



电力信息系统云安全风险分析与评估技术

沈亮, 王栋, 玄佳兴

(国家电网公司信息通信分公司, 北京 100761)

摘要: 结合电力行业对云计算技术的应用, 针对电力云安全分析与评估方法展开了系统研究, 对电力信息系统云环境下的功能实体和业务流程进行全面梳理, 通过静态 STRIDE 威胁建模与动态攻击链算法相结合的方式对云平台面临的主要风险进行了分类识别和量化评估, 并有针对性地提出了适用于电力云系统的安全防护架构, 以促进云计算在电力行业的推广和应用, 并为电力信息系统安全可控提供有力的支撑。

关键词: 电力云; 风险分析; 威胁建模; 攻击链

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018047

Security risk analysis and evaluation techniques in power information system cloud

SHEN Liang, WANG Dong, XUAN Jiaying

State Grid Information and Telecommunication Branch, Beijing 100761, China

Abstract: Combining the power industry with cloud computing technology, a systematic study on safety analysis and evaluation methods of the power cloud was carried out. A comprehensive combing on functional entities and business processes of the power information system under the cloud environment was conducted. Through the combination of static STRIDE threat modeling and dynamic attack chain algorithm, the main risks of cloud platform were classified and quantified. A security protection architecture of power cloud system was put forward to promote the popularization and application of cloud computing in the power industry, and to provide a strong support for the safety and control of power information system.

Key words: power cloud, risk analysis, threat modeling, attack chain

1 引言

电力行业信息化正全面朝着云计算的方向发展, 已应用云计算技术建设了“公共服务云”和“企业管理云”, 在提升电网安全、运营效益、客户服务、新业务拓展等方面起到了全面的支撑

作用, 电力云已成为电力关键信息基础设施的重要组成部分^[1,2]。电力云实时性要求更精准、网络结构更复杂、数据保障等级更严格, 对电力信息系统云安全防护提出了更高要求。国内外关于电力云安全尚未取得系统化的研究成果, 目前亟需针对电力云面临的安全风险进行全面分析评估,



提出实用化风险评估方法,建立相应的安全防护架构,为电力云关键信息基础设施的安全运行保驾护航^[3-6]。

2 电力云平台体系结构

2.1 电力云平台总体架构

根据电力行业“双网双机、分区分域”的安全防护策略,将电力信息网络划分为信息外网和信息内网,信息外网业务由“公共服务云”承载,面向社会大众提供电力“互联网+”服务,信息内网业务由“企业管理云”承载,面向公司内部提供生产办公、经营决策服务,“公共服务云”和“企业管理云”通过电力专用隔离装置进行数据交互^[7-9]。电力云总体架构情况如图1所示。

