

第十六届全国大学生信息安全竞赛—作品赛

决赛作品获奖名单

一等奖（44项）

作品名称	学校名称	奖项级别
AndroFuzz-面向安卓 Native 系统服务的漏洞挖掘技术	海南大学	一等奖
AntiFraud-Ethe: 区块链欺诈行为时序动态检测与追踪系统	武汉大学	一等奖
authentchain——基于 SIFT 和区块链的图像确权和可信交易系统	西安电子科技大学	一等奖
ChatGPT 虚假文本检测系统	湖北工业大学	一等奖
DNN-Shield: 一种支持异构神经网络加速器的 DNN 隐私保护训练框架	清华大学	一等奖
GPoC——基于 GLM 的网络犯罪团伙画像	哈尔滨工业大学(威海)	一等奖
GraphMapper: 基于异构攻击图对抗分析的数据安全保险定价系统	浙江大学	一等奖
GuardShield——分布式防护设备有效性验证系统	广州大学	一等奖
ImageShield-基于 Lab 色彩空间的 DeepFake 主动防御系统	武汉大学	一等奖
MiniDroid: 移动端小程序隐私政策与权限调用一致性检测系统	西安电子科技大学	一等奖
MuLPay: 基于格的高效后量子安全区块链钱包系统	山东大学	一等奖
Ps-CTR: 一种支持隐私保护的可靠 CTR 联邦预测方法	北京工业大学	一等奖
RSAC: 高性能无感知的 HTTPS 加密流量还原系统	国防科技大学	一等奖
SecurePulse: 基于全同态卷积神经网络的远程 PPG 信号身份认证系统	中国地质大学(武汉)	一等奖
ShieldFL-面向联邦学习的投毒检测防御系统	西安电子科技大学	一等奖
Vigilum 助手: 面向移动应用误导界面的智能提示及防范系统	中山大学	一等奖
Watchout! - 基于模糊测试的自动驾驶功能安全测试系统	西安电子科技大学	一等奖
WhisperRec——基于高效非平衡 PCSI 的隐私化社交推荐系统	北京航空航天大学	一等奖
白泽智驾——无人驾驶预期功能安全测评平台	复旦大学	一等奖
蝠音寻踪: 基于反向散射的非侵入式无线窃听窃照检测系统	北京航空航天大学	一等奖
国密 SM4 算法高性能实现及安全应用	北京航空航天大学	一等奖
呼神护卫 EPV——实时抗 ASR 语音识别隐私保护系统	武汉大学	一等奖
基于 Att-BiLSTM 的命令注入漏洞检测技术	南京邮电大学	一等奖
基于 DMA 的恶意代码分析取证系统	武汉大学	一等奖
基于 SM9 认证实时流量的 RPi 和 MN-CNN 模型 IDS 分析系统	中国人民解放军海军工程大学	一等奖
基于 TrustZone-M 函数级内存地址空间随机化的可信实时系统	东南大学	一等奖
基于安全多方计算的云服务密钥保护机制	北京航空航天大学	一等奖
基于触屏行为生理特征融合的持续身份认证系统	华中科技大学	一等奖
基于可逆神经网络轻量化图像隐写软件	中国人民武装警察部队工程大学	一等奖
基于密文域可逆信息隐藏的联邦学习安全聚合认证分析系统	中国人民武装警察部队工程大学	一等奖

基于注意力机制的智能语音伪造攻击检测系统	华中科技大学	一等奖
可解释机器学习在安全中的评估平台	浙江大学	一等奖
“利剑”——融合免杀与流量混淆的远程终端控制软件研究与实现	江苏大学	一等奖
量子蔷薇：基于后量子密码算法的固件认证优化方案	山东大学	一等奖
蜜云——多云存储的蜜口令管理器	南开大学	一等奖
“模估云”：机器学习即服务平台模型类型泄露风险检测系统	西安电子科技大学	一等奖
平安源——基于零知识证明和异步拜占庭共识的区块链源代码平台	北京工业大学	一等奖
声影探真：基于微多普勒效应的多模态活体检测系统	武汉大学	一等奖
丝路安——基于零知识证明的区块链跨境贸易平台	北京航空航天大学	一等奖
图像“保险箱”：基于安全交互设备和感知器网络的量子图像加密系统	海南大学	一等奖
“雾里看花”——基于联邦学习与频域变换的多方隐私保护人脸识别系统	哈尔滨工业大学	一等奖
星罗宙合：面向 AI 大模型的安全且可扩展分片区块链联邦学习系统	北京航空航天大学	一等奖
医链网 HealNet——安全可信的跨链医疗保险系统	电子科技大学	一等奖
增强医疗诊断模型的链上可验证联邦学习系统	北京理工大学	一等奖

