国家电网边缘计算信息系统安全风险评估方法研究

詹 雄[1,2] 郭 昊[1,2] 何小芸[1,2] 刘周斌[3] 孙学洁[4] 陈红松[4]

(全球能源互联网研究院有限公司 北京 102209)[1] (信息网络安全国家电网重点实验室 北京 102209)[2]

(国家电网浙江省电力有限公司电力科学研究院 杭州 310014)[3]

(北京科技大学计通学院 北京 100083)[4]

摘 要 依据风险评估理论,提出了基于模糊层次分析法的国家电网边缘计算信息系统安全风险评估方法。给出了设备层、数据层、网络层、应用层和管理层 5 个方面的安全评估项。在此基础上,针对网络安全评估,通过层次分析法比较评估项的重要程度,再结合模糊综合评价矩阵,计算得到网络安全的整体安全评价数值,据此对网络安全方面进行风险评估,并比较不同场景下的安全评估效果。最后,采用 Microsoft 威胁建模工具构建国家电网边缘计算信息系统威胁模型,对风险进行分析和安全加固。

关键词 智能电网,边缘计算,信息安全,风险评估

中图法分类号 TP309 **文献标识码** A

Research on Security Risk Assessment Method of State Grid Edge Computing Information System

ZHAN Xiong[1,2] GUO Hao[1,2] HE Xiao-yun[1,2] LIU Zhou-bin[3] SUN Xue-jie[4] CHEN Hong-song[4]

(Global Energy Interconnection Research Institute Co., Ltd, Beijing 102209, China)[1]

(State Grid Key Laboratory of Information & Network Security, Beijing 102209, China)[2]

(State Grid Zhejiang Electric Power Research Institute co., ltd, Hangzhou 310014, China)[3]

(School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)[4]

Abstract Based on the risk assessment theory, this paper proposed a risk analytic method based on fuzzy analytic hierarchy process for State Grid Corporation of China Edge Computing Information System. The security assessment items of five aspects of equipment layer, data layer, network layer, application layer and management layer are given. On the basis of this, for the aspect of network security, the importance degree of the evaluation item is compared by analytic hierarchy process. And then combined with fuzzy comprehensive evaluation matrix, the overall security evaluation value of network security is calculated, and risk assessment on network security is conducted, and the security assessment results are compared in different scenarios. Finally, the Microsoft threat modeling tool is used to construct the State Grid Corporation of China Edge Computing Information System threat model, which is used to analyze and reinforce the risk.

Keywords Smart grid, Edge calculation, Information security, Risk assessment

1 引言

随着智能电网建设的不断推进,电力系统的规模不断扩大,智能终端的数量急剧增长,电力业务也呈现出多样性、实时性的趋势,由此产生海量的异构数据。而边缘计算在网络边缘并靠近数据源头,可以就近提供边缘计算服务,是融合计算、存储、网络、应用等核心能力的开放平台,能够满足行业业务实时化、传输低时延、应用智能化等需求。但是,新兴技术的引入,在缓解智能电网系统若干压力的同时,还会带来更为复杂、多样的安全问题。因此,可靠的信息安全风险评估方法是保障边缘计算技术在智能电网系统中顺利应用的关键。实际上边缘计算技术的具体应用还处于开发阶段,相应的安全评估研究少之又少,为此本文依据信息安全风险评估系列标准规范、国家法律法规、国家电网内部的信息安全管理规范以及欧盟 ENISA 提出的物联网安全认证基线,依托物联网、云计算安全评估实施指标,结合边缘计算特性,总结适用于国家电网边缘计算信息安全的安全评估项,并依据模糊层次分析法构建国家电网边缘计算信息安全评估模型,通过构建威胁模型,总结安全加固方案。本文工作期待随着相关边缘计算能安全防护技术的不断发展,边缘计算能在智能电网系统中完美地应用与落地。

2 电力信息系统安全风险评估现状

2.1 电力信息系统风险评估政策与标准

早在 2007 年,电力行业就开始了信息系统安全等级保护与风险评估研究工作。我们参考了一系列关于等级保护、安全防护和风险评估的政策和标准,其中本文参考风险评估标准有《GB/T 22239.1 信息安全技术 网络安全等级保护基本

