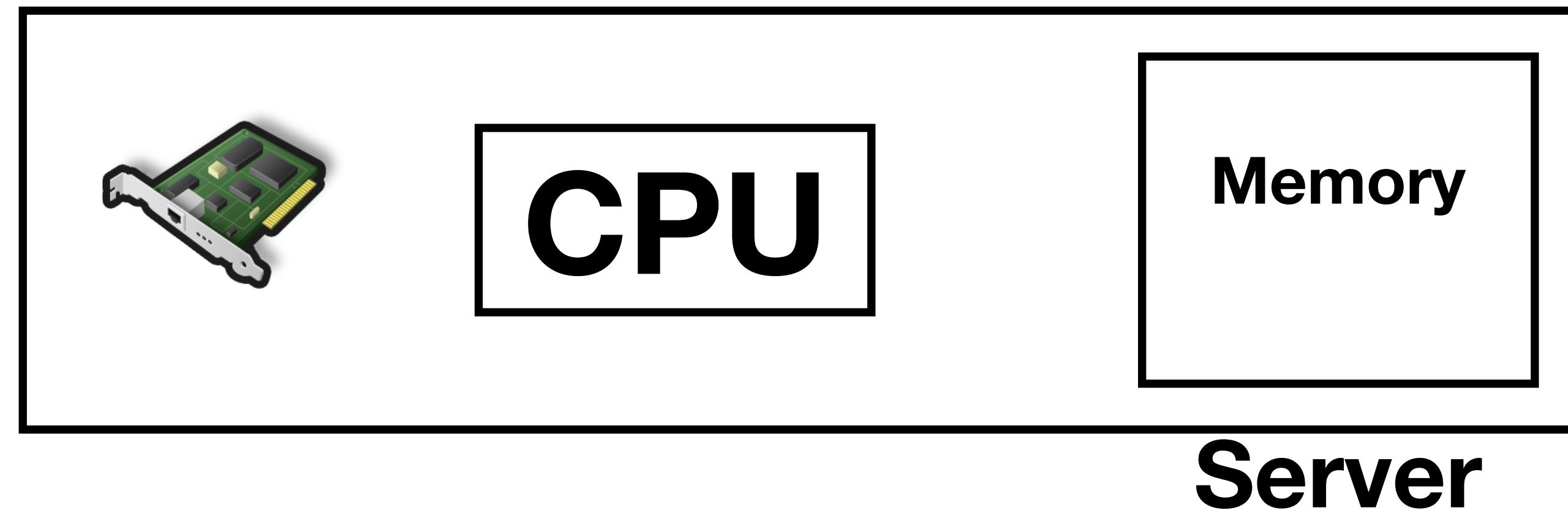


A Double-Edged Sword: Security Threats and Opportunities in One-Sided Network Communication

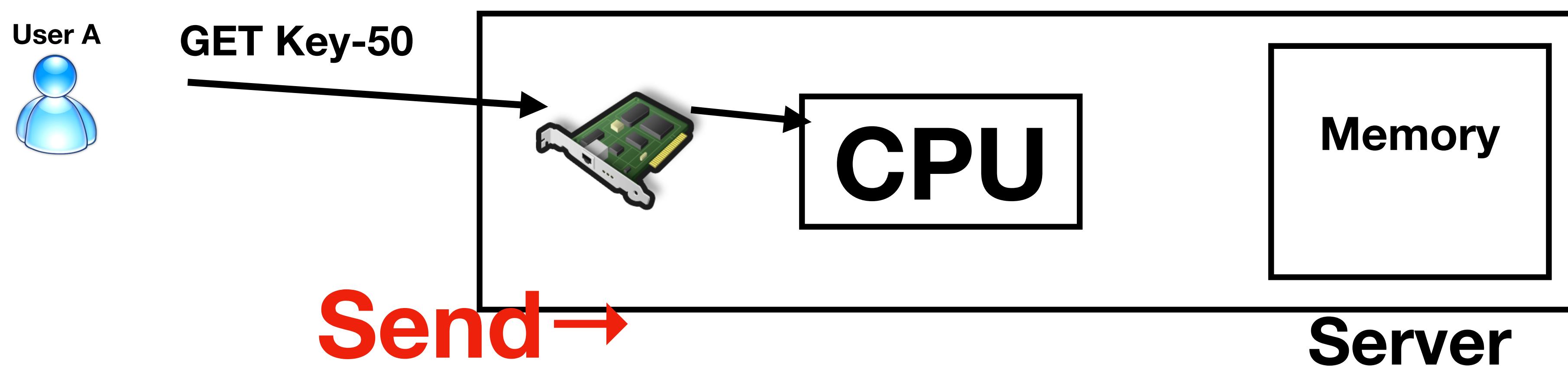
*Shin-Yeh Tsai
Yiying Zhang*



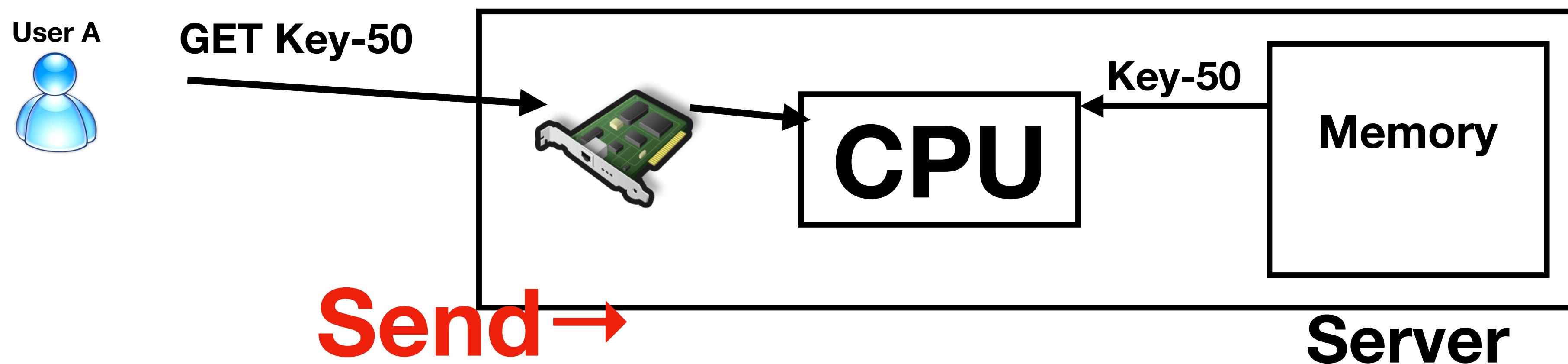
Traditional (Two-sided communication)



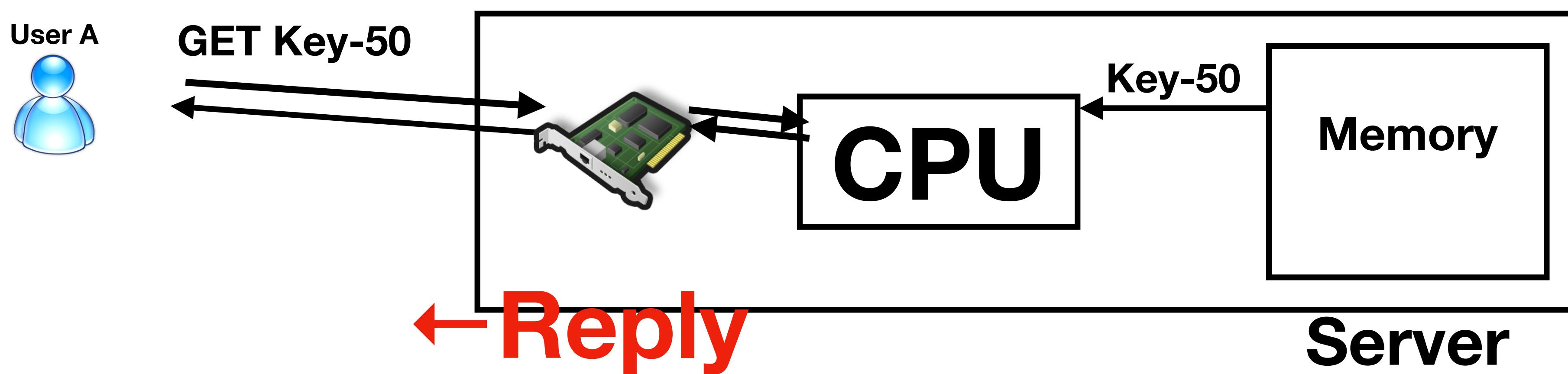
Traditional (Two-sided communication)



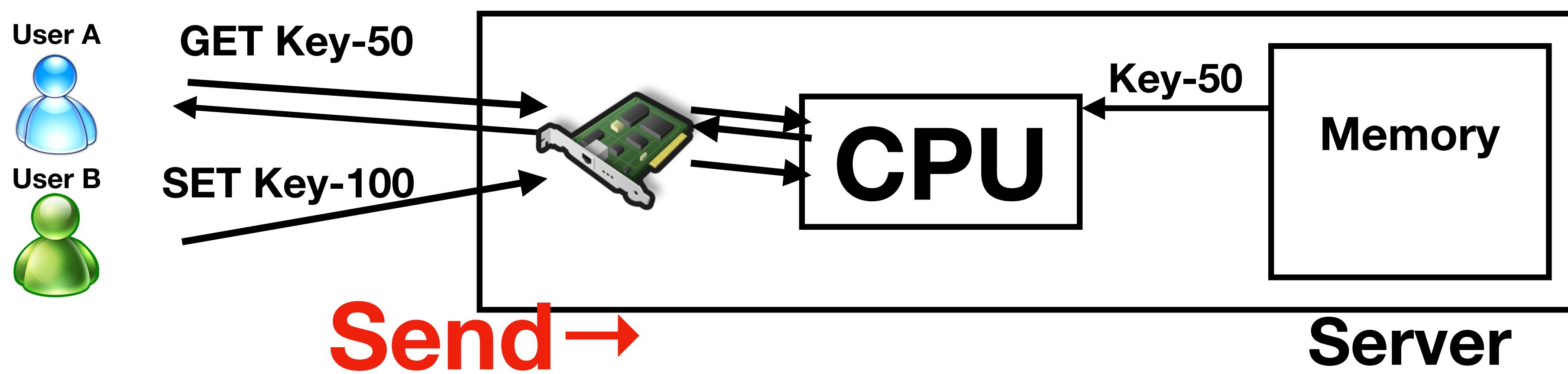
Traditional (Two-sided communication)



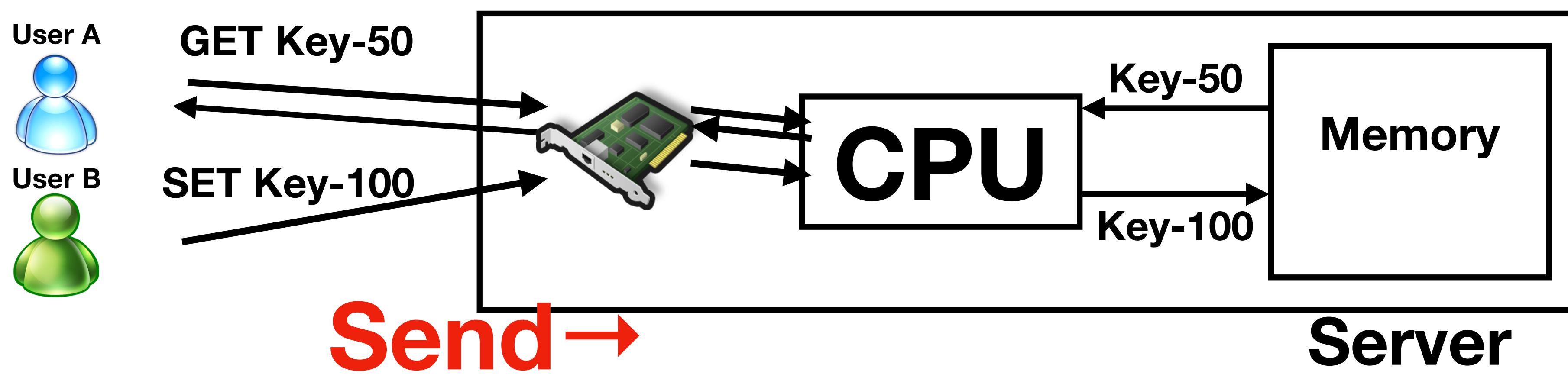
Traditional (Two-sided communication)



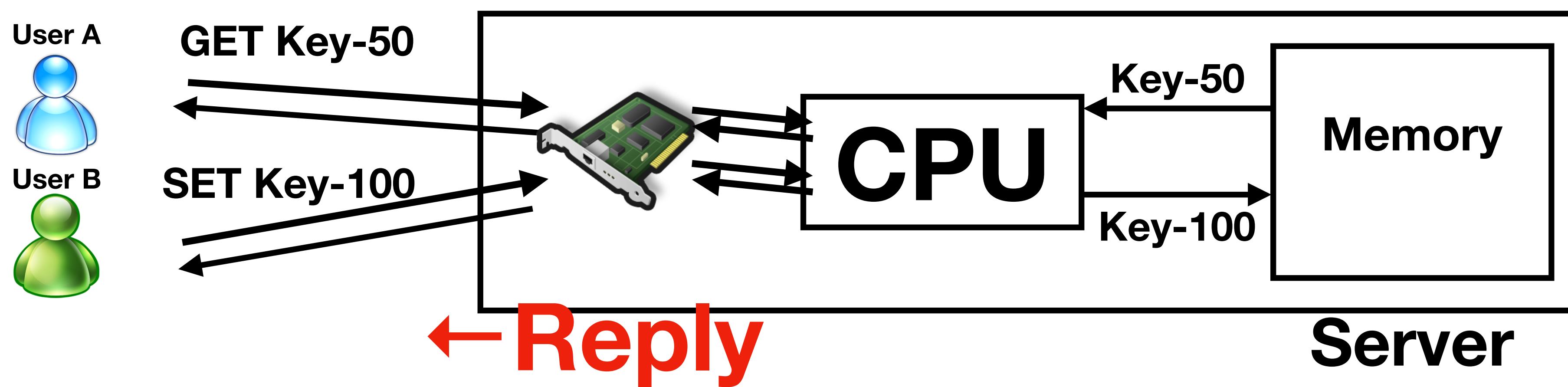
Traditional (Two-sided communication)



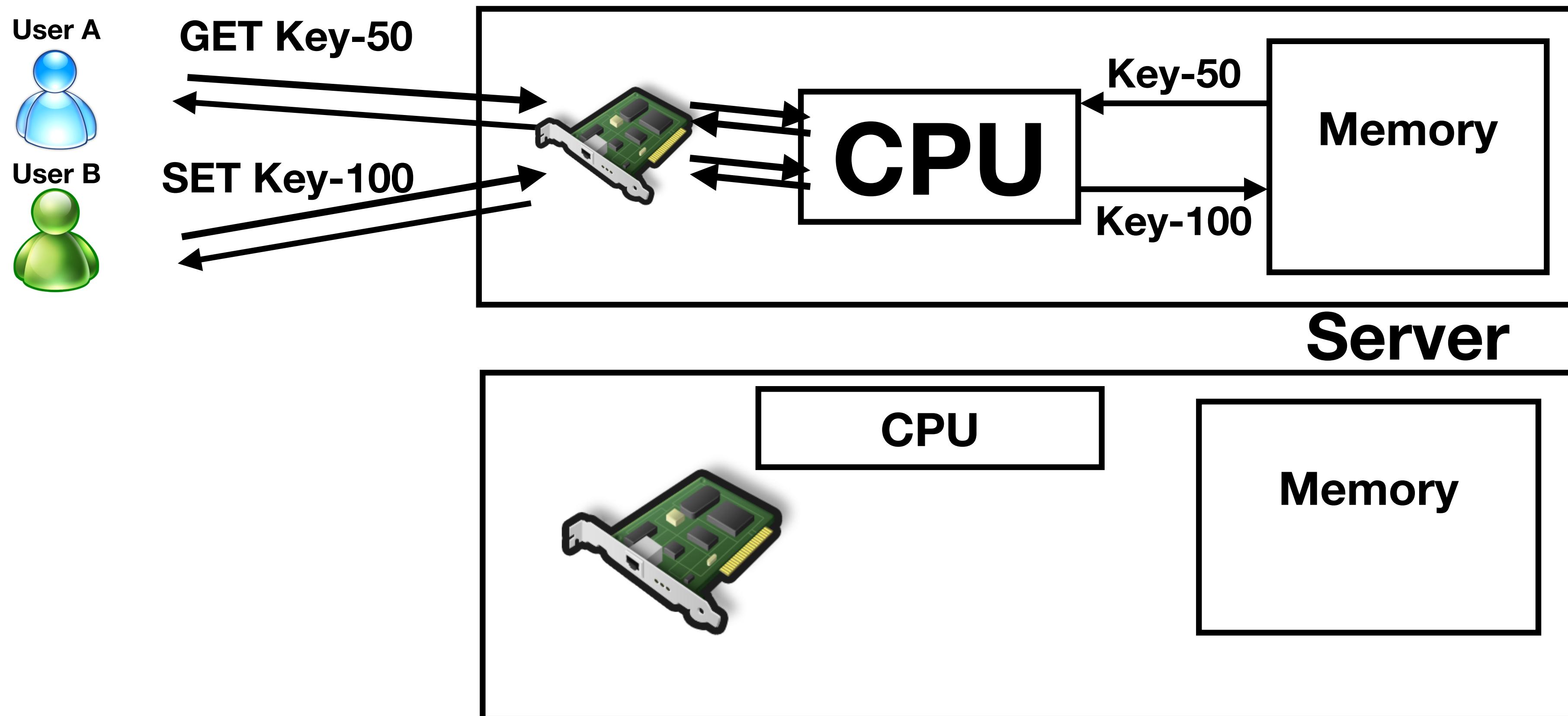
Traditional (Two-sided communication)



Traditional (Two-sided communication)

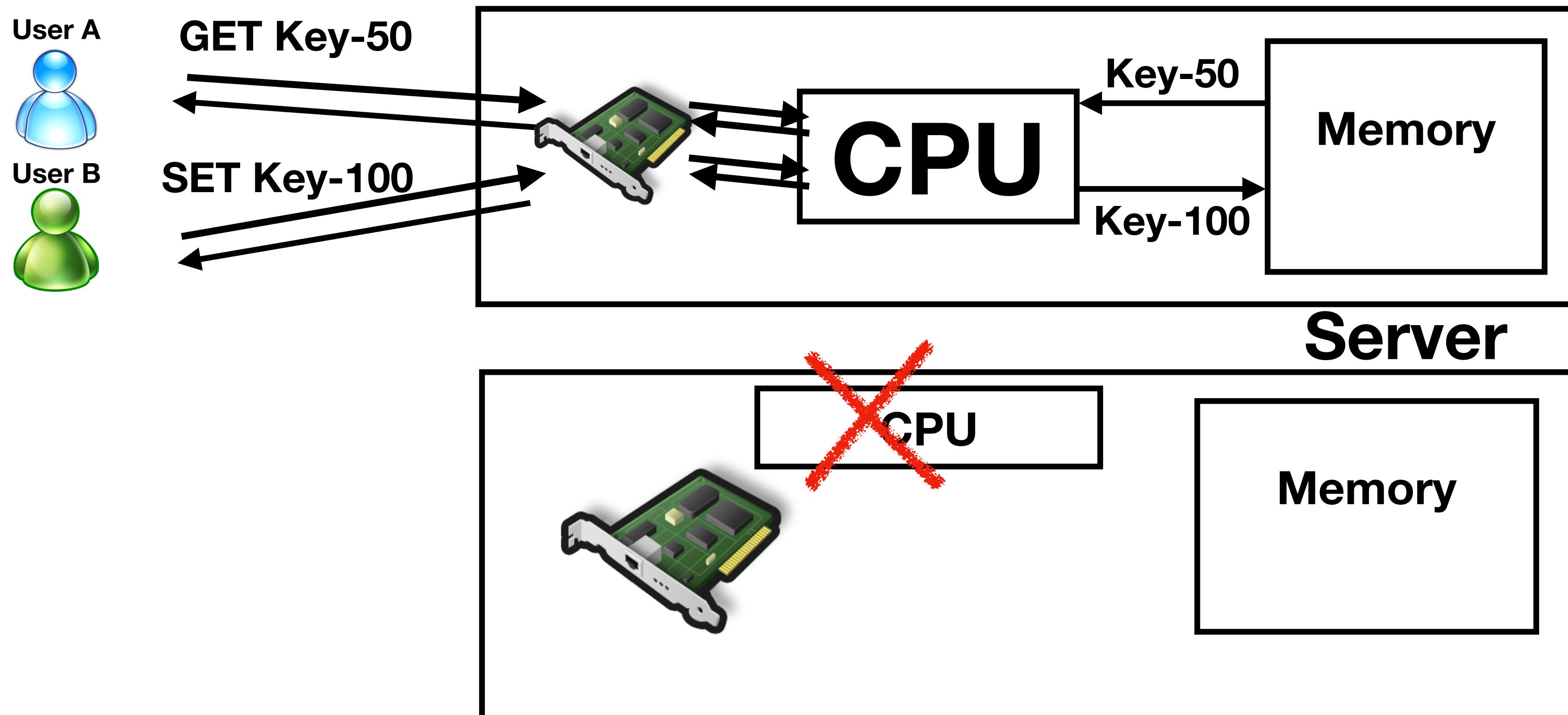


Traditional (Two-sided communication)



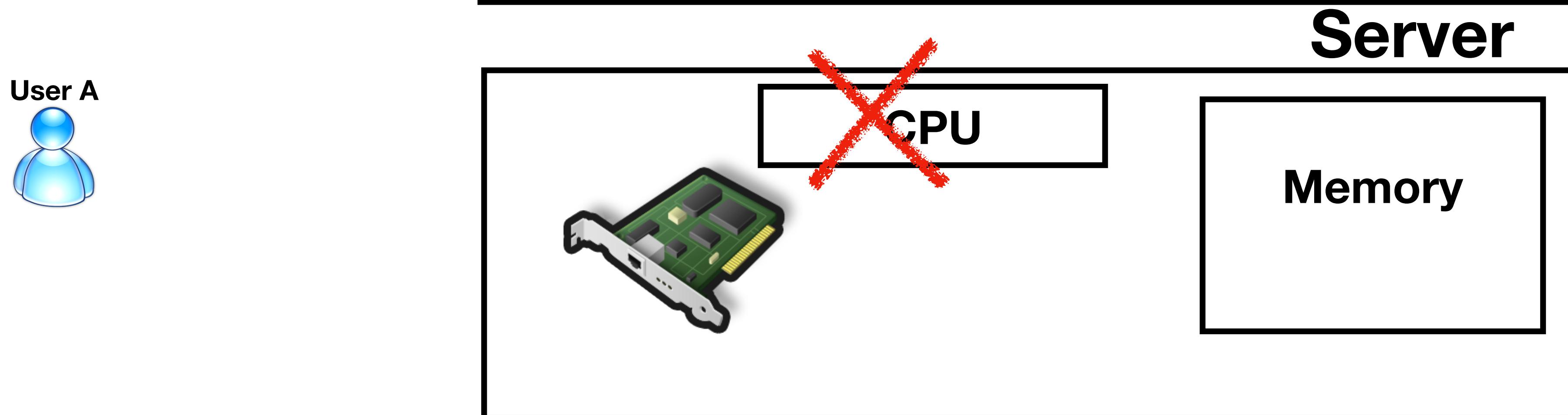
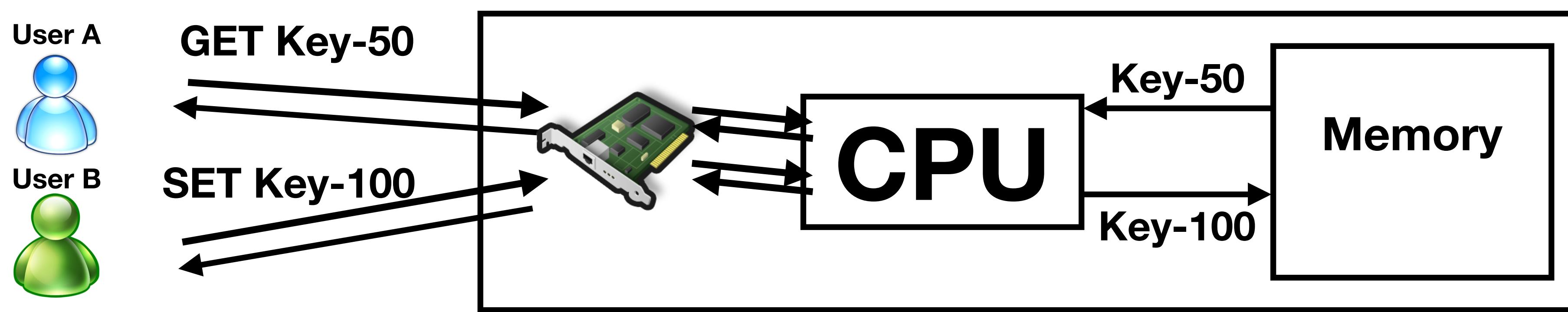
One-sided communication

Traditional (Two-sided communication)



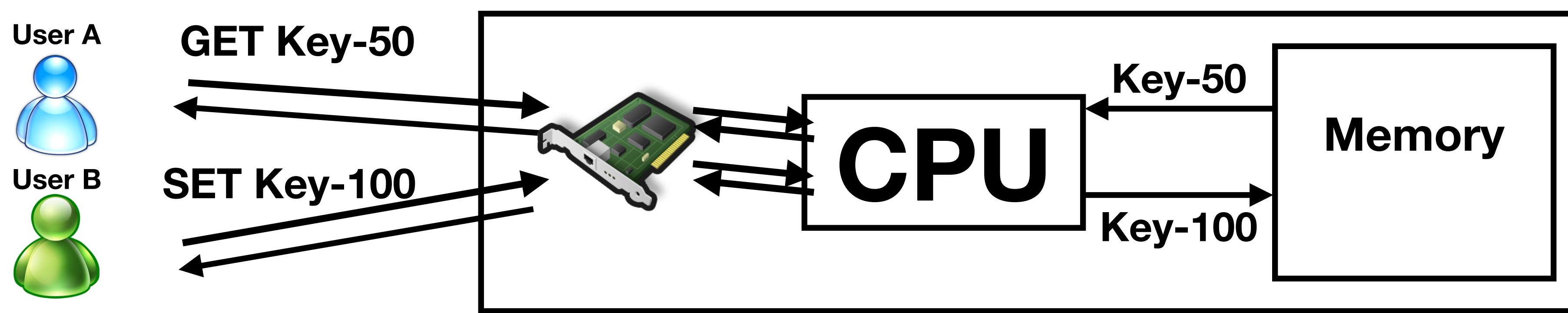
One-sided communication

Traditional (Two-sided communication)

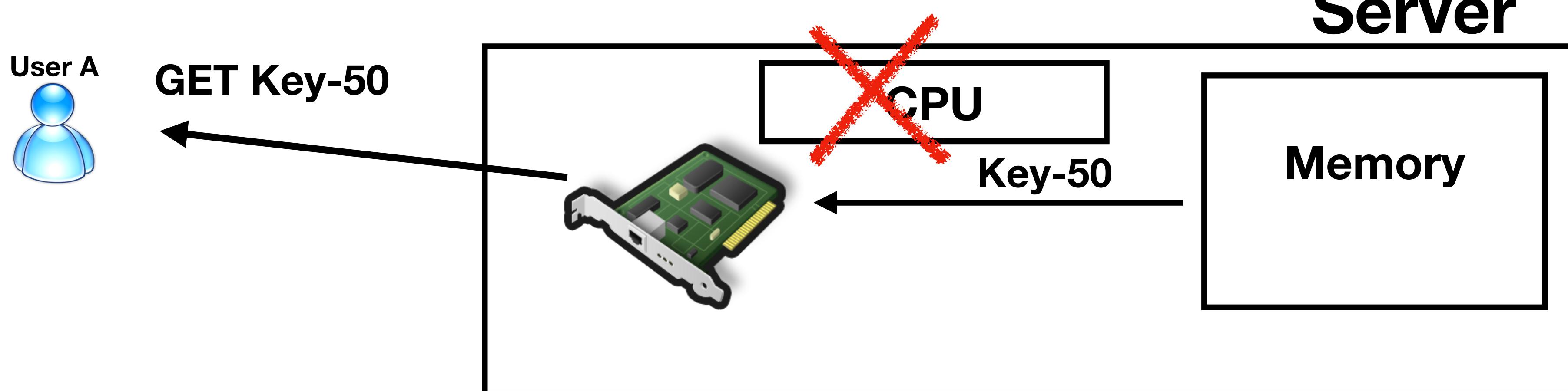


One-sided communication

Traditional (Two-sided communication)