二等奖（66 项）

作品名称	学校名称	奖项级别
AP-Sentinel: 基于融合指纹特征的伪 AP 攻击检测及防御系统	东南大学	二等奖
“CLAWS”——面向办公套件的文件多通道备份管理系统	哈尔滨工业大学	二等奖
CNCG——面向云原生应用的配置安全评估系统	西安电子科技大学	二等奖
CryptoVote: 基于隐私集合求交的安全匿名投票系统	电子科技大学	二等奖
CRYSTALS-Kyber 误用检测软件包	上海交通大学	二等奖
CTFCrackTools	珠海科技学院	二等奖
EyeSpy: 针对无人机人员追踪的物理域对抗方案	西安电子科技大学	二等奖
FraudHunter: 涉诈信息实时感知与溯源系统	四川大学	二等奖
GLM Guardian——生成式语言模型版权保护平台	上海交通大学	二等奖
GPSCatcher: 基于 EMR 信号的隐藏 GPS 探测系统	湖南大学	二等奖
HoneyMIGP——自监测口令泄露查询系统	南开大学	二等奖
InVehicle-IDS: 基于电压指纹的车内网络入侵检测系统	东北大学	二等奖
IoTMonitor——基于全同态加密的智能物联网设备密文异常检测系统	西安电子科技大学	二等奖
IoTVulExcavator: 开源物联网操作系统漏洞检测平台	华中科技大学	二等奖

IPv6 地址高效智能扫描系统	国防科技大学	二等奖
MINI-SEC: 场景驱动的小程序隐私合规检测系统	复旦大学	二等奖
N@ne: 面向公共场所人员流动的隐私认证系统	沈阳工业大学(中央校区)	二等奖
PrivateReading: 保护隐私的智慧阅读助手	安徽大学	二等奖
RealFace: 高可用性 Deepfake 人脸伪造检测系统	中南大学	二等奖
RF-Keyboard: 基于 RFID 标签阵列的身份认证系统	浙江工业大学	二等奖
SecVoice-基于活体检测的声纹认证系统	电子科技大学	二等奖
SEMRA: 云场景下层次化细粒度授权的多用户可搜索加密系统	武汉大学	二等奖
SpufTu: 一种基于 SRAM PUF 的轻量级物联网安全认证系统	国防科技大学	二等奖
Tamer: 面向代码安全的细粒度克隆代码检测系统	华中科技大学	二等奖
阿尔戈斯之瞳: 基于空中集群的无人机防窥定位系统	西北工业大学	二等奖
出行安——基于链上联邦学习的分心驾驶行为联合识别与预警系统	中国人民解放军战略支援部队信息工程大学	二等奖
飞星传件: 面向中小文件的便携式高速隔离传输系统	国防科技大学	二等奖
国密算法 IP 的软硬件协同设计	广东工业大学	二等奖
基于 AI 大模型的高性能智能合约漏洞检测系统	天津理工大学	二等奖
基于 GPT 的离线式口令强度判定器	上海交通大学	二等奖
基于多方隐私求交的医疗大数据安全联邦统计分析平台	中国科学技术大学	二等奖
基于后量子隐私增强保护的电动汽车充电认证方案	山东大学	二等奖
基于联盟链的多权威医疗数据共享系统	东北大学	二等奖
基于麦克风阵列和反射声波成像的身份认证系统	电子科技大学	二等奖
基于嵌入式消息认证码的无人机低通信量安全认证系统	中国人民武装警察部队工程大学	二等奖
基于区块链的零信任安全防护系统	中国人民解放军战略支援部队信息工程大学	二等奖
基于区块链的以太坊地址身份推断系统	南京信息工程大学	二等奖
基于群体认知的虚假新闻智能分析与传播抑制系统	中国人民解放军战略支援部队信息工程大学	二等奖
基于射频指纹特征模糊提取的设备认证系统	上海交通大学	二等奖
基于深度学习的虚假新闻检测系统	中国科学技术大学	二等奖
基于同态加密的非交互式 DBSCAN 聚类隐私保护方案	南开大学	二等奖
基于威胁情报分析的 APT 攻击组织研判系统	北京邮电大学	二等奖
基于物理后门技术的人脸识别模型版权保护	国防科技大学电子对抗学院	二等奖
基于行为指纹的数据归属权鉴别	哈尔滨工业大学	二等奖