2.2 电力云平台结构组成

电力云主要由云基础设施、云平台组件和云服务中心3部分组成,通过云服务中心,实现云

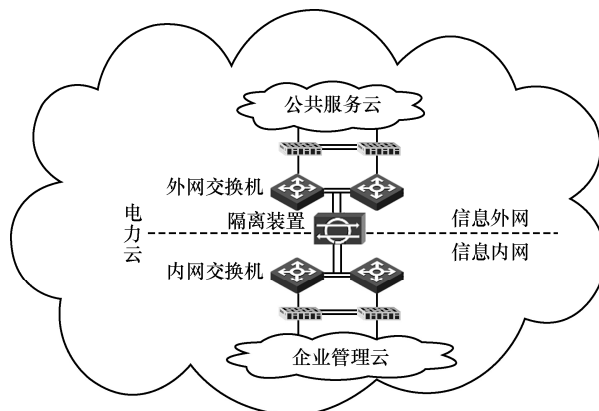


图1 电力云总体架构

基础设施和云平台组件的一体化服务。以公共服务云为例,云平台承载了互动网站、掌上电力、电力交易等业务应用,云平台各组件与服务能力如图2所示。

3 电力云安全风险评估

无论是构建新系统还是升级现有系统,都需

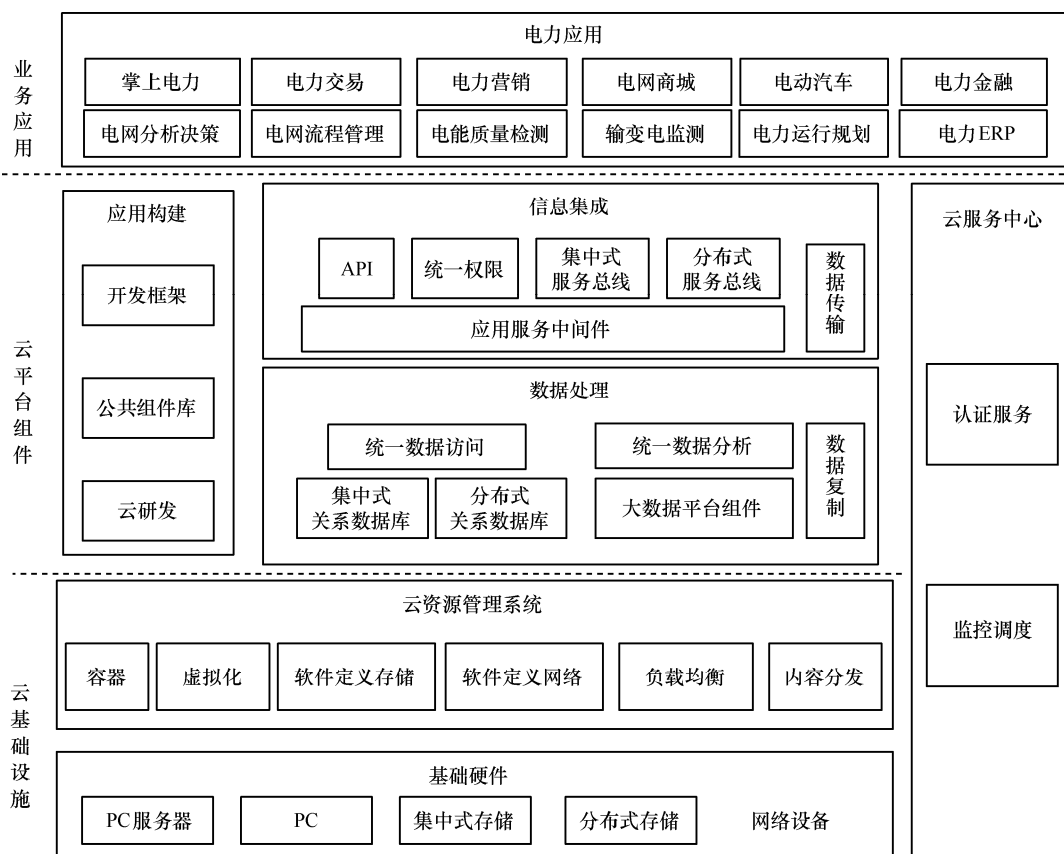


图2 电力云平台组件与服务能力视图

要考虑入侵者攻击系统的可能方式，然后在系统的设计和实施阶段构建适当的防御手段。在一个对安全性要求较高的项目中，对潜在的威胁进行建模分析是不可或缺的^[10,11]，综合应用“静态+动态”的威胁建模分析方法，可检查并分析云平台设计中存在的问题，对平台可能面临的威胁进行归纳总结，帮助研发人员改进，从而全面增强系统的安全性。

3.1 电力云平台核心组件风险

微软公司提出的 STRIDE 模型，即假冒（spoofing, S）、篡改（tampering, T）、否认（repudiation, R）、信息泄露（information disclosure, I）、拒绝服务（denial of service, D）、权限提升（elevation of privilege, E），是一种针对信息系统安全风险评估而设计的建模方法，近年被广泛应用于系统风险分析。通过采用静态 STRIDE 建模方法对电力云平台核心组件结构展开威胁建模，通过将系统分解成为若干组件，分别对各个组件易受威胁攻击的程度进行分析，进而对电力云面临的脆弱性展开分析评估。