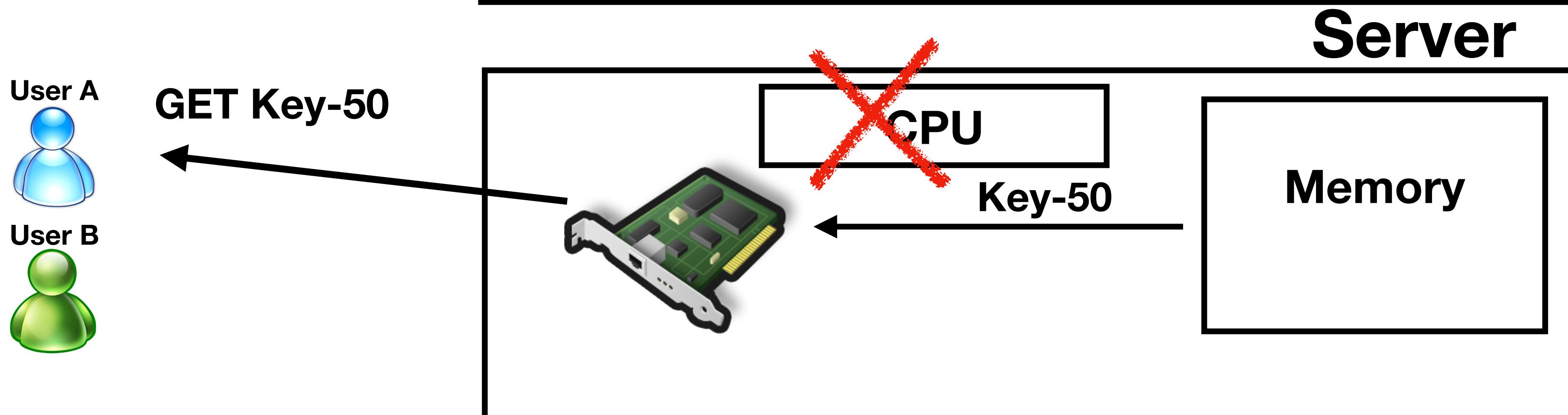
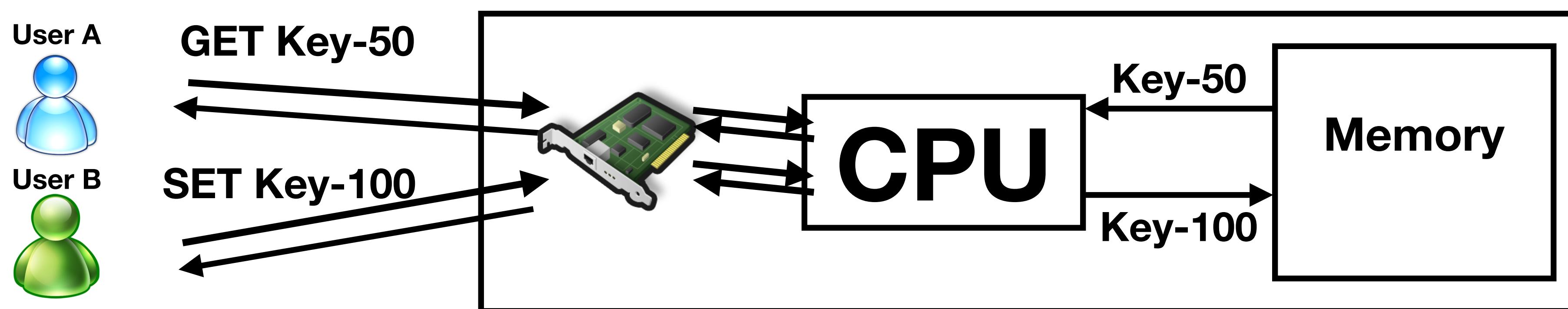


Server



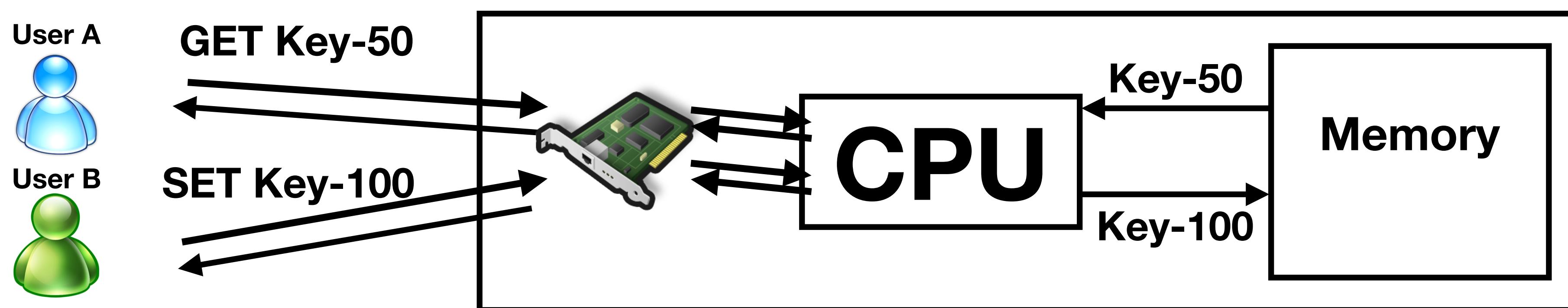
One-sided communication

Traditional (Two-sided communication)

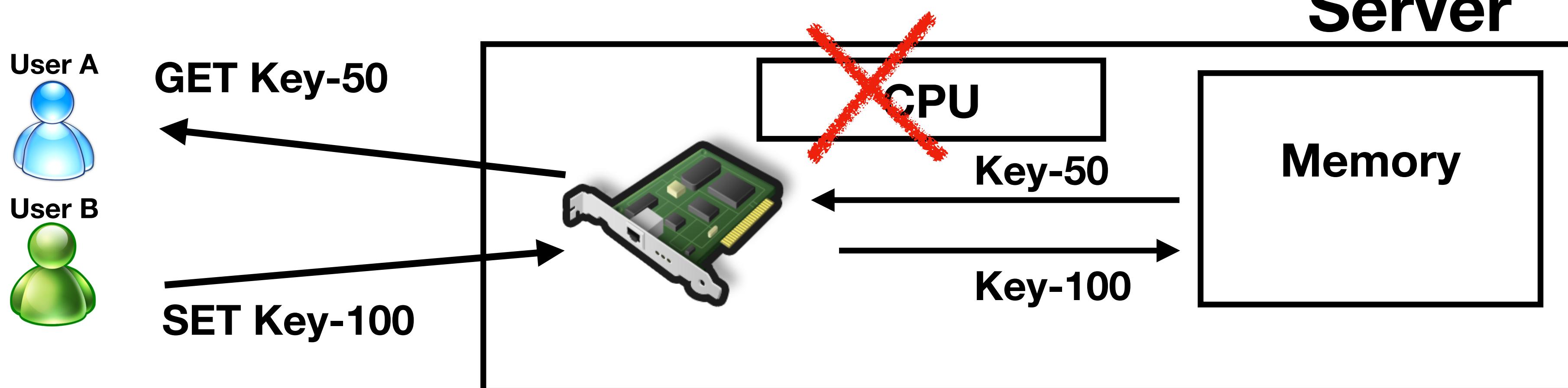


One-sided communication

Traditional (Two-sided communication)



Server



One-sided communication

RDMA

Omni-Path

Gen-Z

NVMeOF

GPUDirect

RDMA

Pilaf
[ATC '13]

APUS
[SoCC '17]

Hotpot
[SoCC '17]

Omni-Path

FaRM
[NSDI '14]

Octopus
[ATC '17]

Orion
[FAST '19]

Wukong
[OSDI '16]

Gen-Z

HERD
[SIGCOMM '14]

NAM-DB
[VLDB '17]

Storm
[SYSTOR '19]

DRTM+H
[OSDI '18]

Cell
[ATC '16]

NVMeOF

DrTM
[SOSP '15]

LITE
[SOSP '17]

KV-Direct
[SOSP '17]

FaSST
[OSDI '16]

GPUDirect

FaRM + Xact
[SOSP '15]

Mojim
[ASPLOS '15]

DrTM+R
[EuroSys '16]

RSI
[VLDB '16]

Performance

RDMA

Pilaf
[ATC '13]

FaRM
[NSDI '14]

Omni-Path

HERD
[SIGCOMM '14]

Gen-Z

DrTM
[SOSP '15]

NVMeOF

FaRM + Xact
[SOSP '15]

LITE
[SOSP '17]

KV-Direct
[SOSP '17]

FaSST
[OSDI '16]

GPUDirect

Mojim
[ASPLOS '15]

DrTM+R
[EuroSys '16]

Hotpot
[SoCC '17]

Orion
[FAST '19]

Wukong
[OSDI '16]

APUS
[SoCC '17]

Octopus
[ATC '17]

Storm
[SYSTOR '19]

DRTM+H
[OSDI '18]

Cell
[ATC '16]

Performance

RDMA

FaRM
[NSDI '14]

Omni-Path

HERD
[SIGCOMM '14]

Gen-Z

DrTM
[SOSP '15]

NVMeOF

FaRM + Xact
[SOSP '15]

GPUDirect

Mojim
[ASPLOS '15]

NAM-DB
[VLDB '17]

LITE
[SOSP '17]

KV-Direct
[SOSP '17]

FaSST
[OSDI '16]

Hotpot
[SoCC '17]

Orion
[FAST '19]

Wukong
[OSDI '16]

Scalability

Storm
[SYSTOR '19]

RSI
[VLDB '16]

DrTM+R
[EuroSys '16]

Cell
[OSDI '18]

DEMONH
[OSDI '18]

RDMA

Omni-Path

Gen-Z

NVMeOF

GPUDirect

Performance

FaRM
[NSDI '14]

HERD
[SIGCOMM '14]

DrTM
[SOSP '15]

FaRM + Xact
[SOSP '15]

NAM-DB
[VLDB '17]

Usability

Mojim
[ASPLOS '15]

DrTM+R
[EuroSys '16]

Pilaf
[ATC '13]

APUS
[SoCC '17]

Octopus
[ATC '17]

Storm
[SYSTOR '19]

Hotpot
[SoCC '17]

Orion
[FAST '19]

Wukong
[OSDI '16]

Scalability

Cell
[ITC '14]

DEATH
[OSDI '18]

FaSST
[OSDI '16]

KV-Direct
[SOSP '17]

RSI
[VLDB '16]

RDMA

Omni-Path

Gen-Z

NVMeOF

GPUDirect

Performance

FaRM
[NSDI '14]

Pilaf
[ATC '13]

APUS
[SoCC '17]

Octopus
[ATC '17]

Hotpot
[SoCC '17]

Orion
[FAST '19]

Wukong
[OSDI '16]

Scalability

Storm
[SYSTOR '19]

Cell
[OSDI '18]

NAM-DB
[VLDB '17]

HERD
[SIGCOMM '14]

DrTM
[SOSP '15]

Usability

FaRM + Xact
[SOSP '15]

Mojim
[ASPLOS '15]

KV-Direct
[SOSP '17]

RSI
[VLDB '16]

FaSST
[OSDI '16]

What about Security?

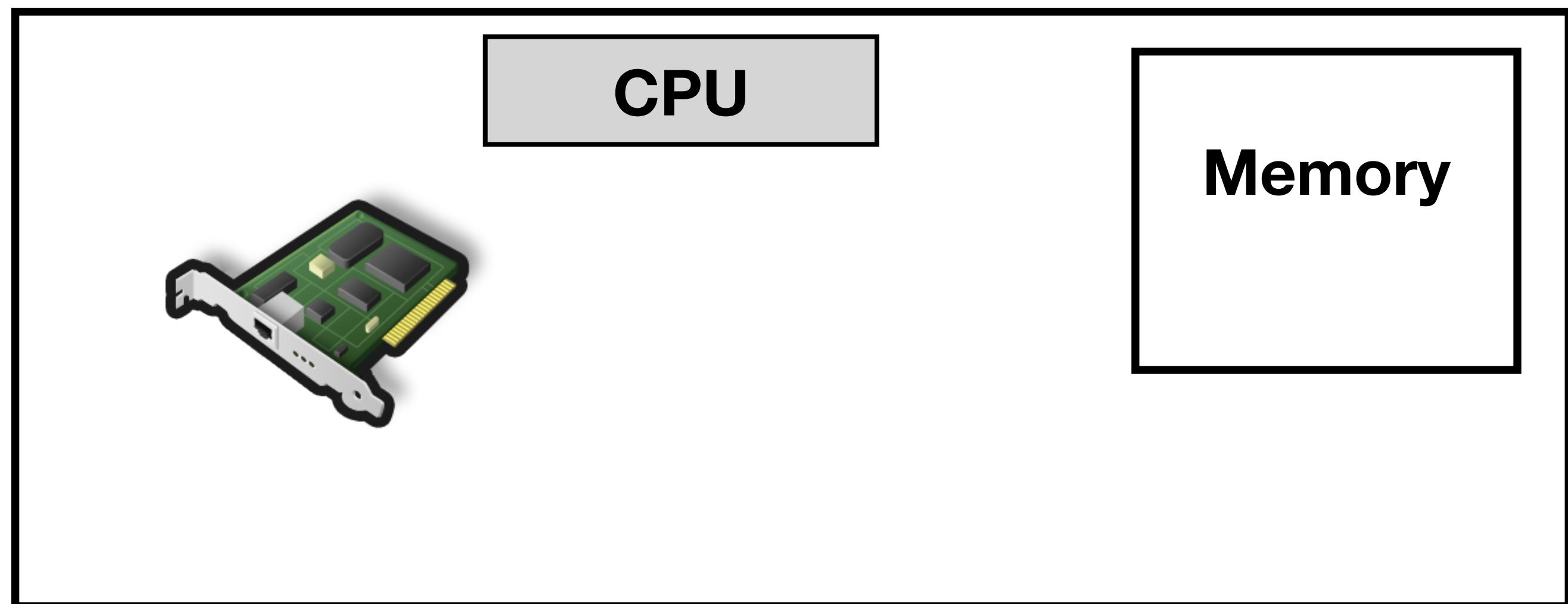
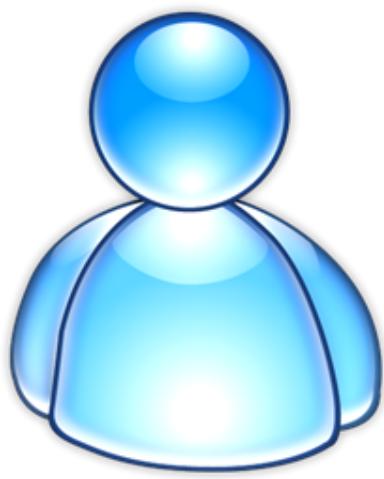
Outline

- Introduction and Background
- Vulnerabilities in One-Sided Communication
- Vulnerabilities in One-Sided Hardware
- Opportunities in One-Sided Communication
- Conclusion

Vulnerability 1: Lack of Accountability

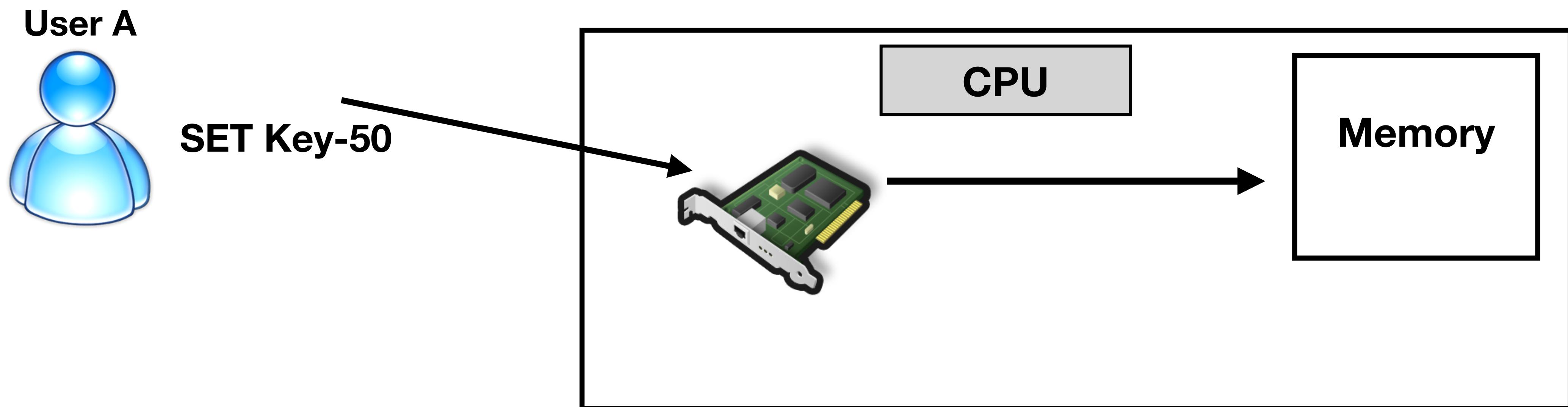
- **WRITE** accountability

User A



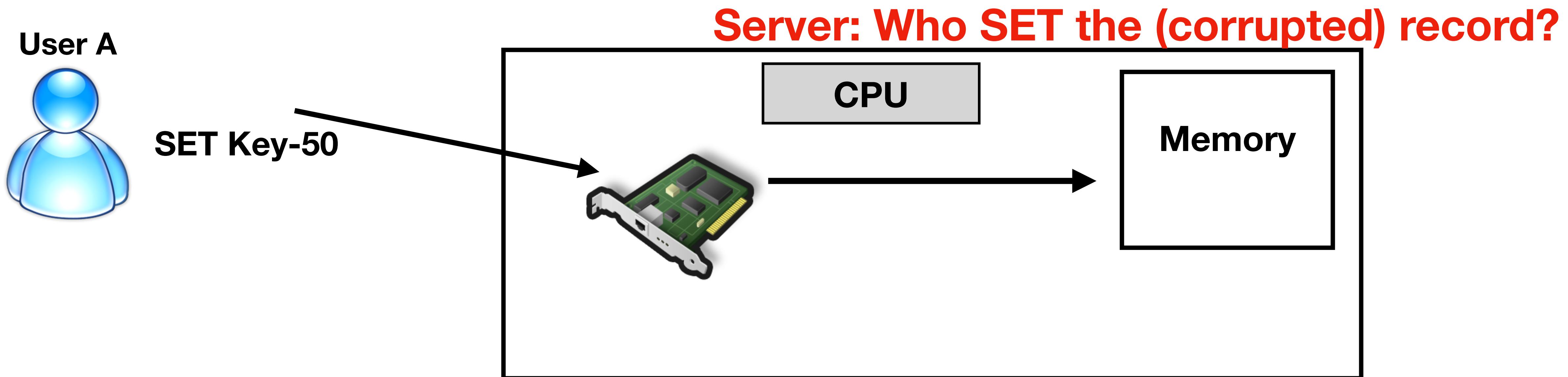
Vulnerability 1: Lack of Accountability

- **WRITE** accountability



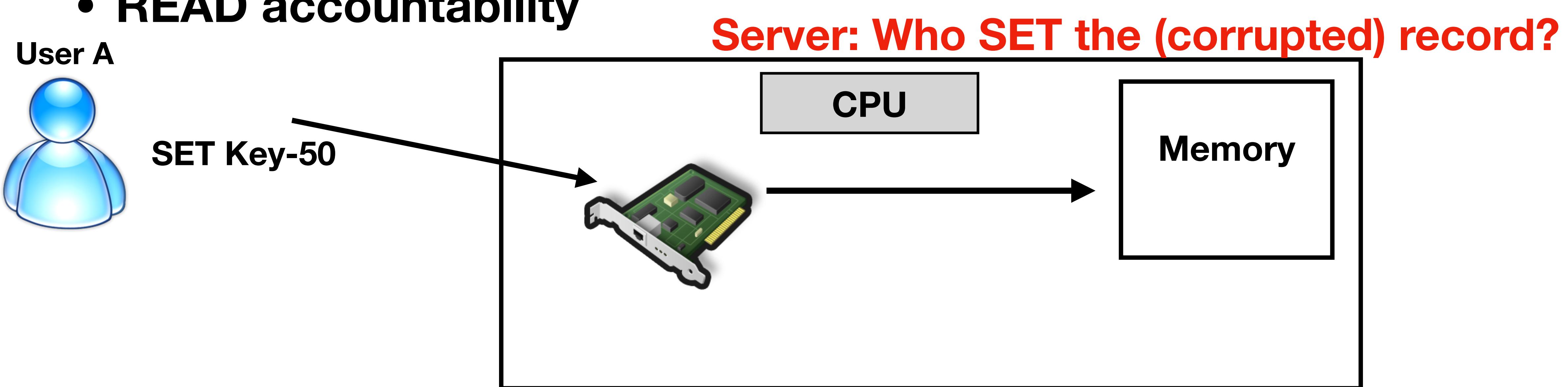
Vulnerability 1: Lack of Accountability

- WRITE accountability



Vulnerability 1: Lack of Accountability

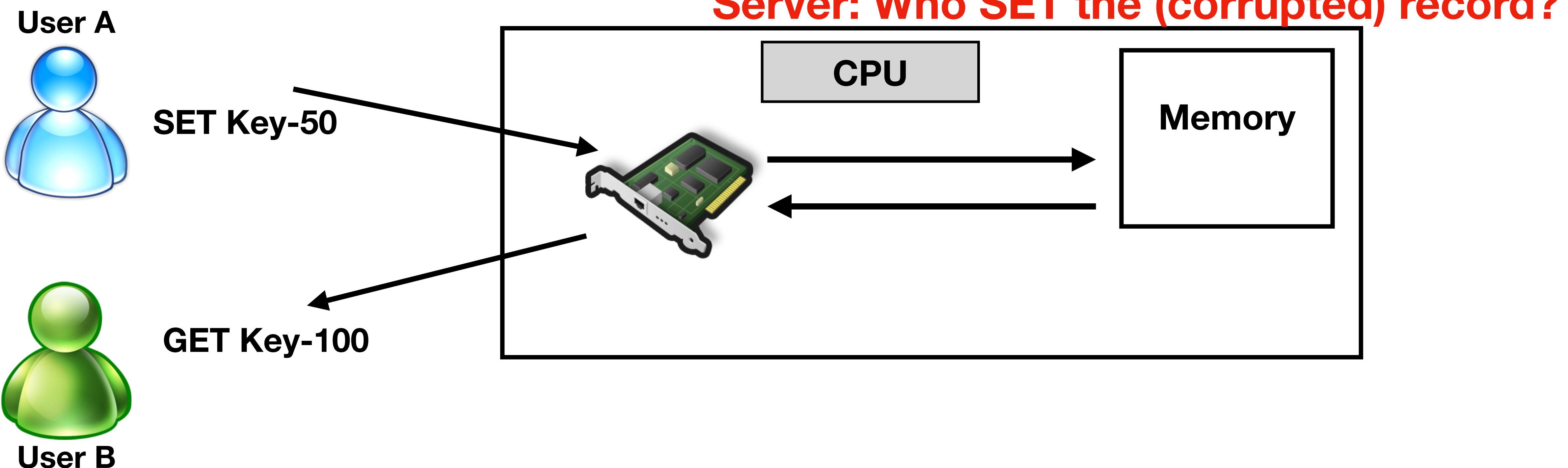
- WRITE accountability
- READ accountability



