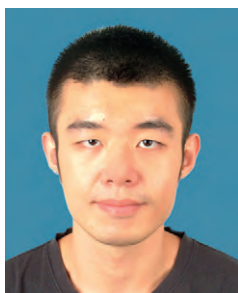


智能电网领域的云计算安全防护

在日益严峻的国内网络安全形势下，建设以特高压电网为骨干网架，各级电网协调发展，具有信息化、自动化、互动化特征的统一坚强智能电网，应该在实践上以云计算为核心战略，数据中心以虚拟化技术进行整合，安全防护作为保护屏障。智能电网发展水平和效用，直接影响电网的运营能力，如何在多层、多级的智能电网需求架构中，找寻到保护智能电网的有效管理工具，可以说云计算安全防护的应用与发展将成为智能电网领域的风向标。

王未 郝颖/国网北京市电力公司信通分公司



王未/助理工程师

0 引言

智能电网云计算在具备超大规模、高可用性、高扩展性、按需服务等优势特点的同时，也存在着一定的危险性。智能电网云计算服务除了提供计算服务外，还必然提供了存储服务。但是智能电网云计算服务当前垄断在私人机构（企业）手中，而他们仅仅能够提供商业信用。对于政府机构、商业机构（特别象电网这样持有敏感数据的商业机构）对于选择云计算服务应保持足够的警惕。一旦商业用户大规模使用私人机构提供的云计算服务，无论其技术优势有多强，都不可避免地让这些私人机构以“数据（信息）”的重要性挟制整个社会。对于信息社会而言，“信息”是至关重要的。另一方面，云计算中的数据对于数据所有者以外的其他用户云计算用户是保密的，但是对于提供云计算的商业机构而言确实毫无秘密可言。所有这些潜在的 danger，是商业机构和政府

机构选择云计算服务、特别是国外机构提供的云计算服务时，不得不考虑的一个重要的前提。

1 智能电网云计算面临的问题

智能电网云计算安全事件频发，严重影响了用户使用智能电网云服务的信心，在2013年关于智能电网云计算的用户调查结果表明，将近80%的用户对智能电网云服务的安全性表示担忧。

1.1 智能电网云计算信任危机

2011年3月，约15万Google Gmail用户的邮件和聊天记录被删除，部分用户账户被重置。2011年8月，Microsoft和Amazon在欧洲的云计算网络大规模宕机，多家网站长时间关闭，数小时后才恢复正常。

在云计算时代，信息系统由云计算服务商建设并对用户提供服务，云计算平台是建立在现有信息系统和基础设施之上的，信息系统面临着同样的安全问题，信息安全威胁由指向用户转移到指向云计算服务提供商，虽然一定程度上可以减少安全事故的发生，将信息安全威胁目标变得更为集中，但同时大规模集中化的云计算平台可为破坏者提供更多的资源和能力支持，导致更大的安全威胁。尤其是电网领域的云计算安全应用应该更为谨慎。信息系统中存储大量电网资料和用户信息，这些数据对于整个社会而言至关重要，没有完善的安全防护体系作为保障隐患重大。若发生如Google Gmail用户丢失信息或Microsoft和Amazon在欧洲的云计算网络大规模宕机事件，那可能导致中国大陆内购电用户的巨大的信息危机和不良的社会舆论。

关键词/Keywords

智能电网·
云计算·
网络安全应用·

1.2 面临更多的安全攻击威胁

由于智能电网云系统中存放着海量的重要用户数据，对攻击者来说具有更大的诱惑力。如果攻击者通过某种方式成功攻击云系统，将会给云提供商和用户带来毁灭性的灾难；另一方面，为了保证云服务的灵活性和通用性，智能电网云系统为用户提供开放的访问接口，但同时也带来了更大的安全威胁。