电力云平台的核心组件包括认证、计算、存储、镜像、网络等，其中每个核心组件通过消息队列进行通信，如图 3 所示。

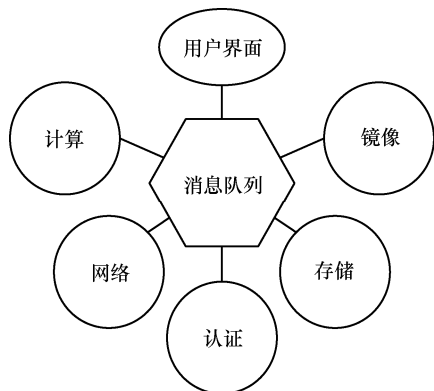


图3 电力云平台核心组件

虚拟机实例的创建是电力云平台最经典和最具有代表性的操作，这里以实例创建流程为例进行 STRIDE 风险评估。图 4 展示了电力云虚拟机创建

流程的具体步骤。首先，需对用户身份进行验证、鉴权，通过验证后，用户与计算节点和数据库建立通信；接着，计算节点通过发送请求创建虚拟资源消息，并加入消息队列，在通过鉴权后进行相应服务查找、检查合法性及镜像请求；然后，查找相应镜像的位置信息，在存储节点处查找镜像文件，同样，对存储容器的访问要经过鉴权；最后，在获取镜像文件后，计算节点分配用户所请求的虚拟资源，对镜像进行加载，最终完成创建^[12]。在此过程中，数据从云端外经云端内相关组件流入，系统同样受到诸多潜在的安全威胁。

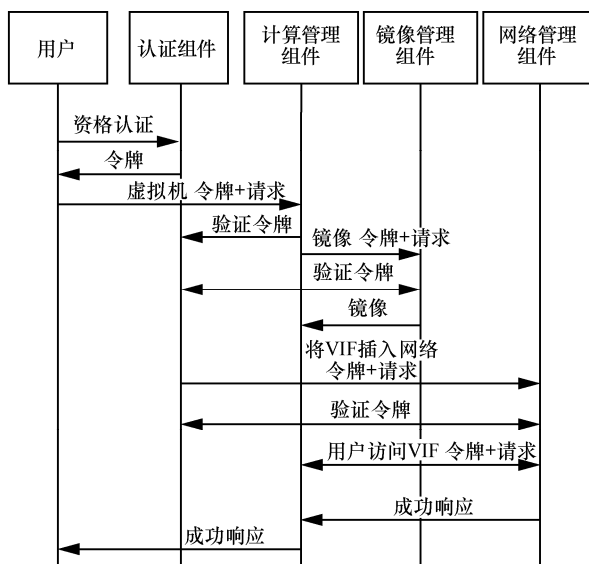


图4 电力云创建实例流程

认证过程是客户端到云端的入口，涉及跨越云端边界，是攻击者入侵的主要途径，同样也是最容易受到安全威胁的环节。主要存在的威胁包括客户端接口的安全性问题、由于账户泄露而导致非法登录、身份欺骗、业务高峰时段导致的网络拥堵、受 DDoS 导致的网络瘫痪、越权访问与操作、入侵服务器 Web 应用、木马上传等。存储服务主要涉及数据安全风险，如虚拟环境中文件传输存在被监听的风险、漏洞导致的恶意用户非法访问、越权操作等。镜像安全同数据安全类似，主要涉及越权获取、非法篡改等。此外，虚拟机



在动态变化扩容缩容过程中，错误的配置或操作也将带来安全漏洞，同时导致资源竞争和滥用。

采用 STRIDE 模型对电力云平台核心组件进行完整的安全威胁分析，将涉及用户端、认证组件、计算管理组件、存储管理组件、镜像管理组件、网络管理组件、物理机和数据库的所有潜在风险进行了归纳^[13]。风险评估结果见表 1。

通过 STRIDE 威胁模型的分析结果可以看到，电力云平台各组件、各实体均面临严峻的安全威胁，任何一部分的防护弱点都可能导致严重的安

全后果，必须采取全方位立体的安全保障措施。

3.2 电力云平台业务应用风险

实际生产环境中，云平台业务应用的运行伴随着资源的调用、节点间相互访问及数据库读写等操作，导致产生威胁的因素也是呈动态变化的。如图 5 所示，系统承载业务时，黑客通过运行了 HTTP、FTP 等服务的外网服务器节点进行攻击，侵入虚拟机或容器层，进而非法访问物理服务器。同时，虽然内网节点与互联网节点进行了逻辑隔离，但由于信息网内网中含有重要信息，仍然

