李锦峰

(+86) 17601019426
lijinfeng@iie.ac.cn
readm.tech

教育经历

2011–2015 中国科学技术大学, 原子分子物理专业.
少年班学院, 严济慈物理英才班

2015–2021 中国科学院信息工程研究所, 计算机体系结构方向.
博士在读，导师：孟丹

研究方向

内存漏洞与攻击.

控制流完整性保护.

计算机体系结构.

研究成果

论文 ***Zipper Stack: Shadow Stacks Without Shadow***, ***Jinfeng Li***, *Liwei Chen, Qizhen Xu, Linan Tian, Gang Shi, Kai Chen and Dan Meng*, to be published in ESORICS 2020 (CCF-B) and in Journal of Computer Security (CCF-B).
基于链式 MAC 的后向控制流完整性保护，安全性高于影子栈 (Shadow Call Stack in Intel CET) 和基于 MAC 的后向控制流保护 (Pointer Authentication on ARM)。同时性能优于基于 MAC 的后向控制流保护。

论文 ***Efficient Return Address Verification Based on Dislocated Stack***, ***Jinfeng Li***, *Qizhen Xu, Liwei Chen, Gang Shi and Dan Meng* , to be published in Journal of IEEE TCAD (CCF-A).
基于 Zipper Stack 的更进一步设计与优化。

论文 ***ABCFI: Fast and Lightweight Fine-grained Hardware-assisted Control Flow Integrity***, ***Jinfeng Li***, *Liwei Chen, Gang Shi, Kai Chen and Dan Meng*, to be published in Journal of IEEE TCAD (CCF-A).
硬件支持的前向细粒度 CFI，目前所有细粒度硬件设计中性能开销和面积开销最低的设计。

论文 ***SCFI: Generic and Efficient Forward Fine-grained Control Flow Integrity based on Coarse-grained ISA Extensions***, ***Jinfeng Li***, *Liwei Chen, Gang Shi and Dan Meng*, 投稿中.
基于 Intel CET 技术中 IBT 扩展的细粒度前向 CFI，不需要硬件改动，无性能开销 (-0.14%)，代码尺寸膨胀 2.9%，(on SPEC 2006)

专利 学生一作发明专利 **13** 项，包括 **1** 项国际专利, 申请中，部分已公示。.

- KHP181111171.2 一种检测堆栈中返回地址被篡改的方法及装置
- KHP181111173.4 一种检测堆栈中返回地址被篡改的堆栈结构
- KHP181111175.6 一种检测堆栈中返回地址被篡改的链式堆栈结构　等

专利 非学生一作发明专利 **6** 项.

其他 部分工程.

- 编写漏洞原理验证平台；
- 参与处理器评估标准设计　等

技能

内存漏洞及攻击技术。

Chisel 语言 (基于 Scala 的硬件描述语言，用于硬件的快速开发。) 和 RISC-V 指令集。

CPU 设计研究：基于 RISC-V 指令集的 Rocket 核心的修改定制。

商用 CPU 控制流完整性扩展的应用，包括 Intel CET，ARM PA，BTI 等。
编译器相关研究：LLVM，gcc 等。

奖项和荣誉

Invited peer reviewer of IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (CCF-A)
学业奖学金
所长优秀奖　等

其他

本科方向　量子通信与计算相关。
实习经历　2014 年 6 月　中科院物理所固态量子实验室潘新宇老师组，参与 NV 色心相关实验。
交流经历　2015 年 6 月　交流学者身份访问 Guoxing Miao, Professor, Electrical & Computer Engineering department, University of Waterloo, Canada.
其他　日语:JLPT N2 级。