能源互联网安全态势体系建设研究

徐　琳，张宏雷
（中能融合智慧科技有限公司，北京 100011）

摘　要： 能源互联网是我国实现能源结构变革，提高能源的安全和绿色水平的关键。因此能源互联网的安全关系着能源互联网的稳定、安全运行。研究能源互联网安全态势感知体系，打造能源互联网安全态势综合监测平台，实现能源互联网安全态势监测分析以及内外网的安全风险监测；打造全球能源互联网安全加固与防护体系，并形成一系列的安全规范，从而实现能源互联网安全风险态势全面感知，安全威胁高效预警，提升能源互联网安全可控水平，全方位、多角度保证能源互联网安全，确保用户切身利益。

关键词： 能源互联网；安全态势；体系建设
中图分类号： TP393　　**文献标识码：** A　　DOI：10.16157/j.issn.0258-7998.223169

中文引用格式： 徐琳，张宏雷. 能源互联网安全态势体系建设研究[J].电子技术应用，2022，48(12)：33-39，46.
英文引用格式： Xu Lin，Zhang Honglei. Research on the construction of energy Internet security situation system[J]. Application of Electronic Technique，2022，48(12)：33-39，46.

Research on the construction of energy Internet security situation system

Xu Lin，Zhang Honglei
(Zhongneng Integrated Smart Energy Technology Co.，Ltd.，Beijing 100011，China)

Abstract： Energy Internet is the key to realize the reform of energy structure and improve the safety and green level of energy in China. Therefore，the security of the energy Internet is related to the stable and safe operation of the energy Internet. Therefore，we should study the energy Internet security situation awareness system，build a comprehensive monitoring platform for the energy Internet security situation，and realize the monitoring and analysis of the energy Internet security situation and the security risk monitoring of the internal and external networks. Build a global energy Internet security reinforcement and protection system，and form a series of security norms，so as to achieve a comprehensive awareness of the energy Internet security risk situation，efficient early warning of security threats，improve the controllable level of energy Internet security，ensure the energy Internet Security in all directions and from multiple angles，and ensure the vital interests of users.

Key words： energy Internet；security situation；system construction

0 引言

能源行业关系国家安全和国民经济命脉，是确保社会经济持续健康发展的重要基础性产业。为深入贯彻落实习近平总书记关于能源领域“四个革命、一个合作”[1-2]战略和网络强国战略的重要论述，不断优化能源结构和布局，加快构建清洁低碳、安全高效的能源体系，以智能化、信息化推动高质量发展，国家相关部门协同打造“共商、共建、共享”的国家级能源互联网，推动能源领域供给侧结构性改革，为国家能源安全提供有力支撑。在国家引导下，能源互联网整合电力、煤炭、石油、天然气等领域产业链信息，实现国内外能源生产、经济、消费、安全等数据有效汇聚和价值挖掘，培育数据开放共享、跨界融合、技术协同创新的能源互联网产业生态，打造覆盖全国能源领域、标准体系统一、智能应用丰富的“国家智慧能源大脑”。

能源安全是国家经济、社会稳定健康可持续运行的关键。近年以来，能源领域遭受的攻击数量激增，油气、电网两大领域已经成为黑客攻击的重点，这两个领域发生的网络攻击安全事件占全部网络攻击事件的一半以上[3]。另外，由于风力、光伏发电站等新能源系统全面使用人工智能、5G 通信等智能技术，数字化程度较高，面临的网络安全风险也更大。因此，为保障能源互联网的安全稳定，能源互联网平台的安全态势感知与防护体系亟需建立。通过建立安全态势感知体系，完善相关安全指引及规范，实时智能感知能源互联网平台关键设施的安全态势，发现恶意攻击，为能源企业及相关主管部门提供应急措施和专家支持，有效阻止网络攻击，保障全国能源系统安全运行，满足国家相关部委、集团、能源行业网络安全需求，打造能源企业网络安全的“顺风耳、千里眼、预警机”，促进能源行业数字化、智能化发展[4-5]。

本文基于能源互联网平台安全需求，研究能源工业互联网平台安全态势感知与防护体系，实现对能源工业互联网平台安全态势的全方位深度监测，以及安全信息交互与共享，实现安全威胁的全面感知与发现；研究能源互联网平台安全检测、加固防护、运维保障及应急处置等动态高效的一体化安全技术保障体系，对安全风险进行控制；支撑完善能源工业互联网平台相关安全指引、规范及操作规程，提高安全运维保障的效率和质量，为相关管理人员安全运维提供支撑。

1 能源互联网现状与安全需求

能源互联网是能源体系与互联网体系的深度融合而形成的全面感知、全程在线、全要素互联的能源新业态，将先进信息通信技术、控制技术与先进能源技术深度融合应用，支撑能源电力清洁低碳转型和多元主体灵活便捷接入，具有清洁低碳、安全可靠、泛在互联、高效互动、智能开放等特征。能源互联网连接能源生产和能源消费，是各能源参与方互联的基础平台，能够实现互联网式的双向交互、平等共享及服务增值[6]。能源互联网以安全可靠的物理融合系统，先进信息通信技术为基础，打造高效互动的能源交互枢纽，实现“能源流、信息流、业务流”一体化融合，助力清洁能源的全面普及和跨越发展[7-8]。因此，打造安全可靠的能源互联网，有助于实现能源结构变革，提高能源安全和绿色水平；支撑电能替代和再电气化进程，实现低碳高效的用能结构，提升电网经济高效和安全运行水平，驱动能源变革，促进社会能效提升。