表 1 电力云核心组件安全威胁

涉及实体	涉及流程	威胁类型	威胁方式
用户端认证组件	认证	S	账户泄露非法登录
用户端认证组件	认证	S	身份欺骗
用户端认证组件	认证	D	DDoS 拒绝服务
用户端认证组件	认证	E	越权访问
用户计算管理组件	云资源相关操作	E	越权访问
用户存储管理组件	存储相关操作	E	越权访问
用户镜像管理组件	镜像相关操作	E	越权访问
用户网络管理组件	网络相关操作	E	越权访问
物理机	无	S	账户泄露非法登录
物理机	无	T	非法修改数据
物理机	无	I	关键信息泄露
物理机	无	E	越权访问
数据库	无	S	账户泄露非法登录
数据库	无	T	非法修改数据
数据库	无	I	关键信息泄露
数据库	无	E	越权访问
所有实体	无	R	双方否认进行过的交互动作

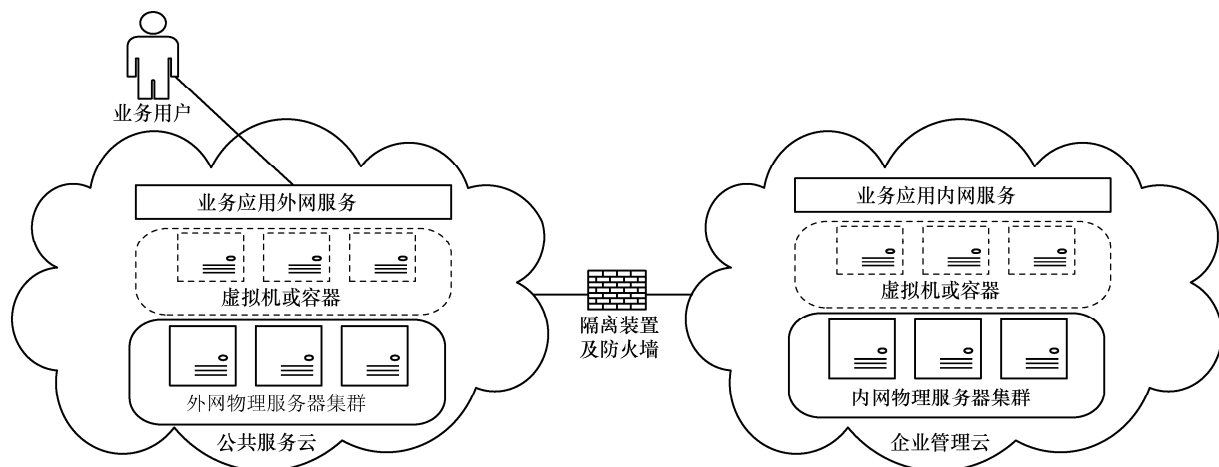


图 5 电力云平台业务应用架构

存在网络攻击窃取内网数据的风险,对于云平台的安全性提出了更高的要求^[14-16]。

网络攻击主要分为5个阶段:探测扫描阶段、渗透攻击阶段、攻陷入侵阶段、安装工具阶段和恶意行为阶段,网络安全攻击的本质呈现出一种链式的流程结构^[17],本文结合信息网络的系统拓扑结构、资产重要性、网络攻击路径和漏洞危害程度,综合推算节点面临的安全风险。攻击链模型通过对网络攻击链式结构上各节点遭受的动态威胁赋以不同的权值,对网络安全风险进行定量计算,进而可为网络安全防护工作提供直观的可视化视图。本文基于攻击链动态风险识别分析方法,可以有效提高电力云风险评估的效率和覆盖面。

图6展示了电力云特定网络攻击的主要方式。从横向看,系统面临从业务层到虚拟机和容器层的威胁。从纵向看,系统面临从业务层到物理机层再到基础硬件层的威胁^[18,19]。随着攻击的不断渗透,根据业务应用、系统及设备的不同,攻击