本文受国家电网公司科技项目(52110118001H,52110418001B)资助。

詹 雄(1978—),男,高级工程师,主要研究方向为电力系统网络安全关键技术,E-mail:zhanxiong@geiri.sgcc.con.cn;陈红松(1977—),男,博士,教授,CCF 会员,主要研究方向为网络信息安全、可信计算,E-mail:chenhs@ustb.edu.cn。

要求 第 1 部分：通用要求》[2]、《GB/T 22239.4 信息安全技术 网络安全等级保护基本要求 第 4 部分：物联网安全扩展要求》[3]、《GB/T 28448.1 信息安全技术 网络安全等级保护测评要求 第 1 部分：安全通用要求》[4]、《GB/T 28448.4 信息安全技术 网络安全等级保护测评要求 第 4 部分：物联网安全扩展要求》[5]和《GB/T 28449 信息安全技术网 络安全等级保护测评过程指南》[6]。

2.2　电力信息系统风险评估方法研究现状

电力行业作为关键基础设施之一，为配合信息时代的发展，不断地引入新兴的信息技术，这使得智能电网成为一个信息融合系统。但是，随着各种信息安全事件的发生，对电力行业的信息安全问题进行研究已经刻不容缓。有效的信息安全风险评估方法是保证电力行业信息安全工作顺利进行的关键。

目前，针对电力行业的安全风险评估工作研究比较基础，多是应用已有的评估理论与模型进行风险评估。杨小彬等[7]在配电网的评估研究中，依据相关的法律规范，采用层次分析法确定单个指标的权重，进而确定配电网综合能效值，并可以指出脆弱环节，以此建立了一套配电网能效指标体系。Langer 等[8]提出了一种网络安全风险评估方法，该方法涉及两个相互关联的分析流，可用于确定与包含传统系统和新型 ICT 概念的智能电网的架构概念相关的风险。苑嘉航等[9]提出一种基于灰度关联和 D-S 证据理论的方法来评估电网企业信息系统的安全风险，首先对指标参数值进行不确定分析，再通过灰度关联和隶属度构造 Mass 函数矩阵，通过 D-S 证据理论将函数进行信息融合，最后通过置信函数值对风险进行排序、评估。

以上研究只是针对电力系统的风险评估方法，虽然国内外在各个领域对边缘计算的研究已经有很多成果，但由于我国电力行业规模巨大，很难对某项新技术立即应用；另一方面边缘计算相关标准化研究并不完备，导致边缘计算与电网结合的例子少之又少，相应的风险评估方法研究几乎空白。但是对于边缘计算在智能电网中应用的安全测评，可以借鉴物联网、云计算等与其相关的安全测评知识并结合边缘计算在不同领域的实际应用进行风险评估方法的研究与总结。

3　国家电网边缘计算信息系统安全风险评估方法

3.1　国家电网边缘计算信息系统安全风险评估指标体系的构建

3.1.1　总体指标设计与描述

随着智能电网建设规模的扩大，需求侧的大量智能终端设备接入电网，产生了海量数据，传统的云端服务模式已经进入瓶颈期。边缘计算技术在智能电网中的应用重点解决海量数据的存储、计算和网络传输速率等问题。为了全面客观地设计基于边缘计算框架的智能电网信息系统安全评估项，本文基于 GB/T 28448，GB/T 22239 等国家标准设计了设备安全、数据安全、网络安全、应用安全以及管理安全 5 个维度的评估项。

3.1.2　国家电网边缘计算网络安全风险评估指标体系的构建

本文以网络安全为例，构建如下评估指标层次体系。

智能电网引入边缘计算技术，部分电网的终端设备会通过网络层与边缘设备进行数据传输，同时边缘设备通过网络层实现更加广泛的互联功能，因此网络规模、数据量、网络接入的增加，导致电网边缘计算的网络安全具有新的挑战。所以针对电网边缘计算的网络安全评估将从设备、通道以及协议安全等方面进行展开，如图 1 所示。

