徐尚志

北京邮电大学

(+86) 15203936797
Email: shangzhi_xu@163.com

教育经历

北京邮电大学 **计算机科学与技术** **本科** 2019.9 – 2023.7 北京

相关课程

大三：操作系统、编译原理、linux开发、软件工程、数据库系统原理、现代交换原理、算法设计
大二：线性代数、电路与电子学基础、离散数学、数字逻辑与数字系统、计算机系统基础
概率论与数理统计、数学建模与模拟、计算机网络、计算机组成原理
大一：大数据分析技术导论、高等数学

工作经历

山石网科 **安全研发岗实习生** 2021.7-2021.9 北京

- 主要从事二进制病毒分析工作，分析病毒行为并书写病毒行为报告

1. 使用IDA，x32dbg，ollydbg等工具，实现脱壳与分析
   发现病毒主要危险行为是：利用MPRESS加壳，加密shell指令，创建新的计划任务，权限提升以及注册表修改。
   相关文档上传至山石网科文档系统；

2. 使用c++ 编写开发PE文件空白填充查找程序
   调用windows API随机填充PE文件中节区之间的空白区域，用于检测与证实查杀引擎单纯利用二进制文件全文匹配、特征码匹配对病毒查杀容易被绕过
   最终成果整理成论文《部分查毒引擎的局限性及验证》发表在《网络安全技术应用》杂志2022年2月刊。

项目经历

1. Java系统漏洞检测 **科研实习生** 2021.2-2022.8 北京

- 北京大学文伟平教授项目

项目目标客户为华为公司，针对反序列化漏洞、XSS漏洞、SQL注入漏洞、空指针调用漏洞，设计开发了一套漏洞检测软件工具。项目主要分为两部分：

1. 基于开源软件Soot将用户代码转换为jimple代码，随后依据污染传播规则进行漏洞挖掘
2. 基于百度开源软件OpenRasp，对恶意攻击流量进行检测并拦截。

结果表现漏洞检出率>90%，漏洞定位成功率>85%，漏洞类型识别准确率>85%,高于市面上常用的codeql工具

个人工作：

1. 参与设计污染传播规则并基于soot将设计思路转换为java程序。
2. 实现了域敏感分析、函数间污染传播检测功能
3. 负责漏洞库的收集建立

2. Fuzz test on Fuchsia **科研实习生** 2022.3-present USA

- 明尼苏达大学-Prof. Kangjie Lu项目

1. 独立科研，针对Google的最新系统Fuchsia借助syzkaller工具进行fuzzing test
2. 项目在调研阶段，正在学习与分析syzkaller源码

3. Python chat_bot & Search-Engine **课程学生** 2021.9-2022.6 北京

- 北京邮电大学课程项目

1. 基于开源工具nltk和parse实现对话机器人脚本语言设计，实现自动化测试、词干提取，句子分词，拼写纠错等功能。
   Github：https://github.com/ShangzhiXu/Programming-practice-chat_bot
   课程设计成绩96/100

2. 基于开源工具nltk，使用Django框架实现了一个搜索引擎的demo。用Selenium爬取新闻，使用tf-idf算法提取新闻中关键词，再使用nltk提取用户搜索中的关键词。用cosine相似度、图片颜色识别来匹配最好的文章。
   Github：https://github.com/ShangzhiXu/Searching-Engine
   课程设计成绩94/100

4. MiniOS **课程学生** 2022.1-2022.6 北京

- 北京邮电大学课程项目

1. 操作系统课程设计，使用c++ 设计并开发了一个操作系统的demo，文件系统、进程管理等参照Linux系统进行设计，内存模块除参照Linux之外，还参照Fuchsia OS设计并实现了Safe Stack机制。
2. 整个项目实现了进程调度、文件管理、内存虚拟页式存储、swapIn/swapOut、block bitmap、中断设计、UI设计、设备管理等基本功能

   课程设计成绩93/100，小组组员中贡献排名第一

个人技能

英语技能

CET6通过	2021
托福105分	2022.4
GRE：V152+Q166+W3.5	2021.11

专业技能

学校课程成绩：86+/100
掌握：c/c++, python, java

相关经验：系统安全，漏洞挖掘，git，python开发，Django，java开发，逆向工程，二进制漏洞挖掘，病毒分析，windows开发，汇编语言，Matlab，IDA，x32dbg，ollydbg的使用，MS Office系列办公软件和程序开发的相关软件

获奖

校级三等奖学金 (2019-2020学年)
大创项目负责人，项目盈利超过30万人民币，项目获得一项专利、一项软件著作
软著：1份
期刊：1篇

第七届互联网+大赛，获得校级一等奖，排名前3%
第十七届北京市挑战杯市赛二等奖，500+参赛队伍
第七届互联网+大赛北京市市赛二等奖，排名前10%