2022年度江苏省科学技术奖提名项目公示内容

项目名称：电力网络实战化深度攻防对抗关键技术及应用

主要完成单位:国网江苏省电力有限公司、南京南瑞信息通信科技有限公司、南京工业职业技术大学、南京理工大学

主要完成人:张明明、侯君、夏飞、袁国泉、赵新建、郭靓、徐磊、张波、赵然、金倩倩、徐建

项目简介：

1．主要技术内容

本项目针对海量电力资产漏洞高效精准挖掘难度大、高级定制化电网攻击监测感知技术复杂、数据攻击防御与协同处置技术缺乏等实战挑战，依托“产学研用”协同创新模式，突破了**红队未知漏洞安全检测、蓝队未知攻击监测、红蓝联动防御反制**等关键技术、操作流程及处置方法，自主研制出系列化国际领先的红蓝队装备，形成以下三项重大创新：

（1）创新提出了电网海量异构资产轻量无损安全检测技术。提出基于群体上下文异常（Contextual Collective Anomaly）的电力终端漏洞智能检测方法，设计了灵活、分布式的三阶段多数据流异常识别框架，实现了电力专用协议漏洞挖掘、电力系统漏洞轻量无损渗透验证等技术，研制了业界领先的全环节红队漏洞检测工具，获得信息安全风险评估服务一级资质。已经挖掘4367个首发漏洞，漏洞自主发现和整改率提升3倍，漏洞通报率下降70%，漏洞挖掘水平央企第一。

（2）攻克了电网业务全流量网络安全实时监测分析技术难题。提出了基于 Trouble Ticket和电力业务特征分析的全流量实时安全监测技术，实现了电力异常行为监测、专用通信协议畸形报文监测、敏感数据全生命周期安全监测等专项监测技术，将专家推荐的问题有效转化为有向图的搜索问题，安全监测性能提升6倍以上。先后研判、发布重大网络安全事件736条，填补了高级定制化电网攻击监测技术空白。

（3）提出了基于联动防御与威慑反制的电网红蓝对抗技术。提出了以零关停为前提的电网数据安全联动防御技术。提出了基于填充的加密数据库加固方案和可搜索加密技术，有效抵御近年来出现的纷繁多样的数据安全攻击手段。发明了基于定制化蜜罐的电力攻击诱捕反制方法，实现红蓝队协同、精准化攻击防御对抗。已实现封锁高危攻击源256个，累计成功应对攻击35.3万余次，向国家上报网络安全保障情况52件，助力国网在护网行动中连续三年列为全国第一。

2．授权知识产权情况

项目技术为公司自主研发，拥有自主知识产权。已拥有授权专利 24 件，论文论著 19件，软著5件（NARI安全编排与自动化响应平台软件、NARI网络安全监测系统软件v2.0.0、NARI网络安全监控预警平台软件、NARI网络安全设备策略管理软件、主动防御平台1.0）。

3．与当前国内外同类研究、同类技术的综合比较

项目基于上述创新技术，研制的基于全场景网络安全态势感知平台（S6000）集成了上述红队未知漏洞安全检测、蓝队未知攻击监测、零关停的红蓝联动防御反制工具，本项目与国内外相关研究水平比较情况如下表所示。

表 1 主要功能参数、技术指标与国内外对比表

技术	比较项	本成果技术	本领域国内外技术水平
红队未知漏洞安全检测	**电力专有漏洞挖掘能力**	发掘电力首发漏洞 4367 个；国内外首个电力专有漏洞库	不具备电力专有漏洞挖掘能力；缺乏电力专有漏洞库
	电力工控协议漏洞自动化挖掘能力	打破了国外智能设备协议漏洞挖掘技术壁垒，协议漏洞覆盖率 65%	芬兰科诺康 Defensic：38% 美国 GE 阿基里斯 Achilles：52%
	电力网络漏洞检测	漏洞挖掘路径自动化生成成功率 95%	绿盟 RSAS，IBM APPSCAN：漏洞挖掘路径自动化生成成功率 62%
蓝队未知攻击监测	**网络协议适配度**	支持传统网络协议和电力专有协议攻击监测	仅支持传统网络协议
	攻防场景可定制化程度	支持可编排的适应性网络攻击实时监测	仅支持固定场景的安全监测
	网络安全实时监测速率	182.08 万条/分钟	启明星辰 IDS 等监测产品：128.69 万条/分钟
零关停的红蓝联动防御反制	**联动防御策略灵活度**	支持 77 种数据采集策略、169 种攻击监测策略、64 种联动防御策略的组合。	仅支持固定场景的联动策略
	威慑反制能力	预设 3 类反制场景，8 种反制措施，可实现对攻击者的威慑、拒止和反向控制。	仅支持基于蜜罐的信息收集
	自动化响应延时	<1 秒	<3 秒