见微知著——基于深度学习的抗局部屏摄水印系统	湖南大学	二等奖
开源软件的软件供应链安全保护系统	杭州电子科技大学	二等奖
开源软件溯源与风险检测系统	中山大学	二等奖
抗干扰攻击的自定义隐私保护交通检测系统	合肥工业大学	二等奖
抗投毒攻击的金融风控联邦学习系统	中国科学技术大学	二等奖
密盾：面向移动终端的多模态敏感信息主被动感知与防护系统	哈尔滨工业大学	二等奖
面向人机交互的可视化模糊测试平台	东南大学	二等奖
面向桌面安全的防盜摄主动防御和泄密溯源算法与平台	浙江工商大学	二等奖
内存取证与图模型结合的恶意软件检测与分析系统	北京邮电大学	二等奖
屏隐慧盾：主被动结合的屏幕防拍照泄密溯源系统	武汉大学	二等奖
守望之门——基于生物信息对比的无存储群辨证卡系统	国防科技大学电子对抗学院	二等奖
戍卫尖兵-高安全交互式小型 AIoT 智慧战车	中国人民解放军战略支援部队信息工程大学	二等奖
双重博弈：面向对抗样本演示攻击的生物指纹识别系统	东南大学	二等奖
威胁情报增强的安全策略编排与智能响应系统	中国人民解放军战略支援部队信息工程大学	二等奖
闲停信泊——基于区块链的隐私保护智能泊车系统	北京航空航天大学	二等奖
信创卫士——基于深度学习的恶意代码检测模型及其在信创环境下的实现	上海交通大学	二等奖
一种基于网络测绘的 LED 显示屏监护平台	湘潭大学	二等奖
隐私保护的 topk 轨迹相似性查询系统及应用	电子科技大学	二等奖
硬件设计安全性和可测性可视化分析系统	西北工业大学	二等奖
支持立体隐私安全的区块链电子发票系统	南开大学	二等奖
支持密态搜索的属性赋权医疗数据管理系统	中国科学技术大学	二等奖
智链通——基于区块链的跨应用账号管理系统	北京航空航天大学	二等奖

三等奖（88 支）

作品名称	学校名称	奖项级别
AncientOne: 面向深暗网的威胁人物信息挖掘与分析系统	北京邮电大学	三等奖
APTShield: 融合语义化内核日志压缩的 APT 攻击链高效追踪系统	浙江工业大学	三等奖
Aware+Fuzz: 一种 RISC-V 架构下基于数据预取机制的缓存侧信道攻击防御方案	东南大学	三等奖
BCTracking: 基于图卷积神经网络的区块链匿名交易追踪系统	江苏大学	三等奖
BLE-Fuzz: 低功耗蓝牙模块模糊测试工具	东北大学	三等奖

