Flush+Reload Microarchitectural Covert Channels in cluster

李敬 Jing Li

2021年7月6日

辛丑仲夏廿七

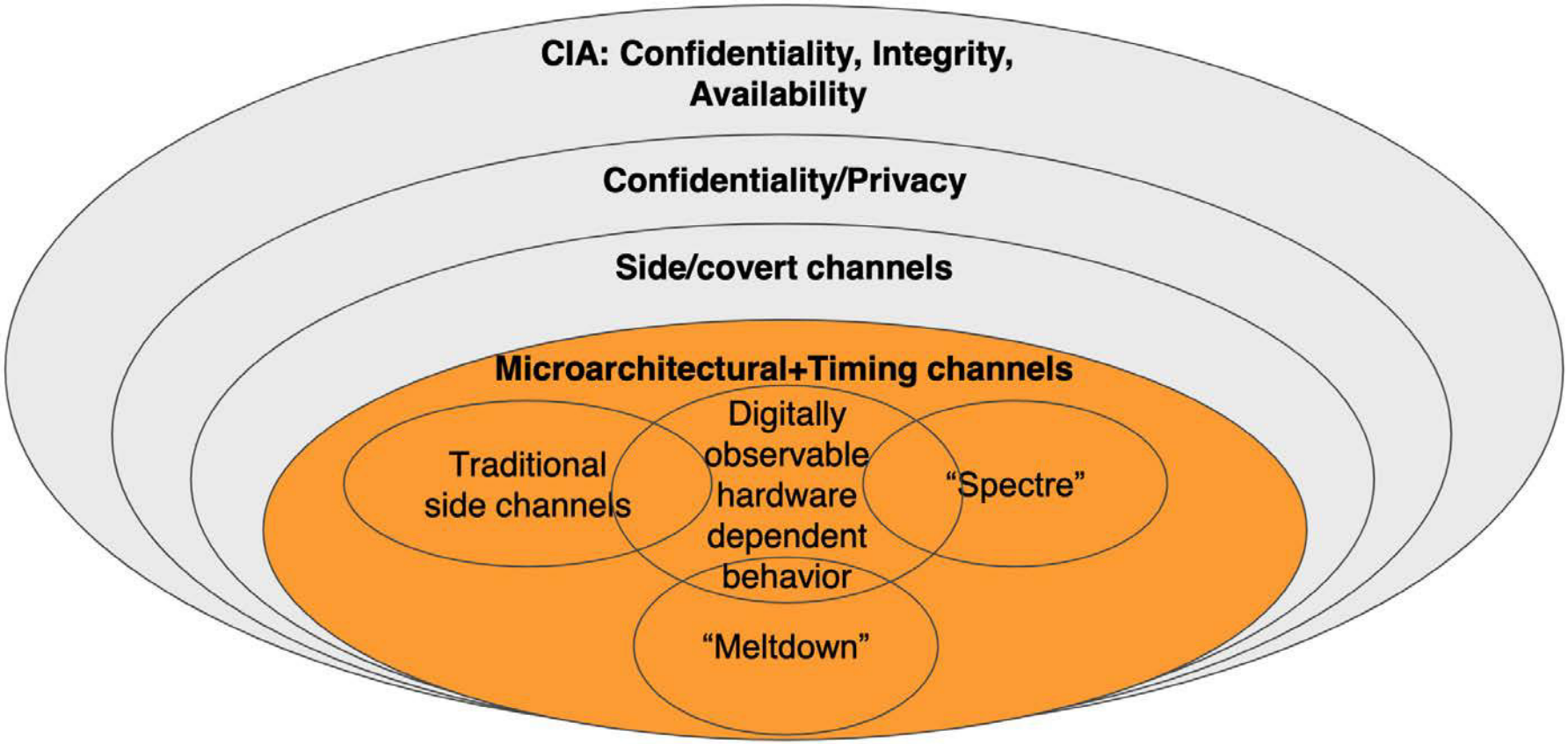
北京 · 怀柔

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

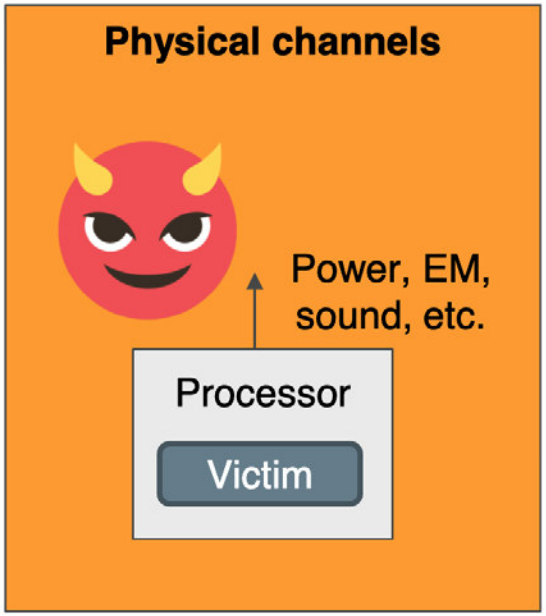
Contents

* Most of this slide reference ISCA 2019 tutorial, Source: https://sites.google.com/view/arch-sec/home

