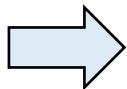


挑战

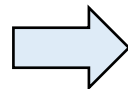
科学问题

研究内容

复杂性：智能软件开发基础库和第三方库庞大，难以筛选脆弱组件



如何挖掘智能软件开发各阶段引入的第三方组件依赖和脆弱性？



第三方组件

第三方开源组件依赖库挖掘和脆弱性分析



智能组件

基于边界神经通路的智能组件脆弱性测试

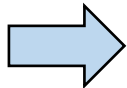


多组件依赖

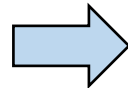
基于第三方组件依赖的智能软件脆弱性分析



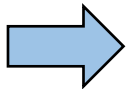
不确定性：智能组件本身的不确定性导致其易受噪声和异常样本攻击



如何有效针对智能组件脆弱点进行覆盖充分性测试？



高隐蔽性：利用第三方组件漏洞攻击智能软件不易被发现



基于组件依赖关系，如何分析第三方组件对智能软件的影响？