1.3 高可用性问题

需要保证用户数据的高可用性以及智能电网云平台服务和用户业务的连续性：云计算环境需要为用户数据提供容错备份手段，另外，软件本身可能存在的漏洞以及大量的恶意攻击，大大增加了服务中断的可能性。如何保障服务软件以及用户应用软件的高可用性已成为云安全的挑战之一。

1.4 缺乏安全标准规则

如今的智能电网云计算缺乏安全标准：IT业务交互关系不断迁移到智能电网云计算环境中，而针对云计算架构的安全模型和标准却未形成体系，大部分风险以及出现问题后的责任承担不清。由于这些安全隐患未得到妥善的解决，加上关于互联网的法律法规少之又少，引发的信任危机是空前的。

到三个维度：安全目标、安全威胁和安全生命周期。安全目标指需进行安全防护的资产（软硬件设备、信息）、行为（登陆登出操作、数据传输）和流程（管理控制流程），不同的服务模式所涉及的安防需求各不相同。安全威胁指可以对网络对象产生影响、破坏的事件，例如地震、洪水、偷盗、滥用、数据泄露、拒绝服务攻击、病毒等。除了传统意义上的风险，智能电网云计算网络中还存在着诸如数据隔离风险、应用程序接口加固风险、合法合规风险等新出现的安全威胁。安全生命周期则是指云计算生成数据需要经历的6个阶段：生成、迁移、使用、共享、存储、销毁。在不同的阶段中及时更新安全解决方案，以此来满足不断变化的安全目标和安全威胁。

如下图所示按照网络层面对智能电网云计算构成体系划分，可分为用户接入层、汇聚层及资源层3个层面，处在最下层的接入层与用户直接接触，依靠用户身份管理及访问控制等手段进行安全防护，确保资源使用的针对性和私密性。汇聚层通过部署防火墙、边界检测防护设备实现网络边界防护，在资源层与汇聚层之间形成有效保护屏障。资源层方面通过实施应用、平台、基础设施的安防措施，以形成对数据及虚拟化的有效保障。

通过进一步对总体架构层面进行细化，可分解为基础设施层面、网络层面、平台层面、数据层面、软件层面。

2 智能电网云计算安全架构

2.1 智能电网云计算架构安全概述

智能电网云计算系统的安全架构设计涉及

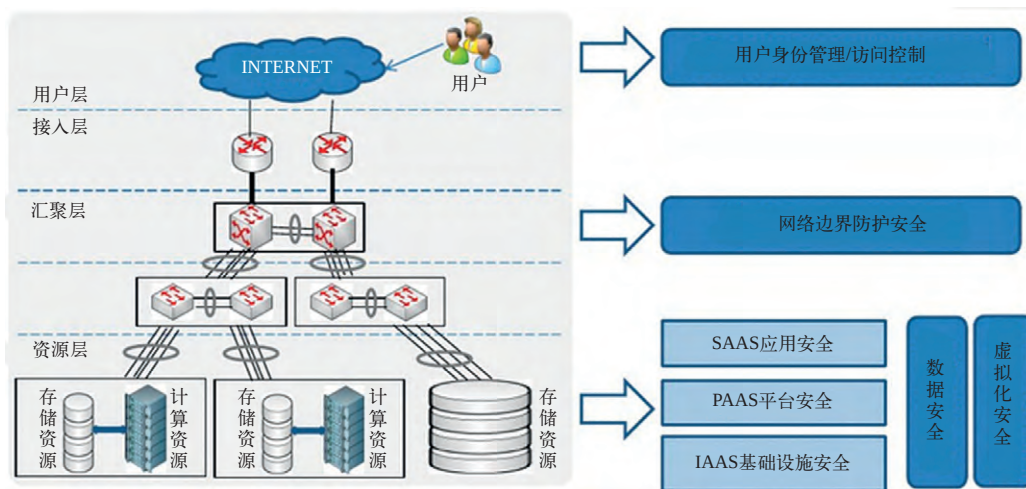


图 智能电网云计算构成体系

2.1.1 基础设施层面

基础设施层面为承载智能电网云计算功能的计算存储设备提供最基本安全防护,包括机房温度、湿度、防洪、抗震、人员访问控制、防盗、监控等措施。这些防护措施的目的旨在保护计算机所在环境的基本安全,为计算机提供平稳运行条件,防止因为外界环境突变或人为因素而产生的干扰,消除外界因素对计算机运行带来的负面影响。