Vulnerability 1: Lack of Accountability

- WRITE accountability

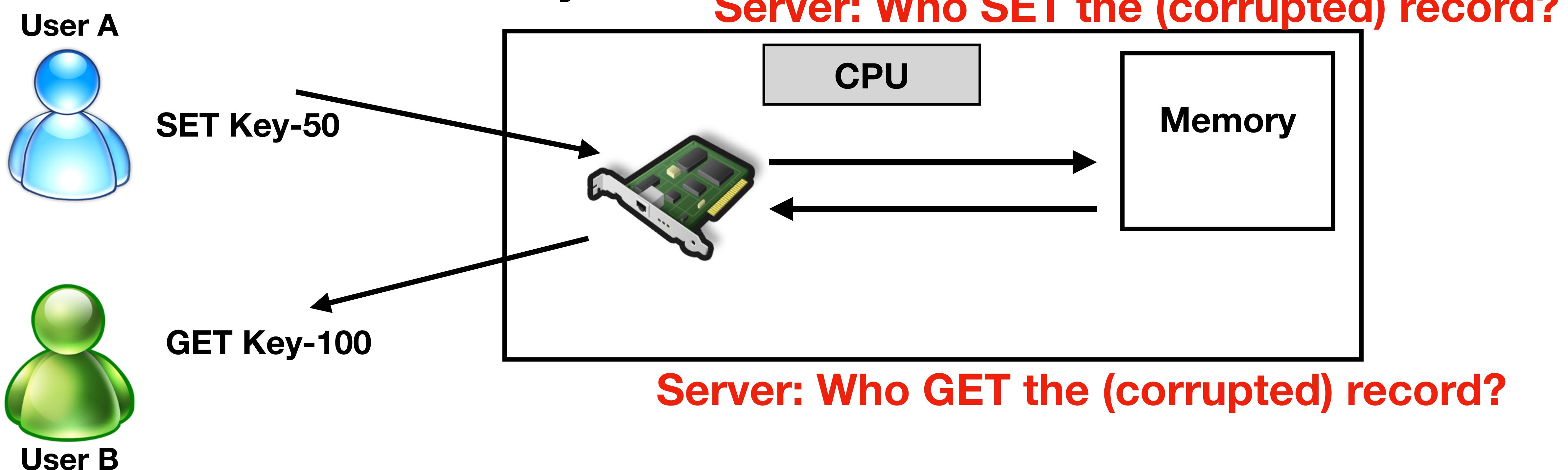
- READ accountability



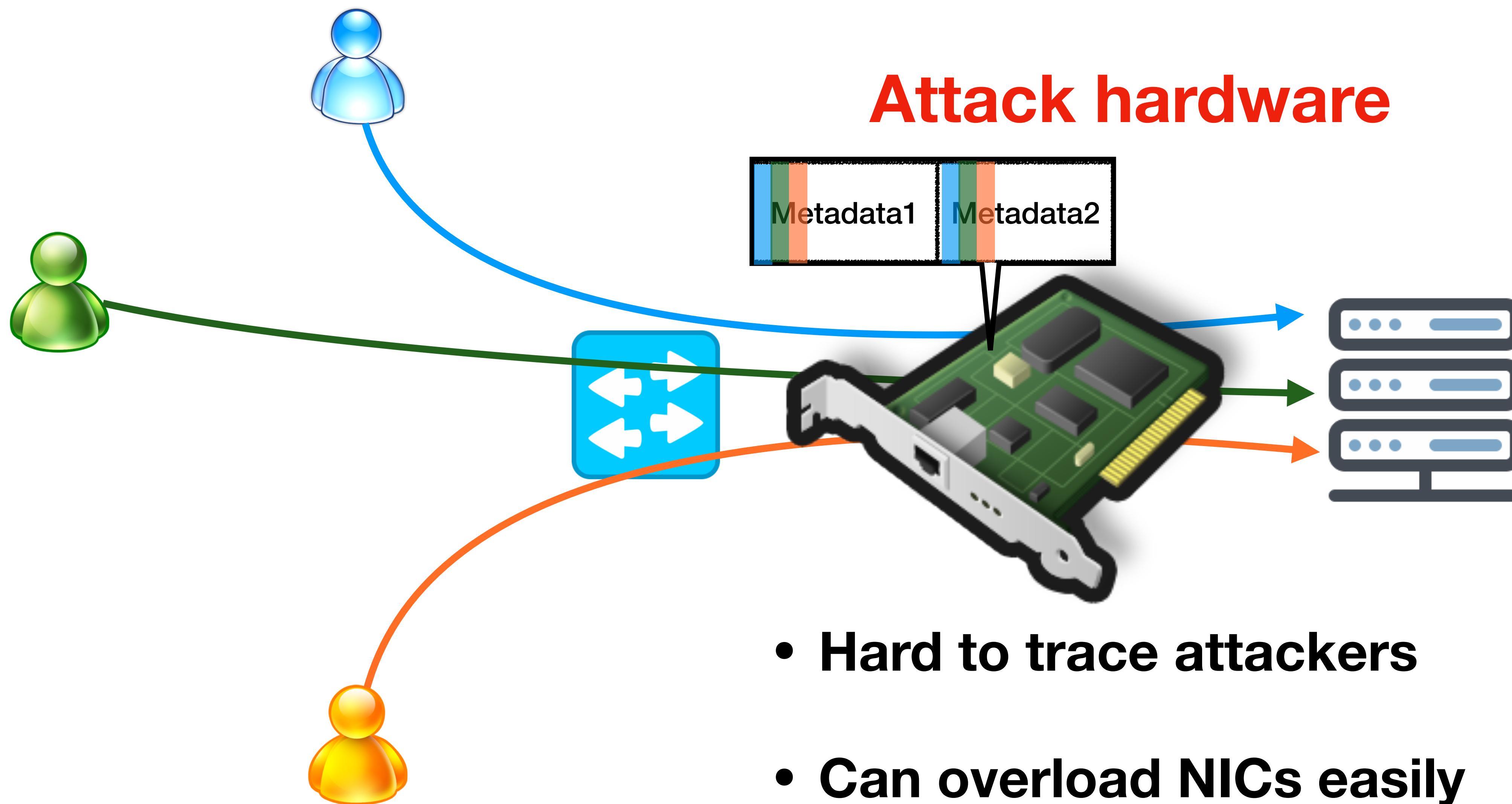
Vulnerability 1: Lack of Accountability

- WRITE accountability

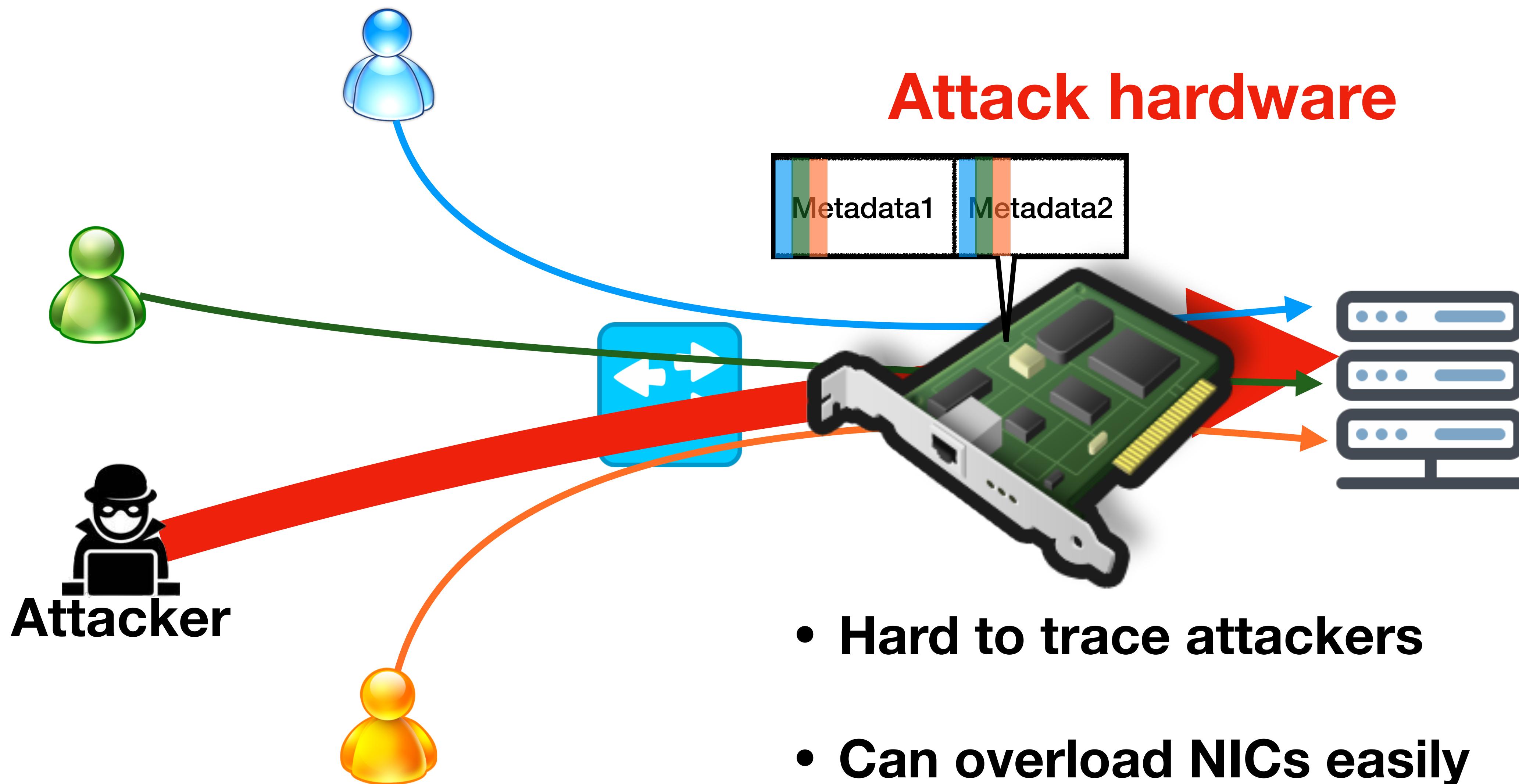
- READ accountability



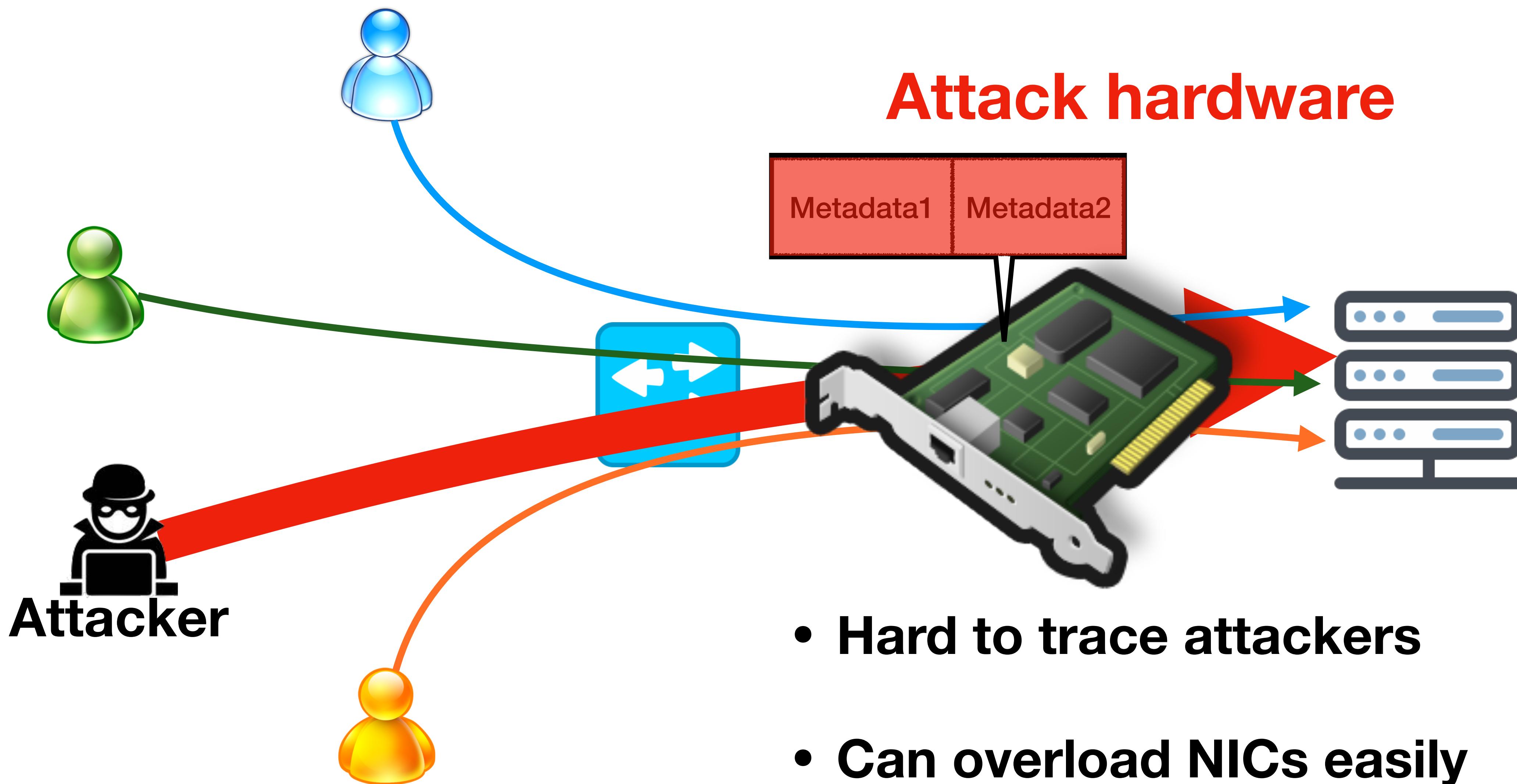
Vulnerability 2: Denial of Service



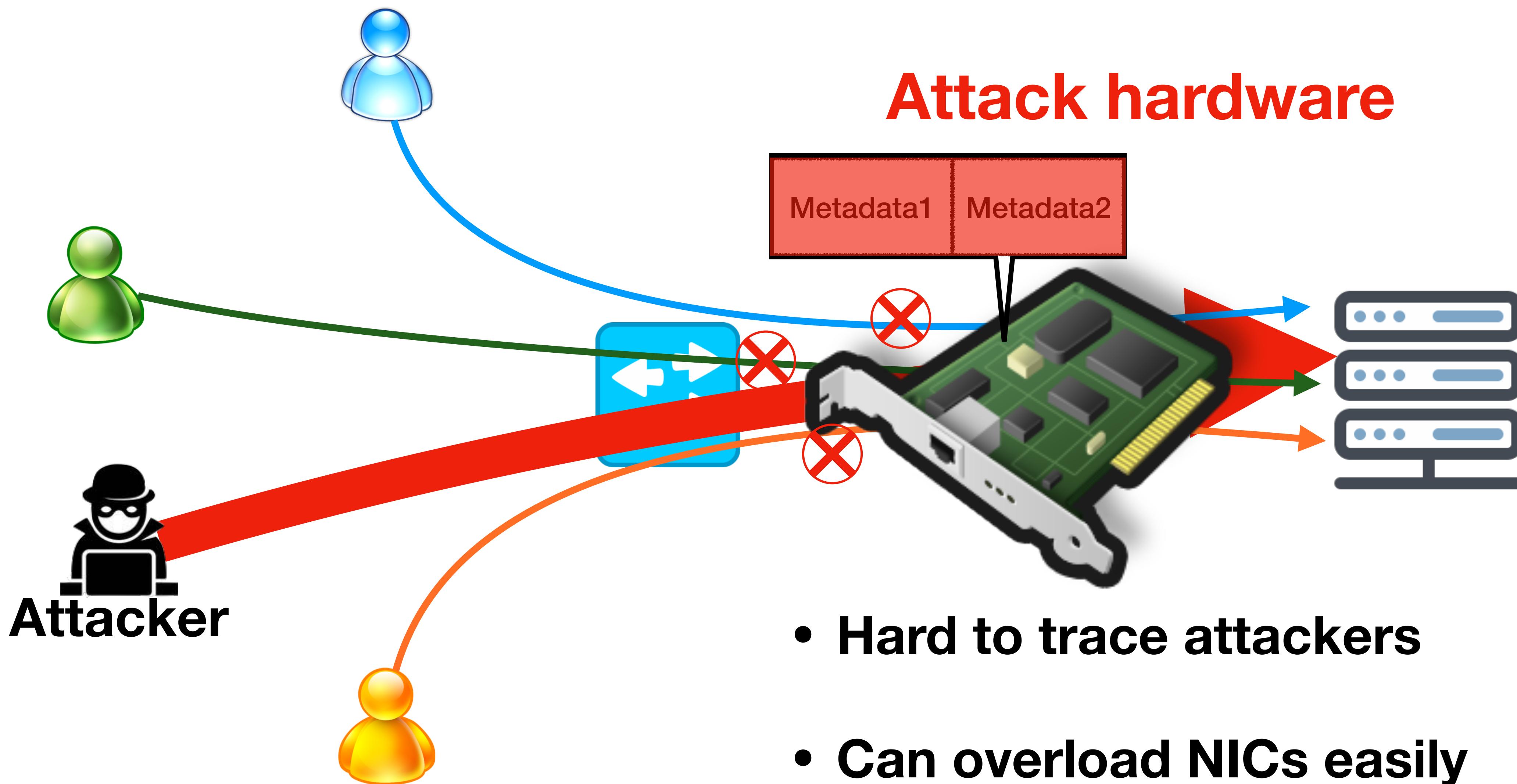
Vulnerability 2: Denial of Service



Vulnerability 2: Denial of Service



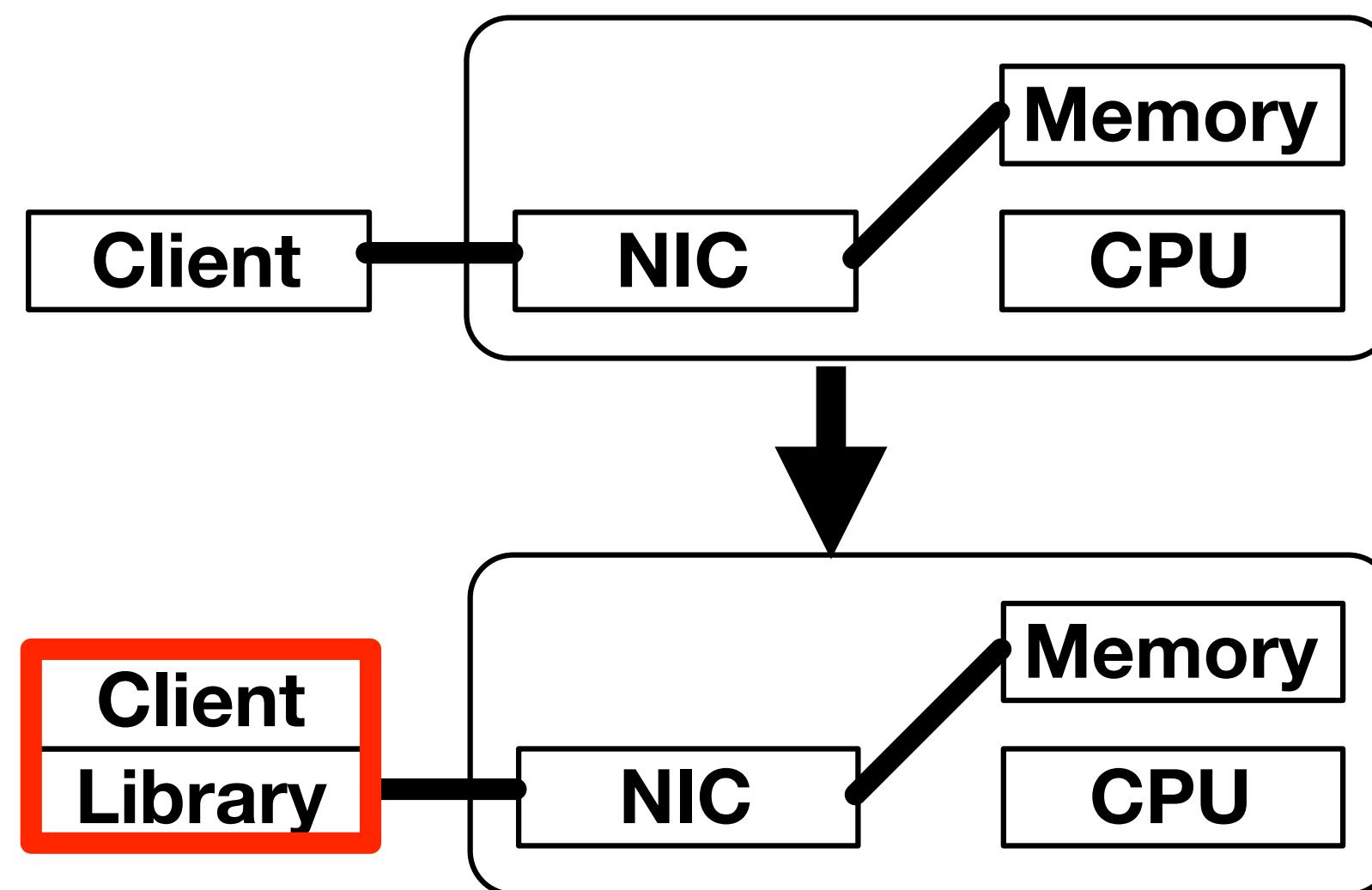
Vulnerability 2: Denial of Service



Discussion and Defense

- Adding intermediate layer at the sender side

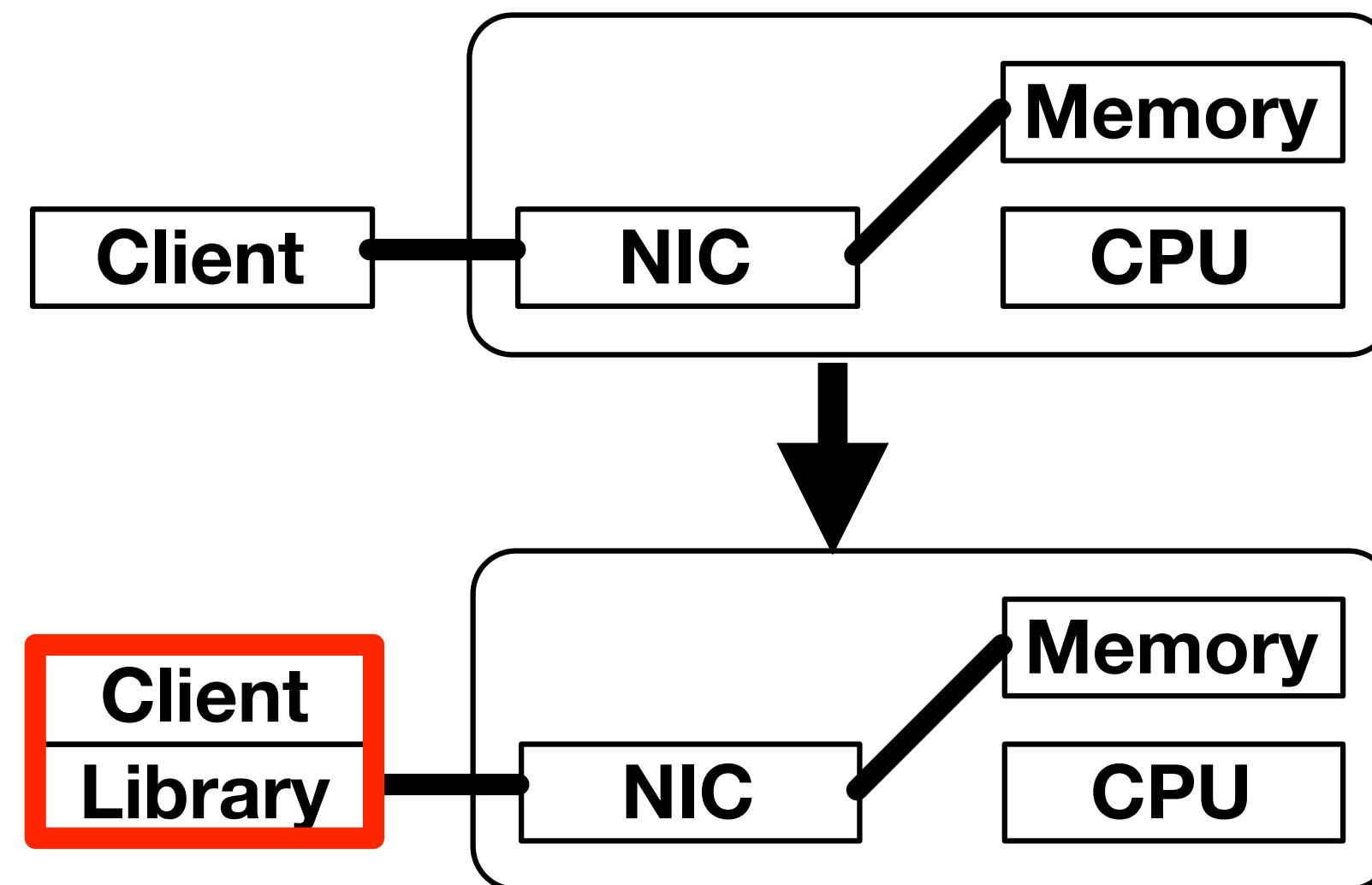
Intermediate Layer



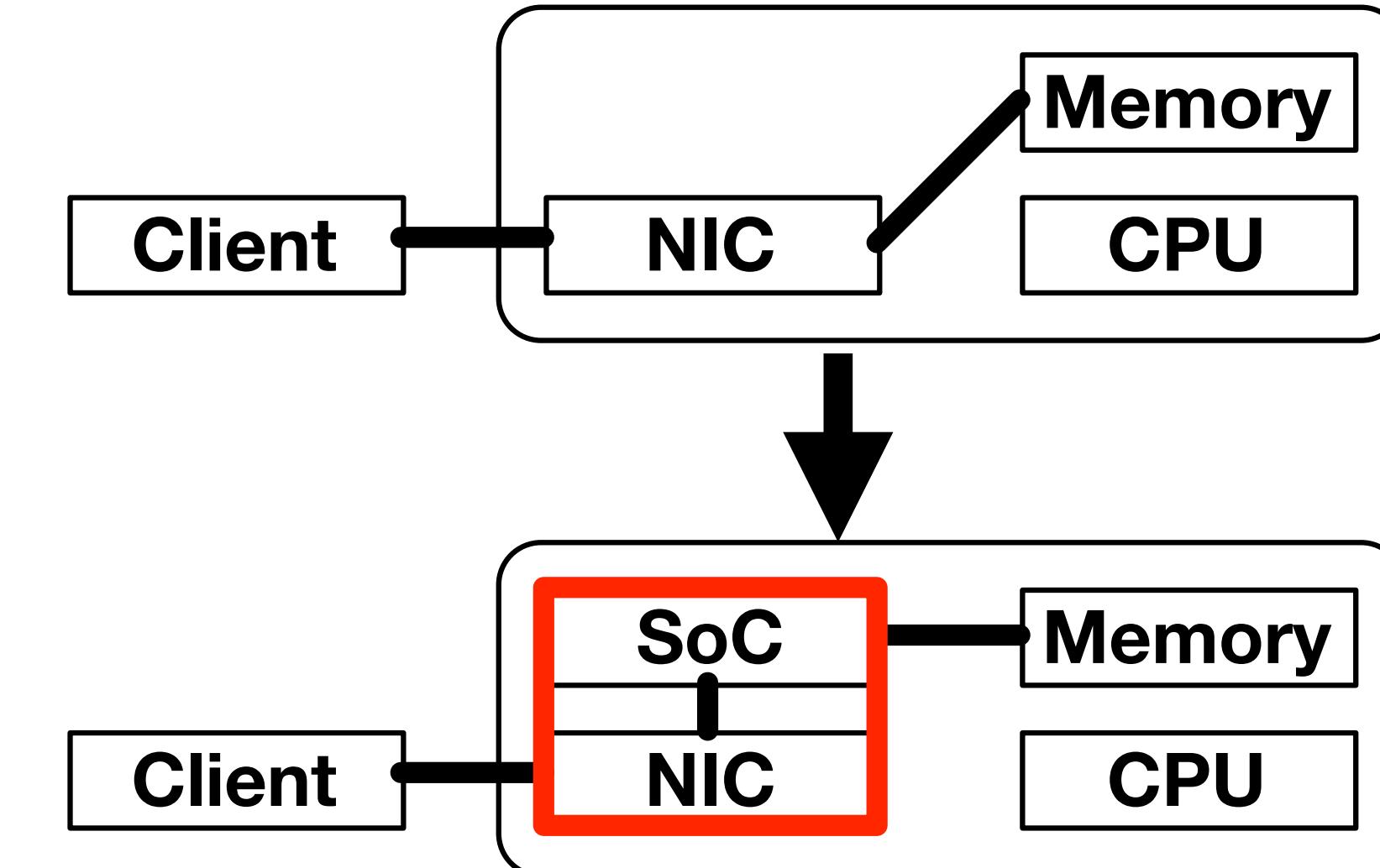
Discussion and Defense

- Adding intermediate layer at the sender side
- Enhancing SmartNIC at the receiver side

Intermediate Layer



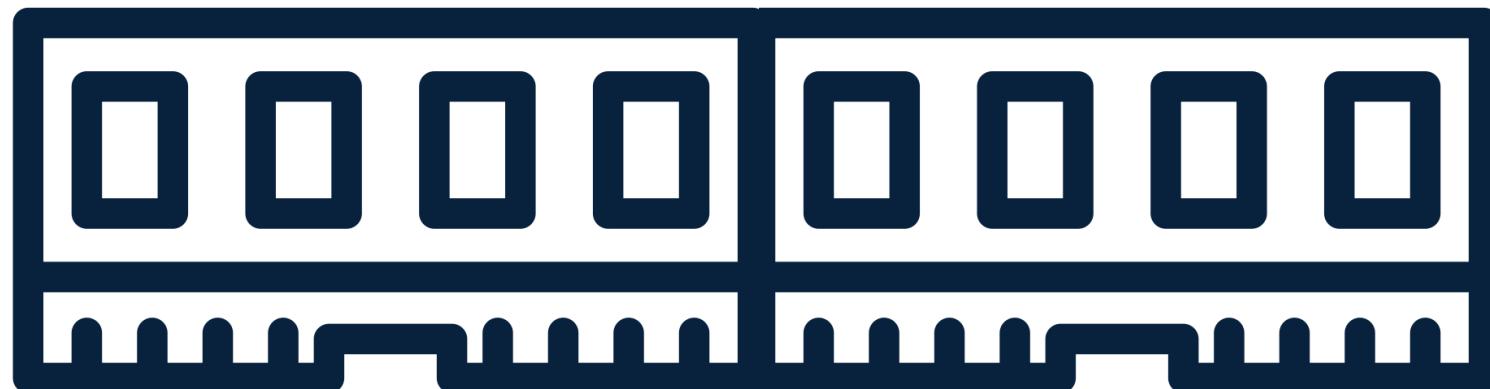
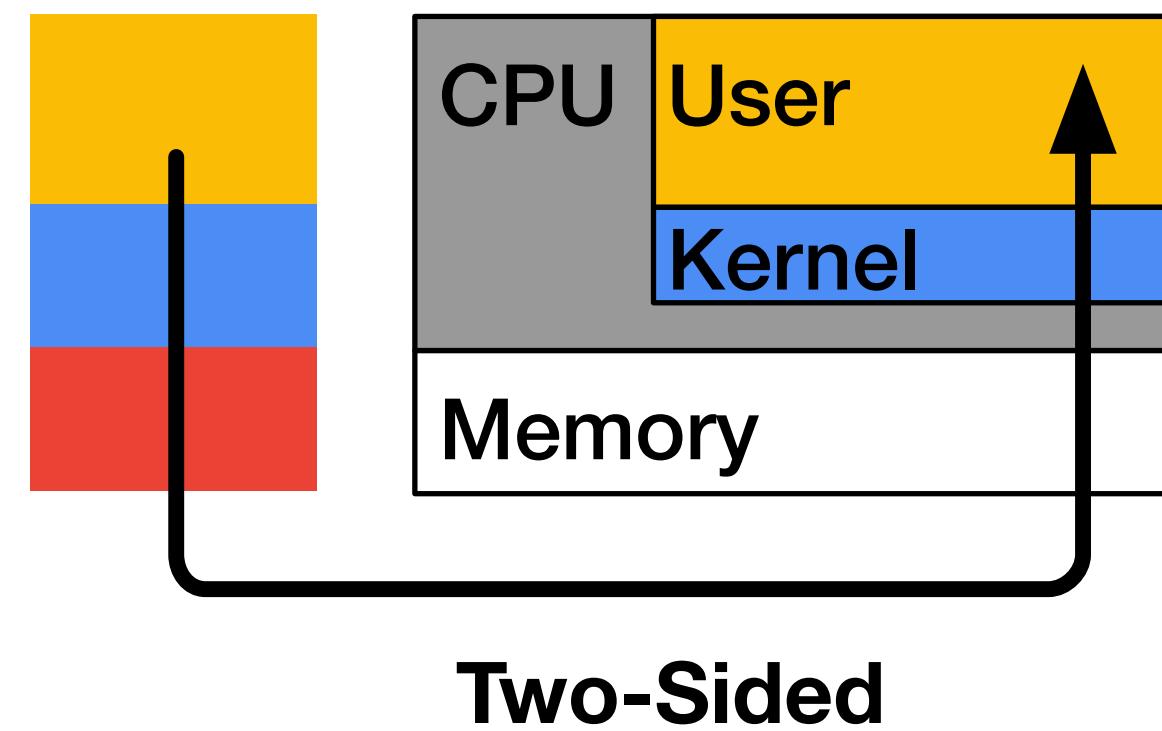
SmartNIC



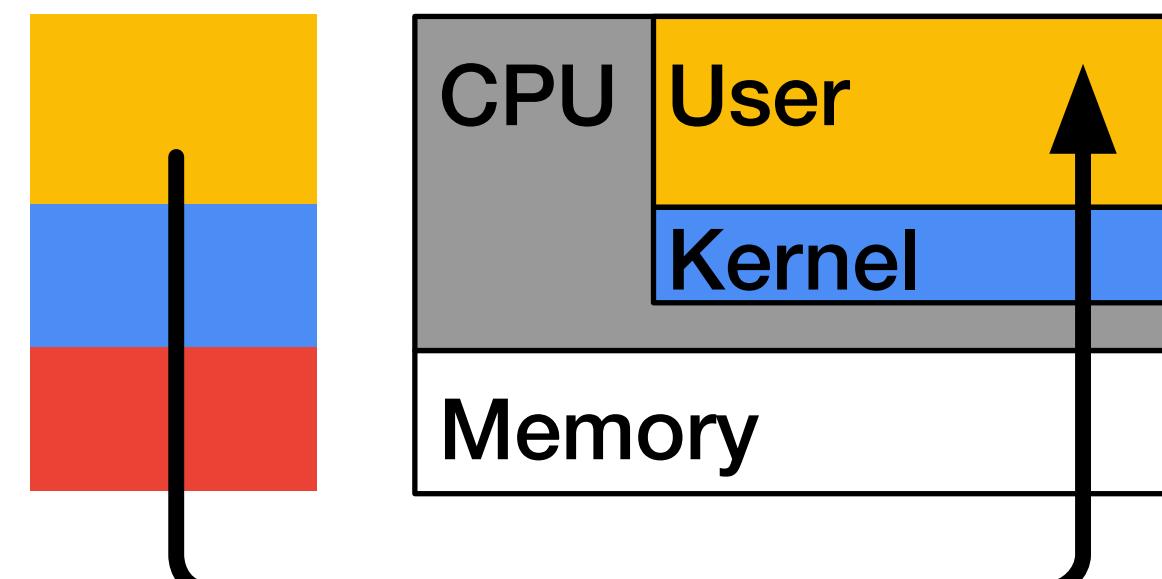
Outline

- Introduction and Background
- Vulnerabilities in One-Sided Communication
- Vulnerabilities in One-Sided Hardware
- Opportunities in One-Sided Communication
- Conclusion

