王立敏

联系方式: (+86) 15600818233　　毕业学校: 南京大学

电子邮箱: wanglimin@smail.nju.edu.cn　　最高学历: 博士

教育经历

2013.09 - 2017.07　**杭州电子科技大学**　**专业：计算机科学与技术**　**本科**

- 三好学生
- 获得过一、二等奖学金
- 优秀毕业生

2017.09 - 2020.07　**中国科学院信息工程研究所**　**方向：计算机体系结构安全**　**硕士**

- **导师：孟丹 所长，朱子元 正高级工程师**
- 三好学生

2020.09 - 至今　**南京大学**　**方向：网络安全，程序分析**　**博士**

- **导师： 卜磊 教授**

2023.09 - 至今　**新加坡南洋理工大学**　**方向：软件基因组项目，供应链安全**　**交换**

- **导师：林尚威 助理教授，刘杨 教授**

研究兴趣

1. Cache侧信道攻击及其相关的微架构攻击与防御.
2. APT攻击检测与防御，韧性架构构建与安全性分析.
3. 软件供应链漏洞影响分析，开源软件生态攻击面检测与漏洞挖掘.
4. 软件基因组项目，源代码冗余去除，以及unique代码片段的挖掘与重用，
5. 大模型提示工程，多等价命题指导的提示以提高大模型任务精度.

项目列表

1. 参与《面向服务器CPU熔断和幽灵等硬件安全威胁的系统解决方案》（核高基）
2. 主导《验伤和最小系统》（华为项目）
3. 主导《操作系统内构入侵检测技术》（华为项目）

论文列表

- Limin Wang, Lei Bu, and Fu Song. "SCAGuard: Detection and Classification of Cache Side-Channel Attacks via Attack Behavior Modeling and SimilarityComparison." In 60th Design Automation Conference (DAC'23). 2023.（CCF-A类国际顶级会议）

- Limin Wang, Lei Bu, and Fu Song. "Locality Based Cache Side-channel Attack Detection." In Proceedings of 10th International Workshop on Security Proofs for Embedded Systems, vol. 87, pp. 49-65. 2022.（EI）

- 王立敏,卜磊,马乐之,于笑丰,沈宁国.基于指标依赖模型构建与监控的攻击检测方法.软件学报,2023,34(6) （CCF-A类中文期刊）

- Limin Wang, Ziyuan Zhu, Zhanpeng Wang, and Dan Meng. "Analyzing the security of the cache side channel defences with attack graphs." In 2020 25th Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 50-55. IEEE, 2020. （CCF-C类国际高水平会议， Best paper candidate）

- Limin Wang, Lei Bu. Causal Control Flow-Guided Attack Detection with CTI，2024，在投

- Limin Wang, Lei Bu. Improving zero-shot task accuracy of large language models with multi-equivalent proposition prompts，2024，在写

- Limin Wang, Lei Bu, Chengwei Liu, Shangwei Lin, Yang Liu. CTI-Driven Open Source Software Supply Chain Modeling (and Attack Surface Discovery)，2024，在写

详细经历

博士期间

研究课题（模型驱动的攻击检测）

概述：针对当前主流的基于规则的攻击检测和基于异常定位的攻击检测方法无法有机结合，难以完成协同工作， 因为无法最大程度实现攻击检测的准确性的问题.我们提出了模型驱动的攻击检测方法.该方法通过着眼于攻击行为造成的状态而非千变万化的攻击行为本身来构建具有泛化性的攻击模型， 以弥补基于规则的攻击检测方法对攻击变种感知性低的缺点，实现对攻击变种的检测．随后， 基于该模型的指导， 进一步降低攻击检测方法的误报率，弥补基于异常定位的攻击检测方法由于导向性不足而误报率高的局限性．最终实现基于规则的攻击检测和基于异常定位的攻击检测优势的有机结合，在能够检测变种的同时降低误报率.

- **1. 华为《体检和最小系统》以及《操作系统内构入侵检测技术》研究项目（面向通用安全领域的模型驱动的攻击检测方法，例如 APT 攻击检测）**
  - 针对攻击及变种层出不穷难以防御的问题.本研究通过对不同攻击变种攻击步骤所依赖的条件，以及攻击步骤实施后对系统/软件的状态影响进行逻辑分析， 形成泛化性较高的攻击模型，并生成由预警指标以及关键指标组成的指标体系.基于指标依赖模型以及导出的监控指标体系，最终实现对 APT 攻击及其变种的精准检测.
  - 产出的论文《基于指标依赖模型构建与监控的攻击检测方法》 已发表在《软件学报》（CCF-A 类中文期刊）.
  - 针对当前攻击检测技术无法快速整合专家知识的问题，本研究亦通过爬取分析网络可获取的攻击知识，包括CVE漏洞库，CWE缺陷库，ATT&CK攻击框架以及网络攻击风险情报等.并将其构建成相应的知识图谱，弥补上层自然语言知识与底层日志信息的语义鸿沟，并与现有的攻击检测技术相结合，通过协同工作可以快速响应零日攻击以及新出现的攻击变种并降低攻击检测的误报率.
  - 产出论文《Causal Control Flow-Guided Attack Detection with CTI》，目前尚在投稿中.