目前，世界各国都在开展能源互联网的研究及建设。2008 年，德国、美国相继提出能源互联网的概念及雏形[9-10]，并大量开展以信息通信技术(Information and Communication Technology，ICT)为基础的高效能源系统研究，致力于能源生产、输送、消费和储能各个环节之间的智能化。之后，日本启动“智能能源共同体”“数字电网”计划，开展能源智能电网研究。欧洲启动未来智能能源互联网(Future Internet for Smart Energy，FINSENY)项目，构建未来能源互联网的 ICT 平台，支撑配电系统的智能化。中国于 2014 年开始开展能源互联网理念及技术体系研究，多年来研究成果显著，需求侧响应、虚拟电厂和综合能源等业务已经初具雏形，各省份的电力市场机制也在不断地发展完善，能源互联网项目在不断探寻参与市场的新模式。

能源互联网的研究目前主要集中在理念内涵、体系架构、核心技术、规划设计等宏观方面，对于能源互联网的安全方面研究较少。江艺宝、丁一等人[11-12]从物联层面、信息及市场层面对能源互联网风险评估的关键问题进行研究，为能源互联网的安全、可靠运行和能源领域的市场化改革奠定理论基础。刘增明[13]通过分析零信任框架设计了基于零信任的能源互联网安全防护架构，从终端接入控制、动态授权管理、统一身份管理、安全作为服务等方面进行研究，为能源互联网安全防护体系设计提供了新思路、新方法。魏峰等人[14]从全事物要素赋码技术、云数据安全管理模式、人网安全互动 3 方面探讨了能源物联网信息安全技术管理及措施，提升能源互联网自身安全认知水平和实践能力，切实保障优质电力供应和提供综合能源服务。王继业等[15]提出了基于信息驱动的全球能源互联网全景安全防御系统概念及其功能框架，为实现全球能源互联网主动防御提供坚实的技术支撑。张向宏[16]等人基于能源互联网源起和概念，研究提出能源互联网技术架构与能源互联网安全防护体系，支撑能源互联网物理安全，数据和能量采集安全，数据和能量传输安全，数据和能量处理安全，以及供应链安全。对能源互联网安全相关文献进行统计分析，安全方面的研究主要包括能源互联网安全防护体系及功能架构、风险评估方法、信息安全管理技术及措施等方面，为能源互联网安全体系建设提供了重要参考价值。但是，为了保证能源互联网实现安全事件事前预测、安全事件发生时主动防御、安全事件发生后智能评估，需研究能源互联网安全态势感知体系，实现能源互联网安全风险态势全面感知，对安全威胁进行高效预警，从而提升能源互联网信息系统安全可控水平，切实保护用户利益。因此，能源互联网主要安全需求有：

(1)构建能源互联网安全态势监测系统，实现能源互联网的内外网安全监测，重点监测能源互联网系统漏洞和入侵事件，对其存在的漏洞和重要信息安全事件进行预警，结合接收到的行业安全态势信息，对能源互联网的安全态势进行监测预警，并定期对其面临的信息安全形势进行分析研判，向相关部门提交及共享安全态势信息。

(2)构建能源互联网安全检测系统，对能源互联网进行安全漏洞扫描、恶意代码检测、系统安全配置核查，重点针对关键业务与流程进行安全审核、漏洞挖掘、安全检测。

(3)构建能源互联网加固防护系统，构建能源互联网的安全防护体系，通过部署网络反扫描、Web 应用防护、非法接入与边界防护、服务器安全加固、主机系统清洗、业务系统安全运维保障、主机主动防御、主机系统灾难应急处置等装备，以不断提升能源互联网安全防护水平。

(4)完善形成相关安全规范，逐步形成能源互联网设计、开发、测试、部署阶段及运维保障的安全指引及规范，为国家形成能源互联网的标准规范体系提供支撑。

2 能源互联网安全态势体系架构

2.1 主要架构

本文针对能源互联网信息安全需求研究能源互联网安全态势体系，主要内容包括能源互联网安全态势监测、安全检测与加固防护、安全规范与指引、态势发布

等。通过这些内容的建立，实现能源互联网安全态势监测能力的搭建，全面提升能源互联网对威胁及攻击行为的发现、研判、验证及预警能力，为能源互联网安全态势的动态发布提供支撑，同时为其他行业提供可复制、可扩展、可推广的示范经验及效能。能源互联网安全态势体系架构如图 1 所示。具体内容如下：

(1)能源互联网安全态势监测，针对能源互联网安全态势进行全方位深度监测，完善安全信息交互与共享，达到对能源安全威胁全面感知与发现的目的，提升能源行业安全态势监测水平。主要内容包括安全态势监测分析、外网安全监测、内网安全监测。

(2)能源互联网安全检测与加固，涵盖能源互联网系统安全检测、加固防护、运维保障及应急处置等动态高效的一体化安全技术保障体系，有效控制能源互联网的安全风险，主要包括安全检测、安全加固与防护等内容。

(3)完善一套能源互联网相关安全指引、规范及操作规程，确保能源互联网安全运维保障的效率、质量及规范。逐步形成能源互联网设计、开发、测试、部署阶段及运维保障的安全指引及规范。

