



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

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

金意儿

360 Marvel Team 负责人

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

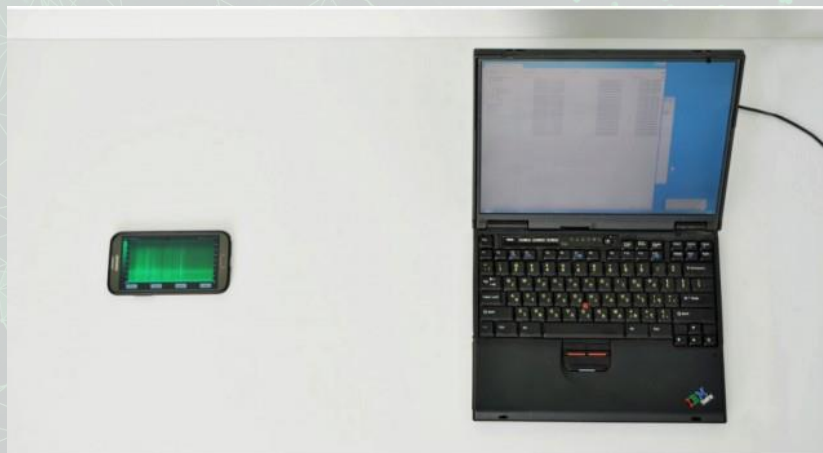
Memory bus通道

Mob时序通道

- 危害和防护建议

原理介绍

举例

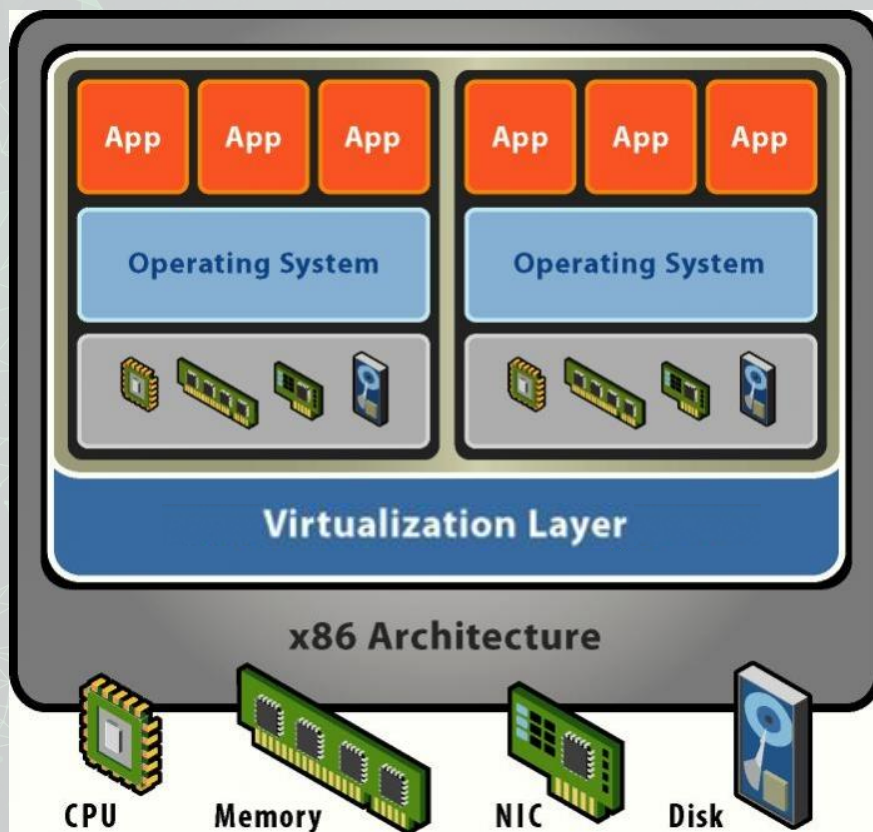


通过收集音频获取邮件密码

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。

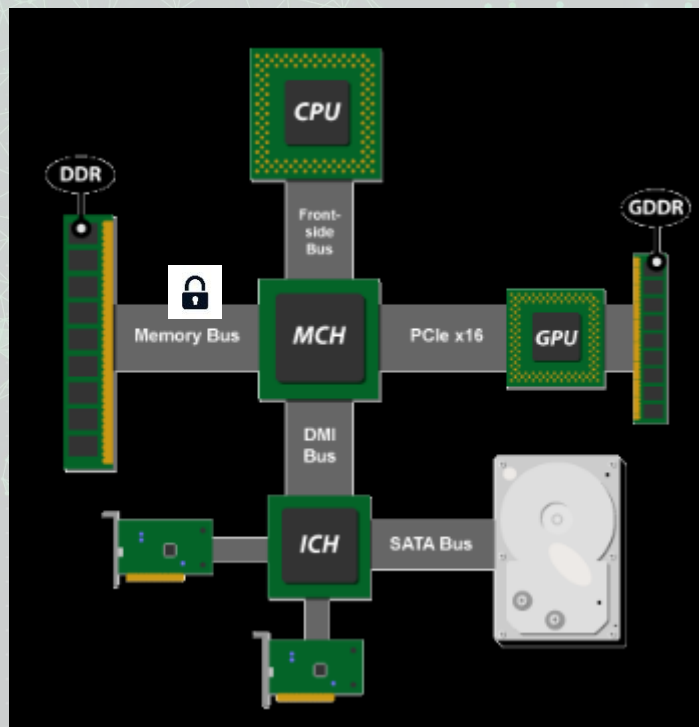
为什么可以在云环境下进行侧信道攻击



MEMORY BUS通道



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

```
lc@ubuntu: ~/Desktop/code
lc@ubuntu:~/Desktop/code$ ./receiver
cpu cycles 0 : 2546638126
cpu cycles 1 : 2566394202
cpu cycles 2 : 2494263365
cpu cycles 3 : 2496486205
cpu cycles 4 : 2520931453
cpu cycles 5 : 2522001851
cpu cycles 6 : 2504733840
cpu cycles 7 : 2489841012
cpu cycles 8 : 2498414911
cpu cycles 9 : 2504977653
lc@ubuntu:~/Desktop/code$
```