2、《模型驱动的 Cache 侧信道攻击检测》研究项目（面向特定安全领域的模型驱动的攻击检测方法，如 Cache 侧信道攻击检测）

本研究分别利用"攻击行为具有局部性"以及"攻击变种通常共享相似的攻击行为"的特性实现模型驱动的 Cache 侧信道攻击检测.

- 利用 Cache 侧信道攻击的局部性，即在某些与攻击相关的步骤中，内存块的数据访问是密集的，而这些行为通常稀疏地分布在不同的攻击步骤中.基于该观察，本研究提出通过嵌入程序运行时的处理器状态，即高性能计数器， 到该程序的静态控制流图中， 并使用 GNN 训练提取控制流图中的关键攻击结构形成模型以识别和分类攻击.
- 该研究的产出《Locality Based Cache Side-channel Attack Detection》已发表在 10th International Workshop on Security Proofs for Embedded Systems （PROOFS 2021， EI 收录)
- 攻击变种通常共享相似的攻击行为，本研究提出通过结合程序运行时信息（例如高性能计数器，访存地址）以及该程序的控制流图来识别与攻击相关的基本块并随后捕获这些基本块执行后导致的 Cache 状态迁移形成攻击行为模型.随后通过对比目标程序的模型与攻击模型的相似度来识别和定位攻击行为.
- 该研究产出《SCAGuard: Detection and Classification of Cache Side-Channel Attacks via Attack Behavior Modeling and Similarity Comparison》 已被 60th Design Automation Conference （DAC 2023 ， CCFA 类国际顶级会议） 接收.

3、《开源软件供应链安全》研究项目

- 利用大模型回答的一致性，我们将大模型的多种自然语言任务抽象为分类任务并进行命题化，利用命题等价性生成不同等价提示，进行fine-tuning或多重zero-shot提示提高大模型精度.
- 预计产出论文《Improving Zero-shot Task Accuracy of Large Language Models with Multi-equivalent Proposition Prompts》，正在撰写中.
- 利用CTI以及开源软件包的开发、提交、维护记录等，通过自然语言处理等手段自动化构建完整的开源软件供应链的角色以及风险模型. 可用于指导后续软件包中的属性变动分析或者开源软件新增代码的非预期功能检查.
- 预计产出论文《CTI-Driven Open Source Software Supply Chain Modeling (and Attack Surface Discovery)》，正在撰写中. 需要注意的是新的攻击面挖掘工作正在同步进行，如能赶上投稿，新发掘的攻击向量相关的内容将被加入本论文.

4、《软件基因组》研究项目

- 借助生物学中的基因片段概念，选取github全量代码，去除其中的冗余代码部分，保留unique代码片段作为软件的基因，后续用于代码大模型的训练以及低代码平台搭建.
- 根据开源软件包的代码新增情况分析代码演化过程，通过聚类感知具有普遍意义的演化方向，分析其中的功能性和安全性语义，并用于代码/软件包推荐等. 后续也将进一步开展非预期代码/功能的检查.

硕士期间　　**研究课题（处理器安全方向）**

- **1、ORAM 安全内存相关研究**

  主要负责在 Gem5 模拟器上进行实验验证

  即修改 Gem5 模拟器， 在研究其内存， Cache 模块的基础上进行修改， 并 且新增 ORAM 模块， 使其具有安全功能.

- **2、针对 Meltdown 和 Spectre 漏洞的 CPU 防御方案的评估**

  - 主要负责利用形式化方法从理论上评估 CPU 防御措施是否安全.采用时序逻辑CTL为微结构关键部件与功能构建抽象模型，并且总结了熔断幽灵漏洞以及相关侧信道问题的攻击模式，利用攻击过程所需的关键状态序列构建安全规格，最终利用修改后的形式化模型检验工具NuSMV来验证模型是否满足安全规格，若不满足，则工具将自动生成反例（即攻击路径）来证明其不满足.需注意的是，本论文修改了模型检验工具NuSMV，使其在验证不通过时可生成多个反例，随后本文收集了这些反例，并编写代码，将这些抽象的反例转换成可读性高的攻击图，便于后续分析其安全性缺陷.
  - 论文《Analyzing The Security of The Cache Side Channel Defences With Attack Graphs》发表在 ASP-DAC 2020（CCF-C类高水平国际会议, Best Paper Candidate）

    研究点1：熔断幽灵硬件漏洞以及相关侧信道攻击

    -- 研究熔断幽灵以及侧信道攻击的攻击机理（包括LLC攻击）

    -- 研究现有POC的实现代码，复现一些攻击

    研究点2：模型检验（时序逻辑）

    -- 主要在于研究计算树逻辑（CTL）的原理，应用和实现

    -- 修改现有的开源模型检验工具NuSMV

    研究点3：计算机体系结构及其建模方法

    -- 研究经典体系结构以及现有的一些抽象机模型

    -- 研究微结构上的漏洞防御措施以及安全机制

本科期间　　**工作内容**

- **1、基于Tensorflow的人脸识别项目**
  （实验室项目）
- **2、小型操作系统的研究与实践**
  （毕业设计）