云环境下侧信道攻击技术

唐青昊 360公司云安全研究部经理

360 Marvel Team 负责人

金意儿 University of Florida

Cyber Immunity Lab

云安全研究部介绍

于2015年成立，国内首支云环境下的前沿安全议题研究团队（对外名称360 Marvel Team），研究方向包括虚拟化系统安全攻防 和 侧信道安全攻防。致力于保持领先的脆弱性安全风险发现和防护能力，成立以来取得如下成果：

- 累计公布56个云安全漏洞，完成pwn2own，pwnfest中的vmware workstation破解项目
- 实现docker，xen，kvm，vmwre环境下的虚拟机逃逸工具
- 打造虚拟化系统加固产品“360云加固” 和 云UEBA产品“云感知”

目录

- 侧信道攻击原理介绍
- 云环境下的侧信道攻击实践

  Memory bus通道

  Mob时序通道
- 危害和防护建议

原理介绍

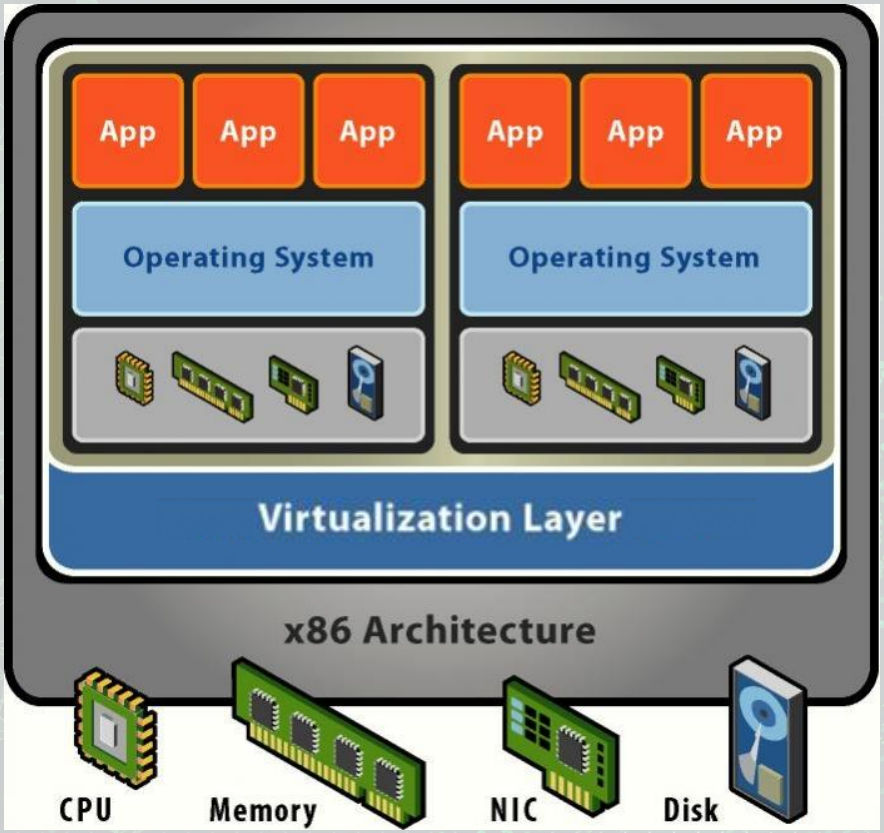
举例

通过收集音频获取邮件密码

什么是侧信道攻击

被广泛应用于在密码学领域，指从其他渠道获取数据标签，确定密码内容。如通过采集电子加密设备运行过程中的能量消耗，电磁辐射，运行时间信息进行密码破解。

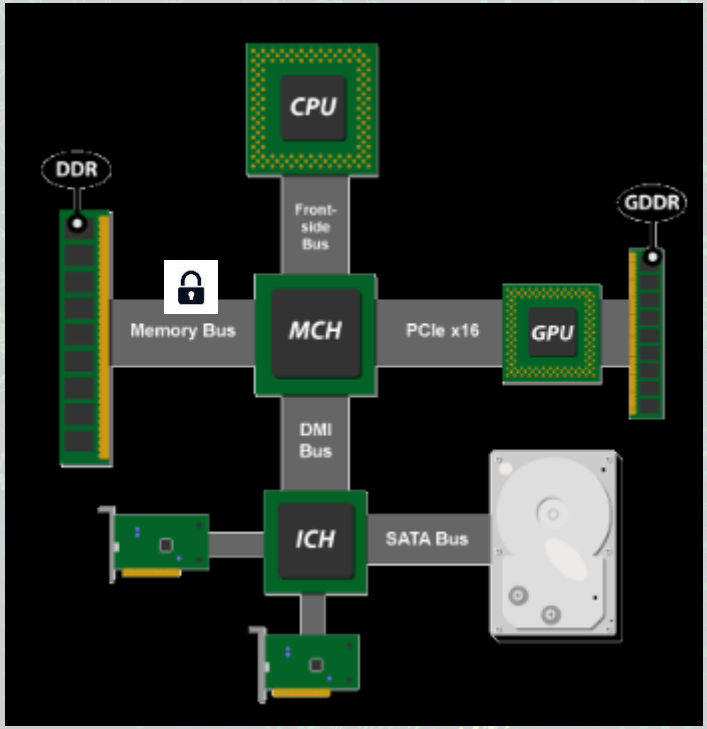
为什么可以在云环境下进行侧信道攻击



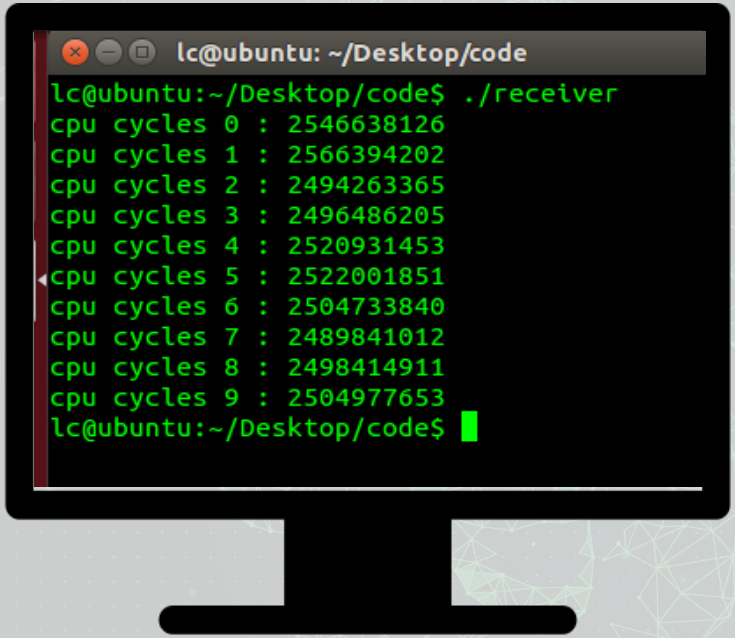
MEMORY BUS通道

工作原理

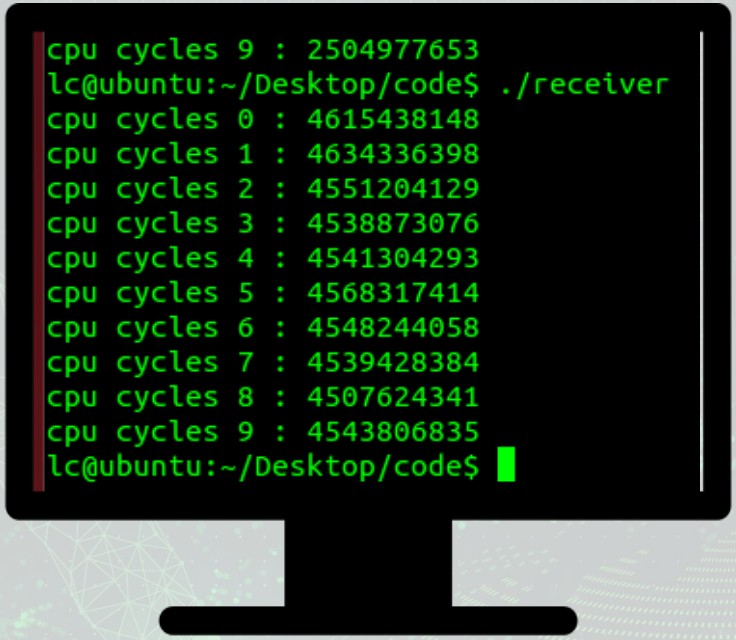
由于执行原子性指令会锁住内存总线。因此在同一台宿主机上的不同虚拟机当中同时执行原子性指令时，其执行时间会明显差异于 不同宿主机上的两台虚拟机同时执行原子性指令的时间。