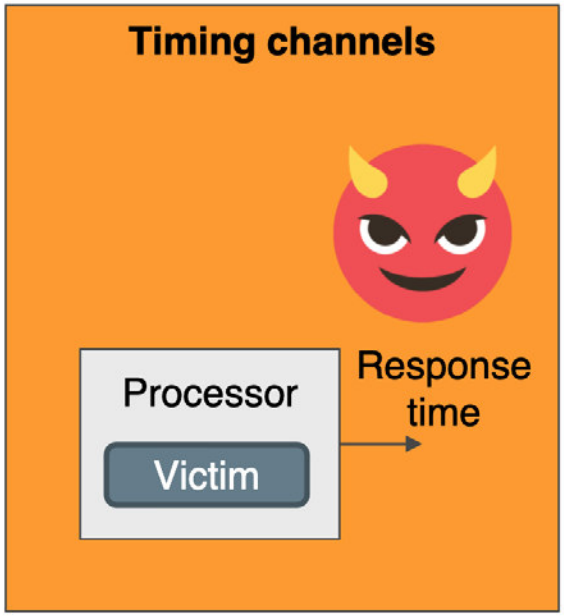
物理计算环境的微体系结构隐蔽信道



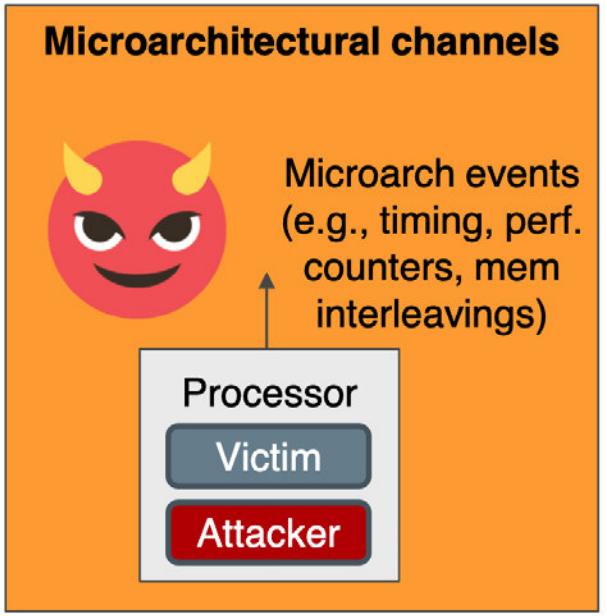
对底层的隐蔽信道区别



Attacker requires measurement equipment → physical access

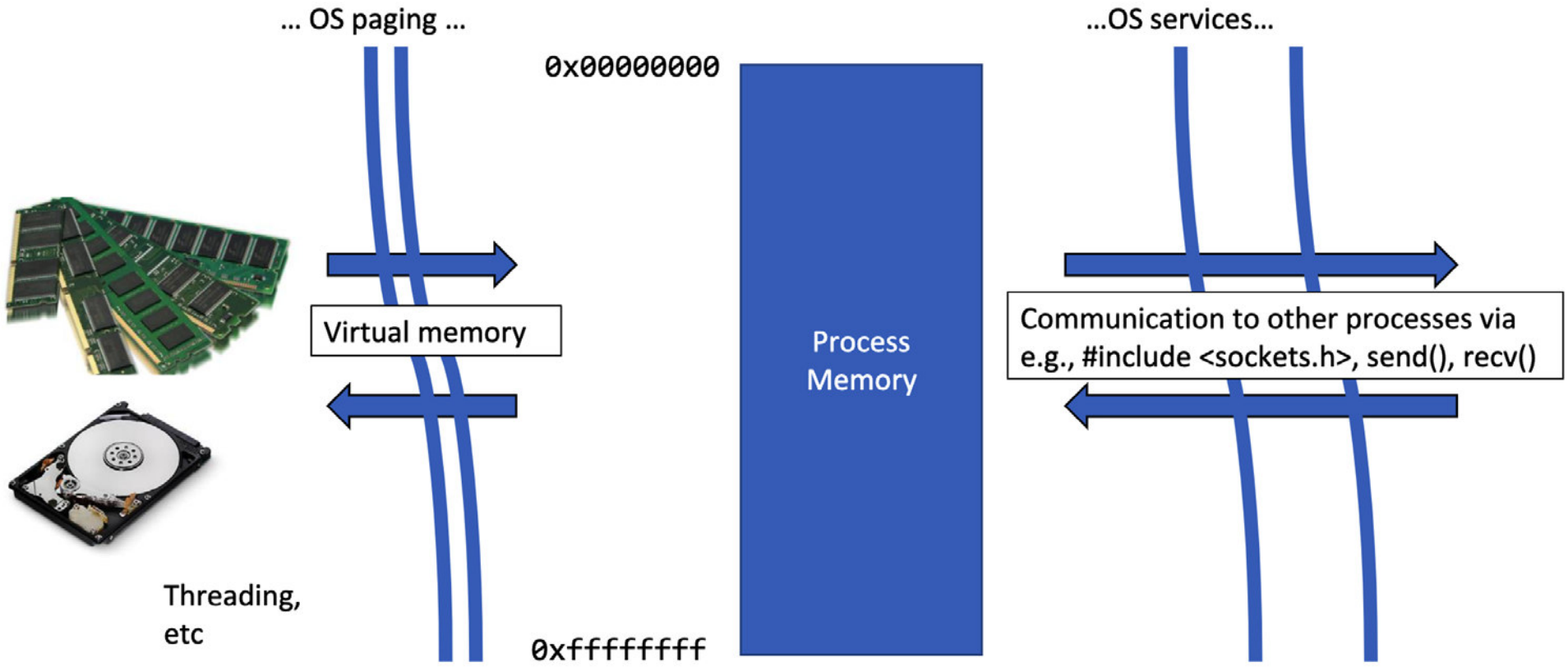


Attacker may be remote (e.g., over an internet connection)