2.2 能源互联网安全态势综合监测系统

2.2.1 安全态势监测分析

全态势监测分析，包括接收行业监管机构、第三方安全检测机构及其相关部门发布的安全态势，对能源互联网内外网监测信息和检测防护情况以及行业安全态势进行聚合分析，并将分析的安全态势数据进行上报及共享。安全态势监测分析功能框架如图 2 所示。

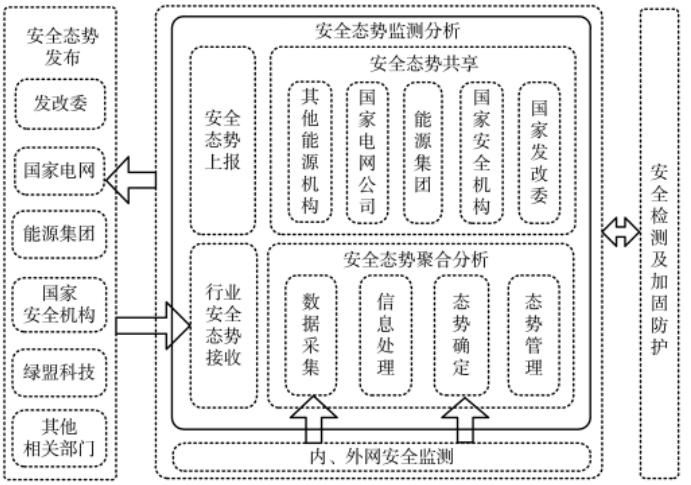

图 2 安全态势监测分析功能框架图

(1)行业安全态势接收

安全态势监测分析系统接收国家安全机构、国家电网安全部门、绿盟以及其他相关部门(例如公安部等部门)发出的能源系统安全态势报告，以结合能源互联网自身安全状况做出适当的安全措施调整。

(2)安全态势聚合分析

安全态势聚合分析能够在大规模网络通信环境中，对能够引起网络态势发生变化的安全态势数据要素进行获取、理解、显示以及将捕获到的安全数据报告给安全态势预警系统来发出安全预警。安全态势聚合分析负责提取、过滤和校准原始数据，并且将数据规范化，做时

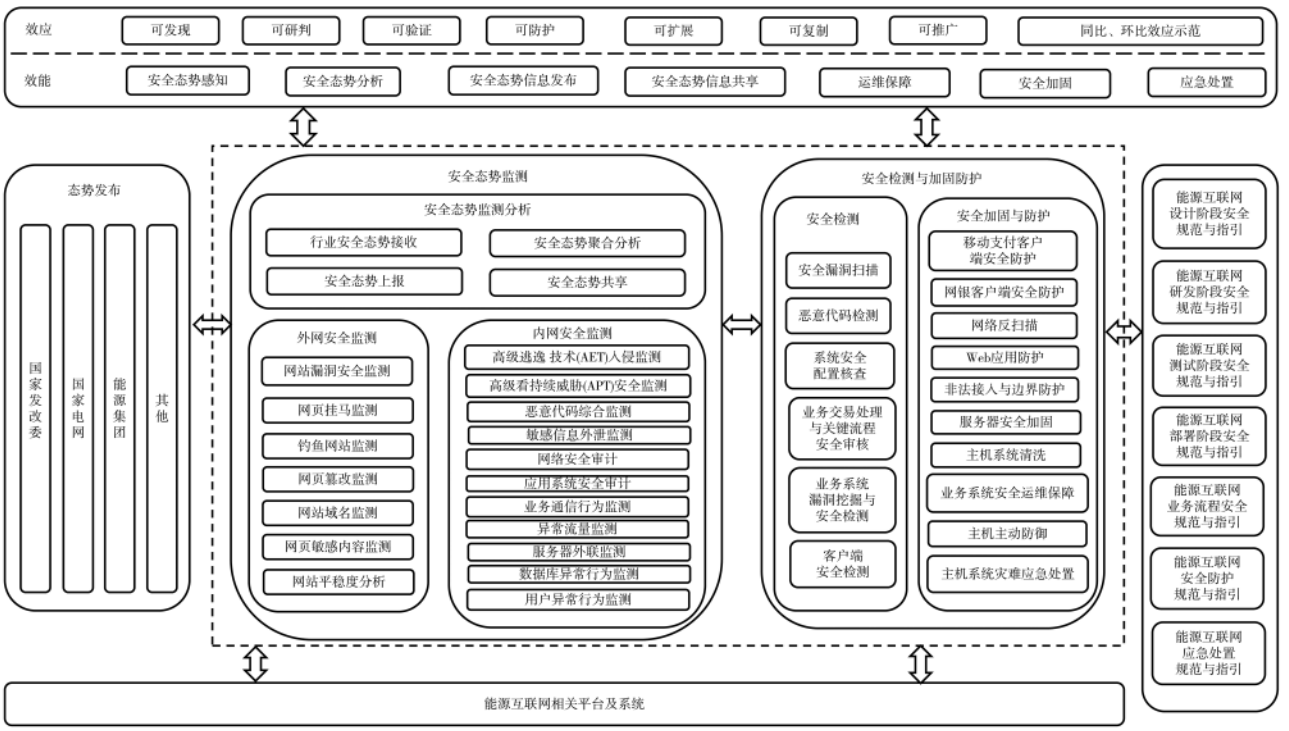

图 1 能源互联网安全体系

空关联，按相对重要性赋予权重；同时负责抽象及评定当前的安全状况并评估可能产生的影响。

(3)安全态势上报

安全态势监测分析系统将形成的安全态势报告上报给国家安全管部门，将能源互联网现状进行汇报并得到专业的指导。

(4)安全态势共享

将分析得出的安全态势报告在同行业进行分享，开展更多的交流学习。

2.2.2 外网安全监测

外网安全监测包含对能源互联网及门户系统网站漏洞安全监测、网页挂马监测、钓鱼网站监测、网页篡改监测、网站域名监测、网页敏感内容监测以及网站平稳度监测。外网监测架构如图3所示。