攻击场景-单通道情况下的同驻检测

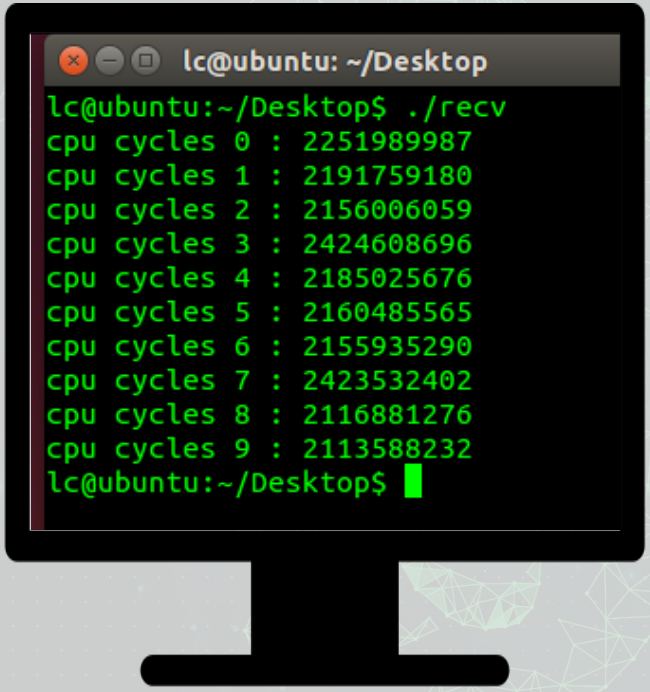


A虚拟机单独执行RECEIVER的情况

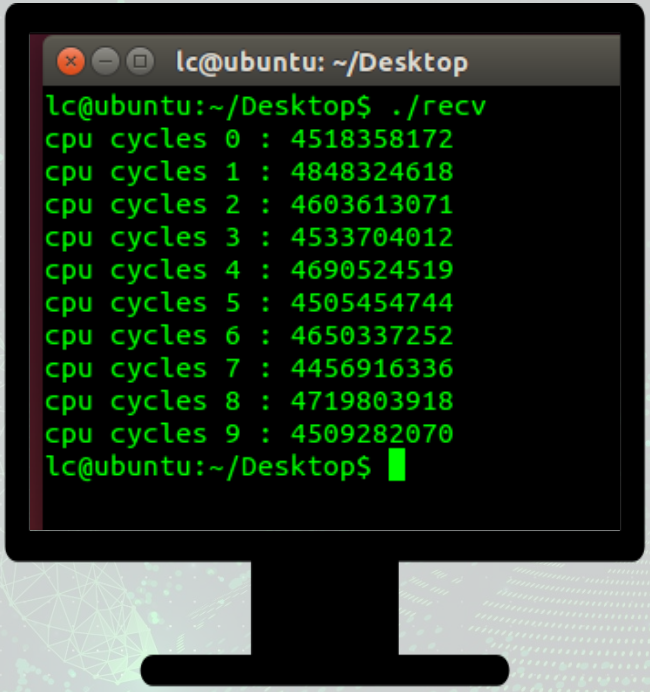


在B虚拟机执行SENDER时，同时在A虚拟机执行RECEIVER的情况

攻击场景-双通道情况下的同驻检测