从物理层面上来看,智能电网云计算系统是由很多网络计算和存储单元有机组合而成的,针对每个单元都需要配置基于主机层面的安全功能,包括防火墙、入侵检测系统、入侵防护系统、软硬件日志管理系统、审计系统等来完成主机保护及审计功能。

2.1.2 网络层面

网络在智能电网云计算中为处在不同位置的单元提供稳定、安全、保密的联通功能。这些单元往往位于不同的网络域中,节点之间的互联互通往往会跨越非安全的公共网络,数据在传输过程中面临着窃听、篡改、损毁等各种风险。数据传输安全需要从发包端、收包端、包传输三个方面进行防护。在收发包终端通过安全输入输出、内存屏蔽、存储密封等基于终端的安全措施来保护数据收发过程中的安全。节点之间的数据传输通过加密隧道技术、数字摘要、数字证书、数字时间标签等措施保证传输数据的机密性,完整性和抗抵赖性。

智能电网云计算节点之间的通信对大数据量传输非常谨慎,对异常流量非常敏感,如Ddos泛洪攻击,蠕虫等。通过流量监控手段可以监测节点间的流量特征,实时发现异常流量并加以管理和控制。对于流量“异常”的鉴别需要以某区域或链路大部分时间的流量统计数据为基准,当某一时刻在这块区域或链路上的流量特征与基准值有很大出入时,则定义为异常情况。流量监控技术普遍存在于网络层到应用层,通过基于数据包和数据流的流量分析、控制工具实现。

2.1.3 平台层面

智能电网云计算平台运行在互联网和大量虚拟机上,将网络上的多台计算机、服务器、存储组

合成一个网络计算机。以云计算平台的角度来看,云计算系统最基本的单元式虚拟机,文件存入云系统时会分割成若干份存储在不同的虚拟机上,在各虚拟机上的每份文件碎片都是并行处理操作的。文件分割、存储、计算管理的全流程由云计算平台执行。承载着不同重要信息的文件可能被存储在同一虚拟机上,需要通过数据隔离和数据保护措施来确保数据安全。由虚拟防火墙实现针对单个虚拟机设置的安全策略和访问控制策略,且虚拟机可分割成为若干组,根据所承载数据的安全需求,配置不同的安全级别,实现安全保护分级。

由于云计算平台本质上为一种操作系统,所以需要完善的补丁和设置管理系统,以应对不断出现的安全威胁和漏洞。

2.1.4 数据层面

数据层面的保护旨在防止重要数据受到来自内部和外部的非授权访问及传输。通过智能电网云计算平台的用户授权、访问管理和数据加密保护来防止外部用户的窃取行为。而防范内部人员窃取数据,则需要通过深度内容检测和行为检测。深度内容检测可以确定数据的重要性并自动转移到安全级别较高的磁盘空间上;行为检测可以监控人员对数据的操作并进行允许、拒绝、警告等响应。

数据的灾难恢复方面是保障数据安全的重要环节,通过对系统关键状态、日志、用户数据进行周期性备份,确保系统在遭受自然或人为灾害后,可重新启用数据、软硬件设备,恢复正常运行。同一云计算系统中,可根据不同业务特点和恢复需求制定差异化的灾备计划。

2.1.5 软件层面

云计算软件借助应用程序接口部署在智能电网平台上,而有些云计算应用极易被滥用和恶意使用,其强大的计算和网络能力可能被用作DDos泛洪攻击、垃圾邮件发送、暴力破解密码等黑客行为。通过深度包检测技术,可准确分析数据包包头,并进行模式识别、行为分析、统计分析来剖析数据包承载信息,提供了针对网络第三层到第七层流量的全方位分析,使云计算系统准确了解应用的使用者及使用方法。