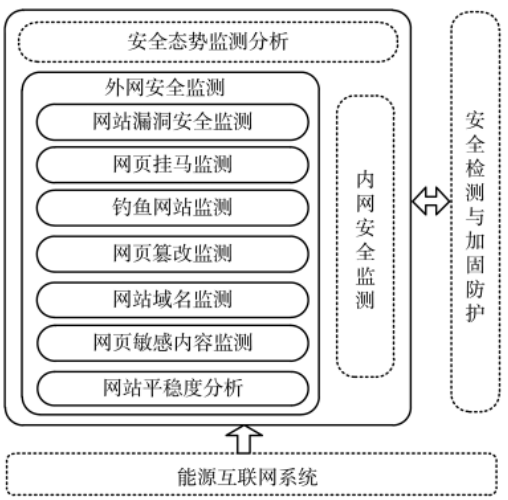

图3 外网安全监测架构图

(1)网站漏洞安全监测

网站漏洞安全监测系统是面向能源互联网的Web漏洞扫描产品，具备开放式Web应用程序安全项目(Open Web Application Security Project，OWASP)通用漏洞的高启发、高强度、交互式的监测能力。自动获取网站包含的所有资源，全面模拟网站访问的各种行为，比如按钮点击、鼠标移动、表单复杂填充等，通过内建的“安全模型”检测Web应用系统潜在的各种漏洞。

(2)网页挂马监测

网页挂马监测采用业内领先的智能挂马监测技术，高效、准确识别能源互联网网站页面中的恶意代码，使能源互联网管理员能够第一时间得知网站的安全状态，及时清除网页木马，避免给能源互联网客户带来安全威胁。

(3)钓鱼网站监测

钓鱼网站监测通过对域名进行500多种变形来监测针对防护目标站点的钓鱼网站，还可根据自定义的关键词组，持续对主流搜索引擎返回的搜索结果进行监测，防止钓鱼攻击者利用搜索引擎这种途径来传播钓鱼网站。另外，对过期域名持续监测，防止过期域名被钓鱼攻击者利用。一旦发现钓鱼网站，钓鱼网站监测系统第一时间作出告警，提供必要的信息，及时提醒识别钓鱼网站，以免用户上当受骗，从而保护用户利益及能源互联网网站品牌信誉。

(4)网页篡改监测

网页篡改监测远程实时监测能源互联网页面状况，学习站点页面正常变更阈值，变更一旦超过正常阈值，篡改监测系统立即进行告警行为。能源互联网管理员可参考网页篡改监测系统的安全建议及时修复被篡改页面，避免篡改事件影响扩散，给自身带来声誉和法律风险。

(5)网站域名监测

网站域名监测系统从运营商网络线路远程实时监测主流ISP的DNS缓存服务器和用户DNS授权服务器的可用性，以及它们对被监测域名的解析结果情况。一旦发现站点域名无法解析或解析不正确，第一时间做报警处理，然后协助恢复域名正常解析，避免域名不可用影响访问者体验，降低域名无法解析给自身造成经济损失。另外，针对网站DNS授权服务器，进行每周一次的DNS记录配置核查，包括：A记录、CNAME记录、NS记录、MX记录、SOA记录、PTR记录。

(6)网页敏感内容监测

网页敏感内容监测系统远程实时监测网站页面状况，在发现页面出现敏感关键词时第一时间发出告警，然后网站管理员可参考监测系统提供的安全建议及时删除敏感内容，避免事件影响扩散，给自身带来声誉和法律风险。能源互联网管理员可以自定义所关心的敏感关键词。

(7)网站平稳度监测

网站平稳度监测系统从运营商网络线路实时监测站点在多种网络协议下的响应速度、首页加载时间等反映网站性能状况的内容，一旦发现网站无法访问或者响应时间超过正常阈值，第一时间告警并提供优化网站性能的方案，避免网站业务中断或响应延迟给访问者带来不好的体验，甚至给自身造成经济损失。

2.2.3 内网安全监测

对能源互联网内网安全监测包括高级逃逸技术(AET)入侵监测、高级可持续威胁(APT)安全监测、恶意代码综合监测、敏感信息外泄监测、网络安全审计、应用系统安全审计、业务通信行为监测、异常流量监测、服务器外联监测、数据库异常行为监测以及用户异常行为监测。内网安全监测架构如图4所示。

(1)高级逃逸技术(AET)入侵监测

高级逃逸技术(Advanced Evasion Technique，AET)入侵监测系统实时监控能源互联网入侵行为，自动识别安全隐患，提供动态的、深度的、主动的安全防御，从智能识别、环境感知、行为分析三方面进行监测和防护。通过