EFTNet——基于环境特征迁移的活体检测算法设计与实现	武汉理工	三等奖
GAN-LLM: 基于 GAN 生成数据的大模型隐私保护	浙江大学	三等奖
HNS-非区块链依赖的去中心化云安全存储系统	合肥学院	三等奖
Homomorphix 信链 ——基于区块链的身份认证 技术与数据治理服务方案	北京理工大学	三等奖
LocAnon: 隐私感知近邻检索与距离计算平台	山东大学	三等奖
Mitten: 多用户场景下健壮的实用密文检索系统	华中科技大学	三等奖
NetGuardian: 基于时序卷积神经网络的恶意流量检测平台	江苏大学	三等奖
OfficeShield:面向远程办公场景的泄密风险感知与防护溯源系统	四川大学	三等奖
PrivacyPilot:基于隐私政策解析的 APP 实时隐私泄露风险提示系统	中山大学	三等奖
Robot Eye: 面向 ROS 的网络安全测试系统	西北工业大学	三等奖
SafeMedNet: 基于区块链的医疗资源访问控制系统	电子科技大学	三等奖
SAFR——基于频域差分隐私的安全人脸识别系统	合肥工业大学	三等奖
SecFace: 基于 EzPC 的轻量级隐私保护人脸识别系统	国防科技大学	三等奖
SecNLP: 一种高隐蔽性的 NLP 模型版权保护框架	海南大学	三等奖
SeTPC: 基于深度学习的 IoT 固件中第三方组件漏洞检测系统	上海交通大学	三等奖
“安管” ——基于跨模态学习的深度伪造诈骗防护系统	郑州大学	三等奖
安翼——诈骗网址检测及防范系统	杭州电子科技大学	三等奖
波达信至——低时延强安全空口接入识别系统	东南大学	三等奖
车载 CAN 总线异常检测	湖北大学	三等奖
“传音入密” ——智能网联汽车属性基加密安全通信系统	江苏大学	三等奖
大规模 P2P 僵尸网络主动探测及画像测绘系统	西北工业大学	三等奖
谛听: 深度伪造音频检测	大连理工大学	三等奖
电子数据取证分析系统	郑州警察学院	三等奖
反诈指挥所——电诈资源库与反诈宣传推荐系统	江苏警官学院	三等奖
分布式数字身份双因子认证协议的设计与实现	北京邮电大学	三等奖
辅助之手--基于 SM4 和 k-hidden 加密算法的医疗数据管理审计系统	武汉理工大学	三等奖
光印防控--基于机器学习和红外线干扰的防拍照系统	中南大学	三等奖
后量子时代的 PGP	山东大学	三等奖
基于“一次一密”的轻量级空口安全传输系统	东南大学	三等奖
基于 ABY3-VSSS 的安全隐私密码管理系统	南开大学	三等奖
基于 go-cqhttp 的社交平台反诈风控机器人	大连理工大学	三等奖
基于 HMI 映射与四方矩阵编码的图像加密	安徽理工大学	三等奖

基于 PACS 和联邦学习隐私保护的医学影像分割系统	华中科技大学	三等奖
基于 Transformer 的双通道视频鉴伪系统	安徽大学	三等奖
基于残差神经网络的暗网流量分类识别系统	齐鲁工业大学	三等奖
基于高交互性蜜罐的网络威胁管理系统	北京邮电大学	三等奖
基于格上可搜索加密与零信任的数字版权监管系统	北方工业大学	三等奖
基于攻击组织基因的恶意代码同源性分析系统	北京邮电大学	三等奖
基于混合图神经网络的源码漏洞检测系统	北京工业大学	三等奖
基于集成学习权限分析的安卓应用风险管理系统	哈尔滨工业大学	三等奖
基于联盟链联邦学习的智能医疗远程健康管理系统	中国人民解放军战略支援部队信息工程大学	三等奖
基于零知识证明的可授权隐私查询系统	北京交通大学	三等奖
基于零知识证明的可追踪可撤销属性匿名凭证系统	哈尔滨工业大学(深圳)	三等奖
基于拟态防护的物联网身份认证系统	北京电子科技学院	三等奖
基于强隐私保护联邦知识网络的人物异常关系检测系统	北京交通大学	三等奖
基于区块链的众包版权泄露捕捉与溯源系统	中国科学技术大学	三等奖
基于设备指纹的安卓沙箱/模拟器检测技术	电子科技大学	三等奖
基于射频指纹识别的无线设备身份认证算法与系统	南昌大学	三等奖
基于深度残差胶囊网络的鲁棒加密流量识别系统	国防科技大学	三等奖
基于深度学习的多模式步态识别身份认证系统	北方工业大学	三等奖
基于深度学习隐写技术的多模态信息暗水印	南京工业大学	三等奖
基于树莓派得动态感知系统	北京信息科技大学	三等奖
基于遗忘机制的否定选择算法在入侵检测中的研究与应用	湖北大学	三等奖
基于隐私集合求交的跨平台好友推荐	哈尔滨工业大学(深圳)	三等奖
兼具隐私保护和监管的电力交易平台	杭州电子科技大学	三等奖
鉴安瞳: 安卓伪冒应用智能监测分析系统	四川大学	三等奖
抗量子密码密文域的情报传输系统的设计与实现	暨南大学	三等奖
链安卫士——区块链多层次风险识别与异常检测系统	北京理工大学	三等奖
链鉴: 基于置信学习的区块链智能合约细粒度漏洞检测系统	海南大学	三等奖
灵犀医链-基于 FISCO BCOS 国产联盟链三元医疗联动系统	江西师范大学	三等奖
零信任环境中基于层级属性密码与区块链的身份管理系统	复旦大学	三等奖
面向 UGC 模式的数字作品版权保护与服务平台	杭州电子科技大学	三等奖
面向安卓平台的应用程序隐私合规检测	上海交通大学	三等奖
面向多场景多类型的 DDoS 攻击检测系统	苏州大学	三等奖
面向金融交易的异常账号检测及层次划分系统	哈尔滨工业大学(威海)	三等奖