成功概率亦有不同。

为了实现动态风险评估,首先采用人工渗透测试的方式获取各节点的入侵成功概率。然后通过基于某种威胁成功入侵概率计算间接损失。为简化攻击链模型复杂度,根据网络安全风险暴露面的实际位置和网络攻击途径,本文约定网络安全攻击方向为由外到内的单向路径,黑客从风险暴露面所在S点,到达应用程序A,然后通过A入侵操作系统B,通过B非法访问宿主操作系统入侵文件系统C获取或篡改数据,也可以非法获取管理权限E,最后可以很容易地就入侵容器F。如图6和表2所示,根据电力云安全专家渗透评估得出,攻击路径S→A、A→B、B→E及E→F的特定威胁成功入侵概率分别为0.2、0.5、0.8和1。威胁成功入侵概率的取值范围为0~1,0和1分别表示无法入侵和轻易成功入侵。通过攻击链分析结果,可以判断出云平台的核心风险点以及风险传播路径,进而可为云平台的安全防护提供有效建议。

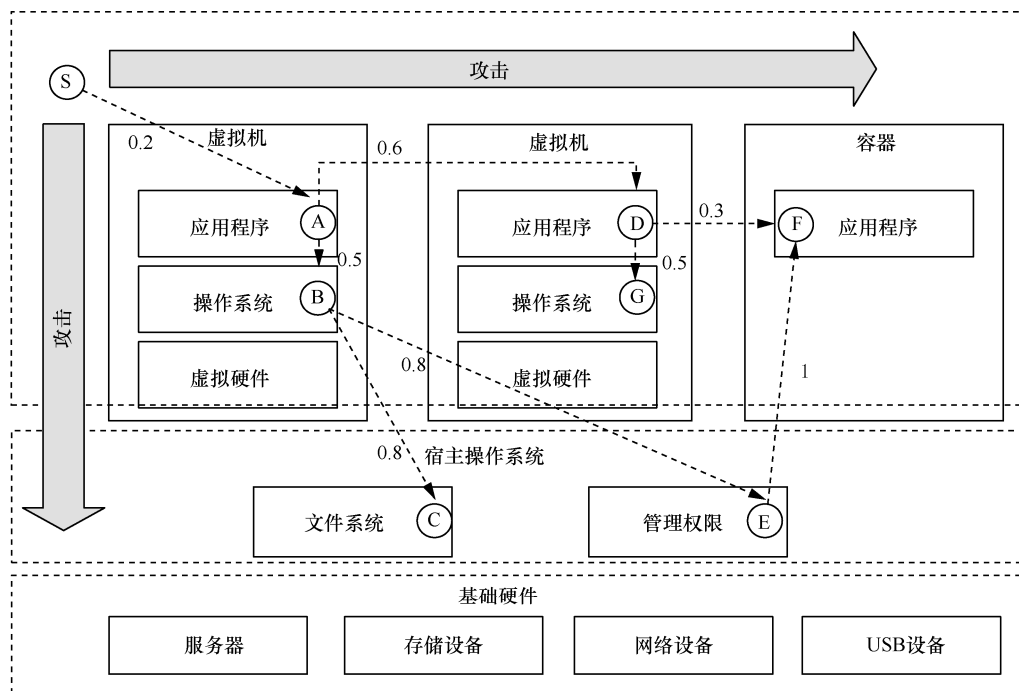


图6 电力云攻击链流程



表 2 电力云攻击链事例

攻击路径	威胁方式	攻击路径	威胁方式
S→A	账户泄露非法登录	B→E	越权访问
A→B、D→G	身份欺骗	E→F	越权访问
B→C	关键信息泄露	A→D	虚拟机渗透

3.3 电力云安全风险评估结果

第 3.1 节和第 3.2 节分别对云平台进行了静态和动态的安全风险评估,下面统一对云平台进行安全风险评估,以提高电力云安全风险的防范效率。根据攻击链信息和每个节点攻击至对应目标节点的某种威胁成功入侵的预期概率和每个节点对应的目标节点的直接损失系数,确定每个节点的间接损失系数。第 x 节点的总损失系数可以通过式 (1) 计算:

$$V_x = D_x + I_x = D_x + \sum_{i \in \text{AllSubNode}} P_i \cdot N_i \quad (1)$$