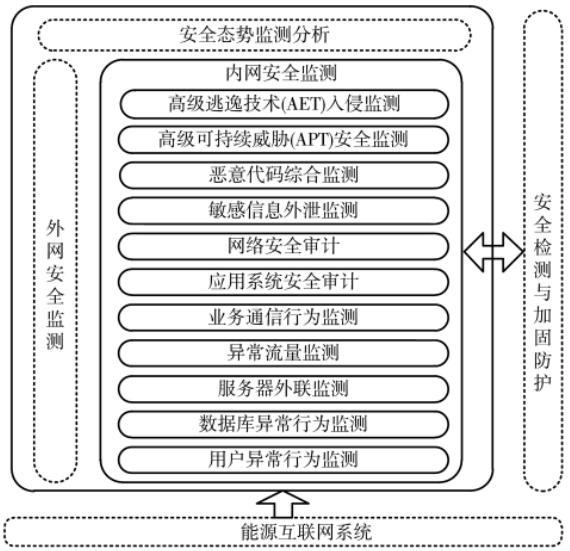

图 4　内网安全监测架构图

逃逸特征扫描，针对网络、传输、应用三个层面进行合规标准化检测，基于静态特征库逐一对数据包分析匹配，发现并阻断单一层面的逃逸；通过对网络层可疑数据包进行分片重组、对传输层可疑数据包进行协议栈解码、对应用层可疑数据包进行应用解码，同时对这三个层面的数据进行重组，通过采用正则表达式压缩算法，动态调整特征库，并进行组合逃逸的模式匹配，监控组合逃逸攻击。

(2)高级可持续威胁(APT)安全监测

高级可持续威胁(Advanced Persistent Threat，APT)安全监测目的在于针对高持续性威胁为能源互联网提供全方位的攻击防护。主要包括应用层攻击检监测、0Day攻击监测、未知木马监测、隐蔽木马链路分析、网络流量处理。APT 安全监测系统采用旁路监听/流量镜像模式，自动监听所在网络中的数据包，通过网络流量处理模块，将抓取的数据包根据规则进行归类，并通过相应的攻击检测模块同时采用攻击监测算法对数据包进行分析和处理，判断数据包中是否包含有网络攻击信息。

(3)恶意代码综合监测

恶意代码综合监测系统具有当前完备的恶意代码特征库(实时更新)和扫描算法，系统引擎对系统中执行的程序代码进行扫描，并利用特征库实现实时的恶意代码监控。

(4)敏感信息外泄监测

敏感信息外泄系统控制能源互联网内部的客户信息、客户密码、交易明细、重要公文等敏感信息通过互联网渠道泄漏。智能化、自动化、网络化、常态化监测计算机上的涉密文件，监测内容包括涉密信息文件名称、存储路径、使用人、IP 地址等。基于定义的策略和规则对电子邮件、论坛、微博、文库等进行过滤和监控，实现信息泄漏行为的审计取证，并提供事件统计分析及报表功能。

(5)网络安全审计

网络安全审计系统主要针对账号管理、访问控制以及操作安全进行审计，账号管理基于唯一身份标识的全局实名制管理，进行统一账号管理策略，实现与各服务器、网络设备、安全设备、数据库服务器等无缝连接；访问控制基于最小权限原则，细粒度地授权命令级权限；安全审计基于唯一身份标识，通过对用户从登录到退出的全程操作行为进行审计，监控用户对目标设备的所有敏感操作，聚焦关键事件，实现对安全事件的及时发现预警及准确可查。全面检查、审查和检验操作事件的环境及活动，发现能源互联网的网络异常行为及事件。

(6)应用系统安全审计

应用系统安全审计实现各类应用系统的操作过程审计，包括登录、查询、新增、修改、删除、统计以及导出操作行为的审计记录，以人为核心，审计为手段，对应用系统审计对象日志做实时监测，满足跟踪源头、取证等需求。

(7)业务通信行为监测

业务通信行为的监控涉及数据传输过程以及传输内容的安全性问题。主要针对传输数据的机密性和完整性、证书真实有效性、双向身份认证的安全性进行监测，防止在通信过程中遭到中间人攻击或破解，进而伪造身份获取敏感信息。

(8)异常流量监测

异常流量监测系统是一套基于流技术的网络流量分析系统，主要功能包括异常流量监测和流量统计分析，能够分析诸如 DDoS 流量、网络滥用误用、蠕虫爆发、P2P 流量等能源互联网网络中的异常流量。系统具备先进的基线生成算法以及丰富的流量异常检测算法。

(9)服务器外联监测

通过部署在主机的功能探针抓取网络数据包、各进程端口的实时信息以及相关的进程基本信息，从网络数据包中提取应用层协议的会话流，主要是针对 HTTP/HTTPS、SMTP 和 POP 协议端口所承载的数据进行分析，从中识别不符合协议规范的数据流，同时提取该会话所属进程的基本信息，以及该会话的远端 IP 的地理信息，形成报警信息。通过对数据包的应用层会话重组，然后再进行相应的应用层协议的分析，从中提取相应的信息，提供给规则匹配引擎，进行协议分析；对违规动作的发起进程、发起进程的用户组、权限等进行关联性分析；通过记录和分析系统内进程的活动信息，进行进程分析，为报警信息提供详尽的参数信息，为关联性分析提供依据。