A虚拟机单独执行RECEIVER的情况



在B虚拟机执行SENDER时，同时在A虚拟机执行RECEIVER的情况

MOB时序通道

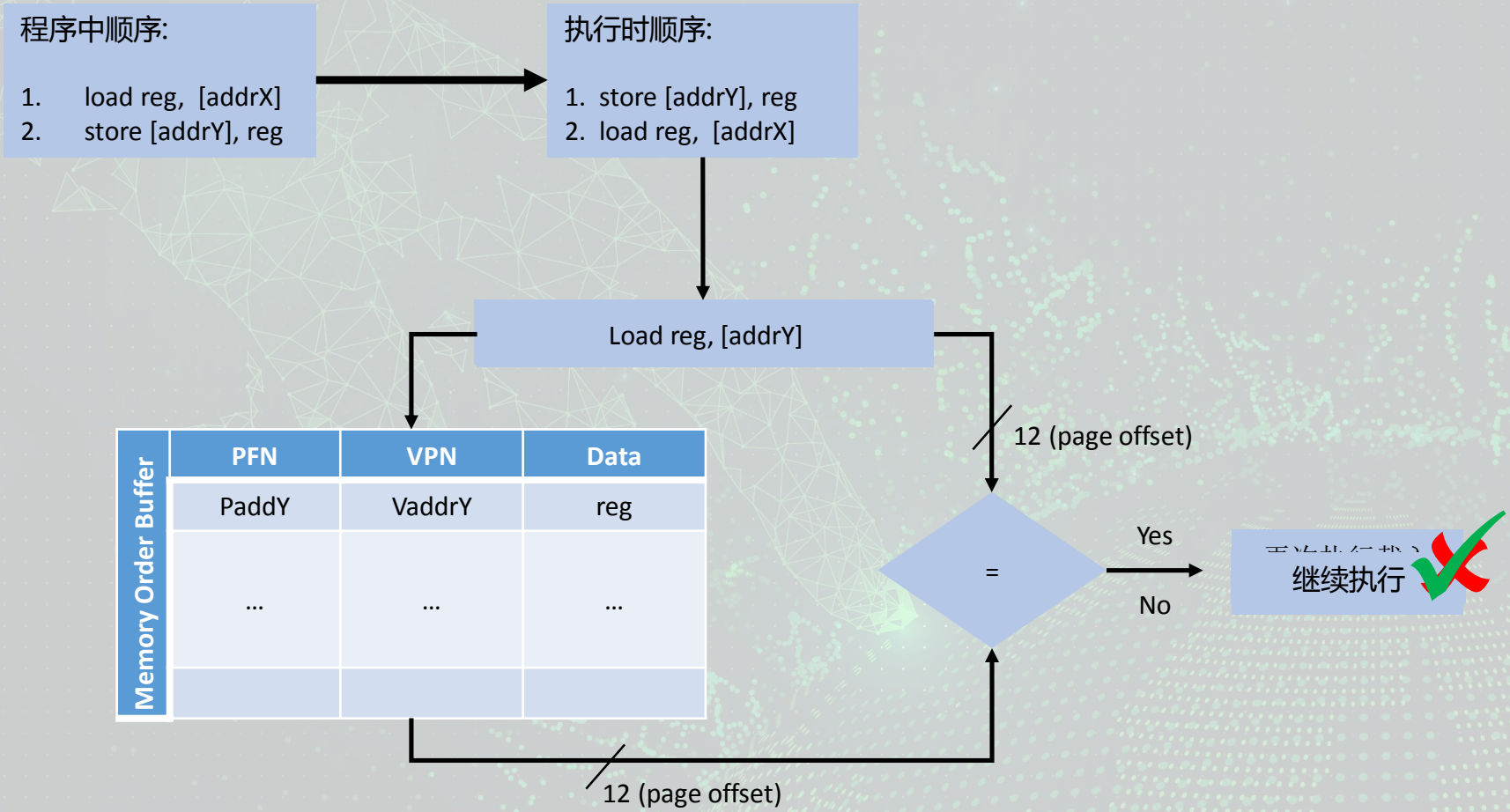
一些概念

MOB是MEMORY ORDERING BUFFER 的全称，中文名字存储器排序缓冲区。（从迅驰开始）是英特尔处理器中关键的微架构组件，它允许内存读取和写入操作进行重新排序。