面向密码算法的多终端伽罗瓦域计算器	中国民航大学	三等奖
面向区块链数字代币的欺诈检测和欺诈团伙溯源系统	华中科技大学	三等奖
面向图像内容理解的 ROI 加密系统	东北大学	三等奖
面向移动智能终端的漏洞检测与修复系统	华北电力大学（北京校区）	三等奖
屏痕追溯——基于屏摄鲁棒性与隐蔽 QR 码的屏摄溯源系统	国防科技大学电子对抗学院	三等奖
“期零寺”——基于联邦学习的分层垃圾邮件检测系统	哈尔滨工业大学	三等奖
企业网络资产暴露面探测系统	哈尔滨工业大学(威海)	三等奖
“神郁”——基于国密 SM2 数字签名算法的双因子身份认证系统	西北工业大学	三等奖
视真-基于痕迹增强的双流深度视频修复检测系统	杭州电子科技大学	三等奖
天罡——基于自研加密算法的北斗全球定位系统与高精度时钟局域网涉密机构加密装置	新疆大学	三等奖
芯片非可控 IP 软核硬件木马安全检测	国防科技大学信息通信学院	三等奖
寻隐者——基于深度鲁棒水印的屏摄内容保护系统	上海理工大学	三等奖
“一码智行”——车-场协同自主代客泊车定位导引系统	江苏大学	三等奖
一种基于符号内存及二维帐篷混沌映射的抗逆向分析系统	常熟理工学院	三等奖
音隐悍将：面向在线场景的说话人匿名保护系统	浙江大学	三等奖
支持多方共享的视频隐私信息遮蔽研究	浙江理工大学	三等奖
知云破晓——云服务软件供应链漏洞治理系统	复旦大学	三等奖
智慧城市背景下基于 IoT 安全网关的智能井盖综合监控系统	北方工业大学	三等奖

优胜奖（110 支）

作品名称	学校名称	奖项级别
AdvPPMLS: 基于对抗扰动的机器学习隐私保护系统	成都信息工程大学	优胜奖
AudioGuard——音频对抗样本自动化检测系统	山东大学	优胜奖
Auto-hunter: 基于自适应残差网络的 Android 恶意软件检测系统	江苏大学	优胜奖
BloomGuard——轻量级的移动群感隐私保护系统	湘潭大学	优胜奖
DeepScan: 恶意代码深度检测系统	安徽大学	优胜奖
EVMFirewall: 基于细粒度访问控制策略的智能合约安全执行系统	浙江工业大学	优胜奖
FilmProtector——面向短视频平台的新型影视侵权行为检测与溯源系统	四川大学	优胜奖
FlowGuard: 面向 TCP/UDP 流量的网络传输管控系统	北京邮电大学	优胜奖
Fortress: 基于无线流量填充的智能家居隐私保护平台	四川大学	优胜奖

