北京郵電大學 Beijing University of Posts and Telecommunications

个人简历 Personal resume

基本信息

姓　　名：李浩东　　出生年月：1995 年 10 月 29 日
民　　族：汉　　身　　高：175cm
电　　话：18810368565　　政治面貌：群众
邮　　箱：lihaodong1029@126.com　　毕业院校：北京邮电大学
户　　籍：北京市房山区　　学　　历：博士研究生

教育背景

2015.09-2019.06	华北电力大学（北京）	控制与计算机工程学院	信息安全（本科）
2020.09-2025.06	北京邮电大学	网络空间安全学院	网络空间安全（硕博连读）

科研成果

研究方向：博士在读期间专注于研究移动互联网和人工智能技术应用。重点研究利用 AI 解决软件工程领域的安全问题，例如恶意代码，恶意软件检测。

发表 CCF A 类会议论文 3 篇：

- MalCertain: Enhancing Deep Neural Network Based Android Malware Detection by Tackling Prediction Uncertainty。缓解安卓恶意软件检测中的概念漂移问题 **ICSE 2024**
- Mitigating Emergent Malware Label Noise in DNN-Based Android Malware Detection 处理数据集中的标签噪声问题。**FSE 2025**
- Understanding Model Weaknesses: A Path to Strengthening DNN-Based Android Malware Detection 处理训练数据集中的长尾问题。**ISSTA 2025**

在投安全领域 A 类论文 1 篇：

- As If We’ ve Met Before: Large Language Models Exhibit Certainty in Recognizing Seen Documents 利用 LLM 的不确定性解决训练数据集中的版权误用问题。**USENIX Security 2025**

专利 1 项。

- 《基于不确定性增强安卓恶意软件检测性能方法及相关设备》

标准 2 项。

- 《T/CAS 943-2024 移动应用生态安全协同治理规则》
- 《T/ZSA 258-2024 移动互联网应用程序未成年人模式功能要求》

项目经历

- **国家重点研发计划项目：移动互联网数据安全防护试点示范（No.2018YFB08030600）**

  研究目标：从移动业务和终端安全需求出发，构建高性能、高安全等级、可动态扩展的移动业务国产密码保障体系，突破终端高安全威胁识别与数据防护、智能化隐私保护、自适应安全管控等关键技术，研制数据防护与隐私保护技术方案，并在移动高速视频云服务、移动业务管控、即时通信等领域应用示范。

  职责：全面了解项目的所有软硬件，负责各家单位软硬件的验收和项目验收过程中的演示工作。重点是高速视频云会议系统和移动政务系统。

- **十三五重点研发-山东：面向离散制造业的安全可控工业控制系统研发（No.2019JZZY010110）**

  研究目标：充分研究最新网络与信息安全技术基础上，对标国际先进的主流安全控制器（PLC）产品，采用最新的国产密码算法，基于模块化和开源硬件理念，设计低成本可扩展的安全智能工业控制器软硬件架构，研制具有自主知识产权的安全工业 PLC，支持智能工控硬件的云化互联；支持主流的现场控制总线接口和协议；采用开放式和硬件开源的体系，确保安全智能、低成本和可扩展；支持嵌入式的身份管理和可信认证的能力；采用国密算法，支持通信加密和内容加密。

  职责：重点负责安全子系统提供整个设备的基础安全支持、认证、访问控制、可信计算和基于国密算法的加解密服务。

- **企事业单位横向委托项目：路面裂缝自动化检测项目**

  项目内容：针对高速公路的路面图片实现病害识别，病害绘图以及修补绘图。保证模型的识别过程中的性能和泛化能力，确保模型的预测可靠。

  职责：模型性能提升。

- **企事业单位横向委托项目：移动互联网应用软件安全评测服务。**

  项目内容：借助相关技术，通过自动爬取和手动下载，掌握应用商店第三方手机软件样本及类型分布情况；借助恶意软件检测技术和手段，实现恶意软件人工标注。

  职责：恶意软件标注

技能特长

中国象棋一级棋士证书。

自我评价

作为一名专注于人工智能与软件工程领域的博士研究生，我具备扎实的理论基础和丰富的实践经验。在博士期间，我深入研究人工智能技术在软件工程中的应用与安全问题，特别是在提升恶意软件与恶意代码检测的性能方面取得了重要进展。我的研究涵盖数据处理、模型优化和系统性能提升三个方向，主要聚焦于利用人工智能模型的不确定性解决实际问题。在数据层面，我实现了数据集标签的去噪，有效提高了数据质量；在模型训练层面，我针对安卓恶意软件数据集中的长尾问题设计了鲁棒的训练方法；在系统层面，我缓解了概念漂移对检测器的影响，显著提升了系统的性能与可靠性。同时，我还关注大语言模型的不确定性研究，探索其在解决训练集版权误用检测中的应用。通过评估大模型的不确定性，我设计了方法来识别被模型学过的样本，降低因版权问题带来的风险。

我擅长跨领域技术的整合，将人工智能技术成功应用于软件工程、路面裂缝检测等多个实际场景。同时，我具备优秀的团队合作能力和极强的自驱力，能够在多元化团队中高效协作，为项目的顺利推进提供保障。此外，我始终保持对前沿技术的敏锐洞察力，致力于将最新的研究成果转化为实际应用，为软件工程和安全领域的技术的发展贡献力量。