MOB组件的4K混淆现象：即每次读取要复制的数据时，一个4 KB对齐的基址将与源缓冲区的4 KB对准基址错误匹配。

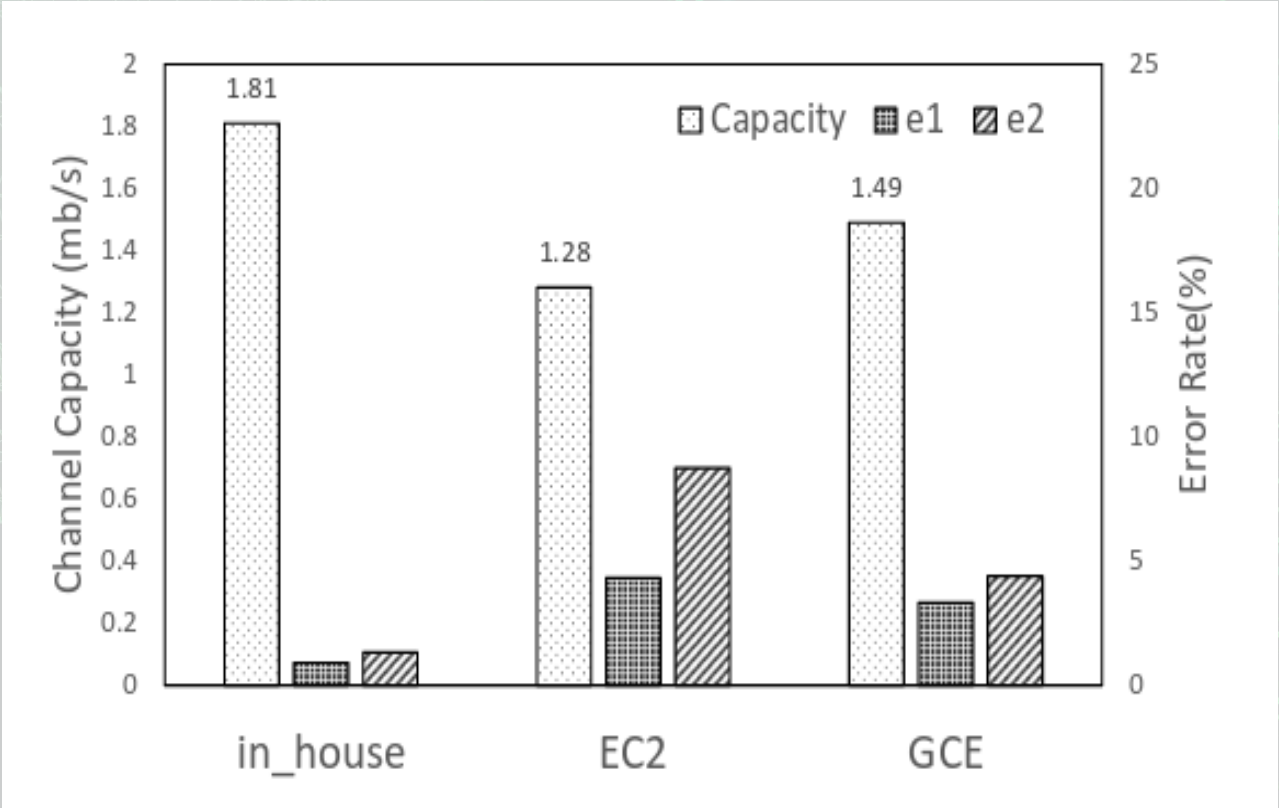
4K-混淆定时信道：当同一宿主机上的两台虚拟机，造成MOB的低12位与存储器地址匹配时，存储器消歧预测不能推测负载时，就会引起4K-混淆定时信道。

load与pre-store的消歧过程



攻击场景-建立虚拟机间的通信隧道

	Instance Type	Processor
EC2	m4.large	2.4 GHz Intel Xeon E5-2676 v3
GCE	n1-standard-1	2.3 GHz Intel Xeon E5 v3



危害和防护

危害

- 侧信道攻击可以影响目前流行的公有云和私有云产品，并且云相关公司较少关注侧信道攻击，此种攻击类型将长期存在。

- 侧信道攻击利用的是硬件本身的特性，其成本远远小于漏洞攻击，且不易修复。

- 侧信道攻击地位：用于补充云环境的其他攻击手段。

  虚拟机逃逸+侧信道攻击

  远程命令执行+侧信道攻击

防护建议

- 基于规则的二进制文件加载时静态审查

  优点：系统资源占用低

  缺点：会产生误报

- 通过干扰反馈对威胁进行感知

  优点：精准发现威胁

  缺点：系统资源占用高

谢　谢

ISC 2017 中国互联网安全大会

360互联网安全中心

tangqinghao@360.cn


ISC
2017
5th
2017 中国互联网安全大会
China Internet Security Conference
万物皆变 人是安全的尺度
Of All Things Human Is The Measure