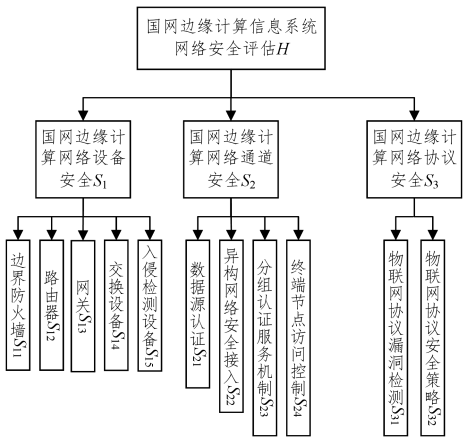

图 1　网络安全评估指标体系层次分析图

3.2　国家电网边缘计算信息安全系统风险评估分析

3.2.1　风险评估应用原理

(1)层次分析法

层次分析法是可以对多方案系统进行分析的一种层次化、结构化的决策方法。将决策者对复杂系统的决策思维过程模型化和数量化。通过使用这种方法将复杂问题分解为若干层次和若干因素，在因素之间进行比较和计算，为方案选择提供依据[10]。本次研究利用层次分析法并不是为了进行最优方案决策，而是依据层次分析法原理，通过构建测评的递阶层次结构模型，对测评要素进行权重赋值，得出基本安全测评要素对整体安全的配置情况。

(2)模糊综合评判

模糊综合评判应用隶属度原则，考虑被评估事物的相关因素，对其进行综合评估，并将评估结果分成一定等级[10]。其主要步骤为：首先建立反应评估项属性和性能的评估因素集和可以描述等级的评价集。然后针对评估项建立评价集合的模糊映射。通过其他方法建立各个评估项的权重分配集合。最后通过评级集合和权重集合的运算，得出综合评价值。

(3)基于模糊层次分析算法的网络安全评估流程

基于模糊层次分析算法的网络安全评估流程如图 2 所示。

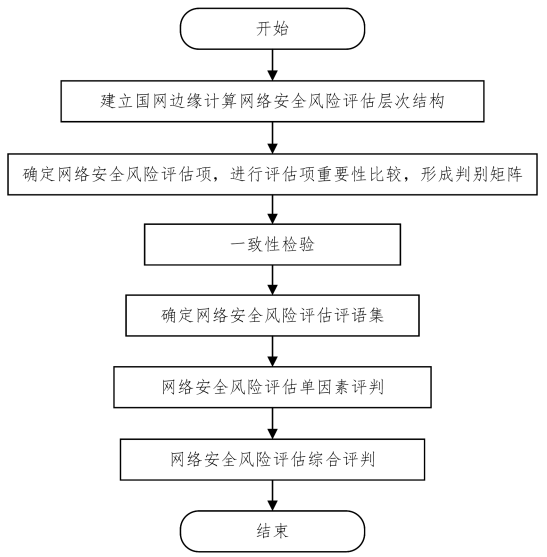

图 2　基于模糊层次分析法的网络安全评估流程图

3.2.2 基于模糊层次分析法的国家电网边缘计算网络安全风险评估实例分析

(1)安全评估因素重要性判别

根据表 1,利用两两比较法构造判别矩阵。

表 1 5 级评估尺度表

标度	定义	取值
1	比同样重要	$b_{ij}=1(b_{ji}=1)$
2	比稍微重要	$b_{ij}=2(b_{ji}=1/2)$
3	比相当重要	$b_{ij}=3(b_{ji}=1/3)$
4	比明显重要	$b_{ij}=4(b_{ji}=1/4)$
5	比绝对重要	$b_{ij}=5(b_{ji}=1/5)$