ICatchYOU: 基于关键区域识别的高效局部对抗样本检测机制	浙江工业大学	优胜奖
InScan—主机安全测绘平台	湖南信息学院	优胜奖
ISP 网络结构快速测绘方法设计与实现	国防科技大学电子对抗学院	优胜奖
KollectGuard: 基于内核日志的云桌面智能无感行为监管系统	浙江工业大学	优胜奖
Purifier+: 面向深度学习模型的数据隐私风险分析和安全增强系统	浙江大学	优胜奖
SM4 的内积掩码实现及性能评估	浙江大学	优胜奖
SSCParse: 面向软件供应链的安全解析工具	北京交通大学	优胜奖
VP Sentinel: 基于 GAN 的安全声纹识别系统	杭州师范大学	优胜奖
暗网网站访问行为发现的方法研究与软件实现	中国人民解放军战略支援部队信息工程大学	优胜奖
不怕视儿	南京审计大学金审学院	优胜奖
大规模数据集连接查询完整性并行验证	南京航空航天大学	优胜奖
抵抗符号执行的 Bi-OP 程序保护系统	常熟理工学院	优胜奖
恶意代码对抗样本攻击分析与防御研究	湖北工业大学	优胜奖
分布式深度学习隐私攻防平台	南京理工大学	优胜奖
公平使者: 面向未来基于同态加密的无偏置去中心化随机信标	山东大学	优胜奖
互补教师网络监督下面向人脸伪造检测的操纵线索解耦学习	浙江工商大学	优胜奖
护财安——基于深度学习的诈骗网址检测工具	湖南中医药大学	优胜奖
幻意-基于对抗机器学习的文本反情感分析系统	江苏警官学院	优胜奖
慧眼识“链”——网页暗链多维检测平台	江苏警官学院	优胜奖
慧眼——自媒体舆情甄别系统	西安邮电大学	优胜奖
火眼金睛——基于深度学习的纹理鉴别系统	深圳大学	优胜奖
基于 IR 切片的自动化代码审计系统	湖南大学	优胜奖
基于 RISC-V 指令集的 SHA-3 实现	山东大学	优胜奖
基于 SDN 的防火墙安全系统及其优化	安徽大学	优胜奖
基于 Yolo 的驾驶员危险行为检测系统	台州学院	优胜奖
基于标签多密钥同态数据封装机制的轻量级隐私保护推荐系统	华东师范大学	优胜奖
基于多级混淆映射的防窃听投影键盘输入系统	哈尔滨工业大学	优胜奖
基于多模态活体检测的人脸识别系统	哈尔滨工业大学	优胜奖
基于多模态特征融合的软件缺陷预测系统	湖北大学	优胜奖
基于风格特征重组的安全人脸识别系统	长沙理工大学	优胜奖
基于改进的人工免疫网络算法的网络攻击分析系统	湖北大学	优胜奖
基于改进克隆选择算法的计算机病毒检测系统	湖北大学	优胜奖

基于后门水印的联邦模型多方授权系统	中山大学	优胜奖
基于机器学习的工业互联网 IDS	南昌大学	优胜奖
基于可信硬件的大规模用户加密人脸识别系统	浙江理工大学	优胜奖
基于模糊层次分析法的信任评估算法的零信任安全系统	湖州师范学院	优胜奖
基于区块链的多层协作车载网络入侵检测系统	四川大学	优胜奖
基于区块链的服务器日志记录系统	西南民族大学	优胜奖
基于区块链的药品供应链数据共享系统	北京理工大学	优胜奖
基于区块链的隐私金融数据共享计算平台	大连理工大学	优胜奖
基于区块链技术的学历证书可信认证系统	西安邮电大学	优胜奖
基于人工智能的缩略图保持图像加密系统	安徽师范大学	优胜奖
基于人机协同的未知工控协议逆向分析系统	南京理工大学	优胜奖
基于人体步态雷达信号的身份认证系统	河北工业大学	优胜奖
基于深度神经网络的街景图像敏感文本检测与识别技术	东北大学	优胜奖
基于深度学习的侧信道安全检测平台	武汉大学	优胜奖
基于深度学习的云端恶意进程检测系统设计与实现	北京邮电大学	优胜奖
基于视频大数据的人群综合治安风险监测与防范平台	湖北大学	优胜奖
基于微过滤驱动的勒索防护与透明加密技术的研究与实现	东华大学	优胜奖
基于无损信息隐藏的医疗图像隐私保护和认证系统	西安邮电大学	优胜奖
基于无线编码信道的隐蔽传输系统	东南大学	优胜奖
基于小型无人机电子数据的取证分析系统	南昌大学	优胜奖
基于信号特征的物联网设备自主动态密钥生成系统	北京理工大学	优胜奖
基于异常损失值的代码模型后门检测和防御系统	华中科技大学	优胜奖
基于隐私保护区块链的去中心化数字身份监管系统	西安邮电大学	优胜奖
基于隐私集合求交集的接触者追踪系统	国防科技大学	优胜奖
基于映射差异的无人化集群网络攻击检测系统	国防科技大学电子对抗学院	优胜奖
基于用户行为特征的潜伏式持续身份认证系统	安徽大学	优胜奖
基于云存储的可搜索加密系统	齐鲁理工学院	优胜奖
假新闻终结者：基于联邦学习的分布式虚假新闻检测系统	东北大学	优胜奖
简绿——区块链跨链的碳交易与绿证交易管理系统	西安邮电大学	优胜奖
鉴视：基于多模态特征融合的误导短视频监测系统	四川大学	优胜奖
江雪——基于孪生神经网络的跨语言恶意代码相似性检测系统	西安邮电大学	优胜奖
抗量子攻击的匿名投票系统	西安邮电大学	优胜奖
可验证的隐私保护疾病辅助诊断方案设计与实现	青海大学	优胜奖

