决问题,代理管理机可以中止其运行并创建一个新类型的移动代理负责完成安全对策的执行。这种安全机制的主要优点是:1)非法入侵者突破防火墙时,在线学习系统可以总结入侵者的特点并制定相应的对策,防止其他的设备遭到攻击;2)工作效率高,大部分的移动代理可以在当地解决安全问题,与传统的安全代理可以在当地解决安全问题,与传统的安全代理相比,有效减少了网络负载;3)安全管理更加便利,管理者可以在一个复杂的网络系统中统一调度安全策略。

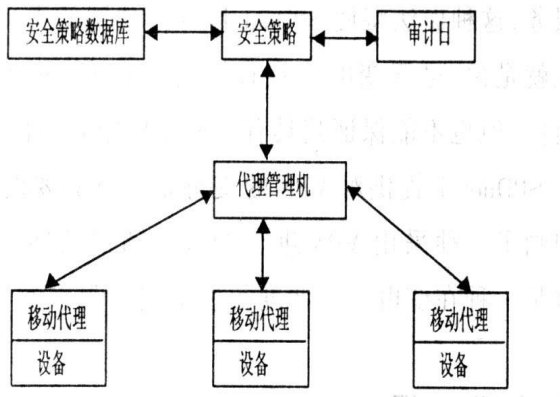

图1 多代理网络安全模型

在一些重要的枢纽变电站中,可以考虑加装基于移动代理技术的网络安全管理系统,对透过防火墙的攻击进行实时检测并采用相应对策,进一步提高网络的安全性能。

4.2.4 虚拟专用(VPN)技术

VPN技术是近几年比较热门的网络技术之一,它为网络的安全提供了一个比较好的解决方案,是一种以费用低廉的公用网络为基础的传输媒体,通过

L2TP、IPSec 等协议及密码技术的处理，向用户提供虚拟的专用网络服务技术。其采用的关键技术包括安全隧道技术、信息加密技术、用户认证技术和访问控制技术。

VPN 有三种典型的应用方式：1) Intranet VPN，用于企业内部各局域网的安全互联；2)个人远程接入 VPN，用于经过授权的移动个人接入企业的局域网；3)Extranet VPN，用于若干个企业的 Intranet VPN 安全互联。VPN 技术也不一定都用于大网络通信，它还可用于公司企业网内部以允许雇员访问某些特定的数据，而限制访问其他数据。

VPN 的突出优点首先体现在它虽然建立于公共网络上，但同使用专用线路连接一样，享有很高的安全性、优先性、可靠性和可管理性，而其建设周期、投入资金和维护费用却大大降低；VPN 的另外一个重要优点是能够在不同平台之间传输数据，而无需对专门的平台的协议操心；同时，除了提供网络这间数据的安全传输，VPN 也可以提供主机到主机的安全隧道。在电力系统中，VPN 技术有着广泛的应用空间。RTU 上网以后，远动数据虽然基本是在 SPDnet 上传输，但是，未来的发展趋势是，在满足电力系统各种运行业务需要的前提下，SPDnet 有可能向社会提供电信增值服务，这种做法将使 SPDnet 具有公共网的很多性质。也就是说，尽管变电站是直接连接在 SPDnet 上相互通信，但也不能保证其具有专网通信的安全性，所以，在 SPDnet 上提供对 VPN 的支持是十分必要的。图 2 勾画了一种采用 VPN 进行的远动通信的网络结构，这是一种在变电站与调度的远动连接上采用 VPN 技术的应用方式，其实现可以简单描述为在调度局域网和变电站局域网的边界都安装一个安全网关服务器，分别提供数据加密、解密的功能，使得数据能够在公共网上安全传输。另外，VPN 技术对远程办公也提供了方便，随着远程办公的流行，预计将来可以在一定程度上让员工在家中实现对电力系统的远程监控和维护。

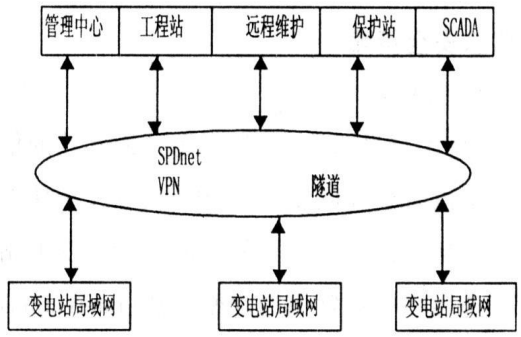

图 2　采用 VPN 技术的远动通信网络

5　结束语

以前在规划、设计变电站计算机网络时，着重考虑的大多是如何实现变电站自动化系统的功能及其运行的可靠性，而网络的安全问题没有得到足够的重视。如今随着国家电力数据专用网建设的深入，特别是远动系统网络化进程的加快，变电站计算机网络安全问题的重要性日益突出。

作者简介

陈文刚(1971—)，男，工程师，山西晋城供电分公司调度所。

(**收稿日期**：2008－02－10)

▲▲简　讯

电力职工在余震中抢修电路

5 月 12 日 14 点 28 分，四川省阿坝州汶川县发生 8 级地震，地震波及广安市邻水县，人们感觉地面一阵晃动，河面、电力线路、房屋发生一定程度的摆动，紧接着手机信号中断，余震不时传来，险情不断。

3 点 26 分，广安邻水供电局职工在巡查线路中发现："坛同镇白洋坝 1 号配变倾斜，中相跌落保险脱开。"险情就是命令，局所领导立即组织抢修人员，带好吊绳、线材，10 分钟后赶到现场，发现配变一定程度的倾斜，使 A 相桩头引线受力，导致 A 相跌落保险受牵引脱开。于是迅速通知停电、验电、挂接地线……采取必要的安全措施后，电力职工们对配变及附属装置进行校正，恢复送电后，又用令克棒听配变运行声音，见无异常后才离开现场。

(**万大成　邱雪松**)