



郑小叶

xiaoyez@zju.edu.cn
https://zxxyy.github.io/

教育经历

浙江大学网络空间安全硕士	2022.09-至今
Simon Fraser University计算机科学与技术交流生	2019.09-2020.06
浙江大学计算机科学与技术本科	2017.09-2022.06

项目经历

Automatically Locating Inconsistent Instructions between Real Devices and CPU Emulators for ARM Extension	2022-09-至今
---	------------

此论文拓展了前期的工作Examiner，利用kgdb通过master-slave架构在kernel-mode下自动化测试ARM指令在QEMU和真实设备上的一致性。

- 在ARMv7、ARMv8架构下搭建自动化测试程序，验证QEMU对Arm、Thumb、Arm64指令实现的正确性。
- 在测试的2,647,46条二进制指令中定位出60,630条不一致指令并分析相关原因。
- 在QEMU开源社区中提交3个相关issue

A Closer Look at the Rust Ecosystem: Evolution and Security Risks	2022-03 TOSEM(CCF-A)在投
---	------------------------

此论文Rust生态系统中存在的安全风险进行了全面调查，探究了Rust生态中的漏洞特征、漏洞存在位置以及漏洞修复方式。

- 收集了433个Rust相关漏洞、300个易受攻击的Rust代码库和218个相关漏洞修复提交。
- 总结了Rust生态中的漏洞类型、漏洞生命周期、漏洞变化趋势以及影响版本范围等。
- 通过Rust编译器插件定位Rust生态中漏洞代码位置信息，为漏洞修复提供指导。

实现轻量级的WEB服务器

使用C++中的socket编程以及多线程编程实现轻量级WEB服务器，实现效果如下：

- 服务器可以与浏览器建立TCP连接（支持多个浏览器同时连接）
- 服务程序能够正确解析HTTP协议，并传回所需的网页文件和图片文件

收获：这个项目让我理解并掌握了C++中的socket编程，加深了我对HTTP协议内容的理解。为了实现支持多个浏览器同时连接，我也了解了用C++进行多线程编程的基本知识。

实现类C语言的mini编译器	大三下学期
----------------	-------

基于Lex、Yacc以及LLVM，使用C++11实现类C语法编译器。该编译器支持一般的整型、浮点型、数组和指针类型，支持变量的声明、初始化，函数声明、调用，分支、循环、跳转等控制流，支持注释。

- 使用Lex结合Yacc对源代码进行词法、语法分析。
- 在语法分析阶段生成整个源代码相应的抽象语法树后，并对抽象语法树进行可视化输出。
- LLVM IR模块中定义的中间代码语法输出符合LLVM中间语言语法、机器无关的中间代码
- 根据本地指令集与操作系统架构，将中间代码编译成二进制目标代码

收获：这个项目加深了我对编译器的了解。从语法分析、词法分析、语义分析以及代码生成这个四个方面了解了编译过程，对编译过程中的数据结构，如抽象语法树、符号表等有了深入地理解。

实现Linux内核相关代码	大三上学期
---------------	-------

使用C语言以及C语言内联的RISCV汇编在QEMU模拟的RISCV架构下，实现Linux内核的模式切换、中断处理以及Linux内核中的进程调度、内存管理。

- 内核模式切换：实现了从M-mode与S-mode，S-mode与U-mode间的切换
- 中断处理：处理时钟中断，在用户态下实现系统调用
- 进程调度：实现了Shortest Job First以及Priority First的算法
- 内存管理：实现了RISCV页表的转换机制

收获：这个项目大大加深了我对操作系统的理解。整个项目是在GDB环境下调试，在QEMU虚拟机下运行，大大提升了我的调试能力。

单周期/多周期/流水线CPU实现	大三上学期
------------------	-------

在ISE平台上运用verilog编写并实现了单周期、多周期以及流水线CPU

- 实现了算数运算指令，跳转指令，分支指令
- 使用Predict not taken，datapath forwarding等策略解决流水线CPU中的控制竞争和数据竞争

Java 图书搜索引擎

这是一个基于 crawlerj4, jsoup, Lucene 三个库的图书搜索引擎，源代码请见<https://github.com/ZXXYy/webCrawler>

- 利用crawler4j库可以从当当网的图书网站中爬取相关的图书内容，再利用Jsoup库可以从HTML文件中解析出图书的标题、作者、分类、出版社等信息
- 通过JDBC可以将图书信息保存在本地的SQLite数据库中
- 通过从数据库导出的图书信息(以json文件格式储存)，使用Lucene库建立图书内容索引

Java 可联网日程表

独立实现了可以添加、删除、编辑日程信息、查看以往日程信息的日程表。具体效果请见<https://github.com/ZXXYy/Java-Calendar-Scheduler>

- 通过Swing库来实现日程表的GUI界面，通过MVC设计模式来对用户操作做出响应
- 通过Socket编程来实现用户与服务器之间的沟通
- 在服务器端通过JDBC来连接数据库来实现对用户行为的记录，以便在用户下次登录时同步之前的操作

Kaggle Rental Listing Competition

该项目与同学合作对Kaggle上的Rental Listing问题进行分析与预测，源代码请见<https://github.com/cjl99/Kaggle-Rental-Listing>。我的主要工作如下：

- 使用Fisher Score筛选数据集中的有效特征
- 使用决策树的算法模型预测用户对该租房的评价

实现MIPS的汇编器与反汇编器

利用C++的STL库中的map, vector, set等容器以及文件流等API，把MIPS汇编语言翻译成二进制机器码以及二进制机器码转化为MIPS汇编，实现效果如下：

- 接受用户输入信息，读入用户需要的操作以及需要转换的文件名，转换完成后输出对应文件
- 准确把MIPS汇编的算数运算指令，跳转指令，分支指令翻译成二进制码，反之亦然

收获：这个项目让我运用了C++中的STL库，以及更加深入地了解了MIPS这门汇编语言。

技能

编程能力

- 熟悉C++/C/Rust语言
- 会使用GDB对程序进行调试，了解makefile一般语法
- 了解x86/ARM/RISCV汇编
- 了解Linux及vim的常用指令
- 了解并使用过Java/Python

英语能力

- 托福成绩99分
- 六级成绩517分
- 四级成绩582分
- 有阅读英文文献的能力
- 可以用英语进行简单沟通

获奖经历

学业优秀奖学金*2
浙江大学(2018,2019)

Entrance Scholarship
Simon Fraser University
(2019)
VPR USRA Science
Graduate Award
Simon Fraser University
(2020)

关于我

踏实认真，勤学好问
代码基础扎实，学习能力强
爱钻研，喜欢体验新事物

兴趣爱好

跑步 🏃
旅游 🌍
vlog 📹