国家电网边缘计算网络安全第二层因素 S 对目标层 H 的判别矩阵如表 2 所列。

表 2 国家电网边缘计算网络安全第二层评估因素的判别矩阵

国家电网边缘计算网络安全 H	国家电网边缘计算网络设备安全 S_1	国家电网边缘计算网络通道安全 S_2	国家电网边缘计算网络协议安全 S_3
国家电网边缘计算网络设备安全 S_1	1	0.5	0.25
国家电网边缘计算网络通道安全 S_2	2	1	0.5
国家电网边缘计算网络协议安全 S_3	4	2	1

对国家电网边缘计算第三层评估因素构造如下判断矩阵:国家电网边缘计算网络设备安全评估因素的判别矩阵 S_1 如表 3 所列;同理,国家电网边缘计算网络通道安全评估因素 S_2、网络协议安全评估因素 S_3 的判别矩阵可以依此构造,如表 4、表 5 所列。

表 3 国家电网边缘计算网络设备安全评估因素的判别矩阵

S_1	边界防火墙 S_{11}	路由器 S_{12}	网关 S_{13}	交换设备 S_{14}	入侵检测设备 S_{15}
边界防火墙 S_{11}	1	0.5	0.25	0.5	0.5
路由器 S_{12}	2	1	0.5	1	1
网关 S_{13}	4	2	1	2	2
交换设备 S_{14}	2	1	0.5	1	1
入侵检测设备 S_{15}	2	1	0.5	1	1

表 4 国家电网边缘计算网络通道安全评估因素的判别矩阵

S_2	数据源认证 S_{21}	异构网络接入 S_{22}	分组认证服务机制 S_{23}	终端节点访问控制 S_{24}
数据源认证 S_{21}	1	0.5	1	0.25
异构网络接入 S_{22}	2	1	4	0.5
分组认证服务机制 S_{23}	1	0.25	1	0.25
终端节点访问控制 S_{24}	4	2	4	1

表 5 国家电网边缘计算网络协议安全的判别矩阵

S_3	物联网协议漏洞检测 S_{31}	物联网协议安全策略 S_{32}
物联网协议漏洞检测 S_{31}	1	2
物联网协议安全策略 S_{32}	0.5	1

(2)层次排序权重计算与检验

以第二层因素判别矩阵计算为例,具体步骤如下:

步骤 1 判别矩阵 P_S

$$P_S=(b_{ij})_{3\times3}=\begin{bmatrix}1 & 0.5 & 0.25\\ 2 & 1 & 0.5\\ 4 & 2 & 1\end{bmatrix} \tag{1}$$

步骤 2 列向量元素求积开方并做归一化处理的权重向量 W_H:

$$\omega_i=\sqrt[n]{\prod_{j=1}^{n}b_{ij}} \tag{2}$$

$$\omega_S=(\omega_1,\omega_2,\cdots,\omega_i=\sqrt[n]{\prod_{j=1}^{n}b_{ij}})^{\mathrm{T}}=\begin{bmatrix}1.2051\\ 1.5183\\ 1.9129\end{bmatrix} \tag{3}$$

$$W_H=(W_1,W_2,\cdots,W_S=\frac{\omega_i}{\sum_{i=1}^{n}\omega_i})^{\mathrm{T}}=\begin{bmatrix}0.1429\\ 0.2857\\ 0.5714\end{bmatrix} \tag{4}$$

步骤 3 计算最大特征值

$$\lambda=\sum_{i=1}^{n}\frac{(AW_S)_i}{nW_{Si}}_{\max}=4.2 \tag{5}$$

步骤 4 一致性检验

平均随机一致性 RI 标准值对应表如表 6 所列,经计算:

$$CI=\frac{\lambda_{\max}}{n-1}=0.073 \tag{6}$$

当 $n=3$ 时,$RI=0.58$,则 $CR=CI/RI=0.082<0.1$,通过一致性检验。

表 6 随机一致性对应表

矩阵阶数 n	1	2	3	4	5	6	7	8	9
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45

同理,计算出第三层评估因素网络设备、网络通道、网络协议安全因素判别矩阵的 CR 值均小于 0.1,因此,各判别矩阵通过一致性检验。

步骤 5 权重计算

根据以上的一致性检验结果,通过一致性检验,那么第二层因素权重矩阵 $W_H=[0.1429\ \ 0.2857\ \ 0.5714]$。

同理,第三层评估因素权重矩阵 W_S:

$$W_S=[S_{i1},S_{i2},\cdots,S_{im}]\ ,i=1,2,3 \tag{7}$$

同上计算,可得国家电网边缘计算网络设备安全权重矩阵 $W_{S=1}$、国家电网边缘计算网络通道安全权重矩阵 $W_{S=2}$、国家电网边缘计算网络协议安全权重矩阵 $W_{S=3}$。

