

# 刘瑞丰

电话: (+86) 13880440705

Email: hustliuruifeng@gmail.com



## 教育背景

2012.9 - 2016.7	华中科技大学	计算机学院	卓越工程师班
2016.9 - 2019.3	上海交通大学	软件学院	并行与分布式研究所(IPADS)

## 项目经历

- 注明: 在虚拟化环境中, 用户虚拟机简称Guest, 宿主机简称Host。Host与Guest都有自己的操作系统, 在云环境下一台Host能承载多个Guest同时运行

2016.11- 2017.5	Fidelius	操作系统/虚拟化
• 项目描述	通过将所有Guest内存页设置为只读, 并将修改页权限、对内存页的修改能力集中在Host一个较小的Code Base中, 实现对Guest内存的保护, 杜绝了恶意Guest攻陷Host后能够窃取别的Guest用户信息甚至操纵别的Guest的行为。与此同时, 我们对内存中关键数据以及Guest写入Disk的数据利用CPU硬件加密引擎进行加密。我们将所需加密的内容浓缩致最小, 以及使用硬件而非软件进行加密, 使得我们在保护Guest数据的同时具有很高的性能。	
• 主要贡献	通过研习Intel手册等资料了解页表和页表项结构, 了解记录Guest状态的VMCS结构, 了解如何利用CPU硬件加密; 运用所了解的信息参与开发; 实现硬件加密接口, 在项目中部署硬件加密模块; 参与后期测试, 数据统计与表格绘制。	
• 项目成果	该项目发表于2018年举行的顶级CCF-A类会议HPCA。	
• 项目收获	这是进入交大以来自己的第一个项目, 从这个项目中, 我迅速加载了自己在Linux环境下的开发能力, 以及对操作系统级别大项目的开发能力。离开了图形化界面, 学会利用vim, tmux, ctags等工具; 学会了一系列Linux的命令; 学会了kernel module的编写, makefile的规则, 虚拟化环境中对虚拟机的管理与使用。	
2017.6- 2017.10	XenVisor	操作系统/虚拟化
• 项目描述	虚拟化环境下的CPU有两种运行模式, 在Guest Mode和Host Mode。我们将不可信的Hypervisor放置于与Guest同一等级的Guest Mode, 用XenVisor替代Host Mode中Hypervisor的位置。原本Guest->Host的机制变为Guest->XenVisor->Host, XenVisor可信切具有较小Code Base, 杜绝了运行恶意Hypervisor对Guest带来的威胁。此外, 我们用CPU新特性VMFUNC加速了不同成员之间的调用, 同时加密内存与Disk对Guest进行保护。	
• 主要贡献	通过研习Intel手册等资料了解VMFUNC的部署与使用; 对Guest的启动镜像进行加密, 并在XenVisor中部署加密模块, 使得加密镜像能成功的在XenVisor上启动; 实现了Guest对磁盘写入数据的加密, 使得data buffer在XenVisor内进行加解密, 而在Hypervisor的buffer里, 以及disk中的内容将始终以密文形式存在。	
• 项目成果	2018年顶级CCF-A类会议OSDI在投。	
• 项目收获	开始学会利用Python与Shellscript写一些能提高效率的自动化脚本。对Guest的创建, 管理, 网络的配置与Guest内部环境的配置更加熟悉, 深入理解了虚拟环境下Host对Guest的内存管理, 进一步锻炼自己阅读文档的功力(Intel Manual)以及大型项目的参与能力。	
2017.11- 2018.4	Cuckoo Migration	操作系统/虚拟化
• 项目描述	将虚拟机从一个Host在不中断运行的情况下迁移到另一个Host一直是Host的任务, Cuckoo Migration将Host的职责浓缩到最小, 这样可以极大程度的降低虚拟机迁移与Host的耦合, 一定程度上消除Host异构对虚拟机迁移带来的限制。Cuckoo Migration利用VMFUNC功能为每个Guest分配两套页表, 在Guest内部构造镜像内存, 依靠Guest自己完成大部分虚拟机迁移工作。	
• 主要贡献	自行构思迁移方案, 实现全部项目, 撰写paper	
• 项目成果	发表于2018年Joint Cloud Computing Workshop。	

- **项目收获** 学会自己架构项目，尽可能多但又不牵强地复用代码，利用宏定义将不同阶段不同模块的代码选择性编译进内核，遇到bug能一步步通过打印一些信息来确定病灶；这次项目也给了我一个奔赴德国开会的机会，带队出国也给了我宝贵的经历。
- 

## 发表论文

- |                             |  |
|-----------------------------|--|
| <b>2018 HPCA</b><br>(CCF-A) | <b><i>Comprehensive VM Protection against Untrusted Hypervisor through Retrofitted AMD Memory Encryption.</i></b><br>👉 <a href="https://github.com/Refone/paper/tree/master/fideliuss">https://github.com/Refone/paper/tree/master/fideliuss</a> |
| <b>2018 JCC</b>             | <b><i>Cuckoo Migration: Self Migration on JointCloud Using New Hardware Features.</i></b><br>👉 <a href="https://github.com/Refone/paper/tree/master/cuckoo">https://github.com/Refone/paper/tree/master/cuckoo</a>                               |
- 

## 个人能力

- 主要使用语言为C/C++，喜爱Python，个人感觉语言不是问题，可以随学随用。
- 熟悉Linux的使用，以及在Linux环境下开发。
- 了解KVM、XEN、QEMU、Linux Kernel。
- 喜欢做一些提高工作效率的小工具，比如：

- |                       |  |
|-----------------------|--|
| <b>Grublist</b>       | 可以远程可视化设置启动kernel的python脚本<br>👉 <a href="https://github.com/Refone/RF-Tools/tree/master/grublist">https://github.com/Refone/RF-Tools/tree/master/grublist</a>        |
| <b>Showtree</b>       | 查看kernel module依赖树的Python脚本<br>👉 <a href="https://github.com/Refone/RF-Tools/tree/master/km-manager">https://github.com/Refone/RF-Tools/tree/master/km-manager</a>   |
| <b>File Encryptor</b> | 利用CPU硬件加密指令，快速对大文件加解密<br>👉 <a href="https://github.com/Refone/RF-Tools/tree/master/file-encrypter">https://github.com/Refone/RF-Tools/tree/master/file-encrypter</a> |
| <b>VM Manager</b>     | 利用shell编写的可以动态生成固定配置guest image并快捷启动的脚本<br>👉 <a href="https://github.com/Refone/vm">https://github.com/Refone/vm</a>   |
- 

## 自我评价

- 我喜欢反思，喜欢自我批判，喜欢追寻问题的本质。
- 相信实践是获得真理的唯一方法，希望在地不断地勤劳实践中一点点进步。
- 对重视的东西十分执着，不在意工作时间，但是深恶痛绝低效，生命应该被更高效地利用。
- 喜欢编程，喜欢凭借着自己的努力用代码实现逻辑的自动化，喜欢自己的工作为别人增添一点又一点的便利，希望自己或多或少的才能能让社会变得更好一点点。