其中, V_x 为该节点总损失, D_x 是直接损失, I_x 是间接损失, P_i 为 x 节点攻陷 i 节点的概率, N_i 为 i 节点威胁发生的严重程度。直接损失描述为威胁成功入侵概率与入侵节点资产重要等级的乘积。资产重要等级的取值范围为 0~1, 0 和 1 分别代表等级低和非常重要。以图 6 中的 B 节点为例, B、C 和 E 节点资产重要等级分别为 0.8、1 和 1, B 节点的总损失系数为 $0.5 \times 0.8 + 0.8 \times 1 + 0.8 \times 1 = 2$ 。表 3 列出了图 6 各节点的风险量化评估结果。

表 3 电力云平台风险量化评估结果

节点	资产价值	直接损失 (D_x)	间接损失 (I_x)	总损失 (V_x)
A	0.6	0.12	0.82	0.94
B	0.8	0.4	1.6	2
C	1	0.8	-	0.8
D	0.7	0.42	0.63	1.05
E	1	0.8	0.6	1.4
F	0.6	0.78	-	0.78
G	0.9	0.45	-	0.45

通过对某电力云平台仿真验证系统的安全渗透数据分析,数据泄露和虚拟机渗透等威胁方式具有较高的风险,需在云平台关键节点上采取技

术手段加强防护措施。

4 电力云系统安全防护架构设计

电力行业具有较好的信息安全基础,在电力云建设的同时也同步开展了安全防护体系的设计。基于电力云安全面临的主要威胁,综合构建态势感知、加固防御和数据保护相结合的云安全立体架构,通过多层次的安全防线联动和协同,形成真正体系化的云安全防护能力,电力云安全防护架构如图 7 所示。

4.1 安全态势感知监控系统

实现对全局信息安全态势的实时感知和监控,是信息安全防护能力达到高级水平的重要标志。结合电力云平台技术架构特点,首先要确保对电力云全部资产信息监控的全覆盖,在网络出口和云平台内部部署网络流量采集探针,解决虚拟机内部流量不可见的监控盲区,通过人工备案和自动探测相结合的方式,对业务应用、容器、虚拟机、操作系统、镜像模板、文件数据、物理设备等资产及其业务数据流进行全面监控,开展合规审计和完整性检测,并通过大数据技术,对应用层日志和虚拟化层日志进行全面采集和深度分析,对安全事件进行统一分类和命名,划分为网络攻击等若干事件类别,制定详细的 PDRR (防护、检测、响应、恢复) 安全应急流程,通过可视化技术,以地理图、仪表图、泡泡图、雷达图等方式实现对电力云安全态势的实时展现。

4.2 平台加固防御技术措施

与传统信息系统架构相比,电力云平台需要更加复杂的加固防御技术措施,应用层应加强 Web 防火墙、入侵防御的安全策略执行程度,仅开放必要的业务端口,严格隔离高权限的运维端口,主动防御外部攻击,及时发现异常行为;云平台层安全加固的主要思路是,在防止通过物理机入侵虚拟机的同时,要防止虚拟机横向地攻击其他虚拟机^[20],也要防止纵向地入侵操作系统,

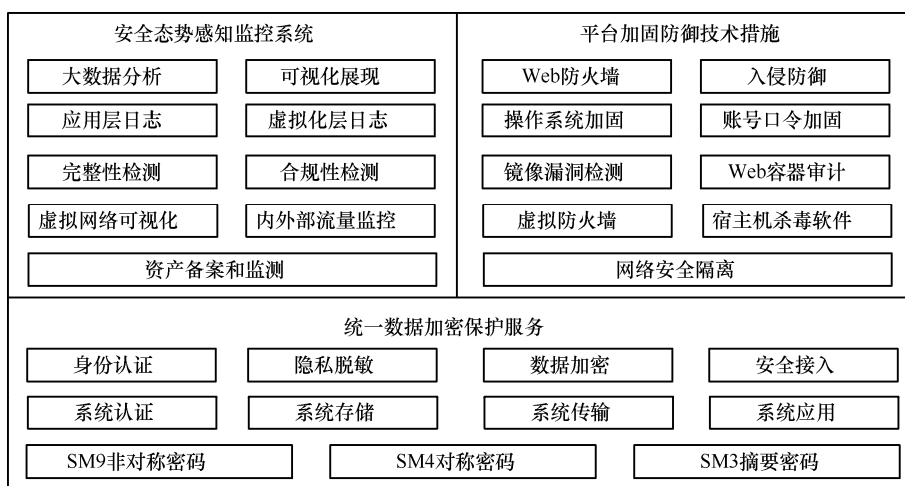


图7 电力云系统安全防护架构

需合理划分云平台功能区域,通过部署虚拟机防火墙、宿主机杀毒软件等方式隔离网络安全区域,同时通过镜像漏洞检测、Web容器审计、操作系统加固、账号口令加固等方式提升云平台防攻击、防篡改的整体防御能力。

