

电力系统信息通信网络设备安全研究

高 鹏, 范 杰, 李尼格

(中国电力科学研究院, 江苏 南京 211106)

摘 要: 随着电力企业信息化建设的高速发展, 针对网络设备安全问题的研究已经成为了一个不可忽视的问题。文章首先介绍了电力系统国内外信息通信网络设备的使用情况; 接着分析了国外网络设备在电力系统中的安全风险, 表明了电力系统网络设备实施国产化的迫切需求; 然后分析了电力系统内部网络存在的安全风险; 最后提出了网络设备全生命周期安全管控的具体措施, 为电力系统网络安全防护提供参考。

关键词: 电力企业; 网络设备; 离线攻击; 国产化; 安全性

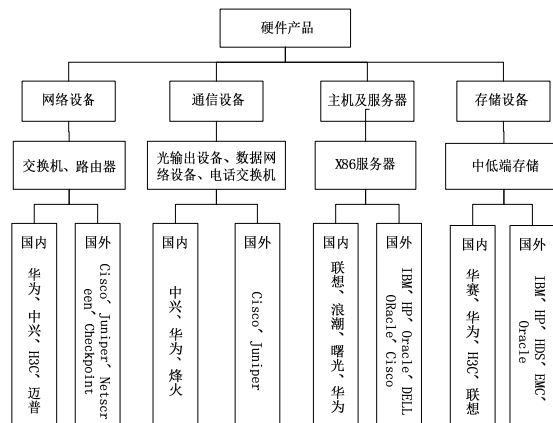
0 引言

上世纪五十年代, 部分发达国家开始研究计算机技术在企业经营、管理、设计、制造等方面的应用, 信息化技术逐步从单机、信息孤岛发展到企业信息化集成。从上世纪八十年代, 我国开始将信息技术应用于各个领域, 由于起步较晚, 在信息化建设过程中普遍借鉴和引入了国外信息通信网络设备^[1]资源。

2014 年 2 月, 中央成立了“网络安全和信息化领导小组”, 突出体现了信息网络安全在国家安全中的重要地位。网络安全和信息化是一项艰巨的工作, 因为它涉及到所有的网络设备, 设备的安全又是整体网络安全的一个重要方面^[2-3]。同时, 随着电力信息化技术的飞速发展, 各单位信息化建设逐步深入, 电力作为关系人民生产、生活的基础产业, 电力信息化建设是电力企业安全生产及生产力水平的重要体现。然而, 由于在信息化建设中引入的国外信息通信网络设备厂商和产品的不可控性, 不断曝出国外厂商信息化资源的安全隐患, 关乎企业、国家的信息安全保障问题也日益突出。近年来, 国家开始扶持国内厂商探索信息通信网络设备资源的国产化^[4-5], 部分网络设备已可替代国外产品。但是由于电力公司信息通信系统仍存在一定数量的国外网络设备在使用, 并且国外网络设备产品的一些核心技术和标准长期被国外厂商掌控, 所以对于电力系统信息通信网络设备安全的研究与分析迫在眉睫。

1 电力系统国内外信息通信网络设备使用情况

电力系统信息通信网络使用的硬件设备主要涉及网络设备、通信设备、主机及服务器和存储设备, 详见图 1。引入的国外硬件设备主要涉及小型机、高端服务器、高端存储设备以及部分网络设备等产品, 小型机以及高端存储设备短期国内厂家还无法与国外厂家相比, 而其他设备如服务器、低端存储设备、网络设备, 目前国内产品功能和性能已能达到电力行业相关要求。尤其是网络设备, 随着国内相关网络设备产品功能和性能的日益完善, 在电力系统信息通信网络中已经具备取代国外网络设备的能力。电力系统目前使用的国外信息通信网络设备包括 Cisco、IBM、HP、Juniper 等厂商, 主要以 Cisco 网络设备为主。使用的国内信息通信网络设备包括 H3C、华为、迈普、中兴、烽火等厂商, 主要以 H3C、华为网络设备为主。



2013 年 1 月, 新华通讯社《参考要闻》发布了题为《路透社称美实验室以国家安全为由移除中国产设备》的报道, 称美国洛斯·阿拉莫斯国家核武器实验室近日以国家安全考虑为由, 移除了其信息系

统中至少两种由中国华三通信技术公司生产的网络设备^[6]。由此可见国外实验室对信息系统网络设备安全的重视,结合相关事件对我们的启示,国家电网公司组织信息安全实验室对电力系统信息通信网络设备的应用情况和存在风险进行了梳理分析。尤以国外网络设备Cisco为例,截至 2012 年底,来自国家计算机网络应急技术处理协调中心(CNCERT/CC)漏洞库公开的Cisco系列网络设备漏洞就有 165 个,主要涉及的漏洞类型包括拒绝服务漏洞、身份验证绕过漏洞以及远程控制漏洞,如被利用可导致网络通讯中断、网络设备瘫痪甚至远程执行恶意程序等后果。同时,国外网络设备可能存在未被发现的安全漏洞或者事先植入的恶意代码,所以加快实施电力系统网络设备国产化非常必要。