$W_{S=1}=[0.1381\ \ 0.1953\ \ 0.2761\ \ 0.1953\ \ 0.1953]$

$W_{S=2}=[0.125\ \ 0.25\ \ 0.125\ \ 0.5]$

$W_{S=3}=[0.5858\ \ 0.4142]$

依此,国家电网边缘计算网络安全评估因素层次总权重如表 7 所列。

表 7 国网边缘计算网络安全评估因素层次总权重

第二层安全评估因素	第三层安全评估因素	权重
国家电网边缘计算网络设备安全 S_1 0.1429	边界防火墙 S_{11}	0.0197
	路由器 S_{12}	0.0279
	网关 S_{13}	0.0395
	交换设备 S_{14}	0.0197
	入侵检测设备 S_{15}	0.0197
国家电网边缘计算网络通道安全 S_2 0.2857	数据源认证 S_{21}	0.0357
	异构网络安全接入 S_{22}	0.0714
	分组认证服务机制 S_{23}	0.0357
	终端节点访问控制 S_{24}	0.1429
国家电网边缘计算网络协议安全 S_3 0.5714	网络协议漏洞检测 S_{31}	0.3347
	网络安全协议策略制定 S_{32}	0.2367

(3)网络安全综合评价

步骤 1 建立评语级

针对每个安全评估因素的风险级别进行描述,如可以划分为高、较高、中等、较低、低。记:$V_1=\{$高,较高,中等,较低,

低}，则可以总结出每个安全评估要素的风险级别统计表，将总体安全状况划分为安全、较安全、中等、较危险、危险，记 $V_2=\{10,30,50,70,90\}$，则整体安全评语集与分数对照表如表 8 所列。

表 8　整体安全分数对照表

安全等级	安全	较安全	一般	较危险	危险
分数区间	[0,20]	(20,40]	(40,60]	(60,80]	(80,100]

步骤 2　网络安全评估因素风险因素信息收集

本文对国家电网边缘计算网络安全下的两个场景的评估要素风险信息进行收集，如表 9、表 10 所列。

表 9　网络安全场景一的评估要素风险信息收集表

第二层安全评估因素	第三层安全评估因素	高	中高	中等	中低	低
国家电网边缘计算网络设备安全 S_1	边界防火墙	1	2	1	2	1
	路由器	1	1	2	3	2
	网关	1	2	1	1	2
	交换设备	2	1	2	1	2
	入侵检测设备	2	0	1	1	3
国家电网边缘计算网络通道安全 S_2	数据源认证	1	3	2	1	1
	异构网络接入	1	1	2	0	1
	分组认证服务机制	1	0	2	3	1
	终端节点访问控制	2	1	2	1	0
国家电网边缘计算网络协议安全 S_3	物联网协议漏洞检测	1	2	1	1	1
	物联网协议安全策略	2	0	2	2	0

表 10　网络安全场景二的评估要素风险信息收集表

第二层安全评估因素	第三层安全评估因素	高	中高	中等	中低	低
国家电网边缘计算网络设备安全 S_1	边界防火墙	0	0	1	2	3
	路由器	0	1	2	3	0
	边缘计算网关	0	0	0	4	2
	边缘计算交换设备	0	1	1	4	1
	入侵检测设备	0	0	2	2	3
国家电网边缘计算网络通道安全 S_2	数据源认证	0	0	0	1	1
	异构网络接入	0	1	0	2	1
	分组认证服务机制	1	0	0	2	2
	终端节点访问控制	0	2	1	0	1
国家电网边缘计算网络协议安全 S_3	物联网协议漏洞检测	0	1	0	2	1
	物联网协议安全策略	1	0	1	0	2

