肖浩宇

Email: hyxiao20@fudan.edu.cn

HomePage: https://haoyu-xiao.github.io

Github: https://github.com/Haoyu-Xiao

教育经历

复旦大学 (FDU), 上海 2020 至今

计算机科学与技术学院网络空间安全专业 **博士研究生** (导师: 张源教授)

哈尔滨工业大学 (HIT), 哈尔滨 2016 – 2020

计算机科学与技术学院信息安全专业 **本科生**

学术成果

- **HouseFuzz: Service-Aware Grey-Box Fuzzing for Vulnerability Detection in Linux-Based Firmware**
  Haoyu Xiao, Ziqi Wei, Jiarun Dai, Bowen Li, Yuan Zhang, Min Yang.
  针对 *Linux* 固件服务提出了三项新型技术，从而提高模糊测试的漏洞挖掘效率：*(1)* 更全面的服务识别技术；*(2)* 多进程模糊测试框架；*(3)* 基于定制化服务协议建模的模糊测试框架。该工作共发现了 *157* 个 *0-day*，目前获得了 *41* 个 *CVE/CNVD* 编号。

  S&P'25 (**CCF-A**) [paper] [code]

- **Accurate and Efficient Recurring Vulnerability Detection for IoT Firmware**
  Haoyu Xiao, Yuan Zhang, Minghang Shen, Chaoyang Lin, Can Zhang, Shengli Liu, Min Yang.
  提出了新型的重现漏洞检测技术，设计并自动化提取漏洞基于攻击语义的已知漏洞签名，在固件上利用已知漏洞快速准确地检测语义相近的未知漏洞。该工作共发现了 *643* 个固件漏洞，获得了 *53* 个 *CVE* 编号。

  CCS'24 (**CCF-A**) [paper] [code]

- **Exploit the Last Straw That Breaks Android Systems**
  Lei Zhang, Keke Lian, **Haoyu Xiao**, Zhibo Zhang, Peng Liu, Yuan Zhang, Min Yang, Haixin Duan.
  揭露了安卓系统服务中的新型资源泄露漏洞，并实现自动化地动态检测，该漏洞能够导致安卓系统崩溃，严重的可以导致设备变砖。

  Oakland'22 (**CCF-A**) [paper] [code]

项目经历

- **针对闭源系统的开源软件漏洞补丁存在性检测 (项目组长).**
  补丁存在性检测是供应链漏洞管理的重要技术，可以发现供应链上游上游组件漏洞是否可能影响下游软件。本项目只需要输入开源上游组件代码和补丁就可以检测任意下游软件（包括闭源软件）是否包含未修复的漏洞。向合作方（阿里巴巴）交付了准确率超过 *94%*，能覆盖 *85%* 以上检测任务的补丁存在性检测工具。

实习经历

- **华为安全工程师实习岗** 2018.08 – 2018.09

  主要内容: 分析安卓系统级高危漏洞

- **腾讯安全工程师实习岗** 2018.07 – 2018.09

  主要内容: 游戏安全对抗，包括编写外挂和分析反作弊机制

安全竞赛

研究生期间:

- 2023 Datacon 大数据安全分析赛卓越团队奖 – 漏洞挖掘赛道

本科期间担任哈尔滨工业大学 CTF 战队 (Lilac) 队长，主攻逆向. 代表奖项如下:

- 2019 X-NUCA CTF 决赛一等奖
- 2019 强网杯全国网络安全挑战赛三等奖
- 2019 全国高校网络运维赛全国第三名
- 2018 全国大学生信息安全创新实践能力赛二等奖
- 2018 TCTF 新人邀请赛决赛第二名
- 2018 DEFCON China BCTF 国际赛第五名
- 2018 全国高校网络运维赛全国第五名
- 2018 第二届“强网杯”优胜奖

其它信息和经历

- 研究方向：专注于二进制安全，博士研究的细分方向是 IoT 固件漏洞检测，包括静态漏洞检测、模糊测试、固件仿真技术。此外，我致力于构建高效智能的二进制程序分析工具。
- 助教经历：(1) 复旦大学 2024,2025 年逆向工程课程助教，承担新版课程和实验设计工作，内容包括反编译、固件逆向等。(2) 复旦大学 2022 年网络攻防实践课程助教。
- 编程技能：目前我偏好使用 Rust 和 Python 开发大型系统，之前我也曾使用 C/C++, Java, Scala 语言开发大型原型系统。