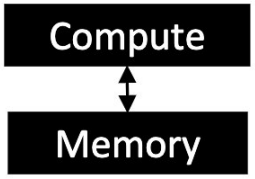
Attacker may be remote, or be co-located

进程隔离与通信

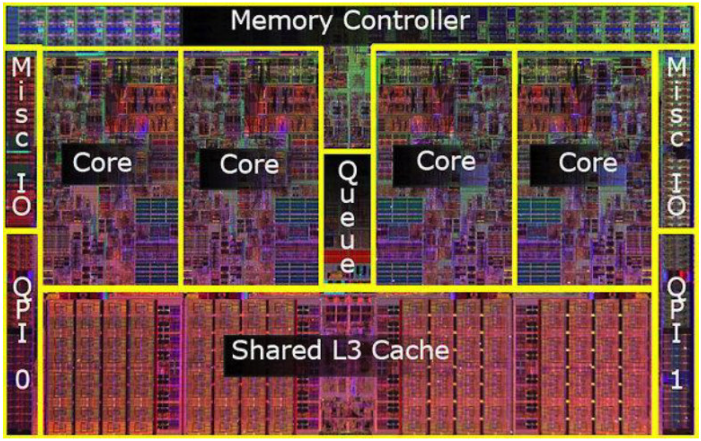

... OS paging ...
0x00000000
...OS services...
Virtual memory
Process Memory
Communication to other processes via
e.g., #include <sockets.h>, send(), recv()
Threading, etc
0xffffffff