联邦学习后门攻击检测与防御系统	南京理工大学	优胜奖
链护翱翔——基于区块链和可搜索加密的数据安全存证共享系统	西北工业大学	优胜奖
密伴——密码设备健康检测器	北京电子科技学院	优胜奖
面向安卓应用的多视窗安全异常漏洞检测系统	南开大学	优胜奖
面向物联网的隐私保护鲁棒联邦学习系统	北京理工大学	优胜奖
面向舆情的重大违规案件举报线索分析平台	湖南大学	优胜奖
面向政务网的安全数据共享系统	江苏大学	优胜奖
面向智能网联汽车的轻量化入侵检测系统	哈尔滨工业大学(威海)	优胜奖
明察秋毫——基于深度学习的数字法治辅助侦测系统	郑州大学	优胜奖
模型安全卫士：基于链上链下协同的智能电网故障预警保护系统	西北工业大学	优胜奖
取信于“链”——面向警用 UAV 执法存证的区块链系统设计	江苏警官学院	优胜奖
融合国产加密算法与 RBAC 权限管理技术的账号风险洞察系统	淮阴工学院	优胜奖
融合神经网络与代码相似性的自动化漏洞检测系统	西安邮电大学	优胜奖
锐目——基于跨域行人重识别的智能化安全识别与取证系统	江苏大学	优胜奖
社交网络图像隐蔽通信关键技术和演示系统	华东师范大学	优胜奖
身体语言的守护者：基于多形态分类模型的医疗安全智能识别系统	武昌工学院	优胜奖
守护之盾：基于生物体免疫理念的车企安全防护系统	中国人民解放军战略支援部队信息工程大学	优胜奖
天眼杀手——多功能网络资产测绘系统	无锡学院	优胜奖
通过 Instrumentation API 插桩进行的 RASP	西南民族大学	优胜奖
网络安全漏洞检测防御平台	徐州工程学院	优胜奖
网络攻击者身份智能研判系统	中南大学	优胜奖
微博用户公开信息隐私泄露智能辅助提示系统	上海交通大学	优胜奖
未“舆”绸缪——面向重大网络空间安全事件的舆情监测及预警分析系统	郑州大学	优胜奖
心灵卫士：基于心理学特征检测的对抗样本生成评估系统	国防科技大学	优胜奖
一网打尽——多源网络空间测绘一致性查询与聚合框架	湘潭大学	优胜奖
一种 web 网站指纹识别技术的设计与实现	桂林电子科技大学	优胜奖
隐介藏形-以图藏图的图像隐写器	齐鲁工业大学	优胜奖
隐桥——基于安全多方计算的隐私保护系统	北京电子科技学院	优胜奖
隐私保护个性化联邦学习缓解模型投毒攻击	青海大学	优胜奖
云安：基于 Linux 痕迹采集的防勒索攻击和云原生安全取证系统	湖北警官学院	优胜奖
云环境中用户数据安全存储与可靠计算系统	浙江工商大学	优胜奖
针对交通目标识别神经网络的后门攻击防御——端到端解耦防御系统	北京交通大学	优胜奖

征信盾-基于 IPFS 分布式系统的征信平台	沈阳工业大学(中央校区)	优胜奖
支持轻量级可信验证的流数据传输系统	北京工业大学	优胜奖
指数加速求解线性方程组的安全委托式量子服务平台	湘潭大学	优胜奖
智链公益——基于区块链的公益基金智能服务系统	北京电子科技学院	优胜奖

第十六届全国大学生信息安全竞赛作品赛组委会

浙江大学网络空间安全学院



2023年8月21日