步骤 3　建立模糊关系矩阵

根据网络安全评估要素风险信息收集表 5 中数据，得到 S_1 下安全评估要素的模糊关系矩阵 $R_{S=1}$：

$$R_{S=1}=\begin{bmatrix} \frac{n_1}{N_{1_1}} & \frac{n_2}{N_{1_1}} & \frac{n_3}{N_{1_1}} & \frac{n_4}{N_{1_1}} & \frac{n_5}{N_{1_1}} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \frac{n_1}{N_{1_5}} & \frac{n_1}{N_{1_5}} & \frac{n_1}{N_{1_5}} & \frac{n_1}{N_{1_5}} & \frac{n_1}{N_{1_5}} \end{bmatrix}$$

$$=\begin{bmatrix} \frac{1}{7} & \frac{2}{7} & \frac{1}{7} & \frac{2}{7} & \frac{1}{7} \\ \frac{1}{9} & \frac{1}{9} & \frac{2}{9} & \frac{1}{3} & \frac{2}{9} \\ \frac{1}{7} & \frac{2}{7} & \frac{1}{7} & \frac{1}{7} & \frac{2}{7} \\ \frac{1}{4} & \frac{1}{8} & \frac{1}{4} & \frac{1}{8} & \frac{1}{4} \\ \frac{2}{7} & 0 & \frac{1}{7} & \frac{1}{7} & \frac{3}{7} \end{bmatrix} \tag{8}$$

步骤 4　建立模糊评价矩阵

结合层次分析法确定的权重，可以得到国家电网边缘计算网络设备安全综合评价向量 X_1：

$$X_1=W_{S=1}\cdot R_{S=1}=[x_{11}\ \cdots\ x_{15}]$$

$$=[0.1855\ \ 0.1645\ \ 0.1793\ \ 0.1963\ \ 0.2745] \tag{9}$$

同理求出 S_1，S_2 的综合评价向量 X_2，X_3：

$$X_2=W_{S=2}\cdot R_{S=2}$$

$$=[0.2501\ \ 0.1802\ \ 0.3336\ \ 0.1525\ \ 0.0835] \tag{10}$$

$$X_3=W_{S=3}\cdot R_{S=1}$$

$$=[0.2357\ \ 0.1953\ \ 0.2357\ \ 0.2357\ \ 0.0976] \tag{11}$$

因此得到综合模糊评价矩阵 X：

$$X=[X_1,X_2,X_3]=\begin{bmatrix} x_{11} & \cdots & x_{15} \\ x_{21} & \cdots & x_{25} \\ x_{31} & \cdots & x_{35} \end{bmatrix}$$

$$=\begin{bmatrix} 0.1855 & 0.1645 & 0.1793 & 0.1963 & 0.2745 \\ 0.2501 & 0.1802 & 0.3336 & 0.1525 & 0.0835 \\ 0.2357 & 0.1953 & 0.2357 & 0.2357 & 0.0976 \end{bmatrix} \tag{12}$$

步骤 5　求出综合评价结果 J：

$$J=W_H\cdot X$$

$$=[0.2326\ \ 0.1866\ \ 0.2556\ \ 0.2063\ \ 0.1189] \tag{13}$$

步骤 6　求出网络安全评估最终得分 Z：

$$Z=J\cdot V_2$$

$$=[0.2326\ \ 0.1866\ \ 0.2556\ \ 0.2063\ \ 0.1189)]\cdot$$

$$[10\ \ 30\ \ 50\ \ 70\ \ 90]=45.846 \tag{14}$$

据此，可得出网络安全场景一的风险评估综合得分为 45.846，说明场景一在满足最基本的安全的基础上，风险评估结果处于中等水平，但仍有较大的改进空间。同理可以得出网络安全场景二的风险评估综合得分为 62.918，说明场景二的风险评估结果良好，在网络安全方面基本可信。