4．应用推广及效益情况

项目成果已在国网江苏电力成功应用，并推广至国家电网公司总部及其余 26 家省级电力公司，国网江苏信通、新疆、天津、湖南电力在应用证明中分别提到项目应用基于自动推理机的电力专用协议漏洞高效挖掘、电力系统漏洞轻量无损渗透验证技术，挖掘 4376 个首发漏洞，漏洞自主发现和整改率提升 3 倍；项目攻克了电网业务全流量网络安全实时监测分析技术难题，安全监测性能提升 6 倍以上，研判发布重大网络安全事件 736 条，填补了高级定制化电网攻击监测技术空白；项目提出基于区块链和虚拟化技术的信息安全攻防演练和攻

击过程立体还原的方法，融合了网络离线漏洞库、知识库搜索库、模拟数据仿真的攻防演练平台。培养了红蓝队尖兵队员 30 余人。

多家应用单位认为本项目漏洞挖掘能力达到国际先进水平，已经实现了对以色列 JSOF、思科、AppliedRisk、德国 TUV 等产品的有效替代，填补了高级定制化电网攻击监测技术的空白，性能与对华禁运的 Fortinet、Okta 等对应技术相当。

专利:

[1]夏飞;周静;王毅;张立强;余伟;吴立斌;张明明;李鹏;季晓凯;蒋铮;王艳青;彭轼;魏桂臣;丁一新;张利;李萌;黄高攀;汤雷.一种蜜罐构造方法及系统.中国：ZL201710202686.6,2020-06-23

[2]夏飞;黄高攀;李萌;宋浒.一种电网高级持续性威胁检测装置.中国：ZL201520859871.9,2016-05-18

[3]刘嘉华; 陈龙; 夏飞; 袁国泉; 周晨曦; 万明; 唐海荣; 孙峰.一种网络事件关联分析和动态预警方法.中国：ZL201410752102.9,2017-08-04

[4]于晓文;陈春霖;赵俊峰;林学峰;金倩倩;姜帆;郭靓;李斌斌;廖鹏;刘剑;夏元轶.基于深度学习和 agent 的联动防御系统.中国：ZL201810554158.1,2019-05-24

[5]俞皓;刘莹;汪玲敏;郭靓;李炜键;刘剑;屠正伟;洪昊;蒋甜;刘强;夏元轶;贾雪;于晓文.一种基于隐马尔可夫模型的电力用户行为深度分析方法.中国：ZL201810496364.1,2019-05-24

[6]廖鹏;夏元轶;郭靓;于晓文;金倩倩;蒋甜;张骞;李炜键;赵俊峰.一种基于深度学习的网络流量协议识别方法.中国：ZL201710779641.5,2018-02-09

[7]张明明;夏元轶;冒佳明;赵俊峰;夏飞;范;良杰，胡俊;邵志鹏;陈牧.基于 PUF 和 CPK 算法的物联网设备身份认证方法、系统及存储介质.中国：ZL202011146373.1,2021-01-26

[8]李千目;侯君;张子辰.一种基于 LSTM 的网络流量预测方法.中国：ZL201810845915.0,2018-07-27

[9]张明明;赵俊峰;夏飞;冒佳明;夏元轶;赵然;许良杰;杨允志;陈牧;陈璐.基于区块链的设备接入认证系统及方法.中国：ZL202011192170.6,2021-07-30

[10]徐建;黄东东;张宏; 李涛; 李千目;张琨; 陈龙; 范志凯; 许福.同构环境下计算节点异常检测方法.中国：ZL201410764758.2,2017-12-12

代表性论文：

[1]标准模型下格上固定长度消息签名方案/南京理工大学学报(自然科学版)/汪洁洁, 许春根, 徐磊, 张星，2015 年 5 卷 566-570 页

[2]云存储上高效安全的数据检索方案/密码学报/徐磊, 许春根, 蔚晓玲，2016 年 3 (4)卷 330-339 页

[3]Trouble Ticket Routing Models and Their Applications / IEEE Transactions on Network and Service Management（Top 期刊） /Jian Xu, Rouying He, Wubai Zhou, Tao Li，2018 年 2

卷 530-543 页

[4]Signature based trouble ticket classification /Future Generation Computer Systems（Top 期刊）/Jian Xu, Hang Zhang, Wubai Zhou, Rouying He, Tao Li，2018 年 1 卷 41-58 页

[5]Hardening Database Padding for Searchable Encryption /International Conference on Computer Communication (IEEE INFOCOM 2019, Top 会议) /Lei Xu, Xingliang Yuan, Cong Wang, Qian Wang, ChungenXu,2019 年 4 卷 2503-2511 页