(10)数据库异常行为监测

数据库异常行为监测针对行为主体身份、地点、操作方式及目标进行全面的监控。实时监控能源互联网数据库活动，对数据库活动进行细粒度审计的合规性管理。

采用基于可信基的数据库通信异常检测技术，首先通过对关键信息系统应用的分析，提取构建一个可信基库，形成一个“纯净”数据库通信的参数集合，即可信因子，可信基库实现对检测数据进行自动过滤、分析，可以有效地从大量的通信数据中提取关键数据检测的知识和规则，生成规则库，提高判别数据库通信中隐含的控制性风险的准确性；利用数据挖掘算法，自动建立用户访问关键数据的通信行为基线，将孤立点分析算法应用于用户行为基线，发现通信环境中异常的用户行为，对异常行为进行有效的控制；采用全局用户分析，各种要素组合关联的方式对真实的用户身份进行追踪锁定，通过定位到人可以使动态建模更加准确，更加精准地发现系统中的异常。通过实时记录、分析和汇报，达到事前规划预防，事中实时监视、违规行为告警，事后生成合规报告、事故追根溯源的效果。

(11)用户异常行为监测

用户异常行为监测系统通过分析用户使用网络的行为来获得用户行为模式、判定用户行为倾向、发现异常行为。用户异常行为监控系统架构如图 5 所示。

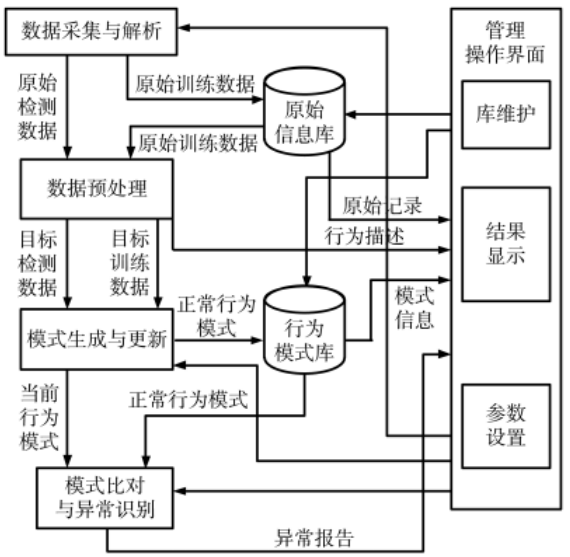

图 5 用户异常行为监控系统架构图

用户异常行为监控系统主要包括五个部分：数据采集与解析、数据预处理、模式生成与更新、模式比对与异常识别、管理操作界面。

数据采集与解析部分主要完成被监控用户的原始网络流量的获取，并根据设定的要求进行协议解析获得需要的用户网络访问原始信息；数据预处理部分是对上一部分解析出的用户行为信息进行关键属性的提取并且进行属性值分划工作，生成方便数据挖掘的目标数据集；模式生成与更新部分主要完成用户网络访问行为模式的生成、更新、管理以及维护；模式比对与异常识别部分主要完成用户当前访问行为模式与正常行为模式的比对，得出异常等级；管理操作界面负责完成模型中的参数设置、监听的结果显示、模式挖掘的结果显示、异常分析报告显示以及对数据库的管理和维护等工作。

2.3 安全加固与防护体系

及时对能源互联网进行安全加固及防护，一方面针对能源互联网客户端系统进行安全防护，另一方面针对服务器端及通信线路进行内网反扫描防护、Web 应用防护、非法接入与边界防护、服务器端加固、主机系统清洗、系统安全运维、主机主动防御以及灾难应急有效的处置。安全加固与防护的架构如图 6 所示。

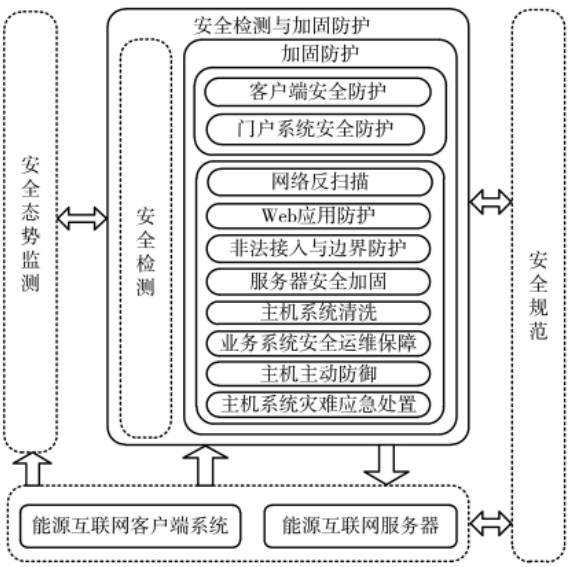

图 6 安全加固与防护架构图

(1)客户端及门户系统安全防护

针对客户端及门户系统进行安全检查，并根据检查结果优化策略(密码复杂度策略、登录策略等)设置参数，调整代码(防止反编译、密码软键盘、关键数据加密、敏感信息保存等)以及修复漏洞，并对用户进行安全意识的培训以及风险提示。

(2)网络反扫描

对目标系统的扫描，是入侵者进行攻击的第一步以用于收集信息。网络反扫描防护能源互联网系统受到普通扫描甚至是隐蔽性扫描，正确识别全连接扫描、半连接扫描、SYN 扫描、NULL 扫描、Xmas 扫描、Full 扫描等各种端口扫描，能够识别慢速扫描、间接扫描等特殊扫描等，避免泄露开放端口、系统版本等可被进一步利用的信息。