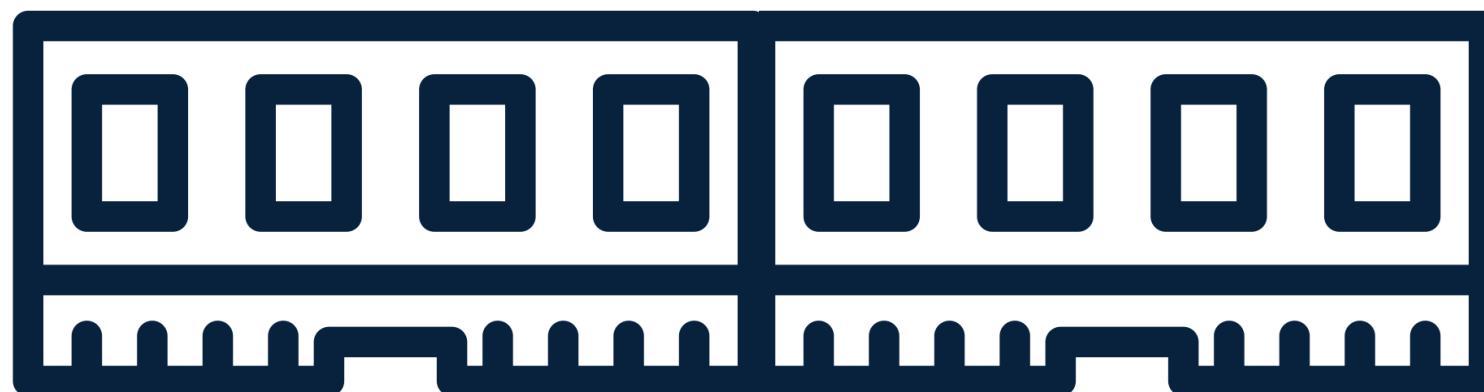
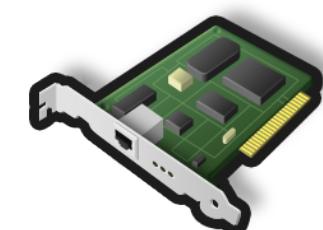
One- and Two-Sided Hardware



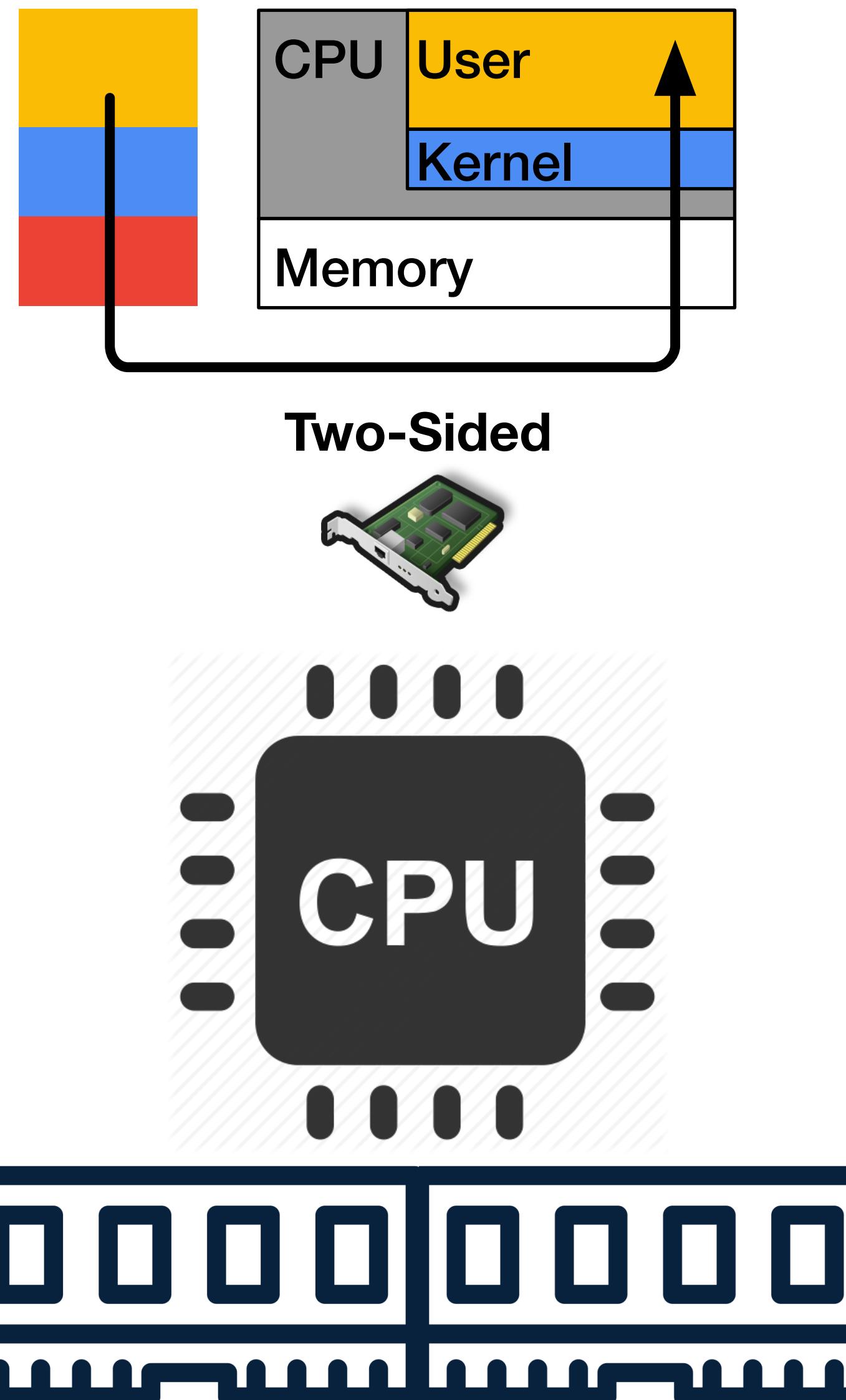
One- and Two-Sided Hardware



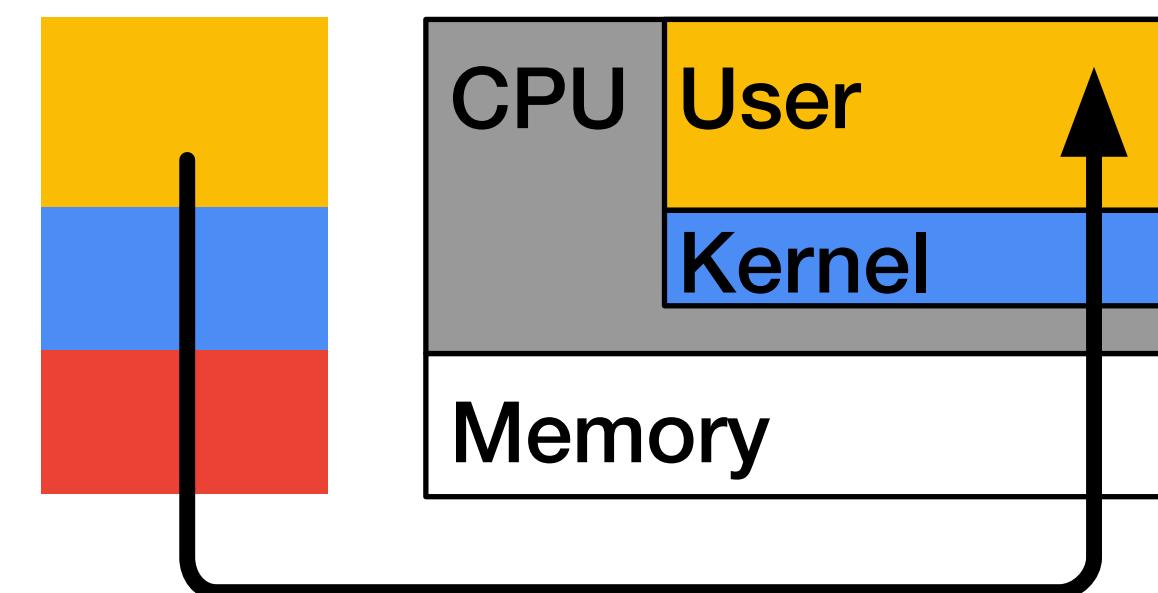
Two-Sided



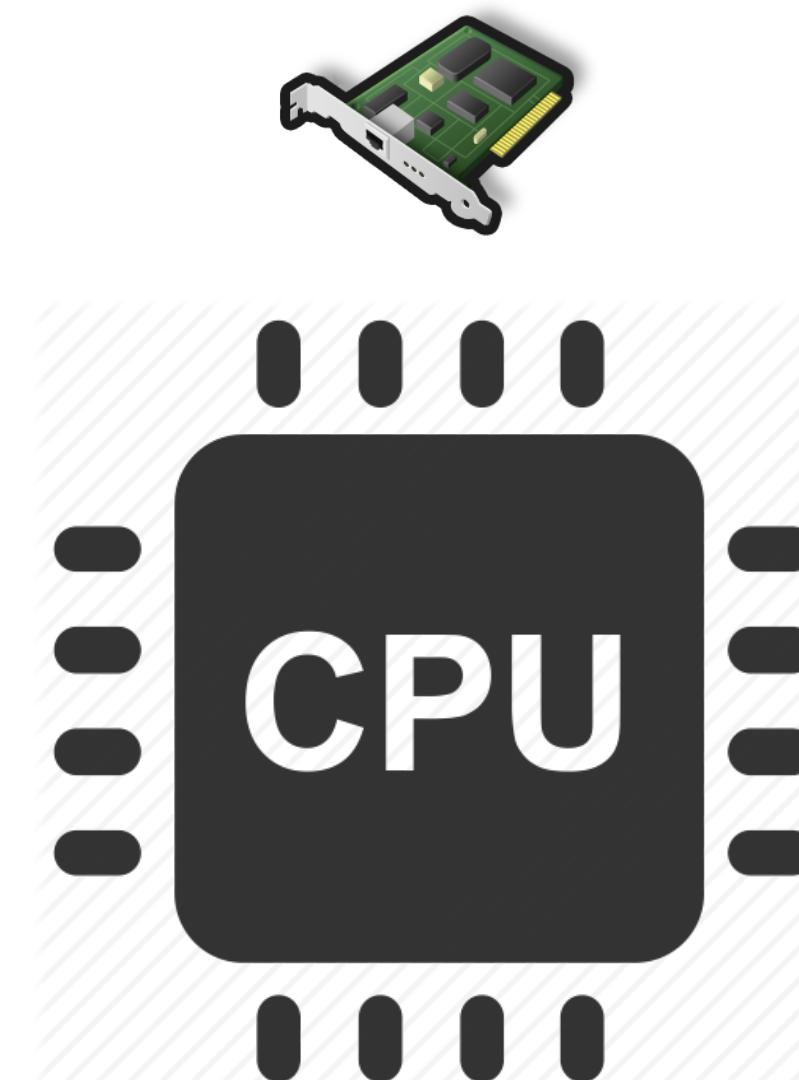
One- and Two-Sided Hardware



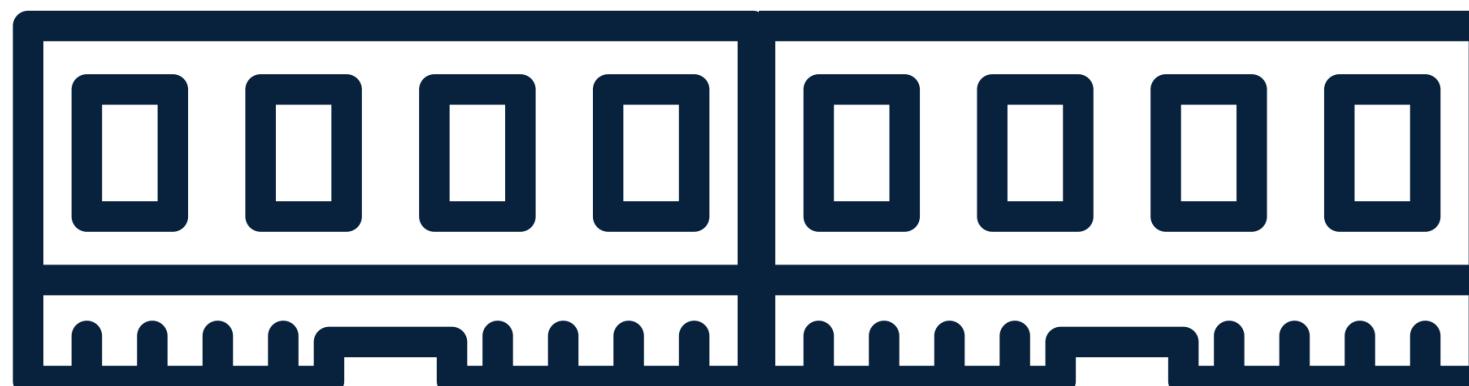
One- and Two-Sided Hardware



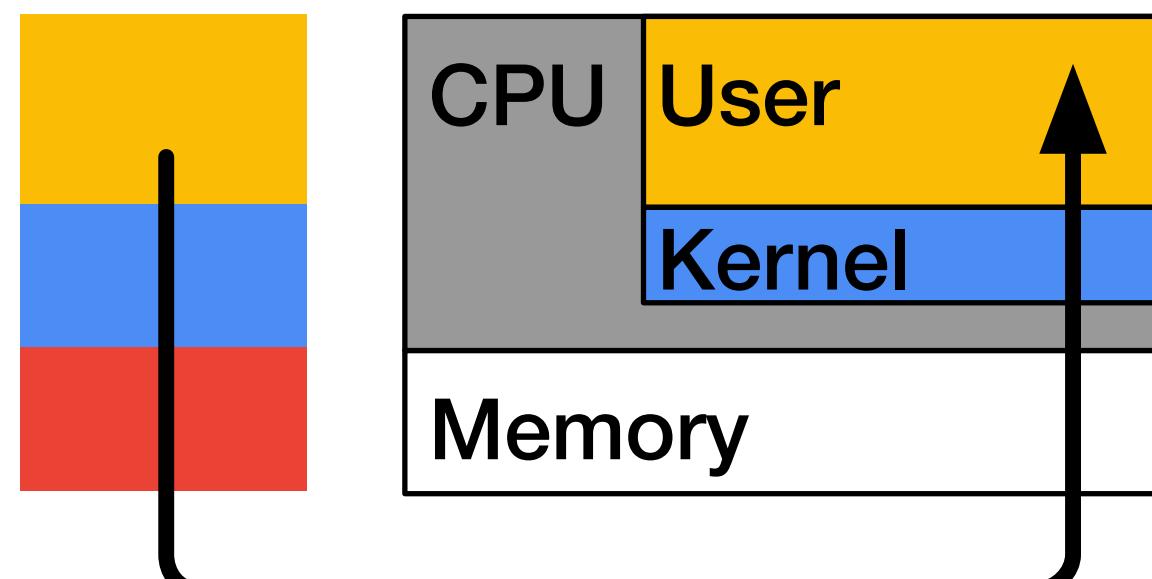
Two-Sided



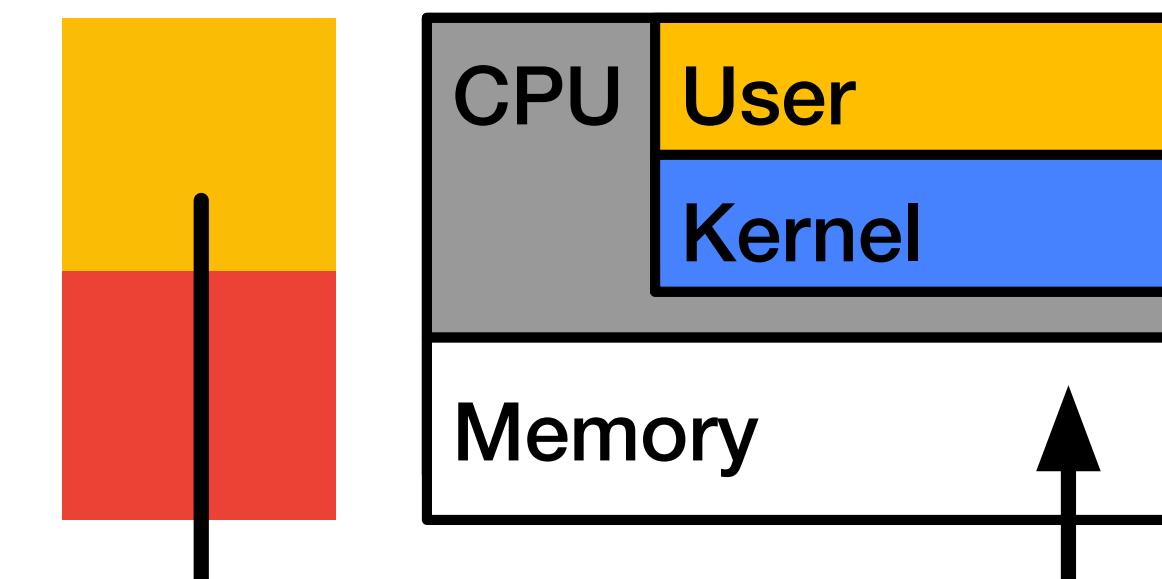
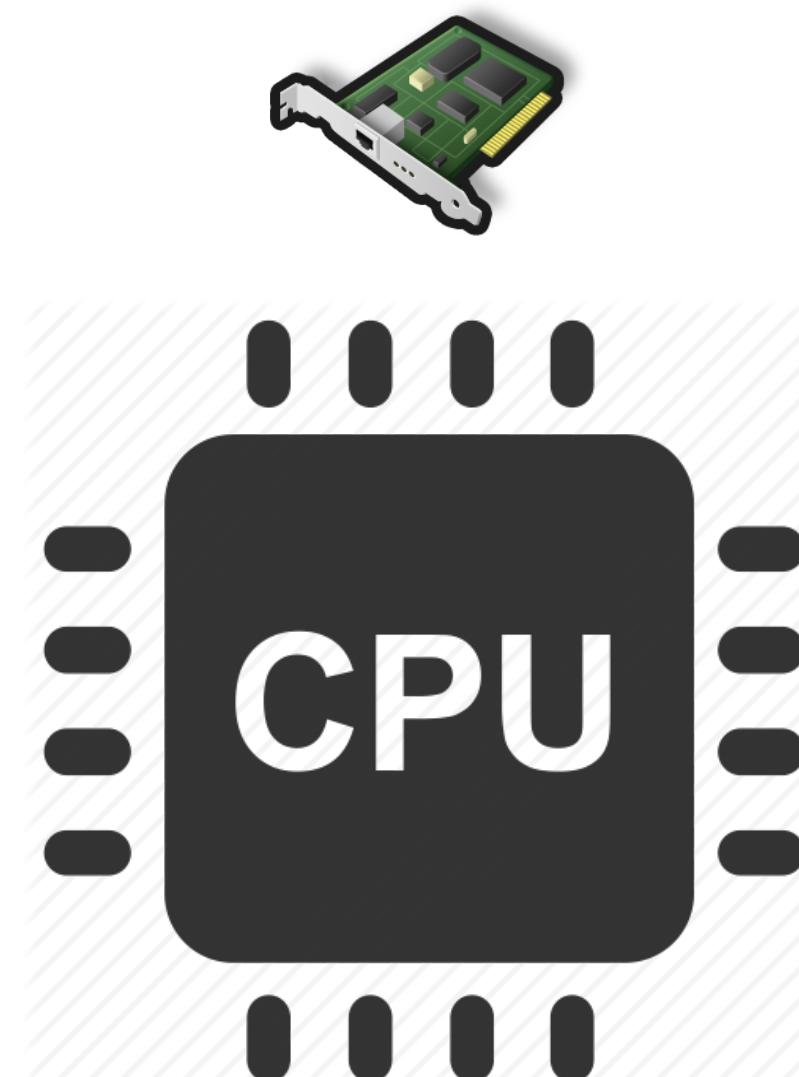
- 1. Address mapping
- 2. Permission checking
- 3. Resource isolation



One- and Two-Sided Hardware

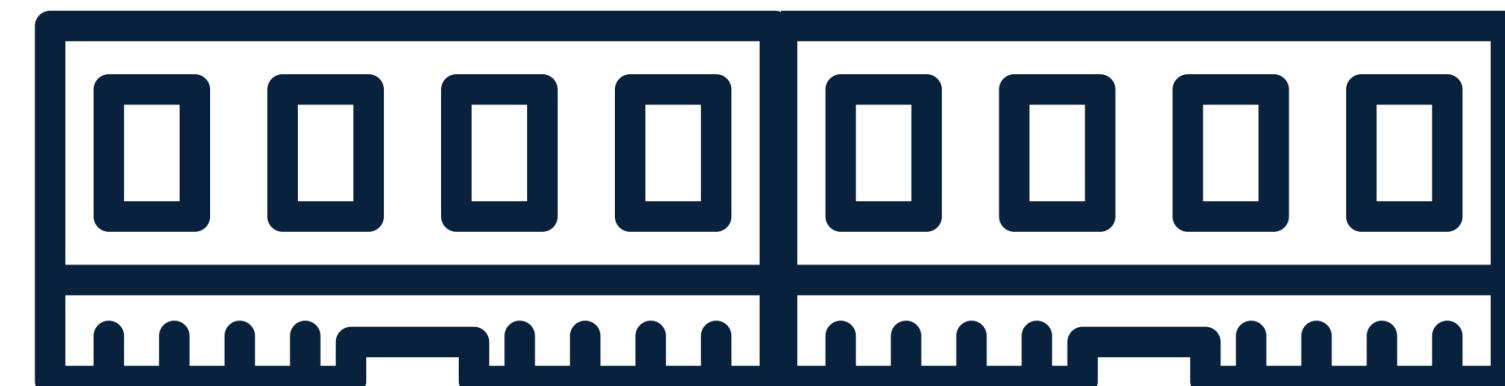
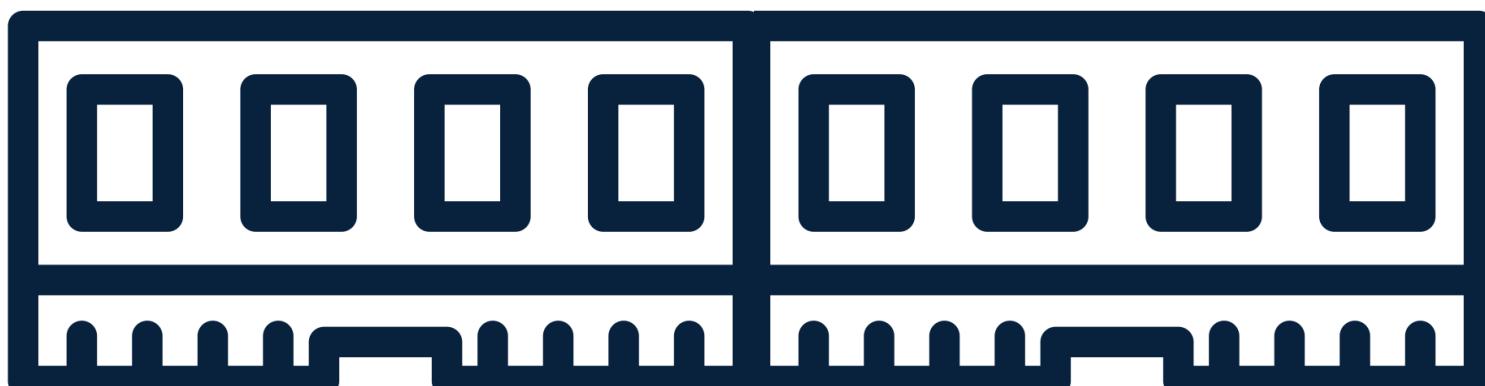


Two-Sided

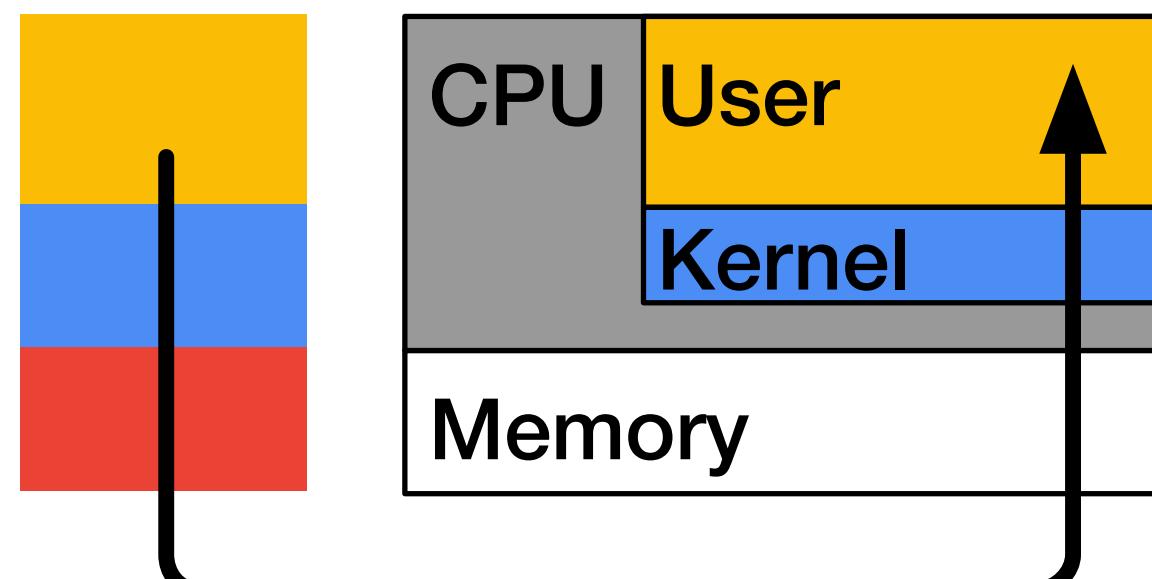


One-Sided

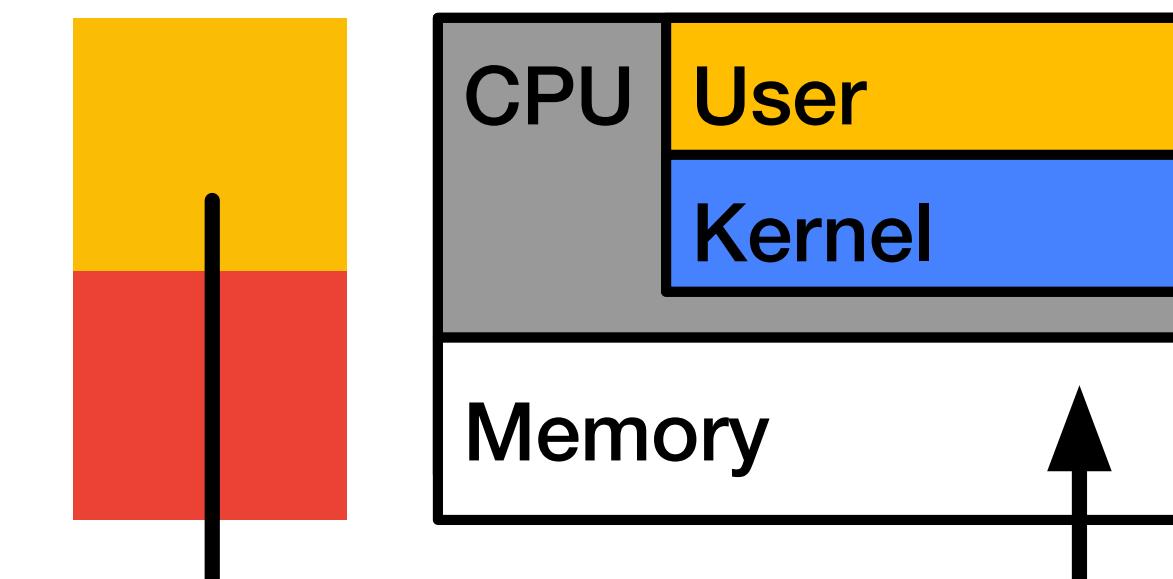
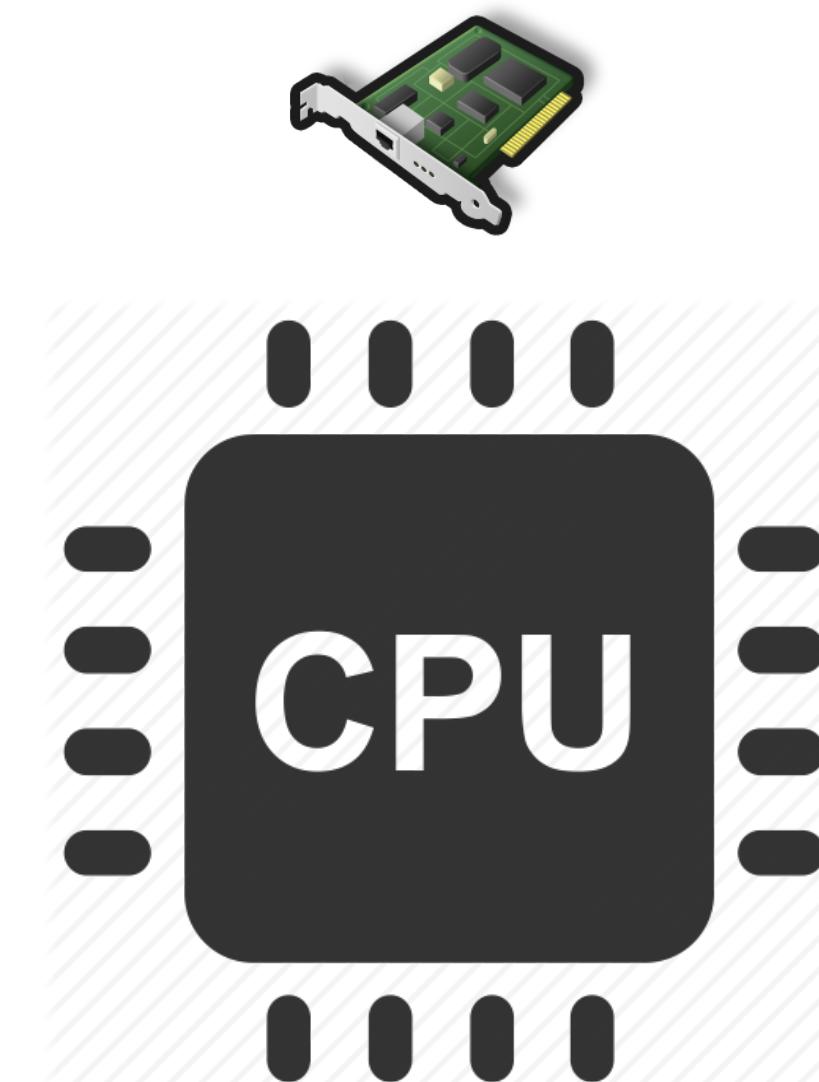
- 1. Address mapping
- 2. Permission checking
- 3. Resource isolation