实际程序跑的HW环境（尤其在数据中心环境）

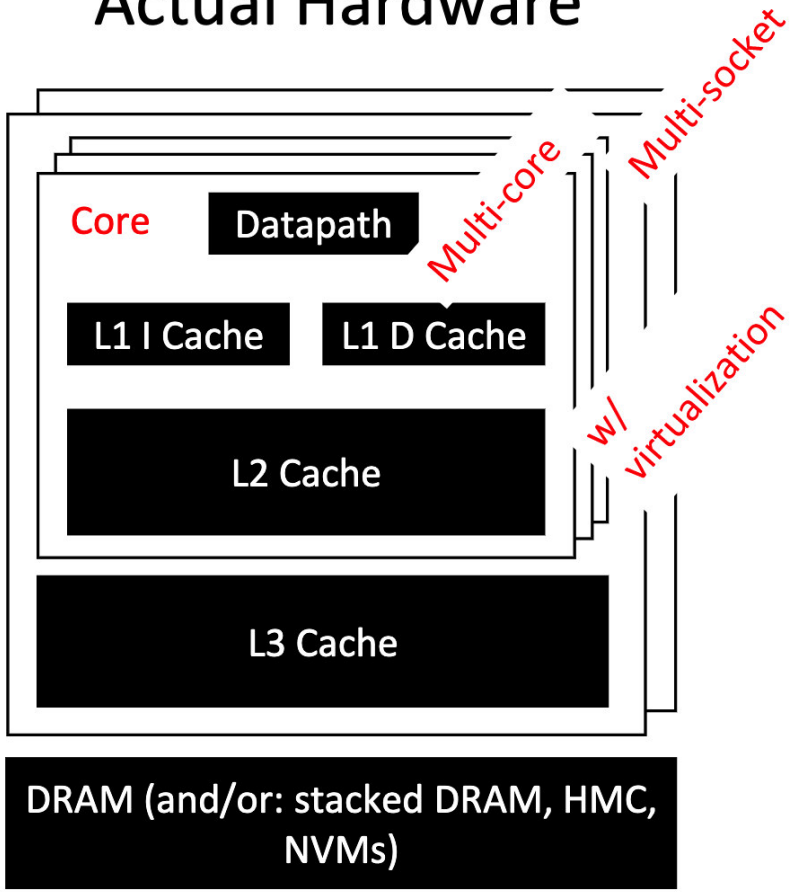
Programmer Interface



OS swaps work on/off

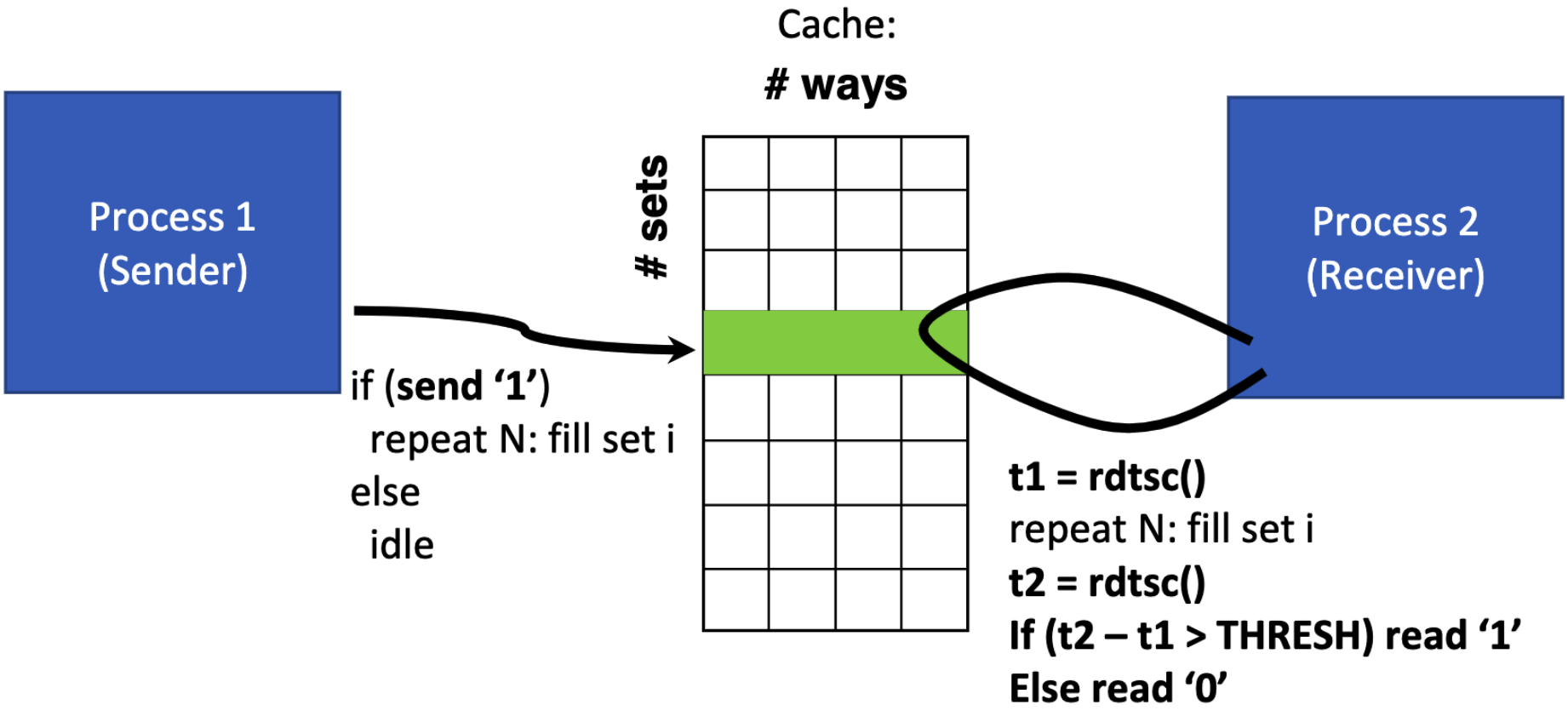


Actual Hardware

