辜汝曦

所在地: 中国武汉

邮箱: 2021302141194@whu.edu.cn ✻ *电话:* 13026121612

教育经历

本科教育 *2021.9 - 至今*

武汉大学国家网络安全学院，网络空间安全专业 中国武汉

- GPA: 3.83/4.00
- A^+ 科目:

  线性代数 (90), 概率论与数理统计 (95), 离散数学 (93),
  电路与电子技术 (97), 数字逻辑与 EDA (94),
  计算机组成原理实验 (97), 数据结构实验 (95), 人工智能实验 (98) 等。
- CET4 成绩: 629/710

高中教育 *2018.9 - 2021.6*

武汉外国语学校，理科 中国武汉

研究方向

人工智能安全 我主要研究人工智能（AI）安全与隐私领域：在该领域内，我探索深度学习模型在其生命周期中的弱点（例如，对抗性攻击、后门攻击）及其对策；我还努力利用这些弱点，应用于深度学习模型的隐私保护和知识产权保护。

科研团队

NIS&P Lab NIS&P Lab 的研究重点是安全领域的三个分支：云计算安全、无线系统安全以及大数据和人工智能安全。我们对各种信息系统背后的安全和隐私问题感兴趣，并希望为物理世界寻找实用和有意义的解决方案。王骞教授是实验室的领导者。我是实验室的一员。

项目经历

隐以为荣: 高效的隐私保护图片识别平台 *2023.6 - 至今*

武汉大学，指导教师：何琨副教授 中国武汉

- 本作品梳理了近年来隐私保护预测的技术路线，着重描述了隐私保护神经网络预测协议的发展，并指出之前的工作存在着在线性层与非线性层协议衔接不畅的问题。针对这个问题，我们设计了一种半诚实敌手模型下，高效的隐私保护神经网络预测框架 Hare。它可在云端预测服务中保护用户隐私数据和卷积神经网络模型参数。
- 我作为团队中的一员。该项目参加了第 16 届全国大学生信息安全竞赛作品赛（初赛进行中）。

智安盾-人工智能安全守卫领军者 *2023.4 - 至今*

武汉大学，指导教师：王骞教授，赵令辰副教授 中国武汉

- 智安盾是全国首个集成了对抗性攻击机理分析的自主安全一体化防御平台,其核心技术全部依托于团队成员的前沿成果。该平台服务于人工智能技术产业化市场，为智能模型构建全方位防御保障，实现人工智能系统在各个领域中安全、可靠的部署和应用服务,推进我国人工智能技术发展与产业化进程。
- 我作为团队中的一名核心成员。

竞赛奖项

一等奖 *2023.06*
2023 年 CATTI 杯全国翻译大赛初赛（复赛进行中） 中国

三等奖 *2022.12*
2022 年全国大学生英语竞赛（已结束） 中国

专业技能

编程语言 C/C++, Python, Java
开发框架 Numpy, Pytorch
开发工具 VS Code, Pycharm, IDEA
其他工具 LaTeX, Markdown, Adobe Photoshop, Audition and Premiere

语言能力

中文 自然流畅
英文 熟练运用
日文 相对熟悉

关于我

喜好 下围棋，尤其是和 AI 下；看书，最喜欢的作家是严歌苓；打网球，目前正在学习中。
个性 我会主动踏出自己的舒适圈，并欢迎全新的技术和挑战：通过学习这些新技术，我可以持续地提升自我并且做出突破。对于自己学习过程中的困难，我会积极寻找可能的解决方案，包括网络搜索与询问他人；我也乐于将自己的经验分享给其他人，让其他人不受制于信息差。