2 电力系统信息通信网络设备安全风险

2.1 电力系统信息通信网络设备安全风险概述

即使自“十一五”以来,电力公司完成了内外网隔离,全面构建了以“三道防线”为核心的等级保护纵深防御体系,“三道防线”有效保障了核心业务系统及数据安全,同时基本杜绝了外部人员直接访问部署于信息内网以及生产控制大区网络设备的可能性^[4, 7]。但是,电力系统安全实验室通过对国内外网络设备安全风险进一步分析发现,如果设备存在安全漏洞或被事先植入后门、木马等恶意程序,即使在物理隔离情况下,依然可以通过如下方式进行攻击。一是采用电磁辐射或无线电信号激活漏洞。攻击者利用工程手段在硬件设备中事先加入可唤醒的程序和指令,并放宽硬件设备的信号辐射标准,使其随时可以被探测以便利用,然后通过对设备发送的电磁信号进行侦收和破译,利用无线辐射病毒激活后门。二是通过移动存储介质或移动终端进行攻击。攻击者将病毒存入移动存储介质或移动终端,当移动存储介质或移动终端与内网通信时,病毒利用网络设备漏洞注入内网。三是存在漏洞的网络设备也可能被内部恶意攻击者利用并实施相应的攻击。

2.2 电力系统内部网络信息通信网络设备安全风险分析

电力系统内生产控制大区和管理信息大区中的信息内网构成了两个与互联网隔开的“离线”内部网络,其涉及的无线电信号(无线电磁波)主要有三

大类,分别为:

- (1) 2.4GHz 电磁波: WLAN;
- (2) 1900MHz-2GHz 电磁波: 2G (GSM、GPRS、CDMA)、3G (WCDMA、TD-SCDMA、CDMA2000);
- (3) 230MHz、3-30GHz 电磁波: 电力微波。

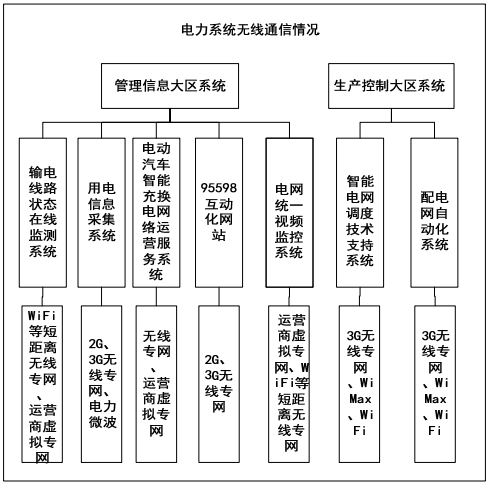


图 2 电力系统无线通信情况

由此分析可知,“离线攻击”可能会对电力系统内部网络设备造成威胁,主要存在以下几个方面的风险:

- (1) 在信息内网中存在大量的国外网络设备、移动存储介质和移动终端,存在被植入后门的风险,攻击者通过激活后门注入病毒或控制设备发起攻击;
- (2) 在信息内网中存在大量的“电磁辐射”,存在遭受“辐射攻击”的风险,攻击者通过接收各类设备的辐射激活后门或注入病毒发起攻击;
- (3) 在信息内网中存在用于内部通信的无线网络,即“无线通信”,攻击者通过无线通信的方式直接对设备和系统发起攻击。

3 电力系统信息通信网络设备的安全防护

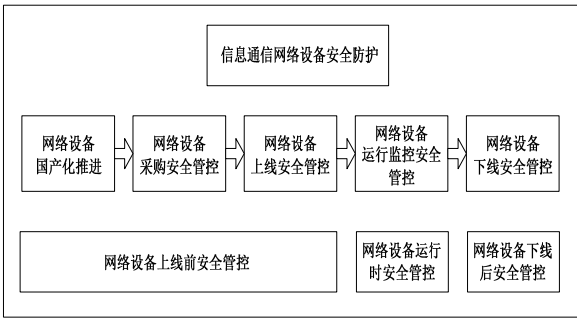


图 3 信息通信网络设备安全防护框架

根据电力系统信息通信网络设备使用现状,借

鉴国内外以及电力系统供应链安全管理思想,结合电力信息系统全生命周期过程,本文重点从国产化推进、采购安全管控、上线安全管控、运行监控安全管控、下线安全管控等方面考虑对电力系统信息通信网络设备进行安全防护^[8-9],如图3所示。