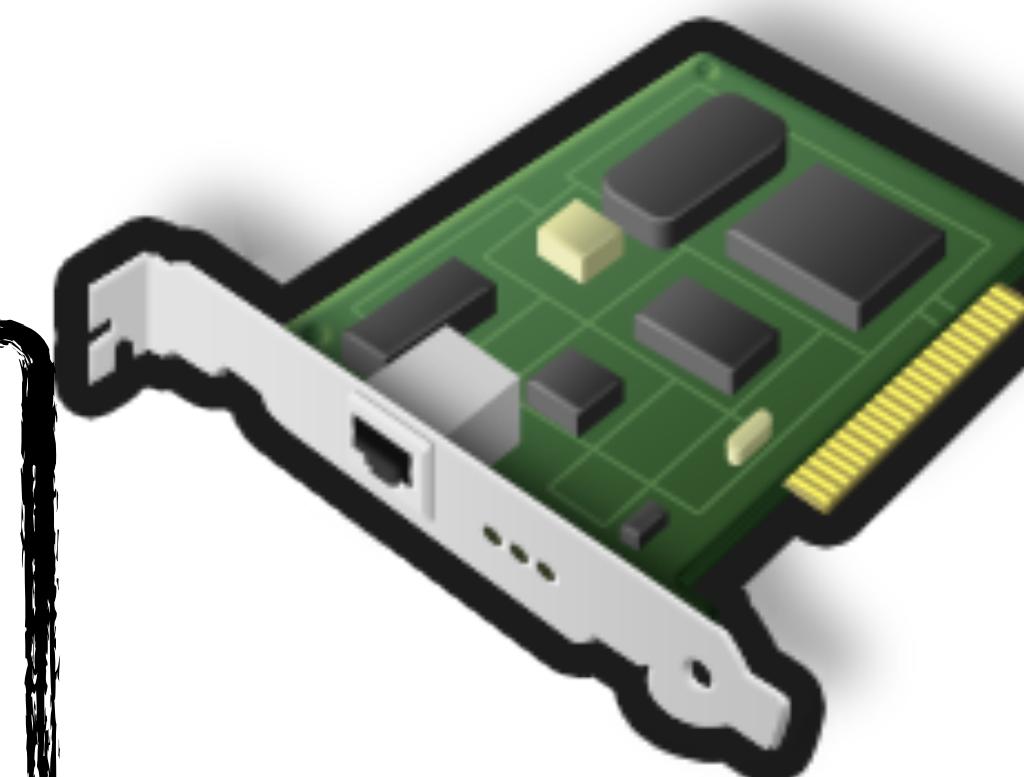
One- and Two-Sided Hardware



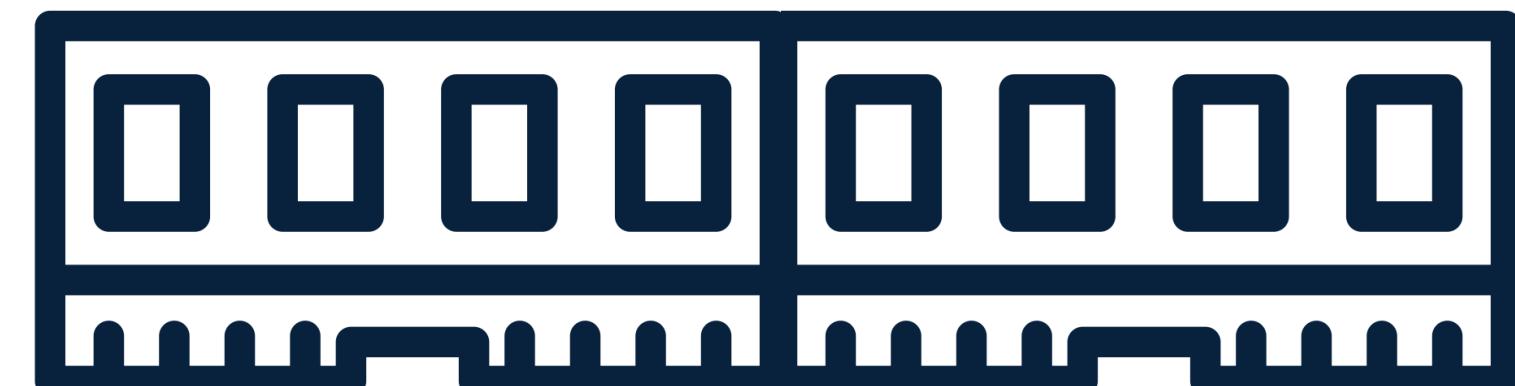
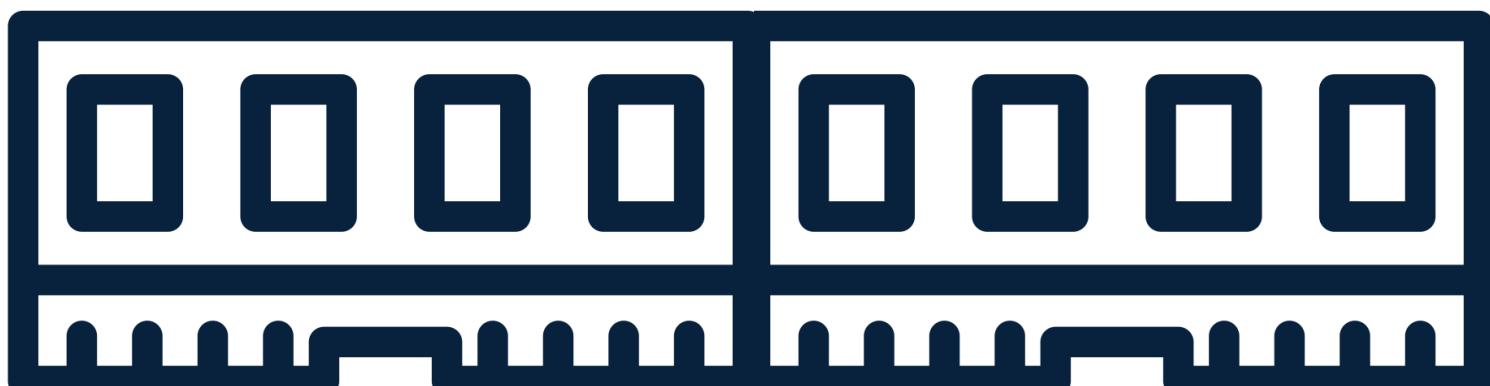
Two-Sided



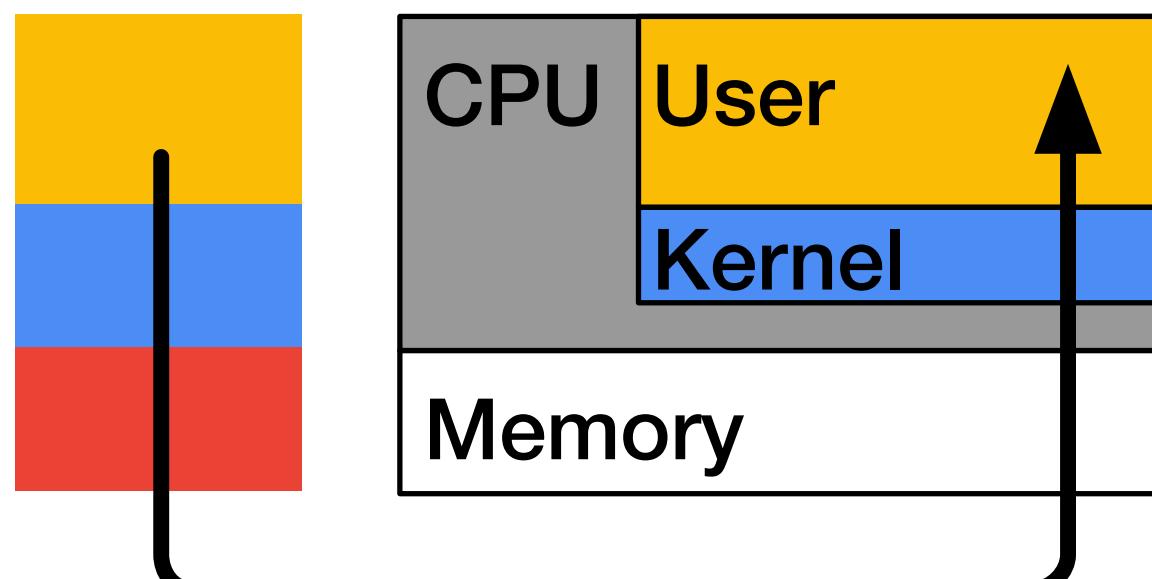
One-Sided



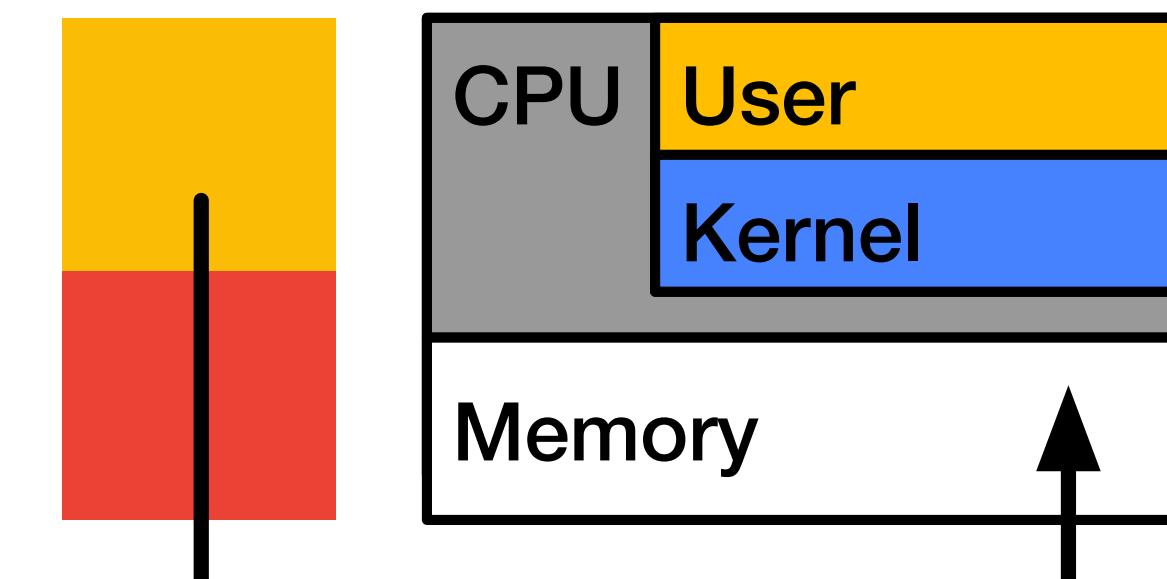
- 1. Address mapping
- 2. Permission checking
- 3. Resource isolation



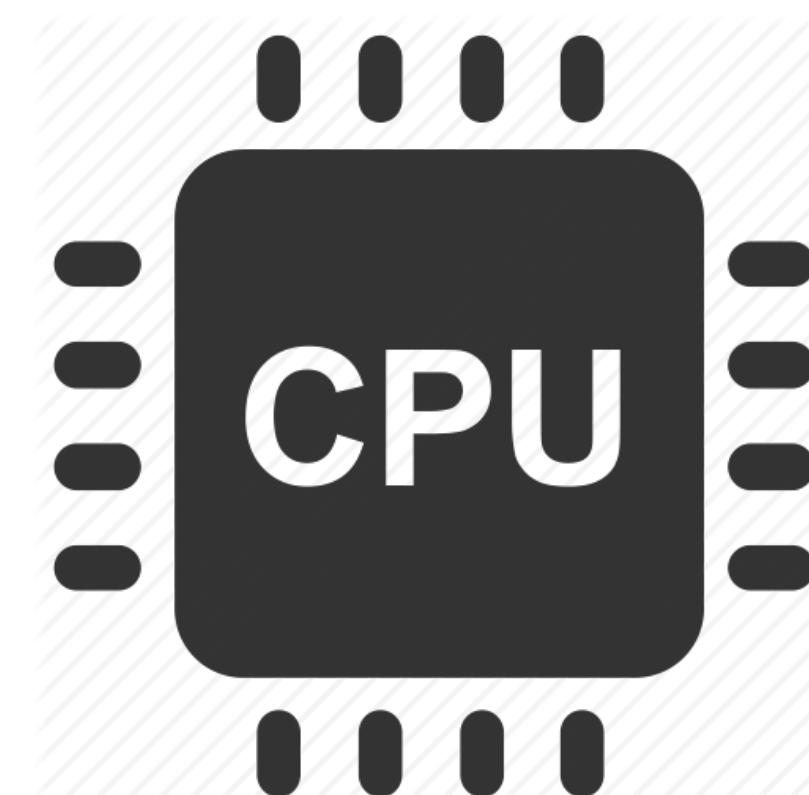
One- and Two-Sided Hardware



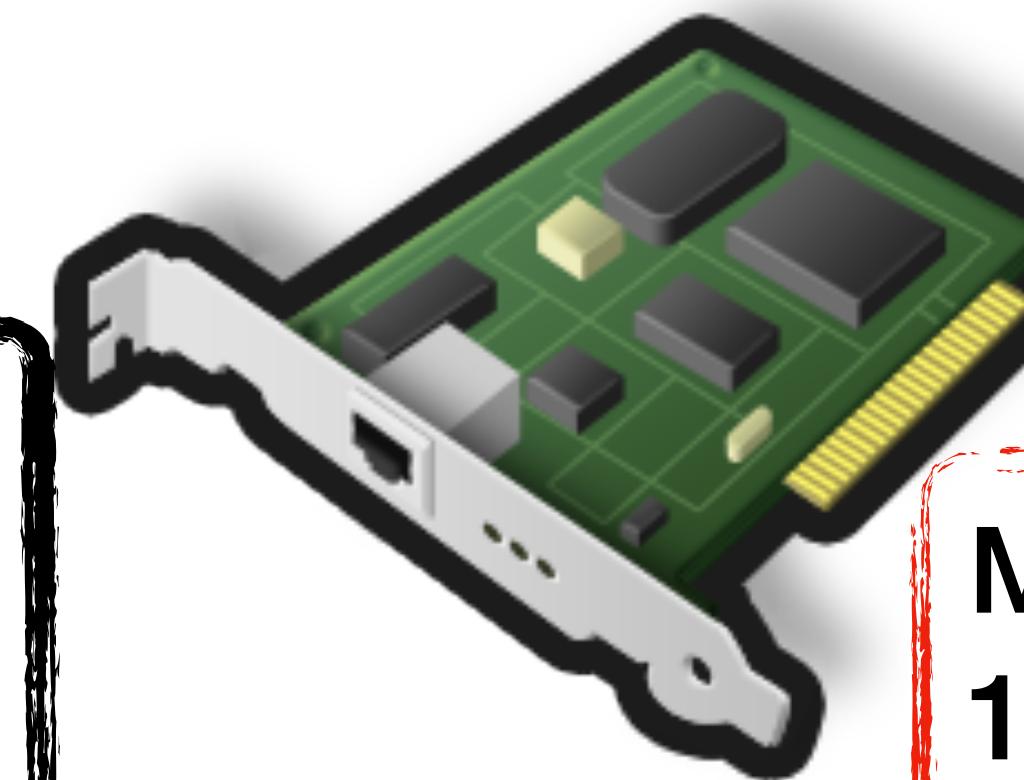
Two-Sided



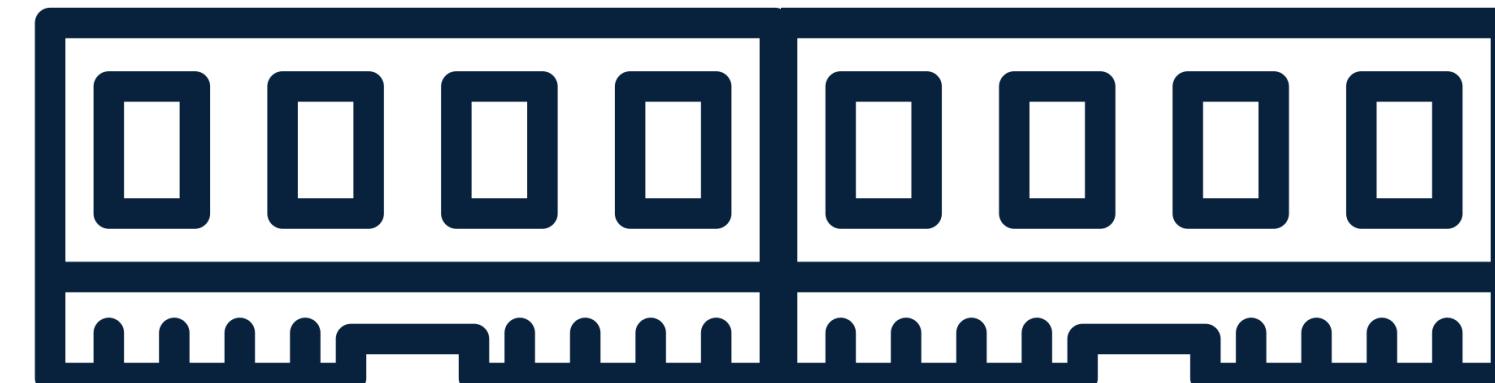
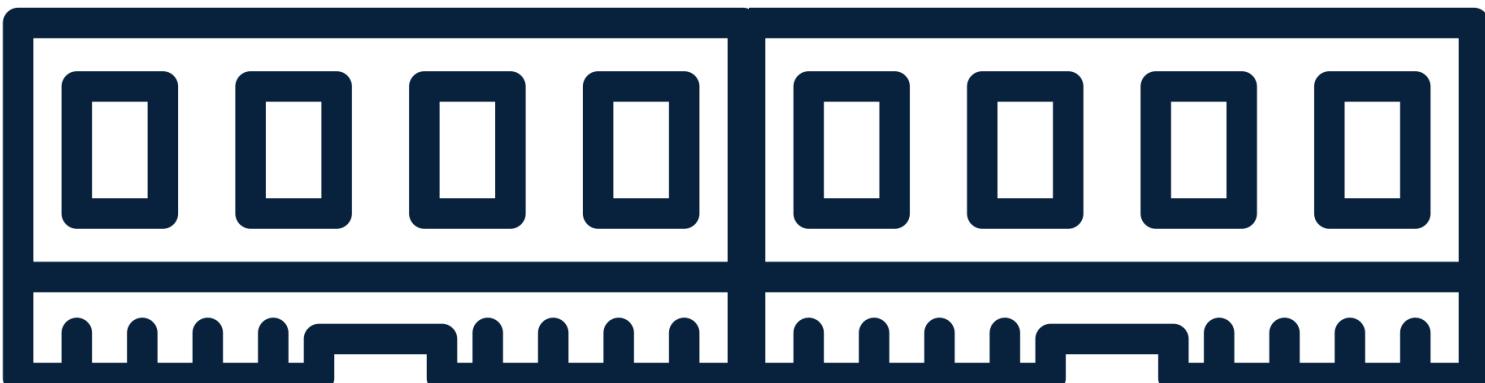
One-Sided



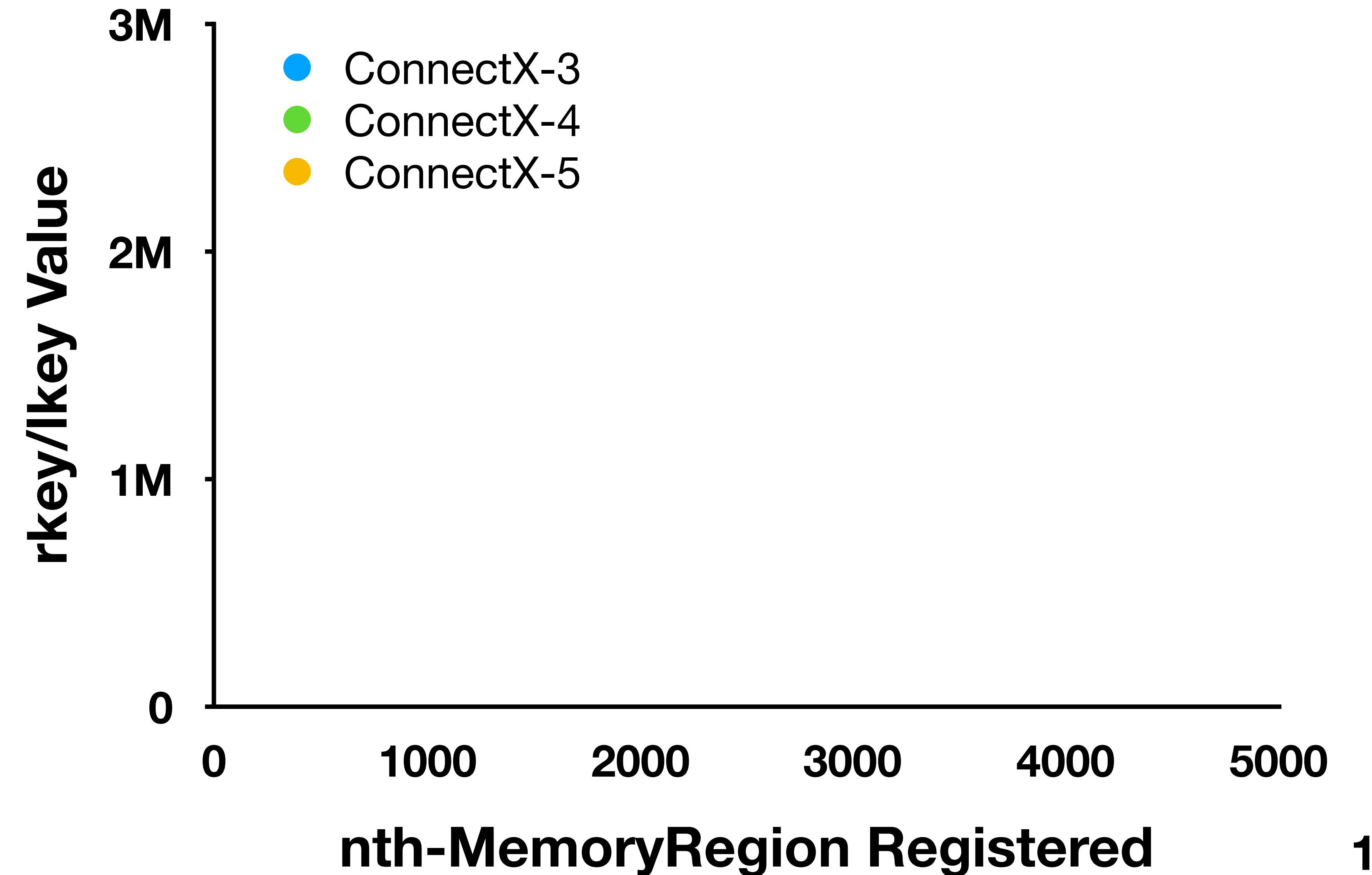
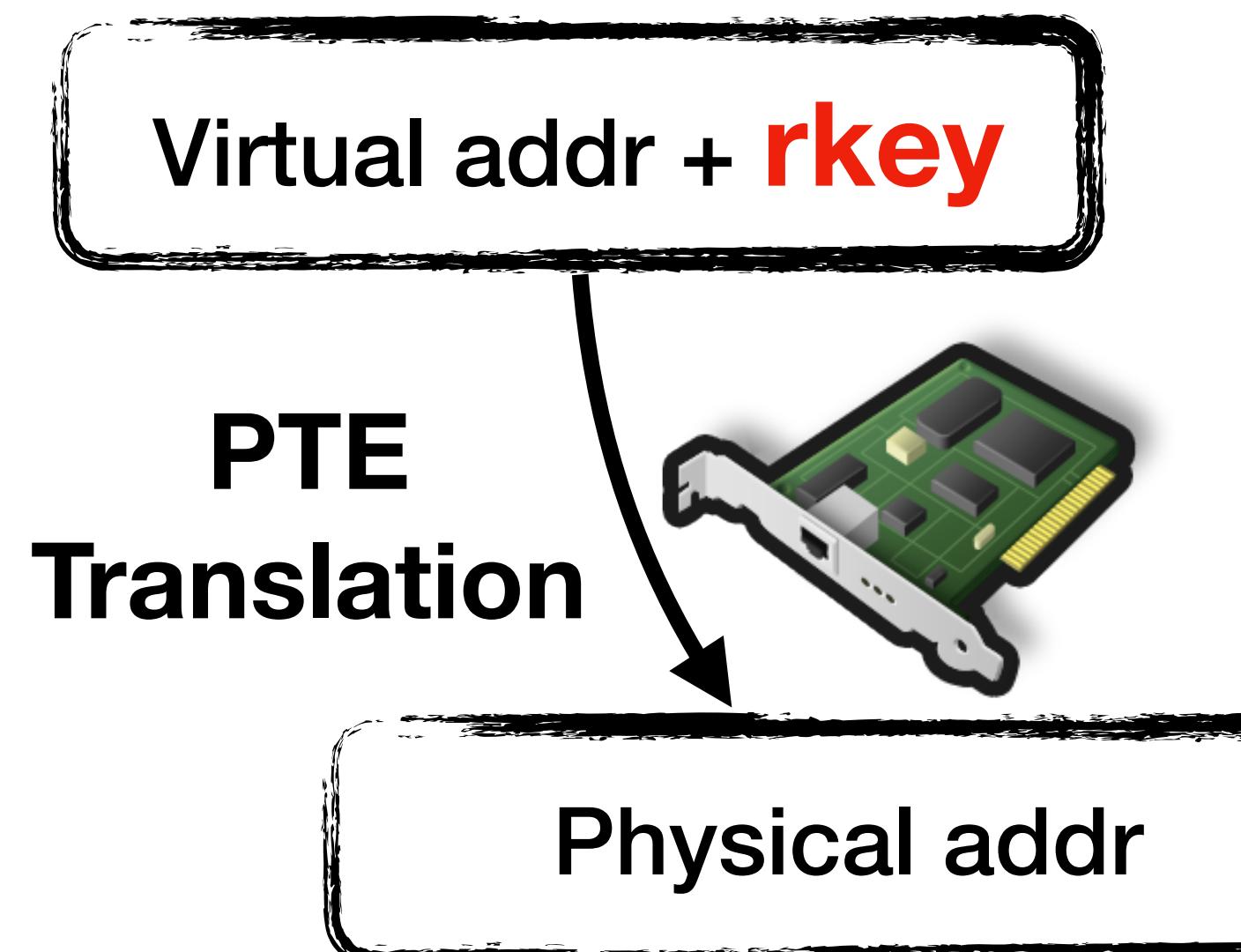
- 1. Address mapping
- 2. Permission checking
- 3. Resource isolation