3.2.3　Microsoft Threat Modeling Tool 建模威胁分析

Microsoft Threat Modeling Tool 是 Microsoft 开发的一个免费威胁建模工具，通过选用系统设备组件以及数据流进行建模，绘制系统架构，随后通过分析建立模型的安全属性、数据流以及信息资产中潜在的威胁来发现系统的潜在风险威胁[11]。该工具所创建的模型为数据流图(Data Flow Diagram)模型，包含数据流、数据存储、进程、交互器和信任边界等元素，通常这些 DFD 元素易受到的威胁类型有：欺骗、篡改、拒绝、信息披露、拒绝服务和特权提升。

(1)国家电网边缘计算信息安全威胁模型

参考边缘计算在其他场景的应用，以及边缘计算在物联网中的层次架构[12]，构建了如图 3 所示的国家电网边缘计算的威胁模型。

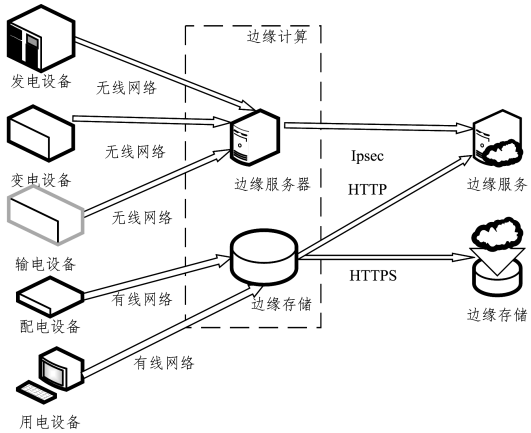

图 3　国家电网边缘计算威胁模型

(2)安全加固

根据威胁分析报告,以终端设备与边缘服务器之间存在的安全威胁,如图 4 所示,进行分析如下:

终端设备资源的访问控制机制薄弱,应及时查看授权设置;终端设备受信任日志可能被未被授权者篡改,应确定受信任级别,不允许其他超出最高信任级别的人登录,让非写入电力终端设备日志的访问者遭遇拒绝访问;终端设备可能遭遇欺骗,向边缘服务器传递不正确数据,或者边缘服务器进程被欺骗,此时应使用标准身份认证机制来标识原数据存储;除此之外,边缘服务器受远程执行代码控制[13],导致终端设备权限异常提升,解决办法为实时对非法恶意代码进行监测。

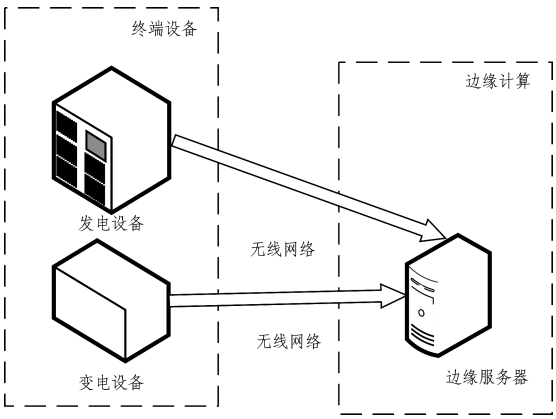

图 4 终端设备-边缘服务器

结束语 本文针对国家电网边缘计算信息系统,研究了适应国家电网边缘计算信息系统安全的风险评估方法,构建了设备安全、数据安全、网络安全、应用安全和管理安全 5 个方面的安全评估体系,结合模糊层次分析理论,对网络安全风险评估因素进行了实例分析,并通过 Microsoft 威胁建模工具构建国家电网边缘计算威胁模型,进行安全威胁分析和安全加固。在此基础上,实现了对国家电网边缘计算信息系统安全的风险评估。

参 考 文 献

[1] 吕华章,陈丹,范斌,等. 边缘计算标准化进展与案例分析[J]. 计算机研究与发展,2018,55(3):487-511.

[2] GB/T 22239:信息安全技术 网络安全等级保护基本要求 第 1 部分:通用要求[S]. 中国国家标准化管理委员会. 北京:中国标准出版社.

