信息安全与对抗技术竞赛组委会

ISCC2026 优秀解决方案申报通知

2025 年 12 月 21 日

信息安全已涉及到国家政治、经济、文化、社会和生态文明的建设，信息系统越发展到它的高级阶段，人们对其依赖性就越强，从某种程度上讲其越容易遭受攻击，遭受攻击的后果越严重。没有网络安全就没有国家安全。信息是社会发展的重要战略资源，国际上围绕信息的获取、使用和控制的斗争愈演愈烈，信息安全保障能力是综合国力、经济竞争实力和生存能力的重要组成部分，是世纪之交世界各国奋力攀登的至高点。

信息安全与对抗技术竞赛（ISCC：Information Security and Countermeasures Contest），于 2004 年创建（国内第一），已连续举办 22 届，同时面向大学生、研究生和中小学生，累计参赛人数 14.5 万人以上，全国 65%以上高校参加，双一流院校 121 所，影响广泛且深远。

ISCC 赛项包括破阵夺旗赛、无限擂台赛、数据安全赛、博弈对抗赛、创新作品赛、智能安全赛等，助力人才培养，体现生命价值。

ISCC 不断追求“更高、更快、更强”，持续培养高品质信息安全与对抗专业人才。

根据 ISCC 组委会讨论决定，新增优秀解决方案征集赛项。请各高校学生根据学习科研竞赛实际情况，积极组织申报 ISCC 竞赛创新解决方案（以下简称“方案”）。

1 方案主题与技术要求

1.1 高性能容器动态管理技术

使用 k8s 和 Docker 技术栈实现动态容器管理，所用环境或依赖项版本需满足验收前最新发布版本或竞赛组委会指定版本。

要求利用分布式容器管理技术，支持设备资源热增删；对于单个节点（配置为 32 核 CPU、256GB 内存），支持不少于 40 个容器的并发创建或回收，单个节

点至少支持 200 个容器的部署。

提供包含最精简题目部署环境的基础镜像容器，镜像存储应小于 300MB，内存占用应小于 500M，在 2 秒内完成容器及内部服务的启动。容器需要支持一键配置和自动化部署。

后台管理端支持批量管理控制已部署容器，包括开机、关机、重启、重置、命令执行、文件下发等功能。支持通过加密或隐蔽通信请求和接收平台动态 flag，动态 flag 更新响应时间不超过 50ms。

具有容器灾备管理技术，能够完成 30 秒级灾备迁移需求（对于单个基础配置要求的镜像），支持并发备份和迁移，实现网络服务不中断。

具有容器监控和日志记录，容器监控至少包含执行命令监控和运行程序监控，日志记录需支持多容器日志集中存储和管理。

具有合理的容器权限配置和安全防护策略，能够有效防止容器逃逸和恶意破坏容器重要文件等风险。

1.2 ISCC 反作弊技术

具有题目 flag 的动态个性化生成能力，实现“一队一次一 flag”，flag 动态生成能力需至少覆盖 Misc、Web、Reverse、Pwn 等常见题目类型。

设计 flag 识别功能，识别错误提交的其他队伍 flag，记录信息包括但不限于提交时间、提交队伍信息、flag 对应队伍信息等，支持根据记录信息绘制队伍间 flag 关联图。

支持 Web、Pwn 等类型题目的埋点检测和信息点识别功能，如记录选手是否访问了关键 URL 或执行了必要的命令。

具有题目水印指纹隐藏技术，能够在题目中自动化植入定制化的隐蔽水印或指纹，水印指纹需要支持“一人一变“。

具有选手行为分析检测技术，通过记录和分析选手答题行为，判断其作弊情况。作弊情况判别精确率不低于 80%、召回率不低于 80%。分析功能需支持不同选手间答题情况相似度分析和可视化等。