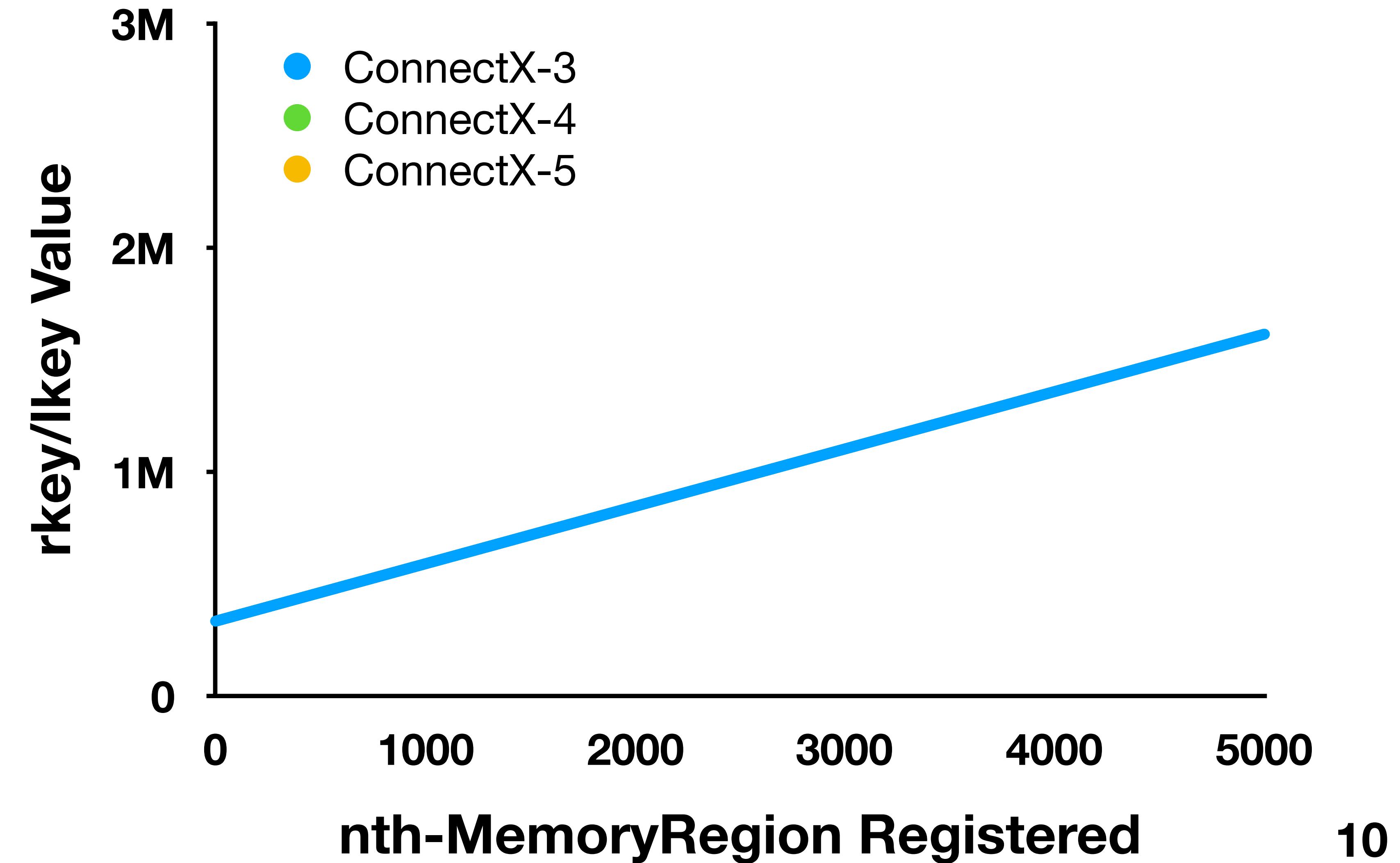
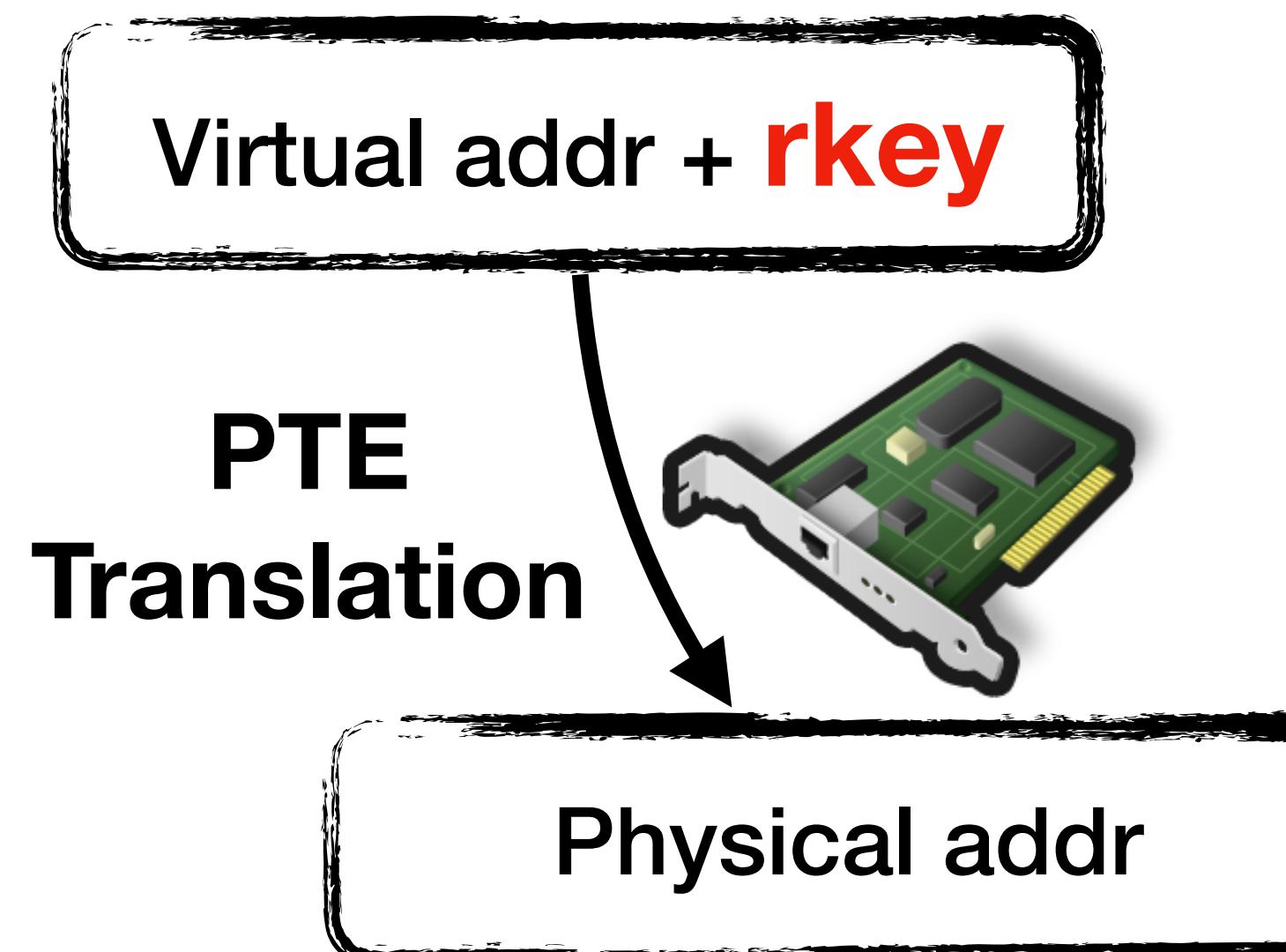
- Memory Region
- 1. rkey/lkey
- 2. Address



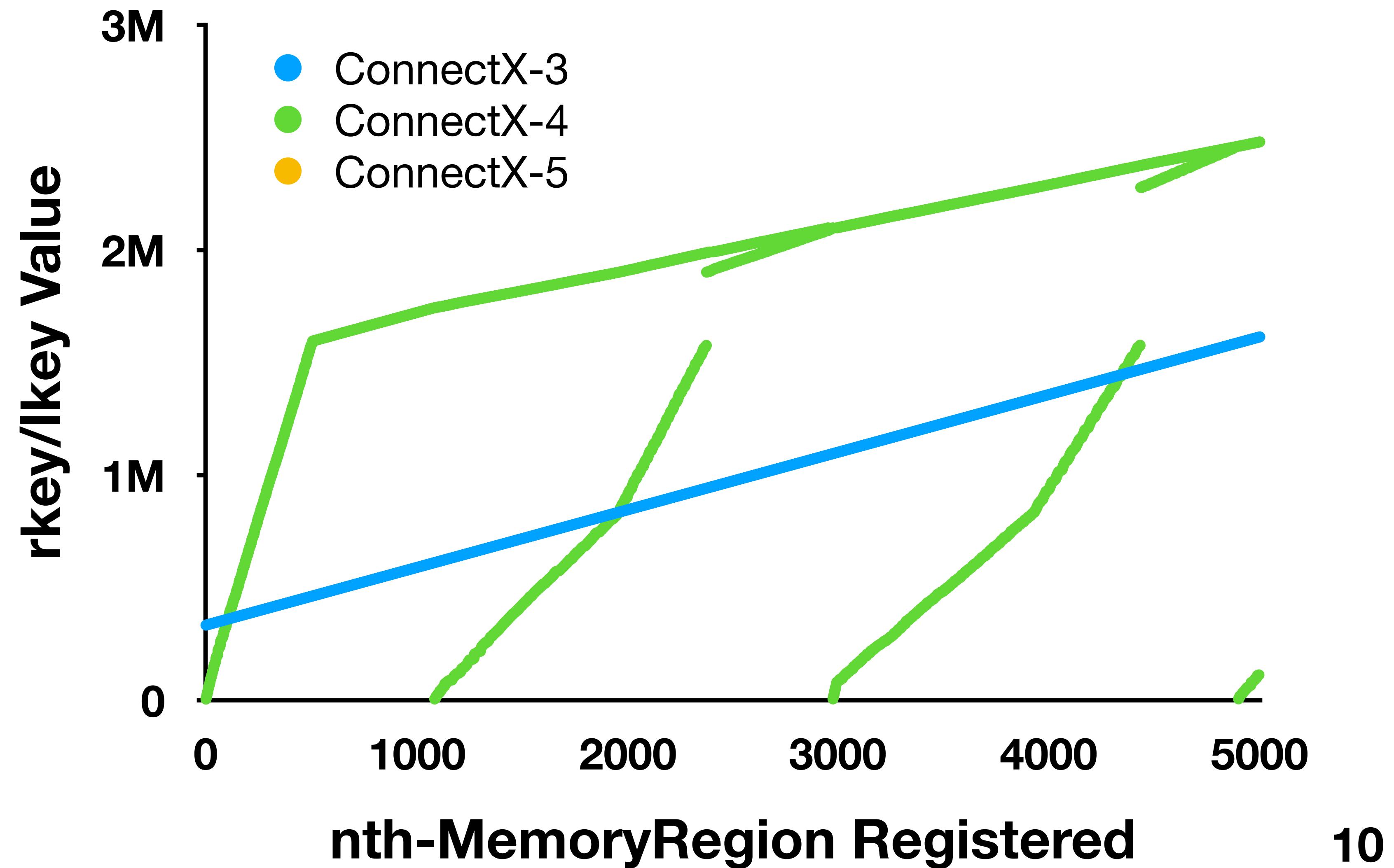
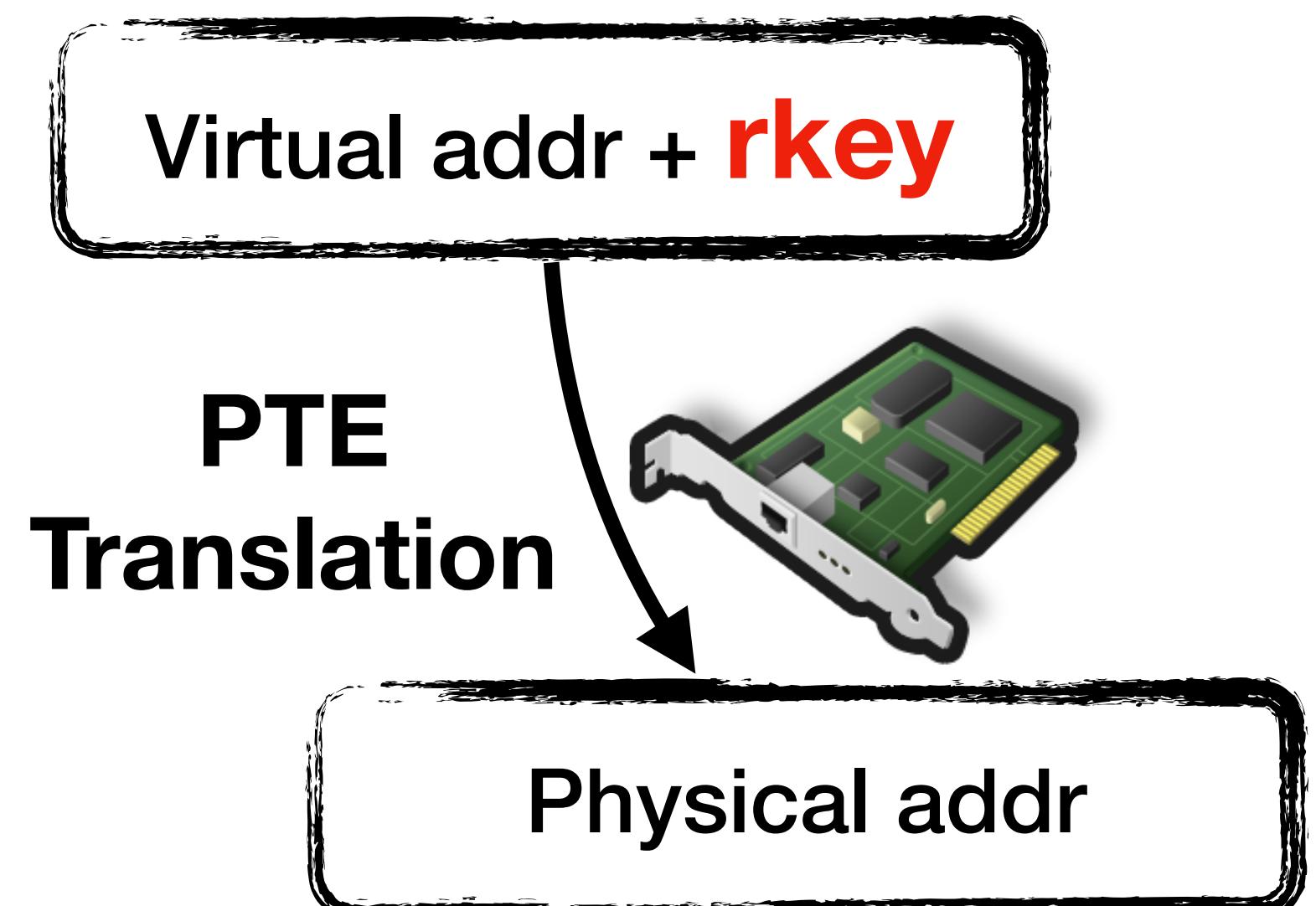
Vulnerability 3 - Predictable Hardware Managed Keys



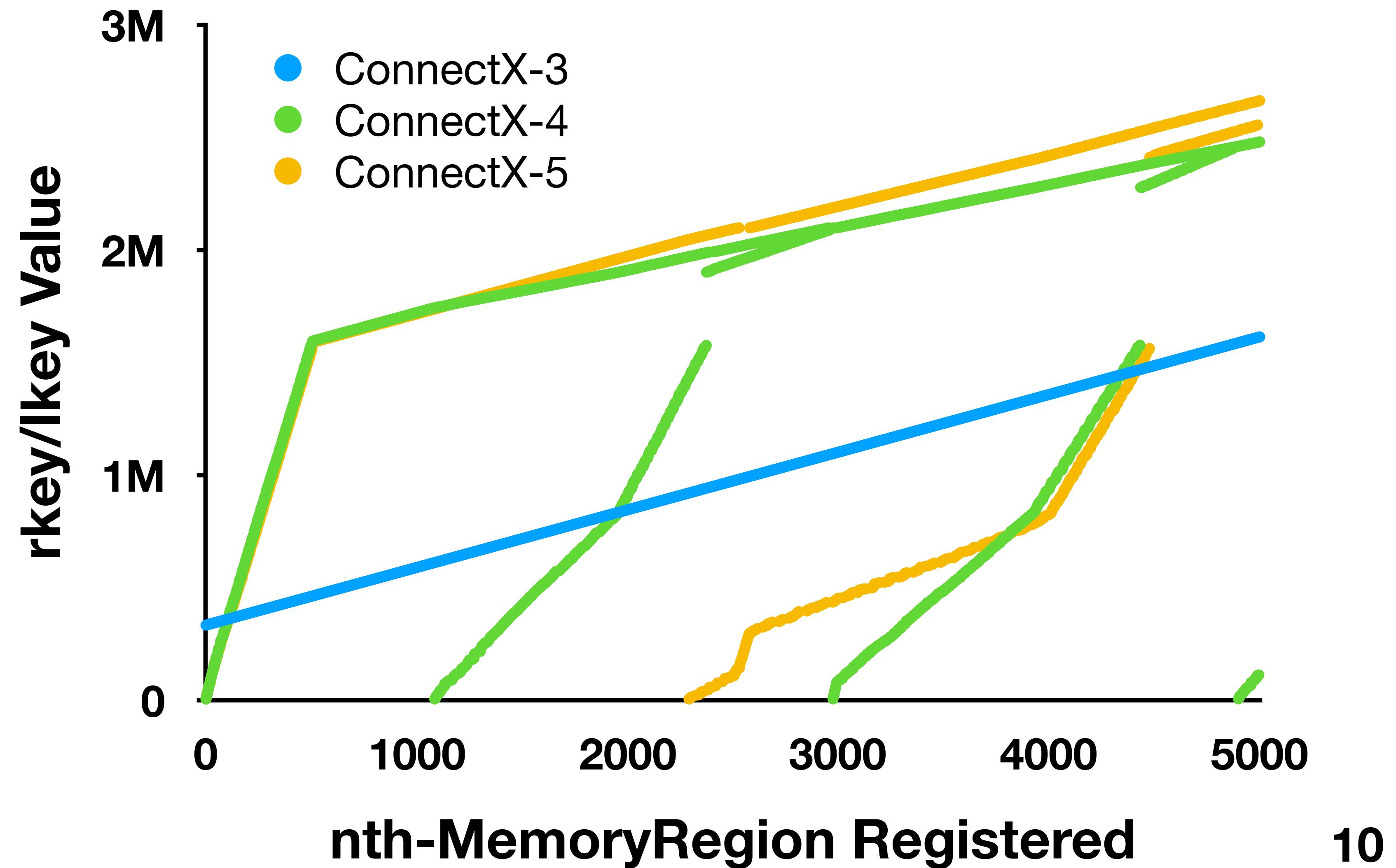
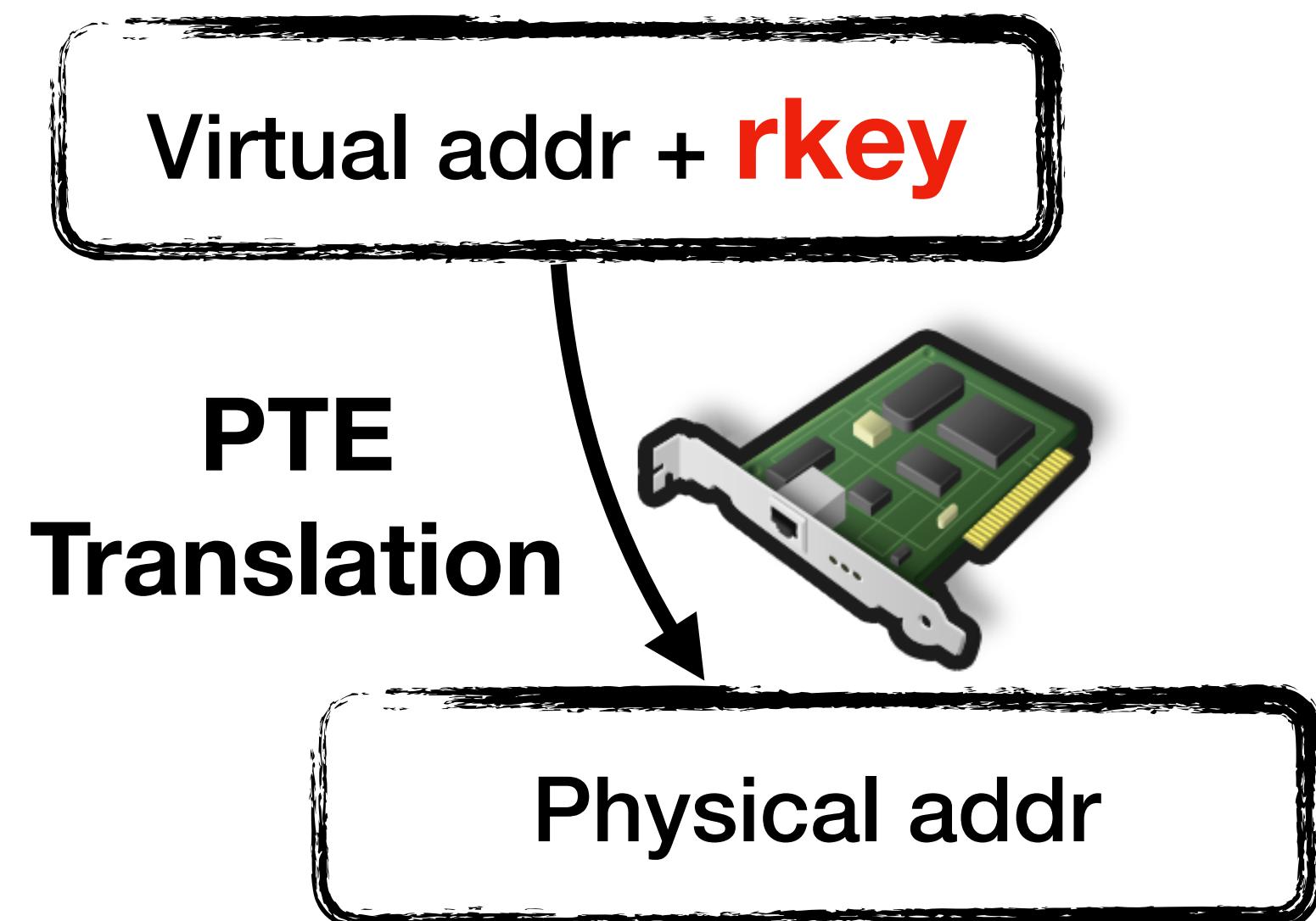
Vulnerability 3 - Predictable Hardware Managed Keys



Vulnerability 3 - Predictable Hardware Managed Keys

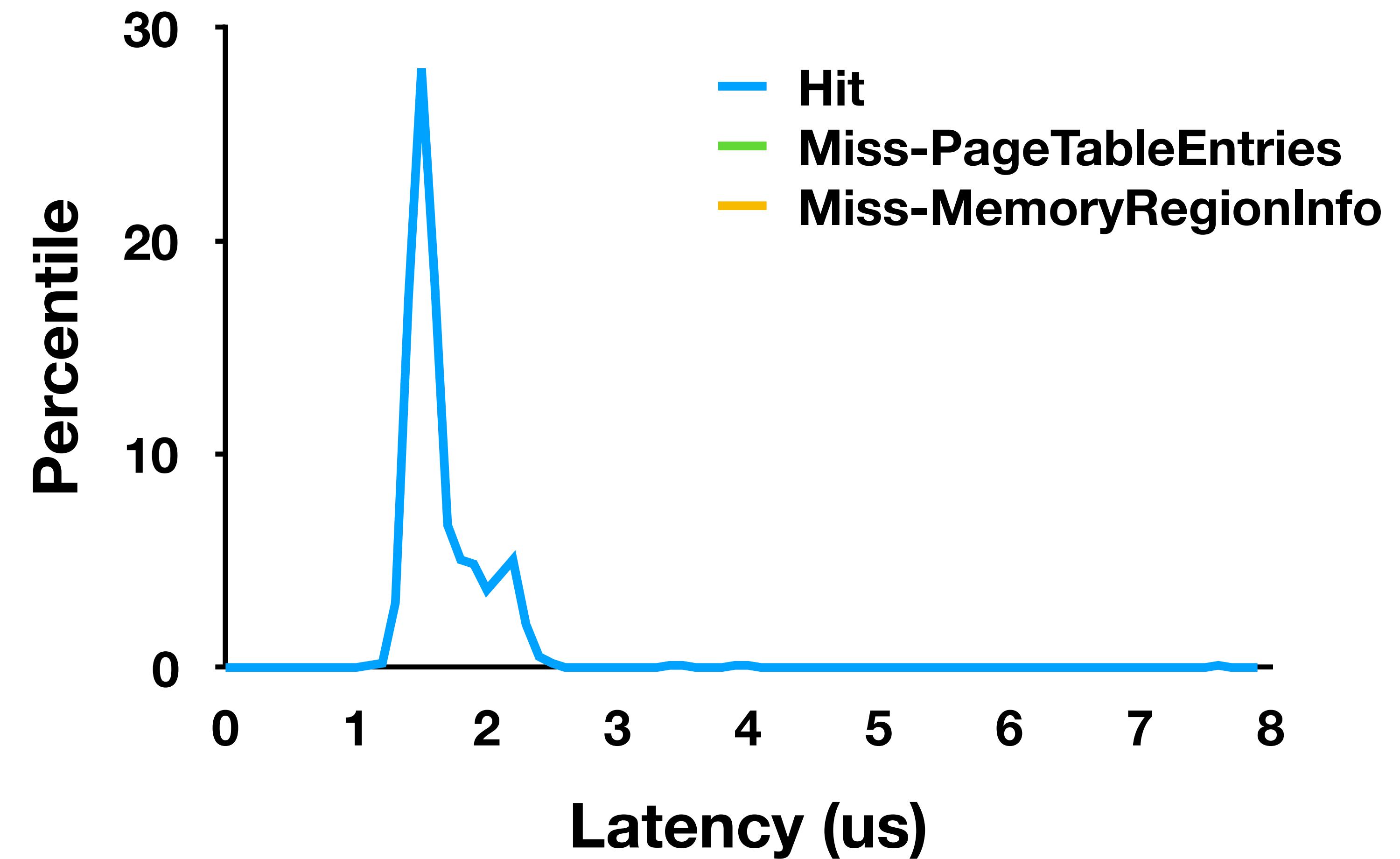
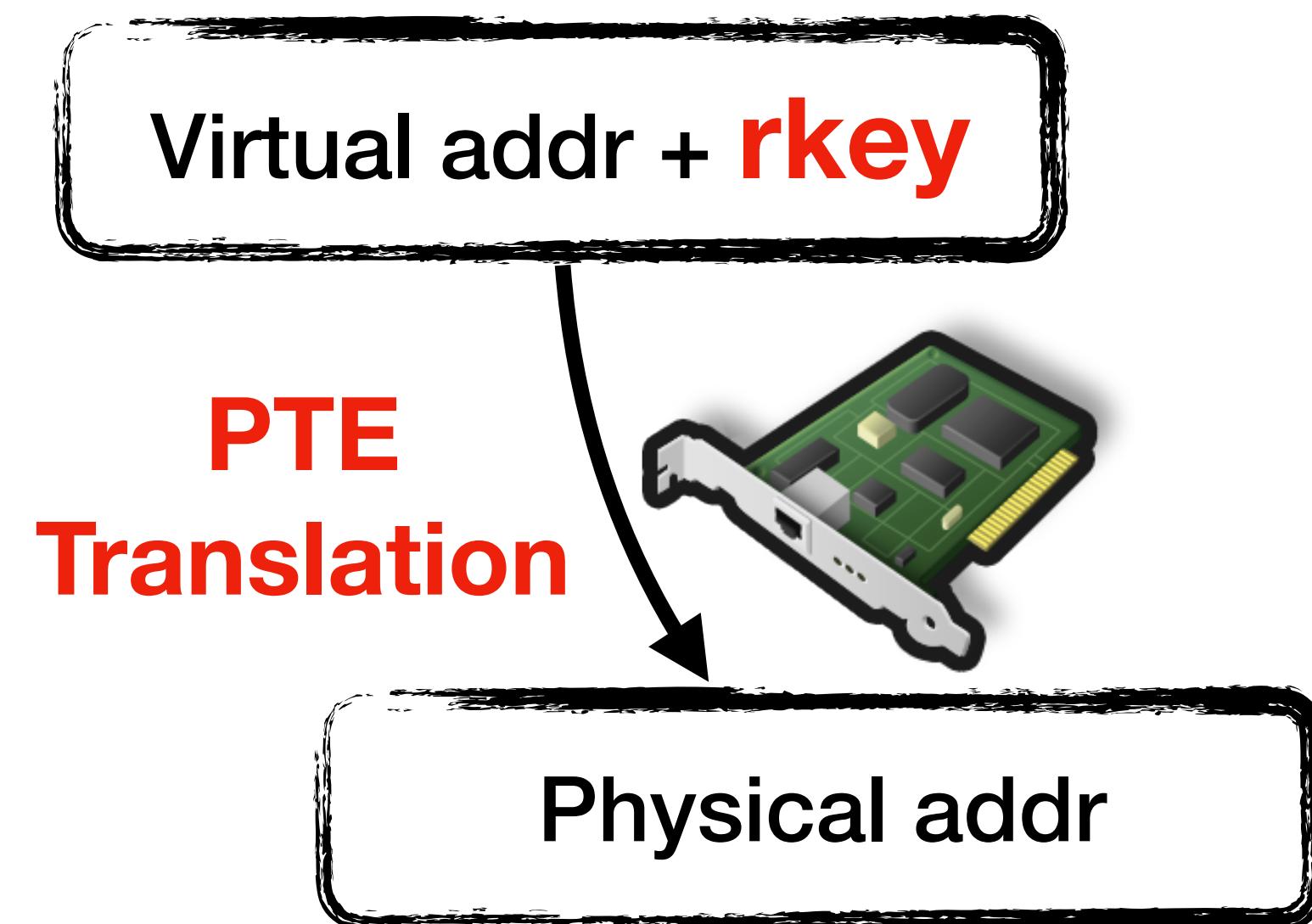