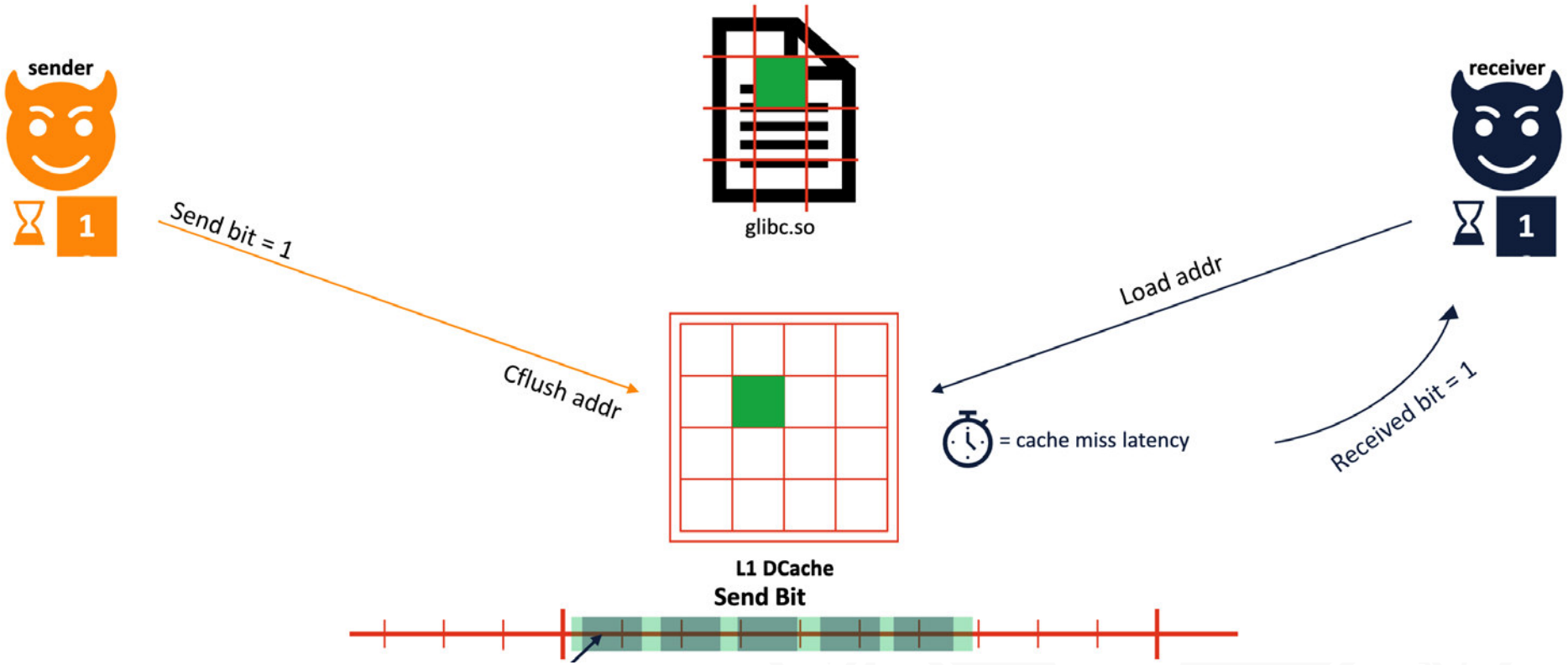


Goal: create a send(), recv() abstraction using HW contention (→ without using the OS/other sanctioned interfaces)