A虚拟机单独执行RECEIVER的情况

```
cpu cycles 9 : 2504977653
lc@ubuntu:~/Desktop/code$ ./receiver
cpu cycles 0 : 4615438148
cpu cycles 1 : 4634336398
cpu cycles 2 : 4551204129
cpu cycles 3 : 4538873076
cpu cycles 4 : 4541304293
cpu cycles 5 : 4568317414
cpu cycles 6 : 4548244058
cpu cycles 7 : 4539428384
cpu cycles 8 : 4507624341
cpu cycles 9 : 4543806835
lc@ubuntu:~/Desktop/code$
```

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

```
lc@ubuntu: ~/Desktop
lc@ubuntu:~/Desktop$ ./recv
cpu cycles 0 : 2251989987
cpu cycles 1 : 2191759180
cpu cycles 2 : 2156006059
cpu cycles 3 : 2424608696
cpu cycles 4 : 2185025676
cpu cycles 5 : 2160485565
cpu cycles 6 : 2155935290
cpu cycles 7 : 2423532402
cpu cycles 8 : 2116881276
cpu cycles 9 : 2113588232
lc@ubuntu:~/Desktop$
```

A虚拟机单独执行RECEIVER的情况

```
lc@ubuntu: ~/Desktop
lc@ubuntu:~/Desktop$ ./recv
cpu cycles 0 : 4518358172
cpu cycles 1 : 4848324618
cpu cycles 2 : 4603613071
cpu cycles 3 : 4533704012
cpu cycles 4 : 4690524519
cpu cycles 5 : 4505454744
cpu cycles 6 : 4650337252
cpu cycles 7 : 4456916336
cpu cycles 8 : 4719803918
cpu cycles 9 : 4509282070
lc@ubuntu:~/Desktop$
```

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

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

程序中顺序:

1. load reg, [addrX]
2. store [addrY], reg

执行时顺序:

1. store [addrY], reg
2. load reg, [addrX]

Load reg, [addrY]

Memory Order Buffer	PFN	VPN	Data
	PaddrY	VaddrY	reg

12 (page offset)

=

Yes

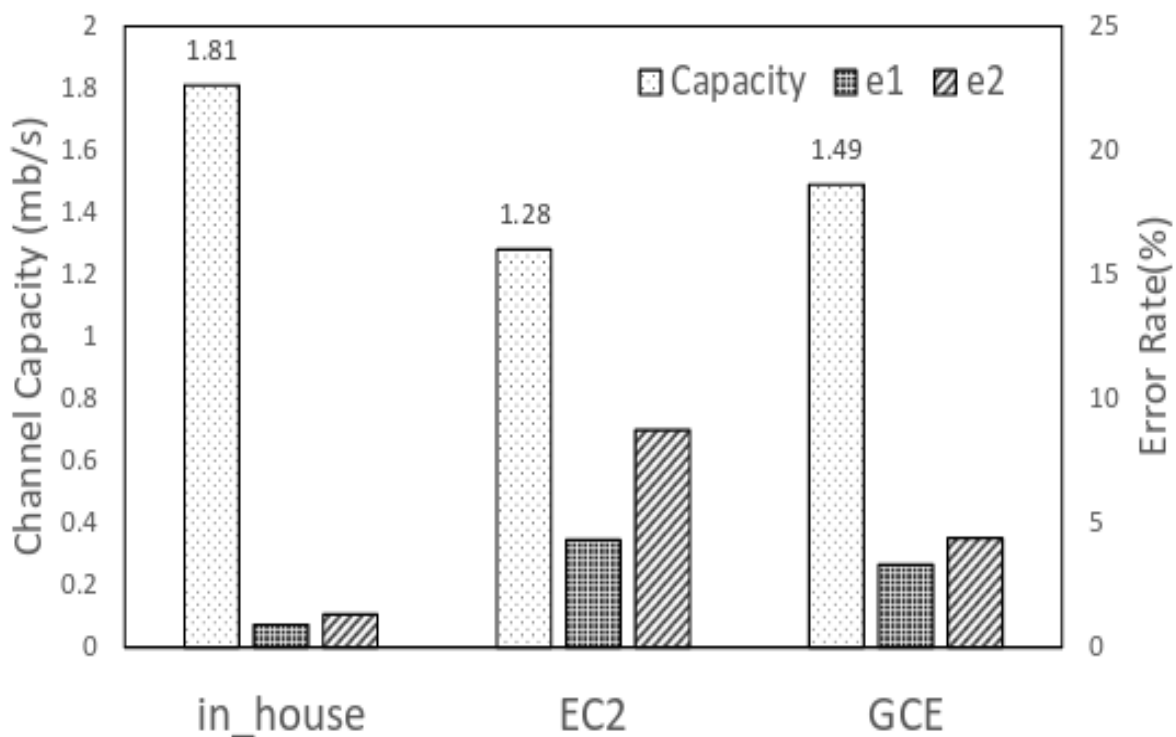
No

继续执行

12 (page offset)

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

- 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

- 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



中国互联网安全大会



360互联网安全中心

tangqinghao@360.cn





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