Vulnerability 3 - Predictable Hardware Managed Keys



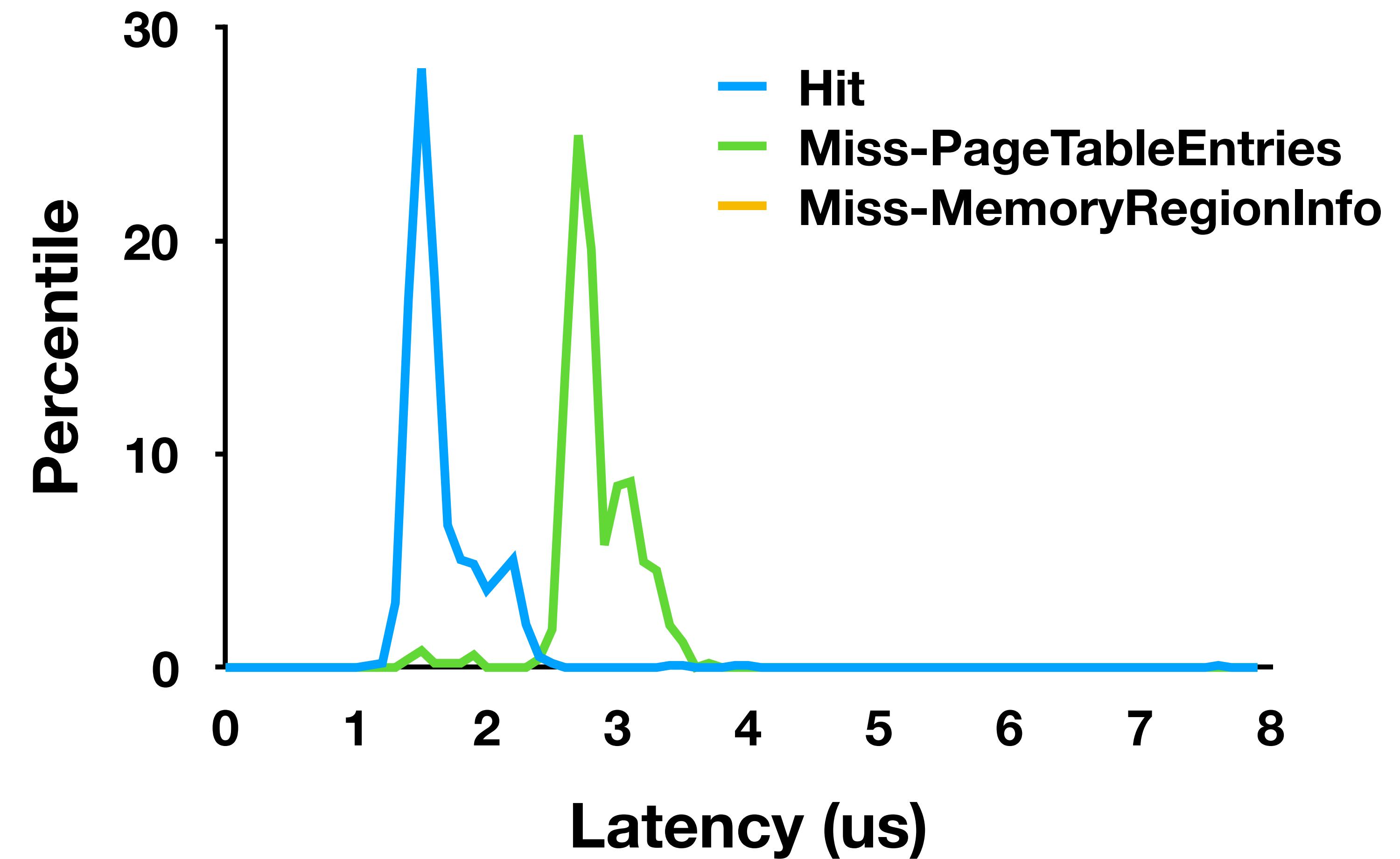
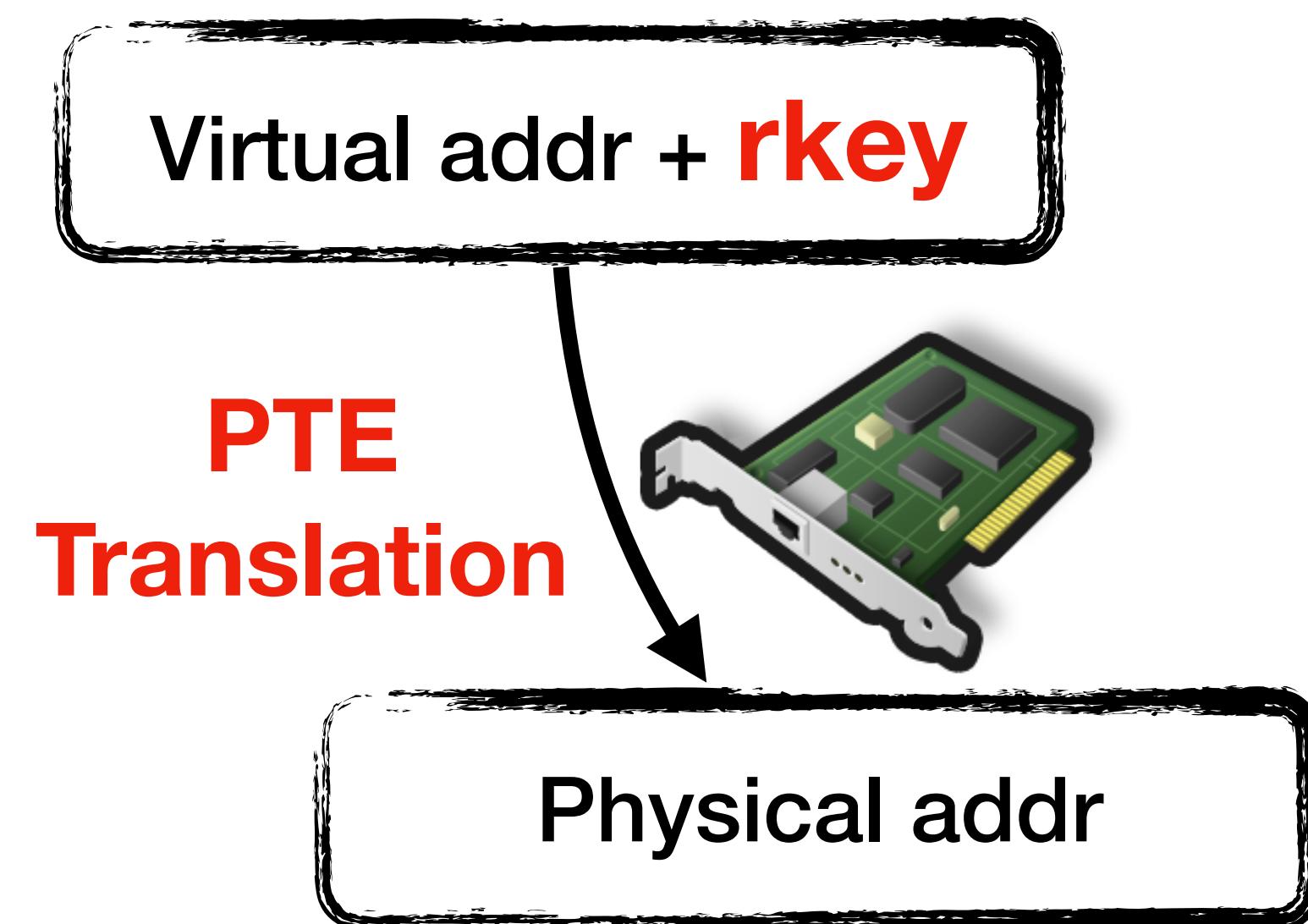
Vulnerability 4 - Side Channel in NICs

ConnectX-5, 1KB READ request latency



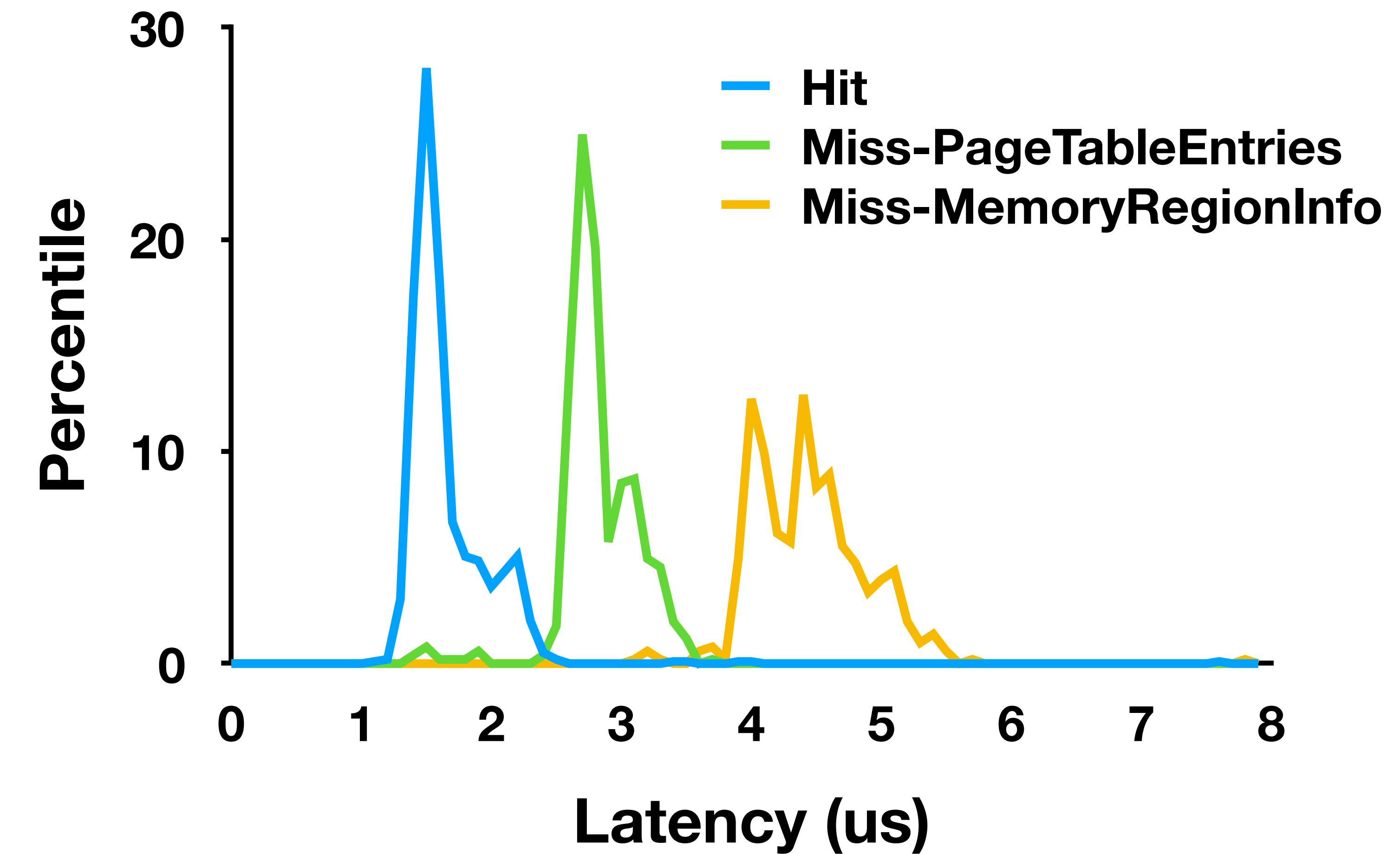
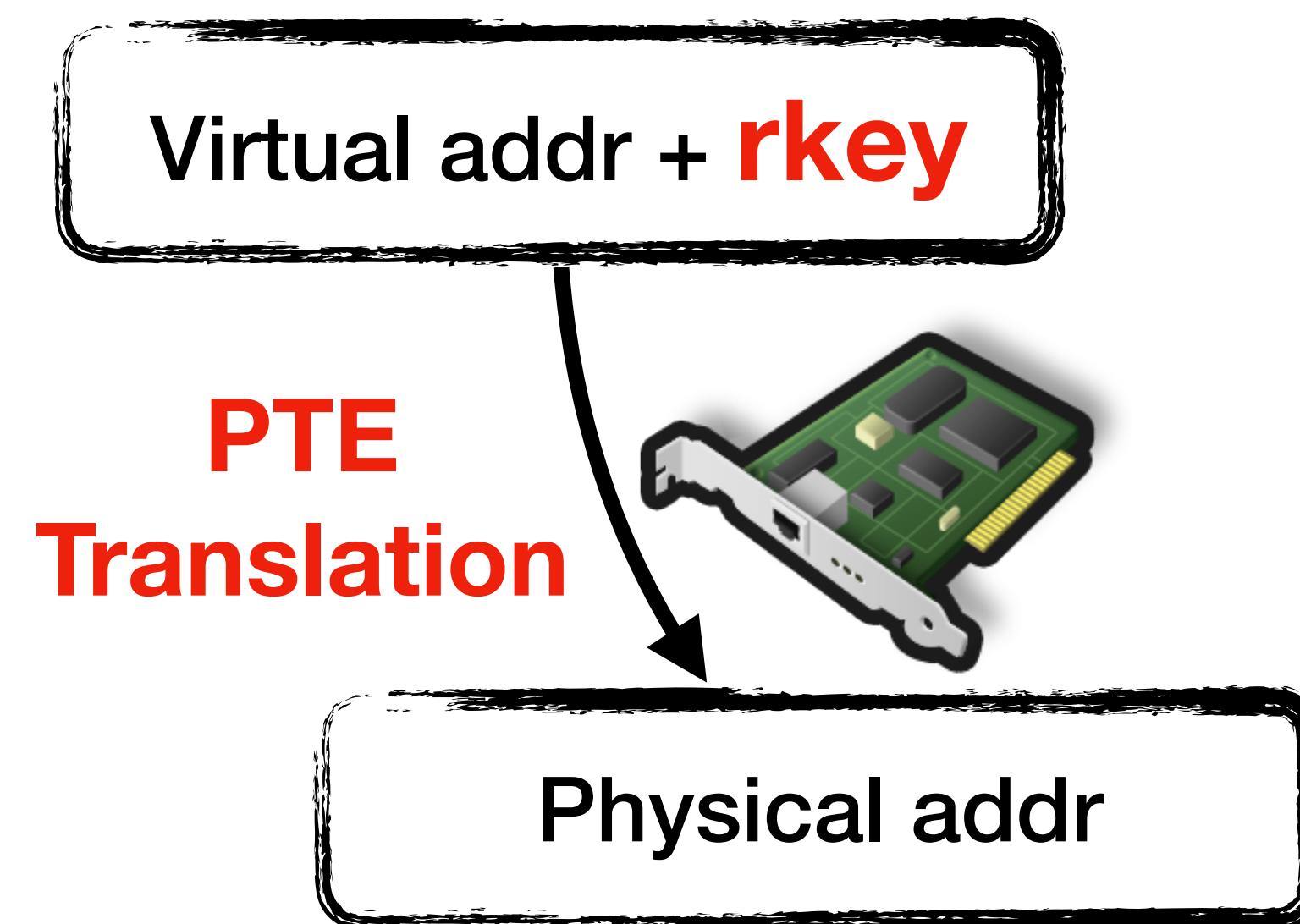
Vulnerability 4 - Side Channel in NICs

ConnectX-5, 1KB READ request latency



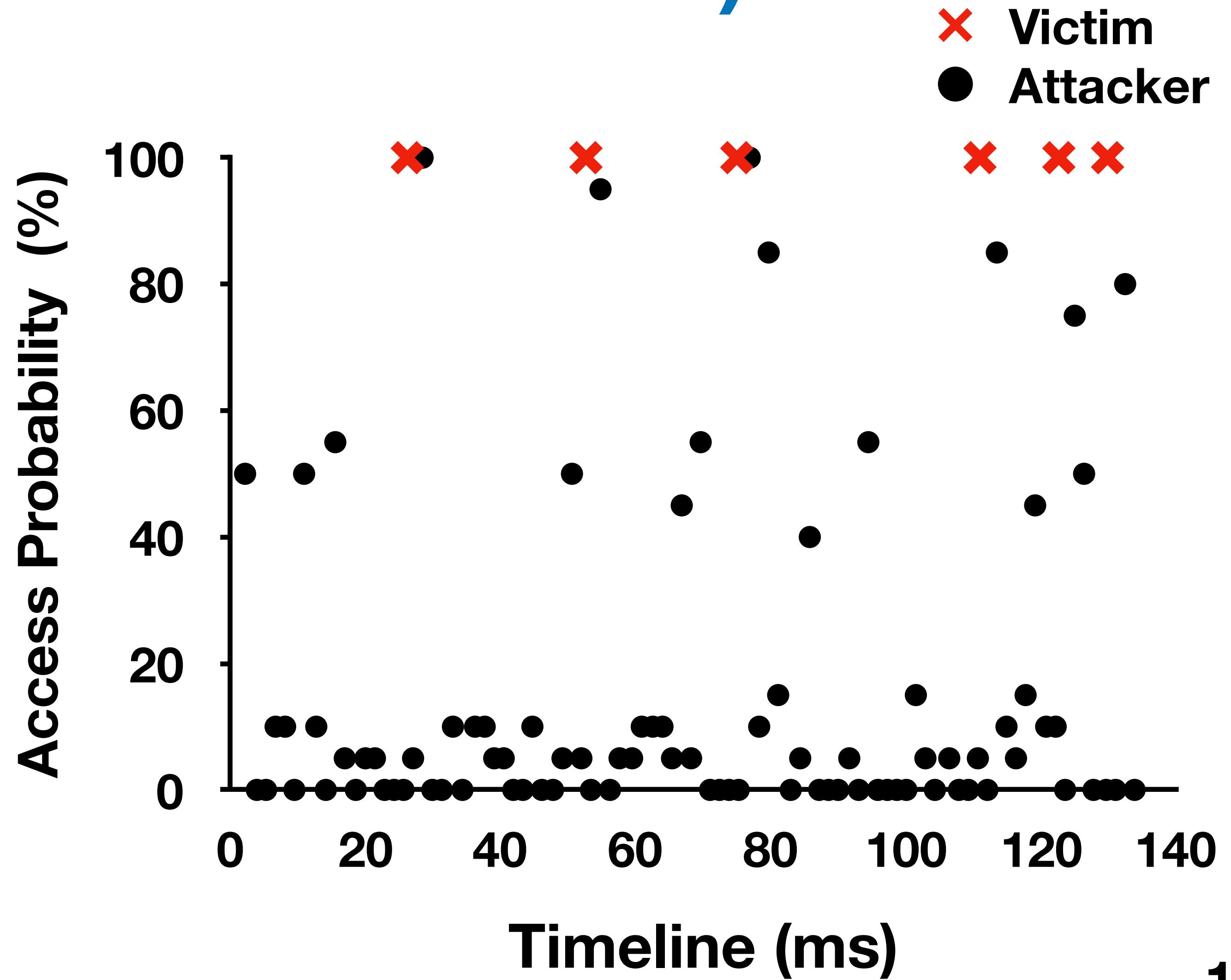
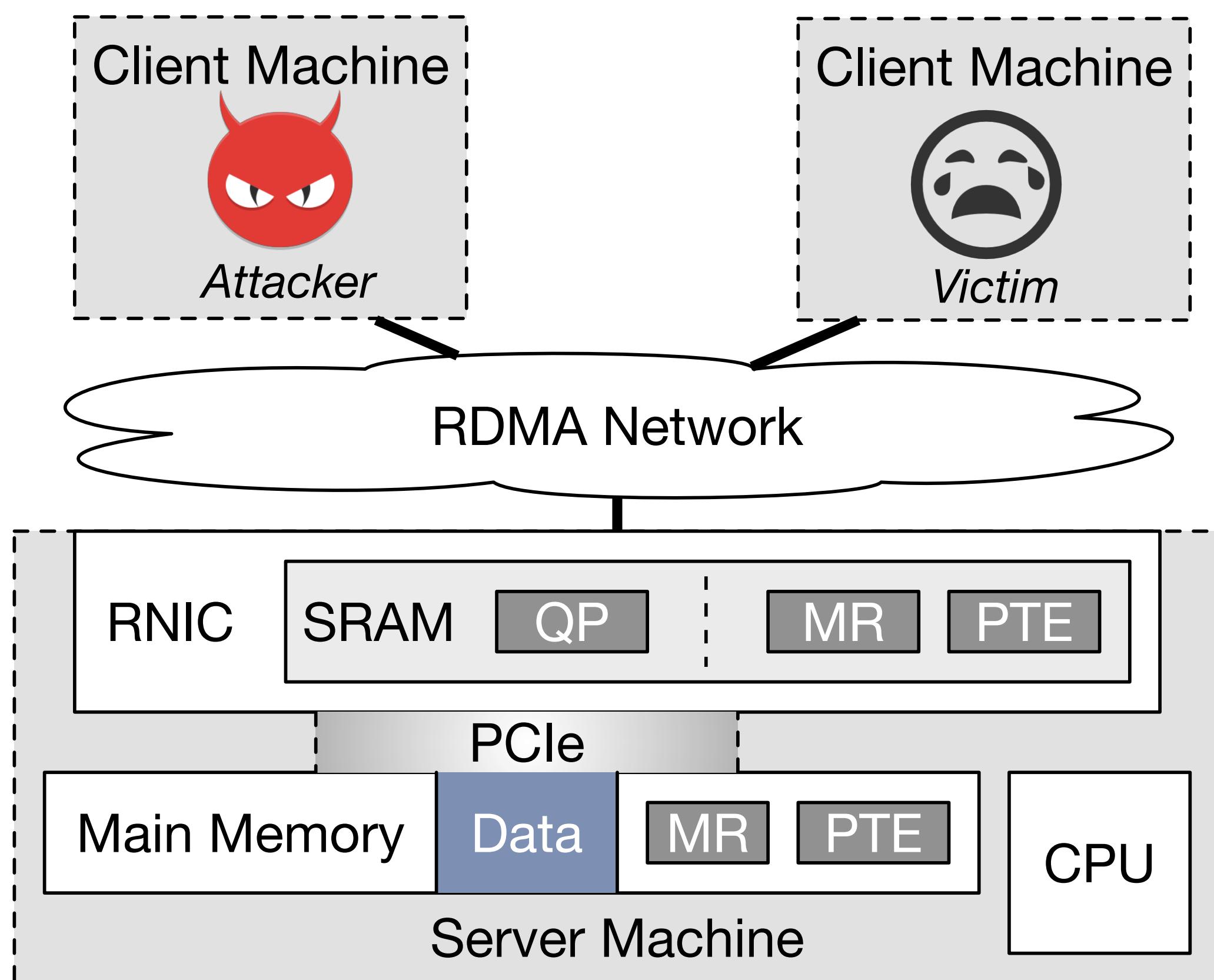
Vulnerability 4 - Side Channel in NICs

ConnectX-5, 1KB READ request latency



Side-Channel Attacks in RDMA

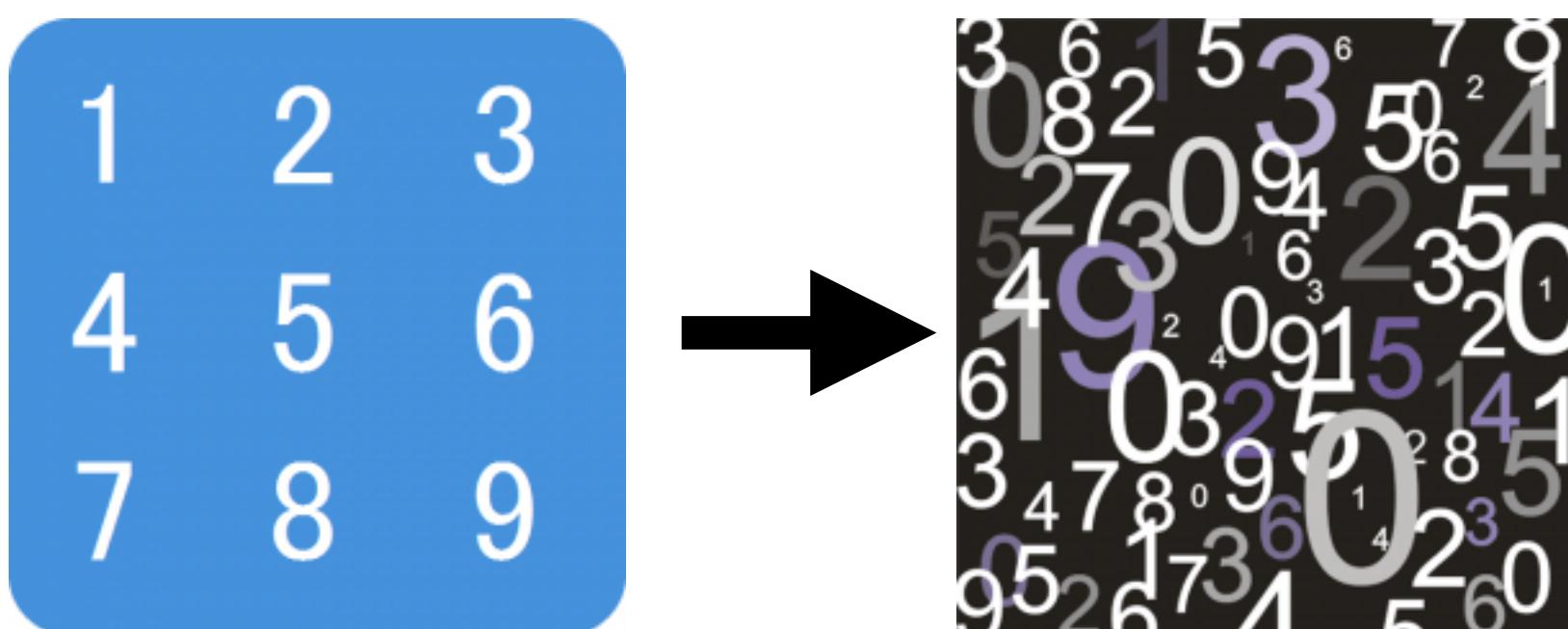
(Pythia, USENIX Sec '19)



Discussion and Defense

- Generate memory registration keys cryptographically

Sequential to Random

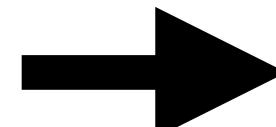


Discussion and Defense

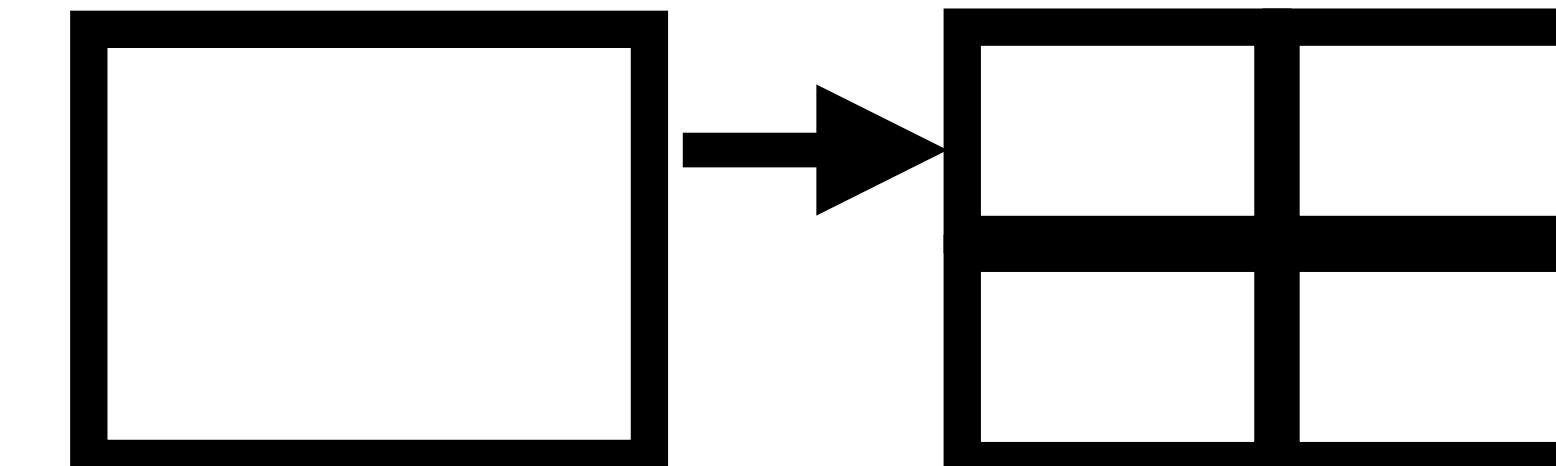
- Generate memory registration keys cryptographically
- Isolate on-board resources for different clients

