**实验12：幽灵攻击实验**

**时间：**第13周

**地点及方式**：教室

**人员：**全体学生

**实验内容：**

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

**实验报告：**

需要提交一份详细的实验报告和截图，来描述做了什么和观察到了什么。**还需要对观察结果进行解释**。还请列出重要的代码片段，然后进行解释。仅附加代码而不作任何解释将不得分。

**评分要点：**

1. 功能完成情况：60%；
2. 代码规范性：20%；
3. 报告质量：20%

**提交方式：**

请在学习通作业模块提交，选择对应的作业编号进行提交，请注意：

* 代码命名为：Lab12\_code\_学号.zip
* 文档命名为：Lab12\_doc\_学号.pdf