· 科普园地 ·

电力系统信息安全及博弈防御系统

王 燕
(南京供电公司,江苏 南京 210019)

摘 要:随着智能电网的发展,电力系统中出现了越来越多的电子设备和通信系统,因而信息安全成为国内外电力系统面临的巨大挑战。介绍了电力系统信息安全的现状,总结了各国对于信息安全的要求,对国内外在信息安全方面的研究现状进行了梳理。在此基础上,提出了电力系统主动应对信息攻击的智能决策系统的框架和实现方法。该智能决策可以帮助运行人员与黑客博弈,决定电力系统的最优应对策略。

关键词:信息安全;斯塔尔博格竞争;随机博弈
中图分类号:TM76 **文献标志码**:B **文章编号**:1009-0665(2014)05-0082-03

由于大量的电子设备和通信系统,现代电力系统存在着诸多信息安全漏洞。恶意的个人和组织、恐怖分子和敌对势力很可能利用这些安全漏洞,发动攻击,破坏电网的正常运行。各国政府对此非常重视,出台了相应的政策法规,期望提高电力系统信息安全。黑客攻击的威胁是始终存在的,因此只有开发出可以发现黑客攻击、并采取相应的防御反击措施的系统,才可以确保电网的可靠供电和经济运行。

1 电力系统信息安全现状

电力信息系统的安全现状不容乐观。电力行业大量使用现代信息技术(IT)以实现自动化。IT技术带来了很多便利,但是也带来了诸多安全隐患。数据采集与监视控制(SCADA)系统和企业管理网络的对接就是一个很好的例子。这样的对接提高了企业运行效率,也将SCADA系统暴露在黑客攻击的威胁下。

电力信息系统中常见的安全隐患有:(1) 网络之间缺乏安全隔离。SCADA系统、配电管理系统(EMS)、企业管理网络等不同安全等级的网络不恰当地连接在一起,造成非授权访问、非法操作、病毒和恶意软件的传播。(2) 网络内部没有完善的安全防御体系。很多网络只是购买了防病毒软件和防火墙。针对信息安全威胁的预防、监控和审计机制严重缺失。(3) 远程通信渠道和通信协议缺乏安全机制。通信渠道中没有入侵检测装置;通信协议没有采用加密技术。(4) 重要设备的密码认证保护不够强。很多时候,人们使用简单的密码,甚至继续使用设备的出厂密码。(5) 电力行业人员的信息安全意识薄弱。很多人不会定期地给操作系统打安全补丁、点击电子邮件中的链接、使用外来的U盘。

电力系统正在成为黑客攻击的主要目标。电力系统是关系到国计民生的关键基础设施。黑客攻击电力信息系统,会影响电力系统的安全、稳定、经济运行,危及电网的可靠供电和人民群众的日常生活,将会引发难以估量的经济损失和大规模的社会恐慌。2007年,全球最大的黑客大会"Defcon"就提出SCADA系统将成为黑客攻击的主要目标。目前已经有电力系统遭到攻击的实例。2000年10月13日,四川二滩水电厂控制系统收到异常信号停机,7 s甩出力890 MW,川渝电网几乎瓦解。2003年1月,Slammer蠕虫扰乱美国俄亥俄州的一家核电厂运行。2003年12月30日,龙泉、政平、鹅城换流站控制系统感染病毒[1]。

2 安全需求

黑客对电力系统的威胁已经引起了各方的高度重视。美国能源部(DOE)在2006年公布,并于2011年更新了关于能源控制系统网络安全的路线图。DOE计划在10年内,升级所有重要的能源控制系统,使之能承受至少一次精心策划的黑客攻击。为此,DOE设立了SCADA系统安全仿真平台(NSTB),模拟针对SCADA系统的黑客攻击,研究相应的防御策略。美国计算机应急准备小组(US-CERT)致力于提高人们对网络安全的认识。北美电力可靠性委员会(NERC)颁布了关键设施保护(CIP)标准,要求各电力企业为重要的网络设施提供相应的防护措施。国际电工通信技术委员会(IEC TC 57)提出要在IEC 62351标准通信协议中采用更先进的加密和认证技术。

在我国,电力系统的信息安全被提升到国家战略安全高度。2002年5月,国家经贸委发布30号令《电网和电厂计算机监控系统及调度数据网络安全防护的规定》。2004年12月,电监会发布第5号令《电力二次系统安全防护规定》。电力行业致力于构建电力系统信息安全保障体系,全面提高防护能力,重点保障电力二次系统、重要电力网络、重要电力信息系统和重要电力生产经营管理信息系统的安全。

收稿日期:2014-04-09;修回日期:2014-06-10