具有 writeup 相似性检测技术，检测选手提交 writeup 间的相似性，并能够标注出 writeup 中的高相似部分。

1.3 高并发 ISCC 网络架构

优化传统的网络架构，增加 CDN、负载均衡以及抗 D 设备，增加 IDS、IPS、WAF 等安全检测防护设备。

设计 DMZ 区、核心交换区、业务服务器区、安管区、异地灾备等区域的防火墙访问控制策略以及 IP 子网划分路由交换部署方式，以达到满足 1 万人并发访问请求。

1.4 AWDP 环境自动化生成

实现 AWDP 虚拟对抗环境自动化生成、配置、验证，支持可视化调整和管理，主要功能需求包括：

网络拓扑自动配置。支持通过 json、yaml 等配置文件，自动化配置网段内虚拟机、虚拟路由器、虚拟网关等设备的拓扑关系。支持网络拓扑的热增删，支持多套同时部署。单个子网（1000 个节点）的部署时间不超过 60min。

拓扑配置可视化调整。支持通过可视化界面调整拓扑结构，并生成对应的网络拓扑、配置文件，配置文件生成时间不超过 15s。

环境管理。支持当前网络状态（连通性、延迟、带宽）检测，检测时间不超过 10s（1000 个节点）；支持当前网络拓扑定时增量备份，增量备份时间不超过 5min（1000 个节点）。提供节点状态检测功能，包括但不限于：节点存活性、服务状态、自定义规则等。支持节点的增删及重置，单个节点的增删和重置时间不超过 1min。

AWDP 环境自动化生成需要支持 k8s 和 Docker 等技术，所用环境或依赖项版本需满足验收前半年内的最新发布版本或长期支持版本。

1.5 ISCC 上网行为管控

实现上网行为管控子系统，部署于系统出口网关，主要功能需求包括：

网络监控。监控选手队伍的互联网访问情况，记录内容包括但不限于：目标 URL、持续时间、协议类型等。单设备（部署在双核 4G 内存的虚拟机上）的网络监控吞吐量不低于 2Gbps，每秒最大可处理网络连接数不少于 3 千，数据记录延迟不超过 50ms。支持 HTTP、HTTPS、FTP、SSH 等常见网络协议。

行为控制。支持依据队伍、源 IP、目标 IP、目标网址或域名、端口、协议等配置上网控制策略，支持黑白名单设置，支持按照时间段进行设置。控制策略从配置到生效的延迟时间不超过 1s。支持控制 IPv4 和 IPv6。

可视化。上网控制需具备图形界面和可视化配置能力。

兼容性。支持部署于主流 linux 操作系统（Ubuntu、CentOS 等），支持部署到子系统验收时的最新发布版本或长期支持版本。

1.6 高性能 ISCC 网关设计

设计实现平台内网网关子系统，用于管理监控选手子网、系统子网和容器子网等不同网段间的网络通信。

具有稳定的并发网络数据转发能力。单设备（部署在双核 4G 内存的虚拟机上）最大数据吞吐量不低于 2Gbps，最大并发连接数不小于 1 万，转发延迟不超过 10 毫秒，最大丢包率低于 0.005%。

具有自动化路由配置功能，依据选手队伍信息自动建立选手设备到系统和分配容器的路由，支持路由的一键批量开启和关闭。批量开关路由时间不超过 5s（1000 条路由）。

具备精细化自定义路由配置能力，能够按照队伍、IP 等条件批量设置或删除路由。支持按时间段设置路由，支持配置路由有效期。单条路由从配置到生效的延迟时间不超过 1s。

提供可视化的路由管理和配置操作。支持部署于主流 linux 操作系统（Ubuntu、CentOS 等），支持部署到子系统验收时的最新发布版本或长期支持版本。

1.7 下一代 ISCC 竞赛平台

信息安全与对抗技术竞赛业务层面需求：

用户端应至少包含：注册/登录、队伍创建/管理、个人信息修改、题目详情、Flag 提交、动态排行榜、公告推送、比赛报名、WriteUp 提交等功能。

管理端应至少包含：赛事全生命周期管理、题目管理、容器调度、网络管理、用户管理、实时监控、数据报表、运维面板等功能。

支持一键部署和配置。

技术层面需求：

使用 B/S 架构和前后端分离设计，使用 Mysql 数据库持久化储存，使用 Doris 存储日志数据，使用 Redis 作为缓存，容器方面使用 Docker 和 k8s 进行管理

