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.
  提出了三项新型技术，提高 *Linux* 固件灰盒模糊测试的漏洞挖掘效率：*(1)* 基于自动化模拟异常处理的服务识别技术；*(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* 个零日漏洞，目前获得了 *45* 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.
  提出了新型的基于漏洞攻击语义的重现漏洞检测技术。该技术首先使用混合执行技术自动化提取基于攻击语义的已知漏洞签名，然后根据已知漏洞签名信息，在目标固件上通过两阶段方法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]

- **Detecting Taint-Style Vulnerabilities in C-Lua Hybrid Web Services of Linux-based Firmware**
  Runhao Liu, Jiarun Dai, **Haoyu Xiao**, Yuan Zhang, Yeqi Mou, Lukai Xu, Bo Yu, Baosheng Wang, Min Yang.
  提出跨 *C* 和 *Lua* 语言的静态污点型漏洞检测技术，用于检测嵌入式固件 *Web* 服务中的安全漏洞。该技术能够自动化去除 *Lua* 字节码混淆，识别 *Lua* 中的独特污点源，和系统性分析跨语言数据流。该工作共发现了 *610* 个零日漏洞，目前获得了 *31* 个漏洞编号。

  NDSS'26 (**CCF-A**)

- **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，该漏洞能够导致安卓系统崩溃，严重的可以导致设备变砖。在本文工作中，我设计和实现了面向安卓系统服务的导向型模糊测试框架，能自动化地在安卓系统服务中检测此类新型资源泄露漏洞。本工作一共发现了 *474* 个安卓系统服务接口中的新型资源泄露漏洞。并获得了谷歌的致谢。

  S&P'22 (**CCF-A**) [paper] [code]

工作经历

- **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** 2019.07 – 2019.09

  主要内容: 游戏安全对抗，包括编写外挂和分析反作弊机制。

- **复旦“逆向工程核心原理”课程助教** 2024.02 – 2024.06, 2025.02 至今

  主要内容：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。先后基于 *retdec* 框架和 *pypcode* 分别编写了两套教学用反编译器框架。

- **复旦“网络安全攻防实践”课程助教** 2022.09 – 2022.12

  主要内容：承担出题工作，包括 *CTF* 逆向和 *PWN* 题。

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。本项目基于符号执行提取补丁和目标函数的语义特征，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。

- **通用“按需分析”二进制数据流分析框架.**

  我正在独立开发一个通用的“按需分析”的二进制程序数据流分析框架，旨在提供高度可控和模块化的数据流分析能力，便于被大模型调用，并与大模型强大的推理能力结合，实现自动化二进制程序逆向。该项目仍处于早期阶段，目前已开源部分有*pcode-rs*——一个用 *Rust* 编写的基于 *Ghidra Sleigh* 的二进制程序反汇编和中间代码生成库。

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。
- 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。