(3)Web 应用防护

Web 应用防护提供网站安全运维过程中的一系列控制手段，基于对 HTTP/HTTPS 流量的双向检测，为 Web 应用提供实时的防护。完整地解析 HTTP，包括报文头部、参数及载荷。支持各种 HTTP 编码(如 chunked encoding)以及各类字符集编码。提供严格的 HTTP 协议验证、

HTML 限制、全面的应用层规则以及会话防护机制。具备 response 过滤能力。

(4)非法接入与边界防护

防止非法接入很重要的因素是在网络边界建立可靠的安全防御措施，非法接入与边界防护子系统重点是防护与监控能源互联网系统网络边界安全问题，以认证、授权、审计等方式追踪用户的行为轨迹，对用户进行行为审计及合规性审计。监控网络边界控制访问与授权的一致性、以及授权的数据交换的安全性等问题。

(5)服务器安全加固

针对服务器的安全加固主要包括系统信息的核查(如系统维护级别、网络配置、补丁情况以及开放端口等)、账号安全(禁用无用账号、严格的口令策略等)、服务安全(关闭不必要的服务、检查 TCP Wapper 等)、网络参数合理性、文件系统安全性以及日志的全面审计。

(6)主机系统清洗

主机系统清洗的核心是做到系统的优化，尽可能地减少主机执行的进程，合理地更改工作模式，删除或禁用不必要的组件，优化文件位置使数据读写更快，减少不必要的系统加载项及启动项等，以预留出更多的系统资源供其他有用程序或用户支配。

(7)业务系统安全运维保障

针对能源互联网业务系统的基础设施，运维专员对其进行巡检等形式的日常维护，并对操作系统以上层级的应用进行压力测试，检测是否能够承受业务高峰期的数据处理。做到及时的版本更新以及安全补丁的更新。

(8)主机主动防御

能源互联网系统的主机承载着大量的数据处理及存储的功能，主机的自身防御是非常必要的。将主机中关键程序的行为控制在提前预设的流程中，最大程度减少关键程序行为异常导致的风险。通过监控主机中运行的关键程序行为，针对每个程序行为同预设规则进行比对，对于非预设行为进行安全阻断，实现对关键软件程序行为的控制。主机主动防御系统保护主机免受网络攻击，控制主机上的程序进行网络访问，未经授权的程序不允许访问网络，还可避免遭受开放端口扫描和利用开放端口进行攻击等一系列的攻击行为。

(9)主机系统灾难应急处置

建立与备份、恢复相关的容灾系统以及应急流程；明确对系统数据的备份方式、备份周期、存储介质以及保存期限等各方面内容；具备可执行的控制数据备份和恢复过程的程序，定期执行恢复程序，检测备份介质的有效性，确保在合理的时间内完成备份恢复；定期开展灾难恢复需求分析、策略及计划的制定、灾备系统建设及演练等工作，并根据实际情况对其进行分析和改进，确保各环节的正确性以及灾难恢复体系的有效性。

2.4 安全规范与指引

本文在建设能源互联网系统安全态势监控体系过程中，针对能源互联网各系统全生命周期各个阶段(设计、开发、测试、部署、运维)、安全检测与加固防护、等级保护等制定相应规范或操作规程，并在应用示范过程中进一步完善和推广。一系列安全规范与指引的建设，将规范能源互联网研发建设及应用过程中的安全要求，确保每一步的建设和操作都符合国家能源安全需求，如图7 所示。

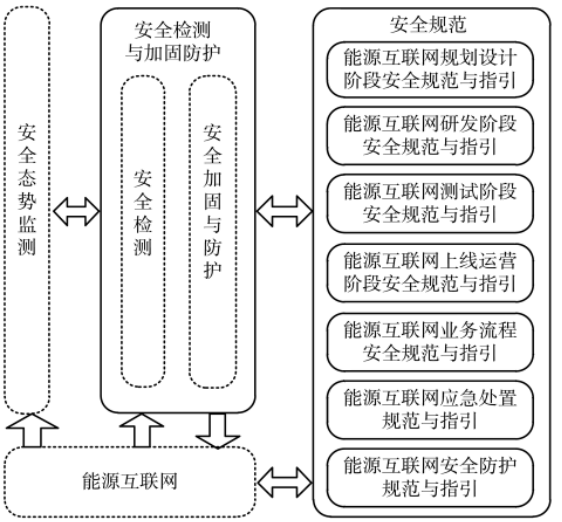

图 7 安全规范与指引

3 结论

文本首先介绍了能源互联网现状及安全需求，然后根据能源互联网安全需求研究能源互联网安全态势体系架构，并基于此架构研究能源互联网安全态势综合监测平台、安全架构与防护体系以及安全规范与操作指引三大类任务，并详细研究每个分项任务的主要技术内容，为能源互联网安全态势体系建设提供明确的指引与建设内容。未来，在完成能源互联网安全态势感知体系以后，基于此体系感知的安全情况，利用人工智能相关技术完成安全态势的评估与预测，为能源互联网安全态势发展情况提供明确的预判指引与防御建议，辅助管理员更好地做好能源互联网安全防御措施，从而更好地支撑能源互联网安全稳定运行。

参考文献

[1] 王海.建设国家能源工业互联网 助力“双碳”目标实现[J].电气时代，2022(1):20-21.

