蔡泫朴

15802183503 | cpeggsjtu@sjtu.edu.cn | 上海

教育经历

上海交通大学 - 网络空间安全 本科 网络空间安全学院（排名9/97） 2015.09 - 2019.06

上海交通大学 - 电子与通信工程 硕士 网络空间安全学院 2019.09 - 2022.03

研究方向

二进制安全研究及工具开发，包括软件及系统安全，IoT安全，二进制层面程序分析。

专业经历

1. 上海交大密码与计算机安全实验室(LoCCS)软件组

主要从事包括智能家居、车载智能系统等嵌入式设备相关的安全研究工作，有相关论文和专利产出。

2. 0ops 队伍成员

主攻CTF中的pwn 和部分逆向，自17年9月起，随队伍参与国内外赛事并参与校内赛出题及校内CTF基础讲授。

参与的国内线下比赛包括：

- 2018、19、20强网杯（全国8，4，3名）
- 2018、19护网杯（全国第6，4名）
- 网鼎杯（全国第4）
- 2018 X-NUCA（第1）、2018 2019 XCTF联赛（第2，第3）
- 2018全国大学生信息安全竞赛实践能力创新赛一等奖
- 2020首届全国职业技能大赛网络安全项目全国第三名，并获“全国技术能手”称号

以及随A*0*E参与国际比赛包括：

- 2019 DEFCON（第4）
- 2019 Plaid（第8）
- 2018 2019 HITCON（第6，第1）等国外比赛

3. 腾讯科恩实验室 - 实习生

竞赛及车联网组：进行DEFCON 2019的内部训练以及车厂固件升级流程漏洞挖掘和测试工作。 2019.04 - 2019.08

安全工具开发组：进行WASI文件的可调试运行时开发，进行基于GDB的和基于IDA的插件开发 2020.03 - 2020.07

4. 奇安信-清华技术研究院，天工实验室 - 实习生 2020.09 - 2021.06

进行物联网设备的漏洞挖掘和科研工作，厂商覆盖Cisco、Netgear、ASUS、NAS、SonicWall旗下的路由器、网关、智能家居等设备，发表学术论文，并在天府杯、GeekPwn等比赛上进行展示；相关漏洞进行了CVE（获2编号）申请。

近段时间正在进行有关基于unicorn引擎对物联网设备固件的代码片段fuzz(AFL) 及路径上的约束求解(angr)工作；相关漏洞进行了CVE（获5编号）和CNVD（获59编号）编号申请。

5. 阿里云安全 - 实习生 硬件安全组 2021.06 - 至今

进行可信计算一体机系统项目开发，负责整个可信计算侧的SGX应用、gRPC服务的数据库应用服务开发和性能调优，以及部分密钥管理相关功能、SDK开发。预计除产品外还有相关论文产出。

学术论文

1. [WiSec'18] Passwords in the Air: Harvesting Wi-Fi Credentials from SmartCfg Provisioning (2nd)

对当下智能家居设备入网阶段时的Wi-Fi凭据泄露问题进行探讨和分析，从设备端固件逆向以及市场上手机端智能家居APP解包分析两个维度，对凭据泄露问题的成因和影响面进行评估。

2. [USENIX'21] Sharing More and Checking Less: Leveraging Common Input Keywords to Detect Bugs in Embedded Systems (2nd)

引入一套基于前端关键字提取以及后端基于angr的污点分析框架，能够对物联网设备由于web服务等前端数据引入的缓冲区溢出和命令注入漏洞进行自动挖掘。

3. **[NDSS'22]** MicroFuzzing: Leveraging Data-flow Analysis for Hybrid Directed Fuzzing onCode Fragments of RTOS Systems（1st，在投）

引入一套以静态污点分析为导向的固件片段代码执行和裁剪的工具，能够对RTOS等不易从入口点起始进行模拟和执行的设备代码进行混合模糊测试，从而对这类设备进行漏洞挖掘

专利

1. 车载诊断系统固件保护方法及系统 (CN202010064511.5)

发明：公开了一种在汽车车载系统环境中的车载诊断系统的固件安全领域，对涉及到的车载诊断系统设备进行固件保护的方案；在其中负责系统、协议设计及实现工作

2. 设备安全检测方法、装置、计算机设备和可读存储(申报中)

发明：USENIX论文转化

3. 一种基于波浪滑翔机的通讯控制系统(CN201721366460.1)

实用新型专利：校内科创项目转化

专业技能

1. 逆向

熟悉IDA、Ghidra、radare2等常用反汇编反编译逆向分析工具使用，在IDA、Ghidra上有实际插件开发经验；

了解包括堆栈内存破坏、信息泄漏、命令注入等安全漏洞成因和修复方案，能审阅汇编代码；

2. 动态分析

熟悉angr，能在二进制层面进行符号执行和污点分析；

熟悉gdb/windbg等常用动态调试器，在gdb上有实际插件开发经验；

熟悉使用unicorn进行模拟执行；

熟悉AFL内部设计，能使用其进行模糊测试fuzz开发；

能使用tcpdump、wireshark等工具进行网络流量抓包和简单分析；

有使用frida等工具进行动态插桩分析的经验；

3. 编程开发

曾获省信息学奥林匹克竞赛（NOIP）一等奖，对程序算法设计和数据结构等方面有一定基础；

有大量使用C, C++, python等语言的项目经历，其他语言（java, js, go, rust等）能较快速上手

其他掌握技能

校内科创

在校学习期间在课堂上参与开发的安全开源项目主要包括：

- 基于Linux 内核模块的用户权限控制及审计系统
- Windows 网络抓包器

英文水平

托福105 + GRE 317，有一定的阅读英文文献以及英文输出能力

其他主要荣誉

上海市优秀毕业生（本科）、校级B等奖学金、校三好学生、优秀团员、学院优秀青年志愿者

2018年度全国互联网发展基金会网络安全奖学金