[3] GB/T 22239:信息安全技术 网络安全等级保护基本要求 第 4 部分:物联网安全扩展要求[S]. 中国国家标准化管理委员会. 北京:中国标准出版社.

[4] GB/T 28448:信息安全技术 网络安全等级保护评测要求 第 1 部分:安全通用要求[S]. 中国国家标准化管理委员会,北京:中国标准出版社.

[5] GB/T 28448:信息安全技术 网络安全等级保护评测要求 第 4 部分:物联网安全扩展要求[S]. 中国国家标准化管理委员会. 北京:中国标准出版社.

[6] GB/T 28449:信息安全技术网络安全等级保护测评过程指南[S]. 中国国家标准化管理委员会. 北京:中国标准出版社.

[7] 杨小彬,李和明,尹忠东,等. 基于层次分析法的配电网能效指标体系[J]. 电力系统自动化,2013,37(21):146-150.

[8] LANGER L,SKOPIK F,SMITH P,et al. From old to new:assessing cybersecurity risks for an evolving smart grid[J]. Computers & Security,2016,62:165-176.

[9] 苑嘉航,李存斌. 基于灰关联和 D-S 证据理论电网企业信息安全风险评估[J]. 陕西电力,2014,42(2):11-15.

[10] 徐洋,谢晓尧. 信息安全等级保护测评量化模型[M]. 武汉:武汉大学出版社,2017.

[11] WILLIAMS I,YUAN X. Evaluating the effectiveness of Microsoft threat modeling tool[C]// Information Security Curriculum Development Conference. ACM,2015:76-83.

[12] 张佳乐,赵彦超,陈兵,等. 边缘计算数据安全与隐私保护研究综述[J]. 通信学报,2018,39(3):1-21.

[13] 陈红松,王钢,宋建林. 基于云计算入侵检测数据集的内网用户异常行为分类算法研究[J]. 信息网络安全,2018,18(3):1-7.

(上接第 420 页)

[7] BOUNOV D,KICI R G,LERNER S. Protecting C++ Dynamic Dispatch Through VTable Interleaving[C]// NDSS. 2016.

[8] ELSABAGH M,FLECK D,STAVROU A. Strict Virtual Call Integrity Checking for C++ Binaries[C]// Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. ACM,2017:140-154.

[9] VEEN V V D,ANDRIESSE D,GÖKTAŞ E,et al. Practical context-sensitive CFI[C]// Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM,2015:927-940.

[10] YAMADA K,SHANMUGAVELAYUTHAM P,KONDA S. Techniques for enforcing control flow integrity using binary translation:U. S. Patent Application 15/430,652[P]. 2017-11-02.

[11] TICE C,ROEDER T,COLLINGBOURNE P,et al. Enforcing Forward-Edge Control-Flow Integrity in GCC & LLVM[C]// USENIX Security Symposium. 2014:941-955.

[12] BLACK R J,BURRELL T W,DE CASTRO M O T,et al. Control flow integrity enforcement at scale:U. S. Patent Application 13/450,487[P]. 2013-10-24.

[13] DAVI L,SADEGHI A R,WINANDY M. ROPdefender:A detection tool to defend against return-oriented programming attacks[C]// Proceedings of the 6th ACM Symposium on Information,Computer and Communications Security. ACM,2011:40-51.

[14] COUDRAY T,FONTAINE A,CHIFFLIER P. Picon:Control Flow Integrity on LLVM IR[C]// Symposium on security of information and communications technology (SSTIC). 2015.

[15] BERNAT A R,MILLER B P. Anywhere,any-time binary instrumentation[C]// Proceedings of the 10th ACM SIGPLAN-SIGSOFT Workshop on Program Analysis for Software Tools. ACM,2011:9-16.

[16] 王明华,尹恒,苏璞睿,等. 二进制代码块:面向二进制程序的细粒度控制流完整性校验方法[J]. 信息安全学报,2016(2):61-72.

[17] ZHANG M,SEKAR R. Control Flow Integrity for COTS Binaries[C]// Proceedings of the 22nd USENIX Security Symposium. USENIX,2013:337-352.