[2] 国家发展改革委，国家能源局，工业和信息化部.关于推进“互联网+”智慧能源发展的指导意见[J].城市燃气，2016(4):4-9.

[3] 油气设施、电网成网络攻击“重灾区”[DB/OL].[2022-07-11].https://finance.ifeng.com/c/8DzzK13WntB.

[4] 徐成，梁睿，程真何，等.面向能源互联网的智能配电网

(下转第 46 页)

[7] GAWER A, CUSUMANO M A. Industry platforms and ecosystem innovation[J]. Journal of Product Innovation Management, 2014, 31(3): 417-33.
[8] WANG Z, GUO C, GAO J, et al. Towards tracking the development process of the server ecosystems using open-source data[C]//27th Asia-Pacific Software Engineering Conference (APSEC). IEEE, 2020: 509-510.
[9] WANG Z, GUO C, FU Z, et al. Identifying the development trend of ARM-based server ecosystem using linux kernels[C]// 2020 IEEE International Conference on Progress in Informatics and Computing (PIC). IEEE, 2020: 284-288.
[10] ZHOU M, CHEN Q, MOCKUS A, et al. On the scalability of Linux kernel maintainers' work[C]//Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering, 2017: 27-37.
[11] ZHANG Y, ZHOU M, STOL K J, et al. How do companies collaborate in open source ecosystems? An empirical study of OpenStack[C]//2020 IEEE/ACM 42nd International Conference on Software Engineering (ICSE). IEEE, 2020: 1196-1208.
[12] TAN X, ZHOU M, FITZGERALD B. Scaling open source communities: an empirical study of the Linux kernel[C]// 2020 IEEE/ACM 42nd International Conference on Software Engineering (ICSE). IEEE, 2020: 1222-1234.
[13] 谢劲松, 符兴斌, 赵文辉. 面向信息产业发展的基础软硬件生态研究[J]. 信息技术与网络安全, 2020, 39(9): 1-5, 11.
[14] 陈硕颖, 杨扬. 我国基础软硬件产业的"生态"瓶颈及突破[J]. 经济纵横, 2018(11): 103-110.

(收稿日期: 2022-04-08)

作者简介:
张晓梨(1991-), 女, 硕士研究生, 工程师, 主要研究方向: 云计算、工业互联网、计算生态。
冯丹(1991-), 女, 硕士研究生, 工程师, 主要研究方向: 云计算、计算生态。
王卓耀(1987-), 通信作者, 男, 博士研究生, 助理研究员, 主要研究方向: 云计算、计算生态, E-mail: wangzhy01@pcl.ac.cn。

扫码下载电子文档

(上接第 39 页)

安全态势感知[J]. 电力自动化设备, 2016, 36(6): 13-18.
[5] 田世明, 栾文鹏, 张东霞, 等. 能源互联网技术形态与关键技术[J]. 中国电机工程学报, 2015, 35(14): 3482-3494.
[6] 刘增明, 崔雪璐, 马靖, 等. 基于零信任框架的能源互联网安全防护架构设计[J]. 电力信息与通信技术, 2020, 18(3): 15-20.
[7] 别朝红, 王旭, 胡源. 能源互联网规划研究综述及展望[J]. 中国电机工程学报, 2017, 37(22): 6445-6462, 6757.
[8] 严太山, 程浩忠, 曾平良, 等. 能源互联网体系架构及关键技术[J]. 电网技术, 2016, 40(1): 105-113.
[9] 王继业, 孟坤, 曹军威, 等. 能源互联网信息技术研究综述[J]. 计算机研究与发展, 2015, 52(5): 1109-1126.
[10] 王继业, 郭经红, 曹军威, 等. 能源互联网信息通信关键技术综述[J]. 智能电网, 2015, 3(6): 473-485.
[11] 丁一, 江艺宝, 宋永华, 等. 能源互联网风险评估研究综述(一): 物理层面[J]. 中国电机工程学报, 2016, 36(14): 3806-3817.
[12] 江艺宝, 宋永华, 丁一, 等. 能源互联网风险评估研究综述(二)——信息及市场层面[J]. 中国电机工程学报, 2016, 36(15): 4023-4034.
[13] 刘增明, 崔雪璐, 马靖, 等. 基于零信任框架的能源互联网安全防护架构设计[J]. 电力信息与通信技术, 2020, 18(3): 6.
[14] 魏峰, 张驯. 能源互联网信息安全技术管控新模式探究[J]. 华电技术, 2021, 43(2): 53-59.
[15] 王继业, 刘道伟, 马世英, 等. 信息驱动的全球能源互联网全景安全防御系统[J]. 电力信息与通信技术, 2016, 14(3): 13-19.
[16] 张向宏, 苏禹. 能源互联网及其安全防护体系建设研究[J]. 微型机与应用, 2015, 34(9): 8.
[17] 郑善奇, 王鸥, 张靖欣, 等. 能源互联网及其安全防护体系建设研究[C]//2016 智能城市与信息化建设国际学术交流研讨会论文集 I, 2016: 106.

(收稿日期: 2022-07-11)

作者简介:
徐琳(1977-), 男, 硕士, 工程师, 主要研究方向: 工业互联网、计算机科学、信息安全。
张宏雷(1984-), 男, 本科, 主要研究方向: 信息安全。

扫码下载电子文档

版权声明