

Yu, Jiawei 于珈尉

求职意向：网络及后端工程师实习，能够在岗6个月

☎ (+86)188-1158-0061 | ✉ jay.waves@outlook.com | 📅 2002年12月29日 | 🌐 jay-waves | 🗣️ jay-waves

教育经历

北京航空航天大学，专业型硕士

网络空间安全学院，网络与信息安全专业

- 北航开源软件安全实验室
- 研究方向：系统级开源软件的缺陷自动化挖掘

北京，中国

2025年09月 - 至今

北京航空航天大学，工学学士

信息类工科实验班，网络空间安全学院，信息安全专业

- 总体成绩：GPA：3.76/4.0，加权平均分：89.69/100
- 主修课程：操作系统 95、数据库 96、数据结构 99、算法分析 91、并行程序设计 94

北京，中国

2021年09月 - 2025年06月

专业技能

英语 CET6: 522, IELTS: 6.5(6)

编程语言 掌握 C++、Python，熟悉 GO、C、Shell、TypeScript

编程范式 了解面向对象设计模式、多线程与多进程编程、网络编程设计思想

开发工具 熟练使用 Git、CMake、VCPkg、Docker 工具。有丰富 Linux 开发与部署经验。

中间件 熟练 MySQL、Redis、ElasticSearch、RabbitMQ 的基本使用

项目经历

预研项目，北京轩宇信息技术有限公司（中国空间技术研究院子公司）

实习 & 测试开发工程师

2025年3月 - 2026年1月

- 项目需求：设计针对嵌入式 SPARC 架构的航天器软件的仿真环境下漏洞检测与发掘方法
- 技术选型：C++23、QEMU、BooFuzz、Capstone、Catch2、CMake+Ninja+VS2026
- 个人职责1：独立设计实现对未初始化访问、释放后使用、内存越界、原子性违反等常见软件缺陷的检测技术。
- 个人职责2：设计完整的虚拟机 Mock 服务，自动覆盖航天器软件的全生命周期状态，测试代码覆盖率达到 97%。
- 项目成果：一篇顶会论文在投，一项发明专利公开。

北京

研究项目，北航开源软件安全实验室

本科生 & 核心技术负责人

2023年6月 - 2024年5月

- 项目需求：设计针对 Navigation2 及相关导航 ROS2 开源库的漏洞检测与自动挖掘方法
- 技术选型：C++17、Python、ROS2、Navigation2、FastDDS、Colcon+LLVM、Docker
- 个人职责1：编写伪装的 ROS 节点，对网络中其他 ROS 节点进行中间人攻击。扰乱网络包的内容、时序、逻辑。
- 个人职责2：通过 LLVM 插桩使 ROS 节点的回调函数延迟执行，最终在 Navigation2 挖掘出大量并发缺陷。
- 项目成果：发表一篇顶刊论文（TIFS2025），披露 33 个 CVE 漏洞和 16 个 CNVD 漏洞

北京

安恒信息技术股份有限公司

实习 & 渗透测试工程师

2024年6月 - 2024年9月

参与 2024 年公安部 HW 行动蓝队防守。

北京

荣誉及获奖

学业及学生竞赛获奖

- 2025 一等奖（杰出学生），开源安全奖励计划（开源漏洞挖掘赛道），中国网络空间安全协会
- 2023 队长 & 第二作者，大学生创新创业训练计划项目（国家级），北京航空航天大学
- 2023 三等奖，全国密码学技术竞赛（决赛），中国密码学会
- 2023 二等奖（专业前10%），学业优秀奖学金，北京航空航天大学
- 2021 二等奖（年级前30%），学业优秀奖学金，北京航空航天大学

北京

北京

新疆

北京

北京

成果-发明专利

面向航天嵌入式软件的模糊测试方法、装置及电子设备

第四作者

ZL202511556692.2

北京航空航天大学

2025年10月29日

基于零知识范围证明的共享单车运行方法及装置

第五作者

ZL202410324969.8

北京航空航天大学

2024年03月21日

成果-学术论文

Detecting Lifecycle-Related Concurrency Bugs in ROS Programs via Coverage-Guided Fuzzing

IEEE TIFS 2025

第二学生作者 & 核心贡献者

doi: 10.1109/TIFS.2025.3592562

成果-原创漏洞编号

CVE

针对 ROS 系统挖掘的漏洞中，共获批 33 个原创 CVE 编号，其中高危级漏洞 9 个，关键级漏洞 9 个

CVE-2024-25197, CVE-2024-25196, CVE-2024-25198, CVE-2024-25199, CVE-2024-30961, CVE-2024-30964, CVE-2024-30962, CVE-2024-30963, CVE-2024-37860, CVE-2024-37861, CVE-2024-37862, CVE-2024-37863, CVE-2024-38910, CVE-2024-38920, CVE-2024-38921, CVE-2024-38922, CVE-2024-38923, CVE-2024-38924, CVE-2024-38925, CVE-2024-38926, CVE-2024-38927, CVE-2024-41644, CVE-2024-41645, CVE-2024-41646, CVE-2024-41647, CVE-2024-41648, CVE-2024-41649, CVE-2024-41650, CVE-2024-44852, CVE-2024-44853, CVE-2024-44854, CVE-2024-44855, CVE-2024-44856

CNVD

针对 ROS 系统挖掘的漏洞中，共获批 16 个原创 CNVD 编号，其中高危级漏洞 4 个

CNVD-2024-16363, CNVD-2024-17402, CNVD-2024-16329, CNVD-2024-16333, CNVD-2024-29065, CNVD-2024-29066, CNVD-2024-29071, CNVD-2024-29072, CNVD-2024-29073, CNVD-2024-29074, CNVD-2024-29075, CNVD-2024-29077 CNVD-2024-18675, CNVD-2024-18675, CNVD-2024-22505, CNVD-2024-22504

自我评价

多次担任项目负责人，责任心强，进度推进积极。对代码质量和文档规范有追求。