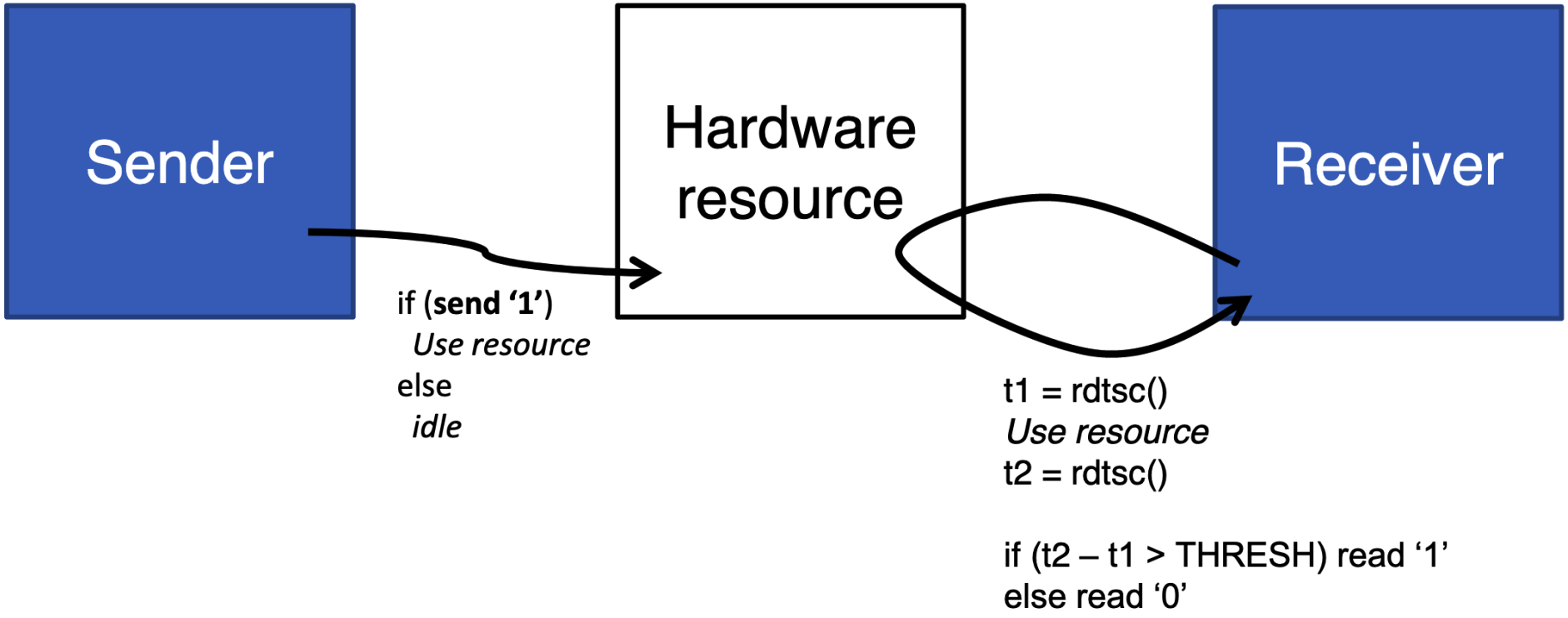
Send 1 bit in Cache



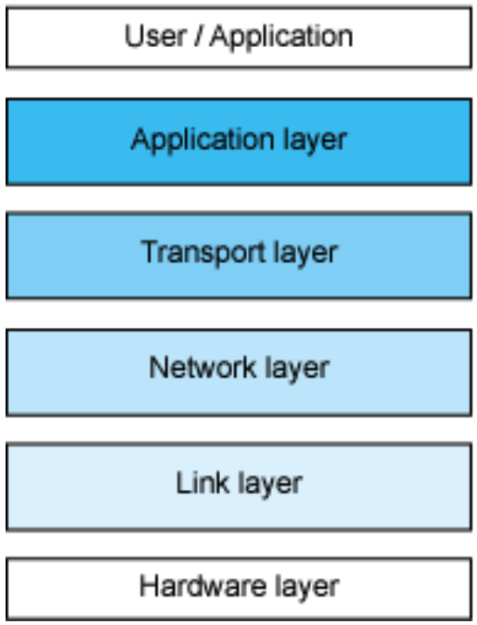
Flush+Reload



Cache之外的HW也可构造



此时的网络栈流程



Network + Transport layer
Handshakes,
Error correction, etc.

