

课程实践报告



**课程 网络攻防技术(314006040)**

**课 序 号 3**

**作业名称 Spectre Attack Lab**

**评分**

**姓名** 邓嘉怡 **学号** 2022141530010

# 作业题目

幽灵攻击于2017年发现，并于2018年1月公开披露，它利用关键漏洞进行攻击，存在于许多现代处理器中，包括Intel、AMD和ARM处理器。漏洞允许程序突破进程间和进程内的隔离，以便恶意程序可以读取来自无法访问区域的数据。硬件保护不允许这样的访问机制（用于进程间的隔离）或软件保护机制（用于进程内的隔离），但CPU设计中存在漏洞，可能会破坏保护。因为缺陷存在于硬件中，很难从根本上解决问题，除非更换CPU。幽灵和熔断漏洞代表了CPU设计中的一种特殊类型的漏洞，它们还为安全教育提供了宝贵的一课。

本实验的学习目标是让学生获得幽灵攻击的第一手经验。攻击本身非常复杂，因此我们将其分解为几个小步骤，每个步骤都是易于理解和执行。一旦学生理解了每一步，就不难理解了把所有的东西放在一起进行实际的攻击。本实验涵盖了以下内容:

•幽灵攻击

•侧通道攻击

•CPU缓存

•CPU微体系结构内的无序执行和分支预测

# 实验步骤及结果 Tasks 1 and 2: Side Channel Attacks via CPU Caches Task 1: Reading from Cache versus from Memory 该代码示例通过刷新缓存、访问特定内存地址并测量访问时间，演示了如何利用 Flush+Reload 技术检测内存访问模式。这种技术在侧信道攻击中具有重要应用，能够在不直接访问敏感数据的情况下，通过分析缓存行为推测出敏感信息。了解和掌握这种技术对于设计更安全的系统具有重要意义，同时也强调了在现代计算环境中硬件层面安全的重要性。 运行多次后，访问array[3\*4096]和array[7\*4096]的速度确实比其他的快，根据数次测试，判断阈值为150 CPU cycles Task 2: Using Cache as a Side Channel 通过刷新整个数组缓存、调用受害者函数访问特定元素、然后重新加载数组并测量访问时间，可以利用 刷新+重加载（Flush+Reload） 技术推测出秘密值。为了避免缓存行级别的干扰，使用一个大数组（256 \* 4096字节）确保每个秘密值对应的数组元素位于不同的缓存行，从而提高推断的准确性。 实验过程： 经过数次努力，将阈值从30-100均尝试过后 在阈值为45时得出结果 且实验结果不稳定，猜测为硬件原因

Task 3: Out-of-Order Execution and Branch Prediction

语句

清除CPU 的cache中size变量的值

不注释

清除了

那么CPU回访问交办的主存中的值

因此CPU会并行执行if语句的访问结果

注释

没清除CPU cache

CPU会直接访问cache

速度快，所以不会

# 实验总结

请对本次实验进行总结，描述通过本次实验学到什么，特别是实验过程的问题的解决过程的总结和体会。