4.3 统一数据加密保护服务

数据安全是云平台安全的最后一道防线,构建贯穿云平台认证、存储、传输、应用全过程的统一数据加密保护云服务是十分必要的。在密码应用上必须坚持自主可控,近年来我国发布了系列国产密码算法,基于密码算法的技术特点和电力云环境架构,通过国产SM9非对称密码算法^[21,22],可将用户或设备ID作为公钥,无需生成数字证书,可以更低成本方式与云计算进行融合,同时配套应用SM4对称和SM3摘要密码算法,构建电力云密钥基础设施,以SaaS模式发布统一的密码服务接口,统一提供密钥生成、分发、销毁等管理服务,为电力云平台提供身份认证、隐私脱敏、数据加密、安全接入等服务,实现电力云数据的加密和隔离,防止数据泄露,确保云平台核心服务的可靠性、可用性与安全性。

5 结束语

电力云作为国家关键信息基础设施,其安全

性是国家网络安全的重要组成部分,必须保证电力云安全的可控、能控、在控。本文在对电力云架构和业务流程进行全面分析基础上,采用动静结合的安全风险分析方法,对应用和平台两个层面面临的安全风险进行了全面识别和分析,同时根据威胁和安全需求,对电力云安全防护体系架构进行了阐述,并给出了具体的技术防护建议。本文的研究成果为正在快速发展的电力云计算平台提供了信息安全保障支撑,是应对电力信息系统云安全新挑战的一种有效尝试,以期为电力行业云计算技术发展和应用提供有效的指导。

参考文献:

- [1] 杨宁, 罗华永, 李兴, 等. 电力资源池基础架构的设计和实现[J]. 电信科学, 2016, 33(3): 142-147.
YANG N, LUO H Y, LI X, et al. Design and implementation of electric cloud's resource pool[J]. Telecommunications Science, 2016, 33(3):142-147.
- [2] 刘俊文, 玄佳兴. 数据中心仿真云平台的功能需求与设计[J]. 电信科学, 2017, 33(5): 176-182.
LIU J W, XUAN J X. Functional requirements and design of simulation cloud platform for data center[J]. Telecommunications Science, 2017, 33(5): 176-182.
- [3] LUO F, ZHAO J, DONG Z Y, et al. Cloud-based information infrastructure for next-generation power grid: conception, architecture, and applications[J]. IEEE Transactions on Smart Grid, 2016, 7(4): 1896-1912.
- [4] 马军伟, 罗红波, 栗秀琴. 电力云计算信息安全问题研