由于智能电网的云计算软件服务通常使用基

于Web的瘦客户端为用户提供鉴权、登陆和应用，且Web浏览器本身存在脆弱性，部署在Web上的应用程序很容易被植入恶意代码，所以需要通过Web应用程序防火墙防范类似跨站脚本攻击、SQL注入等恶意攻击行为。

3 结束语

智能电网云计算系统的安全防护是一个长期且不断完善的过程，云计算系统面临的威胁来自很多层面，由基础设施层面到网络传输层面再到数据应用层面，每一层都有各自的潜在风险，需要运用不同安全技术手段来保证系统的安全运行。安全策略需根据资产的变更及安全需求的变化来进行周期性的检查更新。按照资产的重要性，确定相对应的防护等级，实行有针对性的差异化防范管控措施。

参考文献

[1] 陈全, 邓倩妮. 云计算及其关键技术[J]. 计算机应用, 2009(9).

- [2] 张健. 云计算概念和影响力解析[J]. 电信网技术, 2009(1).
- [3] 卢军. 云计算离企业应用有多远[J]. 信息系统工程, 2008 (9).
- [4] 陈涛. 云计算理论及技术研究[J]. 重庆交通大学学报: 社会科学版, 2009 (4).
- [5] 周孝信, 方杰, 武强, 等. 大型互联电网运行可靠性基础研究 (I) [M]. 北京: 清华大学出版社, 2008.
- [6] 孙宏斌, 张伯明, 吴文传, 等. 面向中国智能输电网的智能控制中心[J]. 电力科学与技术, 2009(2).

(收稿日期: 2015-03-30) EA

作者简介

王未 (1989-), 男, 本科, 助理工程师, 主要研究方向为信息网络安全。

郝颖 (1985-), 女, 本科, 助理工程师, 主要研究方向为信息网络安全。

(上接第542页)

通道, 并实现三遥功能, 不仅光伏电站侧投资较大, 电网侧的耗费也是十分巨大, 而用公网通信在保密性和可靠性上又不够。

按国网《分布式光伏发电并网工作意见调度实施细则(征求意见稿)》中要求, 分布式光伏发电项目应实时采集有功功率、无功功率、发电量和各并网点的开关状态、电压、电流, 并上传至调度机构。对暂不具备条件的项目, 可通过电能计量装置和电力用户用电信息采集系统上传部分运行信息。需远程遥控的项目, 应能接收、执行调度端远方解并列、启停机和调整发电功率的指令。

6) 在光伏电站入网前, 根据地区供电特性、负荷分布、负荷密度, 综合考虑电网规划情况, 并考虑年度负荷曲线、年度气候特征等因素, 作为光伏电站接入点的参考。在电网规划时, 也应考虑光伏发电对电网的影响。此外, 传统的配电网计算分析和规划设计方法已经不适用于包含大量分布式光伏发电的配电网, 因此, 必须针对新型的电源结构和供电方式, 研究适合分布式光伏

系统接入的配网分析理论和规划设计方案。

4 结束语

化石能源的不可再生性以及太阳能发电的普适性, 导致光伏发电大量接入电网已经是不可逆转的趋势。如何在光伏电站大量接入电网的同时, 消除其可能带来的负荷平衡、安全稳定、调峰调压、继电保护等问题, 保证电网对客户高可靠性供电, 是一个十分复杂的话题。应当从规划、设计、运行、调度控制、智能电网建设等多各方面综合考虑, 应对光伏电站大量接入所带来的挑战。

(收稿日期: 2015-03-30) EA

作者简介

周照智 (1980-), 男, 本科, 工程师, 主要研究方向为电力通信网的规划建设、运维检修、专业管理和集约化。