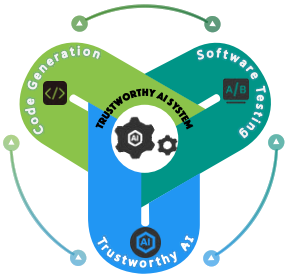
软件学院导师团队与招生意向信息表

<table>
<tr><td>团队名称</td><td colspan="2">可信人工智能系统(Trustworthy AI Systems) 团队</td><td>团队负责人</td><td>张旭鸿</td></tr>
<tr><td>联系人</td><td>张旭鸿</td><td>邮箱</td><td>zhangxuhong@zju.edu.cn</td><td>电话</td><td>15533600750</td></tr>
<tr><td colspan="2">意向学生需求数</td><td></td><td colspan="3"></td></tr>
<tr><td colspan="6">主要团队成员</td></tr>
<tr><td>姓名</td><td>职称</td><td colspan="2">研究方向</td><td colspan="2">个人主页</td></tr>
<tr><td>张旭鸿</td><td>研究员</td><td colspan="2">可信人工智能、大模型应用与隐私、软件与系统安全</td><td colspan="2">https://person.zju.edu.cn/zhangxuhong</td></tr>
<tr><td>纪守领</td><td>研究员</td><td colspan="2">人工智能与安全、数据驱动安全、软件与系统安全、大数据挖掘与分析</td><td colspan="2">https://person.zju.edu.cn/sji</td></tr>
<tr><td>李振源</td><td>研究员</td><td colspan="2">系统安全、入侵检测、入侵知识图谱、安全态势感知平台</td><td colspan="2">https://li-zhenyuan.github.io/</td></tr>
<tr><td>潘家雨</td><td>研究员</td><td colspan="2">通信性能优化，强化学习，通信系统</td><td colspan="2">https://jiayupan26.github.io/</td></tr>
<tr><td>杜天宇</td><td>研究员</td><td colspan="2">大语言模型、人工智能安全</td><td colspan="2">https://tydusky.github.io/</td></tr>
<tr><td>团队介绍</td><td colspan="5">可信人工智能系统团队（Trustworthy AI Systems Lab, TRAIL）围绕可信人工智能（Trustworthy AI）、代码生成（Code Generation）、软件测试（Software Testing）三个方向及其交叉展开研究，致力于自动化构建可信安全的人工智能系统，已有和进行中的研究工作主要集中在人工智能算法的对抗攻防、AI 驱动的代码模糊测试、LLM 驱动的领域特定语言（DSL）生成。
 

团队现有教授/研究员 5 人，均有丰富的海外学习工作经历。团队负责人为国家级青年人才计划入选者张旭鸿研究员，曾在美国微软 LinkedIn 任职；纪守领长聘教授、博士生导师，可信人工智能研究中心主任；李振源研究员毕业于浙江大学计算机学院，期间在新加坡国立大学访问交流，曾在华为 2012 可信实验室任职；潘家雨研究员毕业于美国俄亥俄州立大学电子与计算机工程系；杜天宇研究员毕业于浙江大学计算机学院，曾在美国宾夕法尼亚州立大学从事博士后研究工作。团队在 ACM/IEEE Trans. TDSC、TIFS、ToN、TPDS 和 IEEE S&P、ACM CCS、USENIX Security、NDSS、CVPR、KDD、ICDE、VLDB 等权威期刊和会议上发表论文 100 余篇，获最佳论文奖 10 余项，研制了多个安全分析、检测和加固系统，应用于国家重要部门和华为、阿里等大型商业平台。

近年来团队培养的博士、硕士研究生，毕业生直接就业单位包括国防科大、中科院软件所等高校科研院所，阿里巴巴、华为、蚂蚁金服等多家知名的 IT 企业。当前团队科研经费充足，科研氛围浓厚，学生有大量机会参与众多研究与工程项目，展现个人能力，实现学术追求与工程实力提升。

实验室具有优良的国际合作关系，与普林斯顿大学、加州大学伯克利分校、佐治亚理工学院、伊利诺伊大学——香槟分校、弗吉尼亚大学、宾夕法尼亚州立大学、悉尼大学、IBM T. J. Watson 研究中心的多位教授/研究员具有长期稳定的合作关系，实验室每年有多位同学被选派至上述学校继续深造、访学研究。</td></tr>
<tr><td>项目情况</td><td colspan="5">团队先后主持国家自然科学基金重点项目、面上项目、青年项目、国家重点研发计划项目、工信部高质量专项项目、国家创新特区项目、浙江省重点研发计划项目、阿里巴巴科研基金、蚂蚁金服科研基金、华为科研基金等。</td></tr>
</table>

团队与企业合作情况	团队近年来主持多项企业合作项目，研究成果在华为、阿里巴巴、蚂蚁金服等头部企业落地应用，取得了良好的应用效果，建立了紧密的合作关系。
对学生的要求	1、坚韧、勤奋；2、追求学术研究与工程能力双提升；3、较好的计算机基础知识和动手能力。 欢迎对人工智能、系统安全等方向感兴趣的同学。
团队可以在宁波开设专业课程情况	