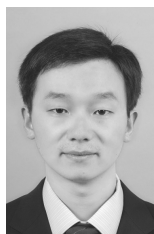


- 究[C]//中国电机工程学会, 2013年10月12日, 长沙, 中国: [S.l: s.n.], 2013.
- MA J W, LUO H B, SU X Q. The research on information security issues of power cloud computing[C]//China Society of Electrical Engineering, October 12, 2013, Changsha, China: [S.l: s.n.], 2013.
- [5] KOTOWSKI J, OKO J, OCHLA M. Deployment models and optimization procedures in cloud computing[C]//International Conference on Computer Aided Systems Theory, July 18-24, 2015, San Francisco, USA. Berlin: Springer, 2015: 805-812.
- [6] KAVIS M. Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS) [M]. New Delhi: Wiley India Private Limited, 2014.
- [7] 陈永卫, 张中华, 吉晓佳. 基于云计算的电力调度软交换系统研究[J]. 电力系统通信, 2012, 33(11): 88-92.
- CHEN Y W, ZHANG Z H, JI X J. Research on soft dispatch system of power dispatching based on cloud computing[J]. Power System Communication, 2012, 33(11): 88-92.
- [8] 任梦吟. 智能电网下的云计算隐私保护与安全存储研究[D]. 成都: 电子科技大学, 2015.
- REN M Y. Research on privacy protection and security storage of cloud computing under smart grid[D]. Chengdu: University of Electronic Science and Technology, 2015.
- [9] WEI L, ZHU H, CAO Z, et al. Security and privacy for storage and computation in cloud computing[J]. Information Sciences, 2014, 258(3): 371-386.
- [10] 刁姚鹏. 云技术在电力系统不良数据处理中的研究与应用[D]. 南京: 东南大学, 2015.
- XI Y P. Research and application of cloud technology in defect data processing of power system[D]. Nanjing: Southeast University, 2015.
- [11] WANG H. Proxy provable data possession in public clouds[J]. IEEE Transactions on Services Computing, 2013, 6(4): 551-559.
- [12] RUJ S, STOJIMENOVIC M, NAYAK A. Decentralized access control with anonymous authentication of data stored in clouds[J]. IEEE Transactions on Parallel & Distributed Systems, 2013, 25(2): 384-394.
- [13] 周延. 改进的 STRIDE 威胁模型研究[D]. 武汉: 华中科技大学, 2015.
- ZHOU Y. The research of improved stride threat model[D]. Wuhan: Huazhong University of Science and Technology, 2015.
- [14] HO S M, FU H, TIMMARAJUS S S, et al. Insider threat: language-action cues in group dynamics[C]//Hawaii International Conference on System Sciences, June 4-6, 2015, California, USA. Piscataway: IEEE Press, 2015: 2729-2738.
- [15] BURGER E W, GOODMAN M D, KAMPANAKIS P, et al. Taxonomy model for cyber threat intelligence information exchange technologies[C]//ACM Workshop on Information Sharing & Collaborative Security, November 3, Scottsdale, Arizona, USA. New York: ACM Press, 2014: 51-60.
- [16] 杨泽明, 李强, 刘俊荣, 等. 面向攻击溯源的威胁情报共享利用研究[J]. 信息安全研究, 2015, 1(1): 31-36.
- YANG Z M, LI Q, LIU J R, et al. Research on the use of threat information sharing for attack-oriented tracing[J]. Information Security Research, 2015, 1(1): 31-36.
- [17] 孙建坡. 基于攻击链的威胁感知系统[J]. 邮电设计技术, 2016(1): 74-77.
- SUN J P. The threat perception system based on attack chain [J]. Designing Techniques of Posts and Telecommunications, 2016(1): 74-77.
- [18] 庄刘, 魏中许. 基于情报信息的空防安全威胁评估回归模型研究[J]. 四川师范大学学报(自然科学版), 2015, 38(3): 460-465.
- ZHUANG L, WEI Z X. Research on regression model of air defense security threat assessment based on intelligence information[J]. Journal of Sichuan Normal University (Natural Science Edition), 2015, 38(3): 460-465.
- [19] LO C C, CHEN W J. A hybrid information security risk assessment procedure considering interdependences between controls[J]. Expert Systems with Applications, 2012, 39(1): 247-257.
- [20] 王笑帝, 张云勇, 刘楠, 等. 云计算虚拟化安全技术研究[J]. 电信科学, 2015, 31(6): 1-5.
- WANG X D, ZHANG Y Y, LIU D, et al. Research on security of virtualization on cloud computing[J]. Telecommunications Science, 2015, 31(6): 1-5.
- [21] SHAMIR ADI. Identity-based cryptosystems and signature schemes[J]. Lecture Notes in Computer Science, 1984, 21(12): 47-53.
- [22] GE W J, HU X H, DENG Y. Research of IBC model and application in web-security system[J]. Omer Mlaon, 2010, 27(9): 120-124.

[作者简介]



沈亮 (1969-), 男, 国家电网公司信息通信分公司教授级高级工程师, 主要从事电力信息化管理工作。



王栋 (1985-), 男, 国家电网公司信息通信分公司高级工程师, 主要从事电力信息安全工作。

玄佳兴 (1990-), 男, 国家电网公司信息通信分公司工程师, 主要从事电力信息化工作。