3.1 网络设备国产化推进

网络设备国产化推进目的在于规避国外网络设备安全风险的不可控性,确保电力系统网络设备可控、能控、在控。电力企业可以联合国内厂商共同开展各种国产网络设备资源的国产化改造及测试工作,按照“先易后难、先外网后内网”的原则,在保证电力系统正常运行前提下,进一步推进国产化进程。

3.2 网络设备采购安全管控

网络设备采购安全管控主要规范网络设备在资质审核、设备选型、安全准入等方面的要求,确保采购的网络设备符合安全性要求。在采购产品前先建立健全信息化网络设备资源的安全准入机制;在设备选型环节对网络设备供应商企业安全资质、人员安全指标、服务质量评价、网络设备资格准入条件进行审查,对关键设备开展产品预先选型和全面安全检测,及时发现各种潜在的安全后门、策略配置及恶意代码风险;在招标采购环节明确网络设备的投标安全技术要求,并在采购合同中明确对厂商保密条款和安全责任的约束。

3.3 网络设备上线安全管控

网络设备上线安全管控主要确保网络设备上线运行前满足国家或公司对于信息安全的要求。上线前由内部安全专业队伍对网络设备进行安全性测评,保证网络设备硬件安全,避免存在安全漏洞或被事先植入后门、木马等恶意程序;上线时由内部队伍实施,确保网络设备在部署、配置、运行环节的安全性,以及在身份鉴别、访问控制、日志审计方面的完整性。

3.4 网络设备运行监控安全管控

网络设备运行监控安全管控主要通过加强信息系统安全监测、加强信息安全督查,保证网络设备安全运行。1) 电力公司应与国家信息安全测评中心、总参三部等国家安全技术团队合作,进行网络设备漏洞挖掘和风险预警工作,总结、完善电力公司安全漏洞库并开展漏洞库深化应用工作,常态开展各种漏洞检测及漏洞跟踪修复工作。2) 电力公司应建立电力公司网络设备安全风险防范预警机制,

优化完善公司内外网监测系统,对各类网络设备补丁漏洞修复状态、异常访问状态、特殊端口使用状态、网络服务状态及设备性能状态实时监控,并针对各类风险及时处置。3) 应综合电力系统信息通信网络设备整体情况,在全网开展网络设备安全专项督查工作,对专项督查工作中发现的安全隐患进行全面整改,对相应安全风险的防范进行顶层设计,纳入到电力公司常态的安全督查工作。

3.5 网络设备下线安全管控

网络设备下线安全管控主要确保网络设备下线或报废时不会对系统产生风险,同时不会出现信息泄露。网络设备下线工作必须由内部队伍进行,按照标准流程规定做好下线前评估以及过程记录,重点做好剩余信息的删除以及设备的销毁工作。

4 结论

随着国家进一步加强网络安全和信息化管理以及电力行业信息化工作的不断推进,网络设备作为电力网络构建的基础单元,其信息安全是电力系统安全的重要组成部分。本文通过对国外网络设备安全风险的分析,以及对电力系统网络安全风险的研究,表明了加快电力系统网络设备国产化,加强网络设备全过程安全管控的必要性;同时,本文结合电力系统实际情况,提出了关于电力系统网络设备的安全防护措施。即使如此,随着电力系统信息化对安全性要求的不断提高,仍需要进一步加强国内外网络设备安全以及防护措施研究。

参考文献:

- [1] 刘晓辉.网络设备[M].北京:机械工业出版社,2007.
- [2] 罗凯.网络设备安全分析与解决措施[J].电力信息化,2012(02):81-83.
- [3] 杨富国.网络设备安全与防火墙[M].北京:清华大学出版社,2005.
- [4] 国家电网公司.国家电网公司电网等级保护纵深防御示范工程实施方案[R].北京:国家电网公司,2009.
- [5] 国家电网公司.国家电网公司等级国产化改造示范工程推荐技术方案[R].北京:国家电网公司,2009.
- [6] 凤凰网.美核实验室停用H3C设备称存在安全隐患.
http://tech.ifeng.com/telecom/special/zhonghua/content-3/detail_2013_01/08/20948974_0.shtml,2013.
- [7] 国家电网公司.电力二次系统安全防护重点工作要求[R].北京:国家电网公司,2008.

[8] 左晓栋.美国政府 IT 供应链安全政策和措施分析[J].信息网络安全,2010(5):10-12.

[9] 蒋诚智,刘婷婷.电力信息系统供应链安全管理研究[A].2012 年电力通信管理暨智能电网通信技术论坛[C].2013:287-290.

作者简介:

高 鹏（1987—），男，江苏人，工程师，主要研究方向为电力系统信息安全，E-mail：gaopeng2@epri.sgcc.com.cn;

范 杰（1989—），男，江苏人，工程师，主要研究方向为电力系统数据库安全；

李尼格（1985—），女，江苏人，工程师，主要研究方向为电力系统信息安全。