Data layer
Protocol to modulate channel:
Prime+probe (cache)
Flush+reload (cache)

Physical layer
Resource contention (the channel):
Private cache
Shared last-level cache
RAND unit

模拟测试Demo

```
lj@fate-host:/home/app/lijing-work$ ./fr-send -f /mnt/lijin
g/home/app/lijing-work/covert-channel-tutorial/build/lj9
Please type a message (exit to stop).
< hello,ucas,2021
< [+]This is Flush+Reload Microarchitectual covert channel.
< exit
Sender finished
lj@fate-host:/home/app/lijing-work$
```

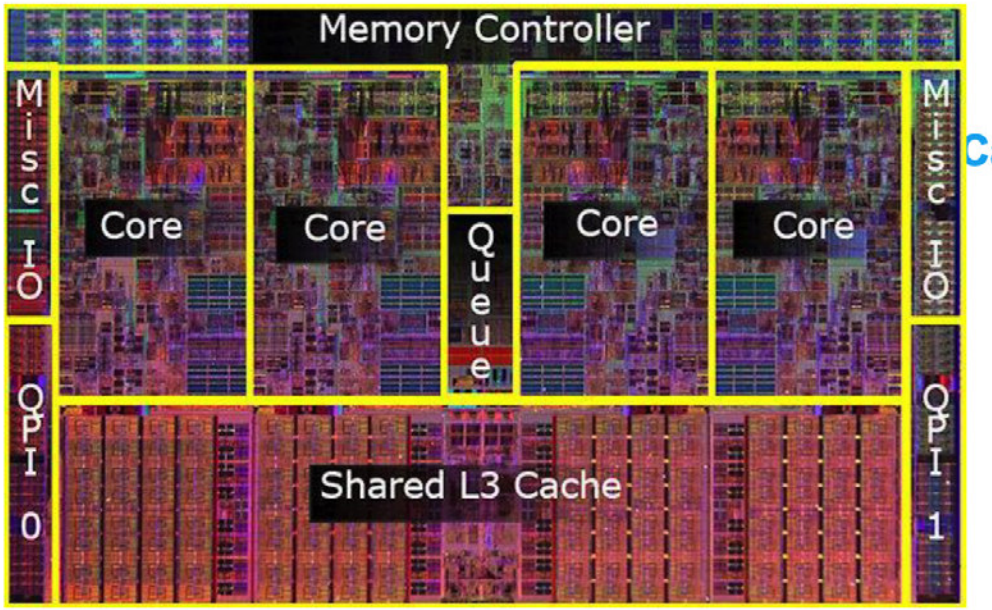
某分布式节点主机，Send进程（端），lj用户，共享远端挂载的文件lj9

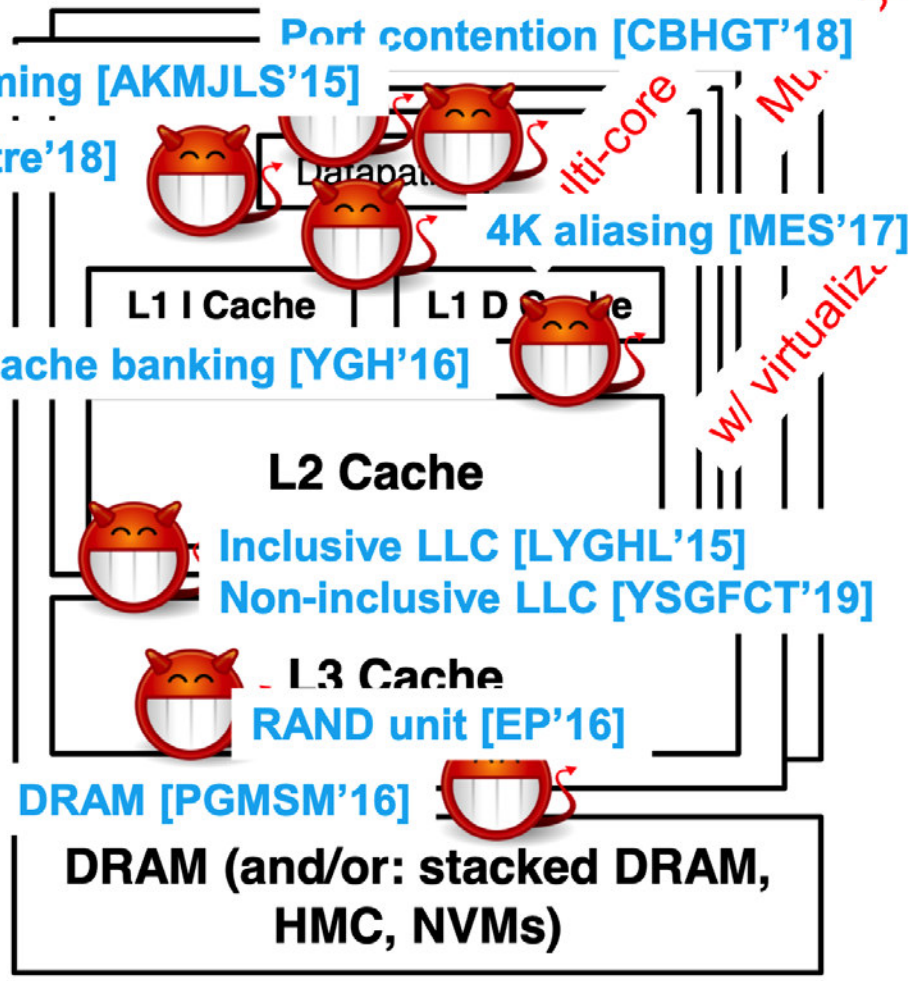
```
app@fate-host:~/lijing-work$ ./fr-recv -f /mnt/lijing/home/a
pp/lijing-work/covert-channel-tutorial/build/lj9
Listening...
> hello,ucas,2021
> [+]This is Flush+Reload Microarchitectual covert channel.
> exit
Receiver finished
app@fate-host:~/lijing-work$
```