API 交互使用 RESTful 风格，并提供资源（包括题目、容器、网络、用户等）管理的 API 接口，以便于二次开发。

UI 层面应展示信息安全与对抗技术竞赛的特色以及专业性。

支持部署于主流 linux 操作系统（Ubuntu、CentOS 等），支持软件验收时最新发布版本，或长期支持版本。

所用开发框架及其依赖项需支持软件验收一年内发布版本或长期支持版本。

1.8 其他相关选题

由项目组自行提出提升 ISCC 能力的主题。

2 方案文档撰写与命名

解决方案按照申报书等附件要求撰写。

每个项目需要填报 4 份文档，如果方案不涉及知识产权等材料，则无需填写相关内容，每份文档需要提供 word 版和 pdf 版。

按文件命名规范命名文件，提交时将所有文件压缩成一个压缩文件，压缩文件命名为：学校名称-方案名称-日期。

1. 学校名称-报名表-方案名称-日期
2. 学校名称-申报书-方案名称-日期
3. 学校名称-原创性声明-方案名称-日期
4. 学校名称-知识产权授权协议-方案名称-日期
5. 学校名称-XXX-方案名称-日期

3 内部遴选和评审

信息安全与对抗技术竞赛优秀解决方案申报和评优评奖共分为 3 个阶段：

1. 高校内部遴选阶段。自通知发布日起 30 个自然日内，各高校分别组织内部申报审核工作，所提交的方案由本校内部团队审核遴选出典型方案，统一提交至信息安全与对抗技术竞赛组委会联系邮箱。
2. 组委会组建初选评审组。自方案提交截止日起 15 个自然日内，评审组将

初选方案前提交至竞赛组委会。

3. 组委会评优和信息发布。方案初选结束日起 15 个自然日内发布评审结果。

4 方案级别评定

优秀解决方案设 3 级奖项，依据评定级别支持 0.5-5 万元经费。

一等奖：1-2 名。

二等奖：3-4 名及以上。

三等奖：5-6 名及以上。

具体获奖数量视申报总量情况可能有所调整。

5 方案交付与验收

申报材料经评审获奖后，项目团队需根据所选课题提交以下相应的交付材料，以供组委会验收。交付物应完整、可复现，并符合方案中承诺的技术指标。

交付代码：包含完整的系统功能代码。

部署与运维文档：详细的环境部署指南、API 接口说明、技术文档、配置及操作手册。

测试报告及附带资源：提供测试方案、测试脚本和测试报告等文档，证明方案功能和性能等达到预期指标，若有其他支撑测试的资源也需提供（如测试数据集等）。

方案交付截止时间：方案评审结果发布日起 45 个自然日内。

组委会验收和信息发布。组委会组建专家组进行解决方案的测试与验收，方案交付截止日起 15 个自然日内发布方案评审结果。

6 方案经费拨付

方案经费分 2 次拨付：方案评优通过后 15 个自然日内拨付总经费的 50%，解决方案验收通过后 15 个自然日内拨付总结费的 50%。

7 方案提交与联系人

重要时间节点：

1. 方案申报：征集通知发布日+30 个自然日
2. 方案初审：方案提交截止日+15 个自然日
3. 方案评优：方案初审截止日+15 个自然日
4. 方案交付：评优结果发布日+45 个自然日
5. 验收评审：方案交付截止日+15 个自然日

方案提交电子邮箱：iscc2004jbgs@163.com

联系人姓名：宋老师、张老师

联系人手机号：15700077559、18404901915

通信地址：北京理工大学网络空间安全学院办公室

邮编：100081

8 方案附件

1. 申报书
2. 报名表
3. 原创性声明
4. 知识产权授权协议