某分布式节点主机（同上），Recv进程（端），app用户，共享远端挂载的文件lj9

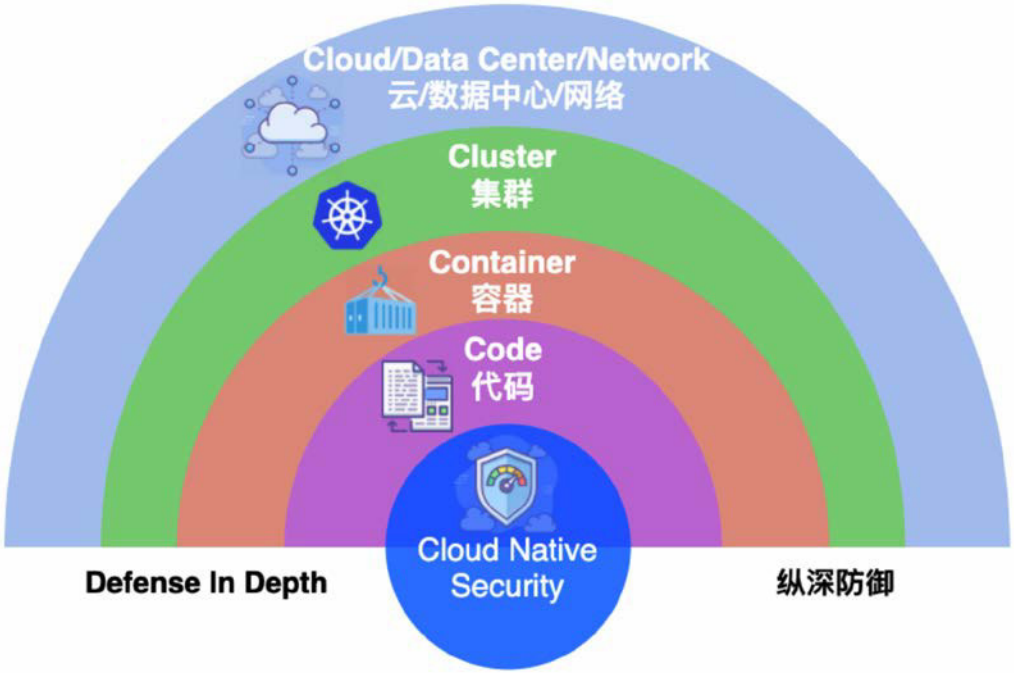
糟了 来晚了

Many potential channels at our disposal





用间此兵之要，三军之所恃而动也



Problem：

- **构建一个较难被探测到的隐蔽信道**
  - ▶现在的方法大多基于网络通信协议，或许在co-located集群中尝试硬件方法

Key Idea：

- **微体系结构的侧信道攻击用于集群环境隐蔽信道传输**

Mechanisms ：

- **Flush+Reload，进程间共享页，比对进入Cache的时间差来隐蔽通信**

Results ：

- **跑通一个Demo**
- **防护需修改或加固底层硬件实现，检测较困难**

感谢批评指正

THANKS