Sequential to Random

1	2	3
4	5	6
7	8	9



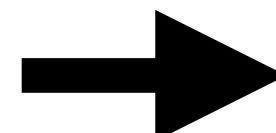
**On-board
Resource**



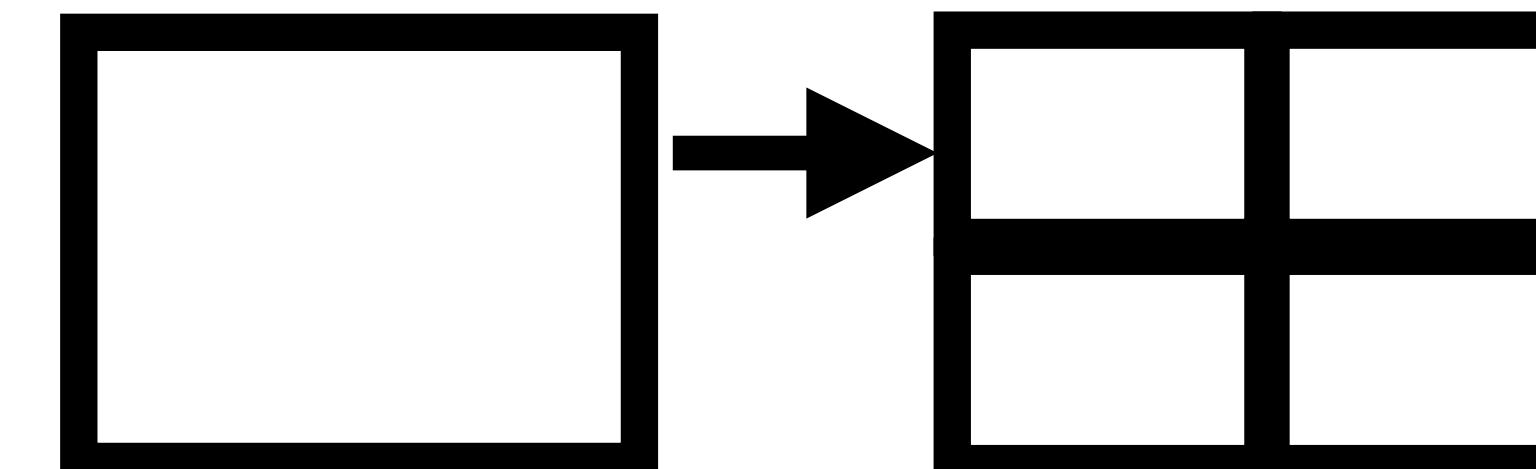
Discussion and Defense

- Generate memory registration keys cryptographically
- Isolate on-board resources for different clients
- Enhancing SmartNIC at the receiver side

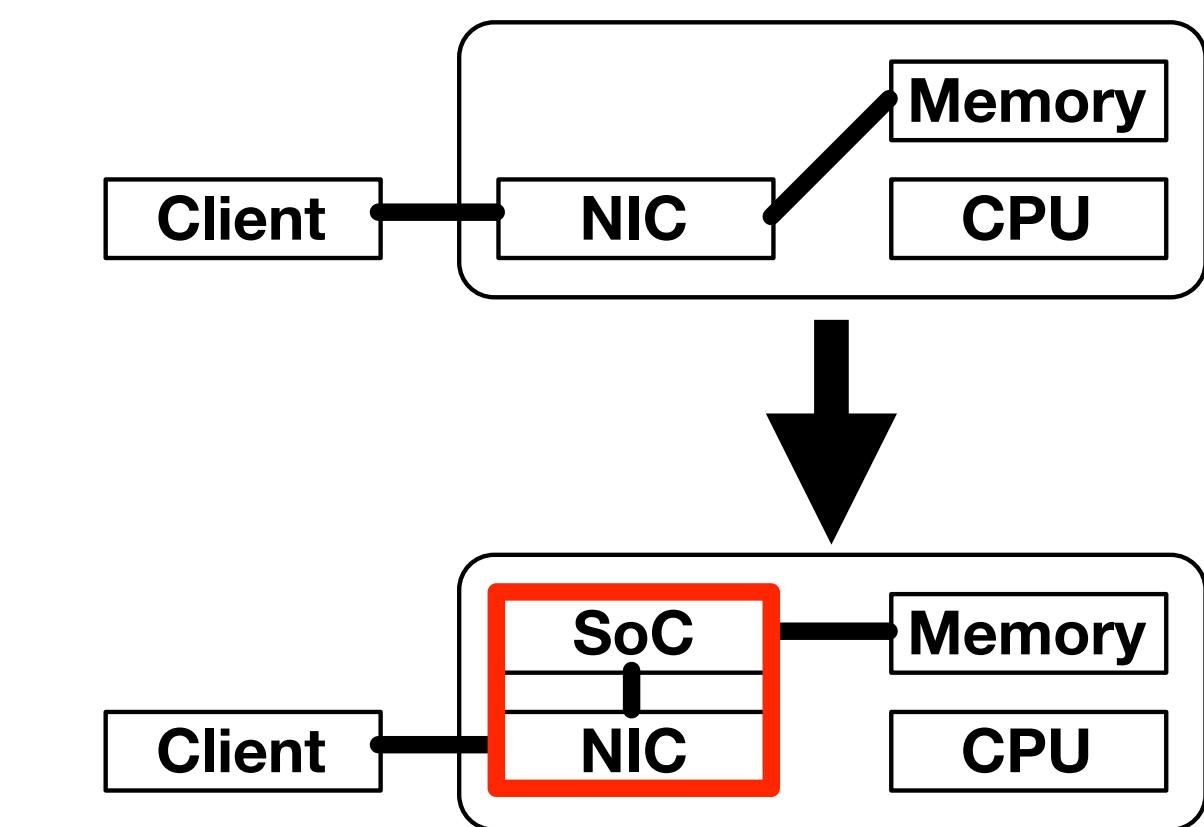
Sequential to Random



On-board Resource



SmartNIC

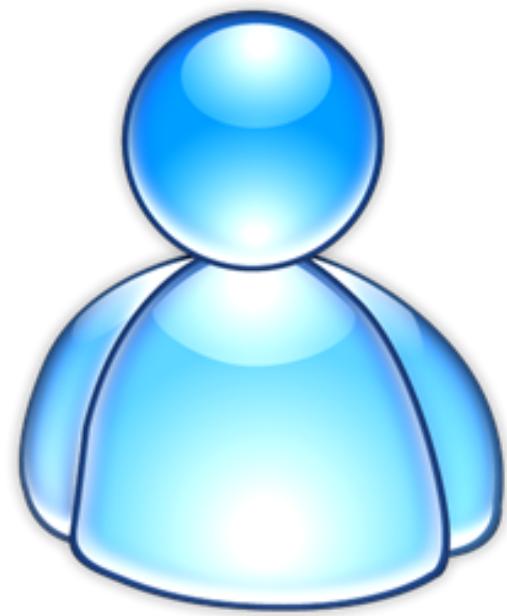


Outline

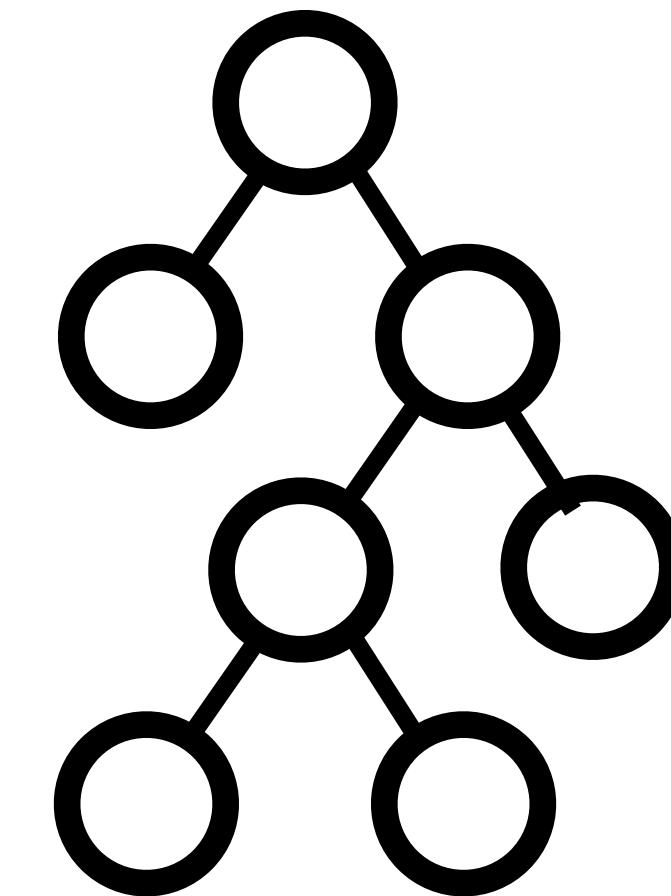
- Introduction and Background
- Vulnerabilities in One-Sided Communication
- Vulnerabilities in One-Sided Hardware
- Opportunities in One-Sided Communication
- Conclusion

Opportunity of One-sided Communication

ORAM Access

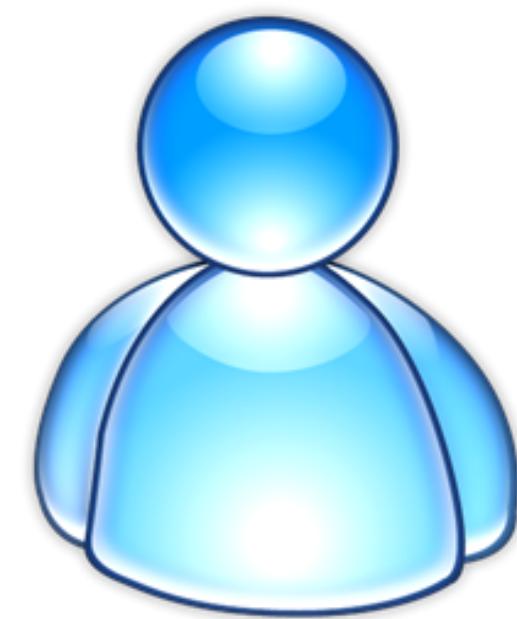


Server

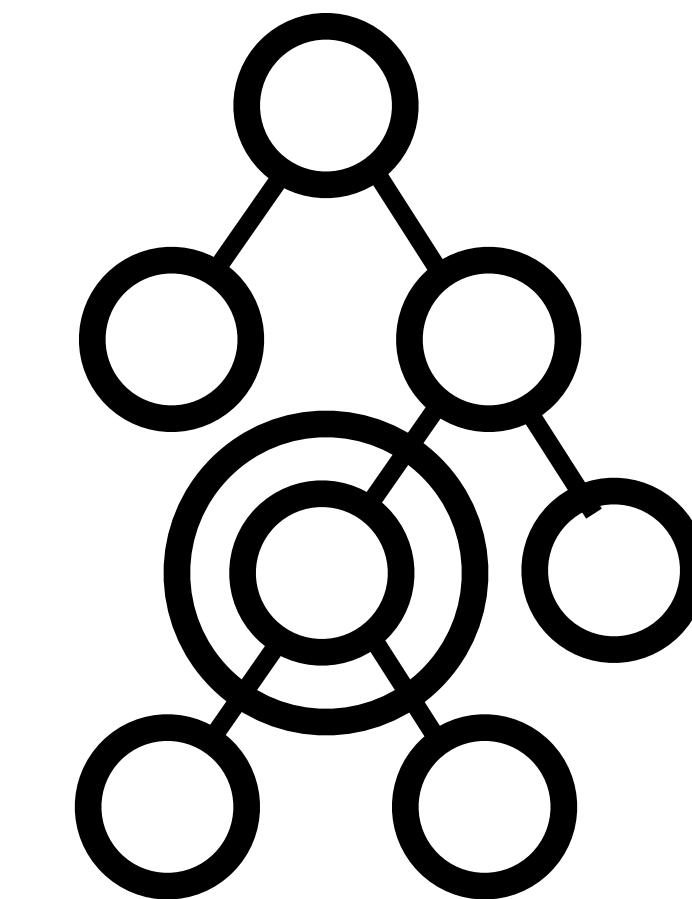


Opportunity of One-sided Communication

ORAM Access



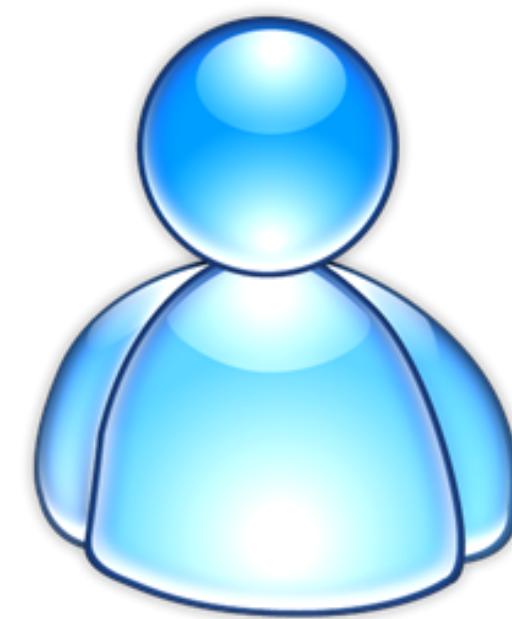
ORAM READ/WRITE



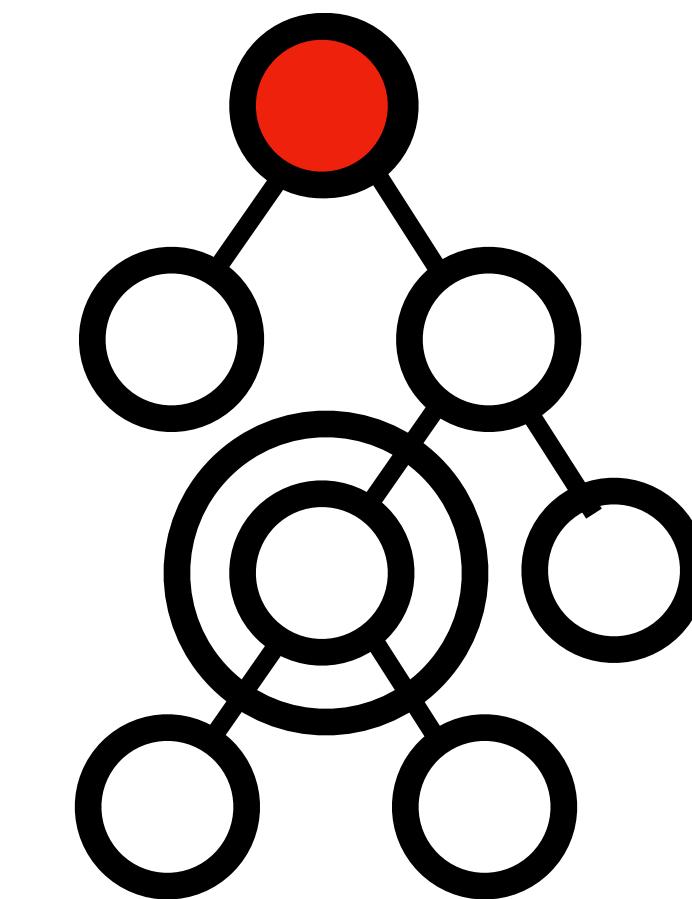
Server

Opportunity of One-sided Communication

ORAM Access



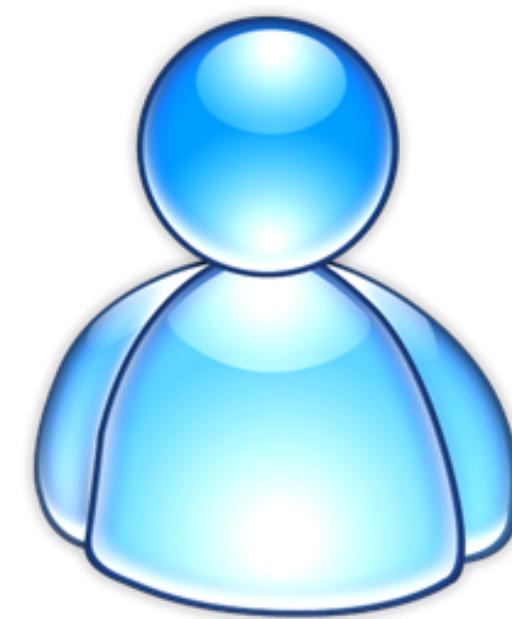
ORAM READ/WRITE



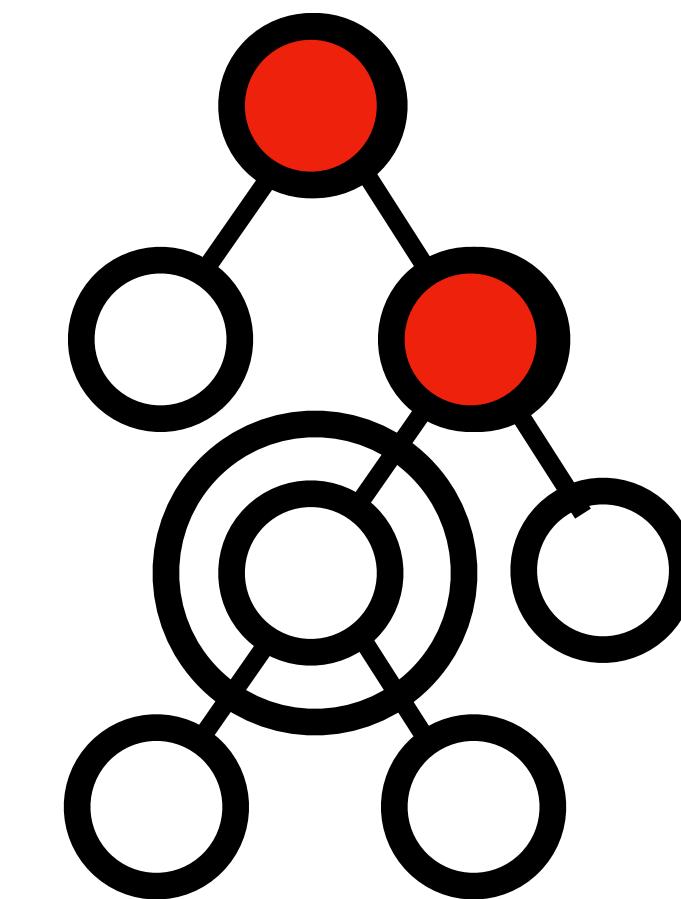
Server

Opportunity of One-sided Communication

ORAM Access



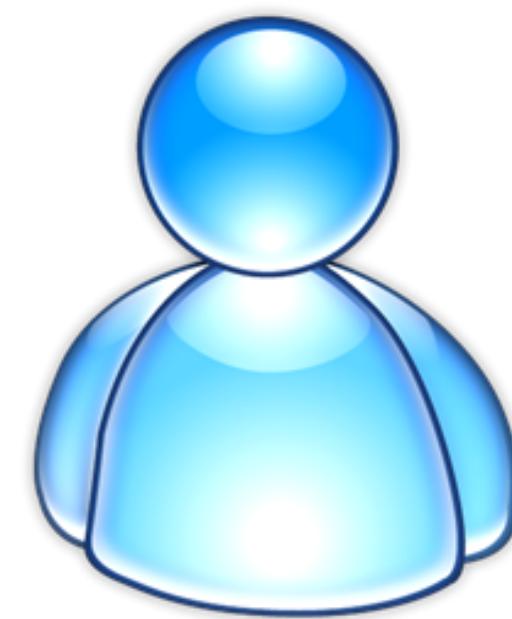
ORAM READ/WRITE



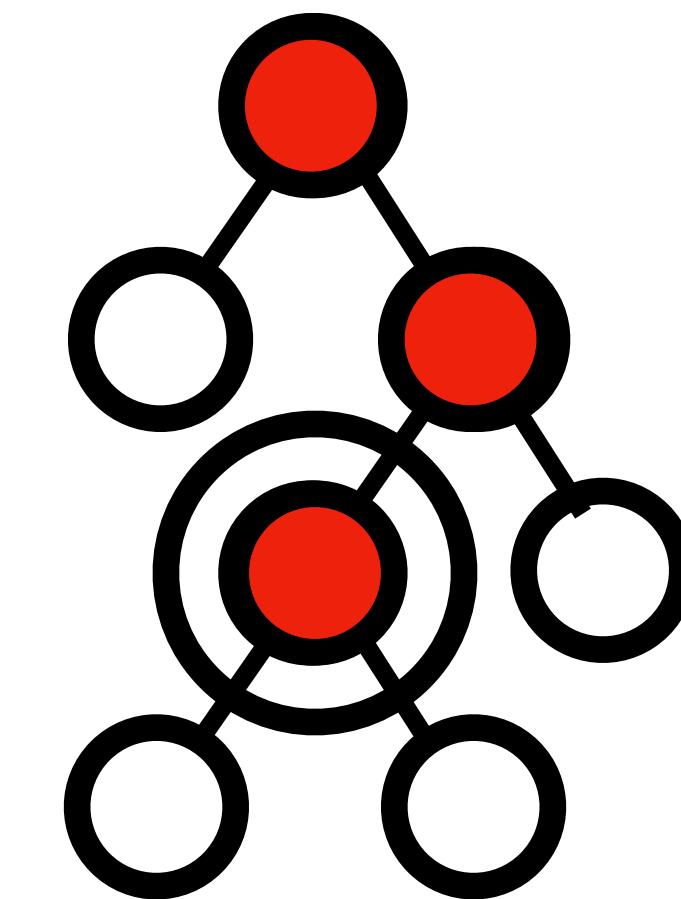
Server

Opportunity of One-sided Communication

ORAM Access



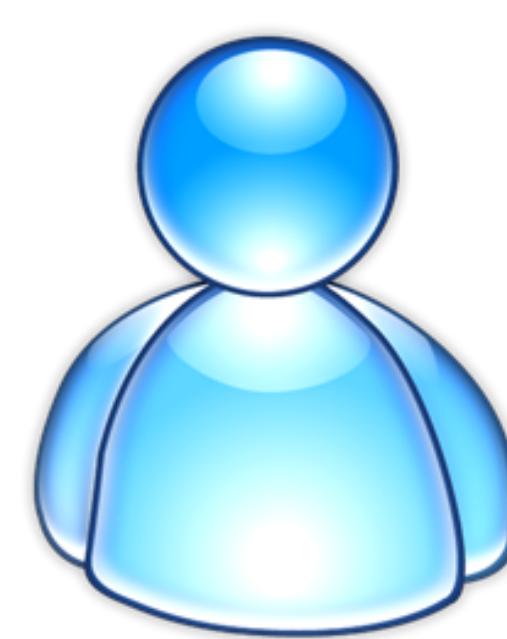
ORAM READ/WRITE



Server

Opportunity of One-sided Communication

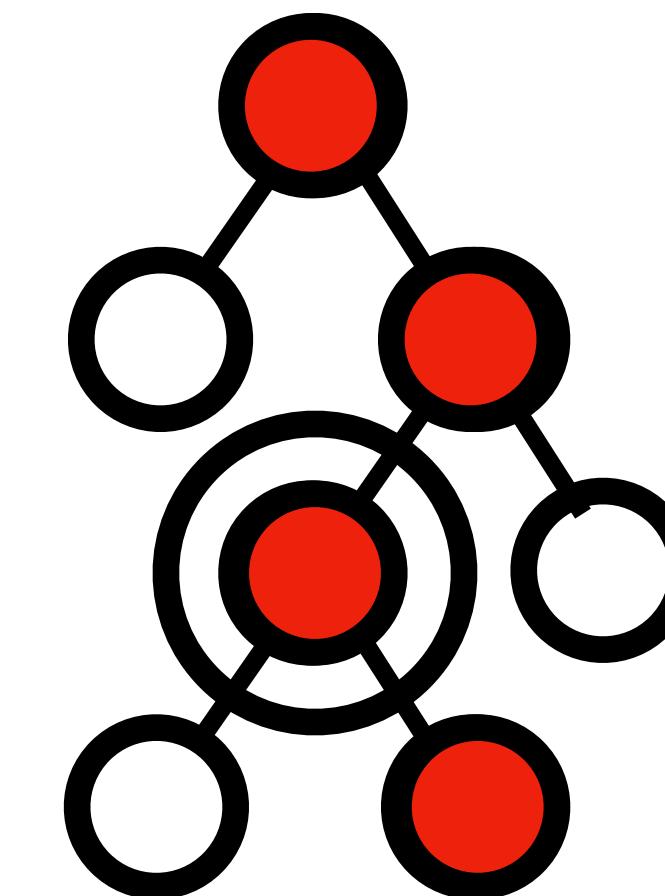
ORAM Access



ORAM READ/WRITE

The diagram illustrates the process of ORAM access. It features two main icons: a blue user icon on the left and a black server icon on the right. A horizontal red double-headed arrow connects them. Above the arrow, the text "ORAM READ/WRITE" is displayed in red capital letters. The server icon is accompanied by a small network graph consisting of several nodes connected by black lines, with some nodes highlighted in red.

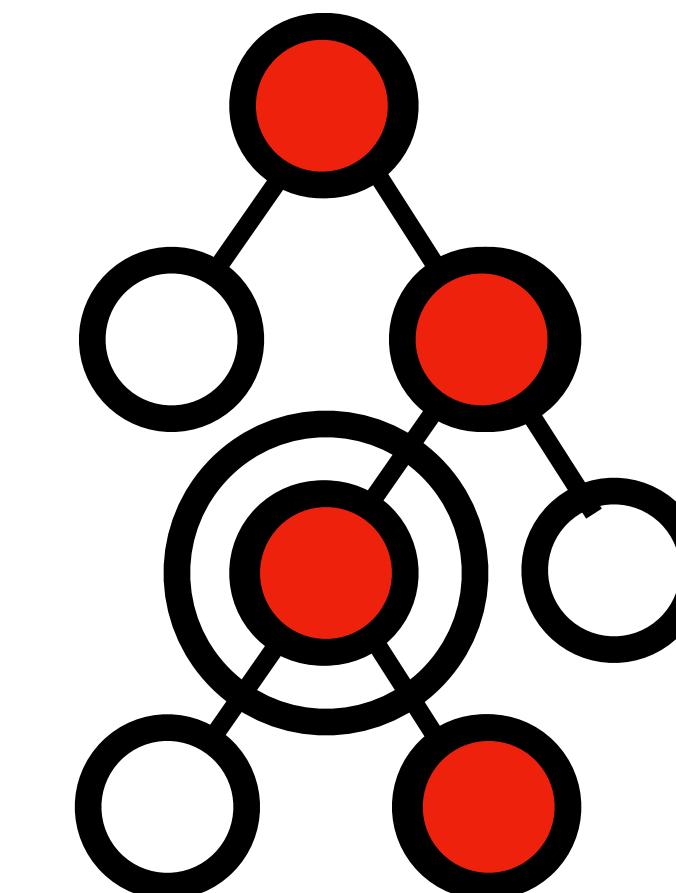
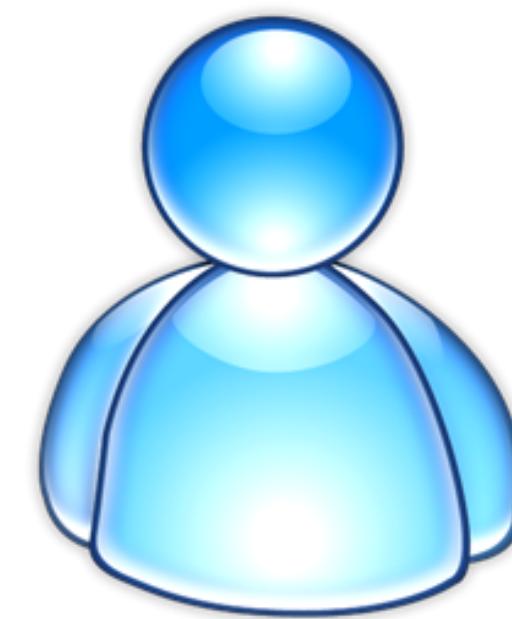
Server



Opportunity of One-sided Communication

ORAM Access

Server

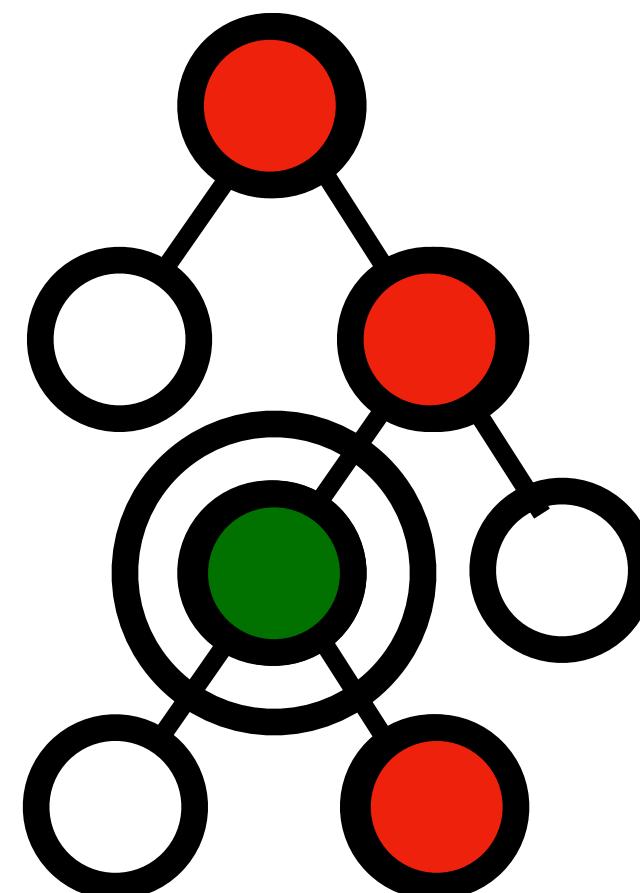
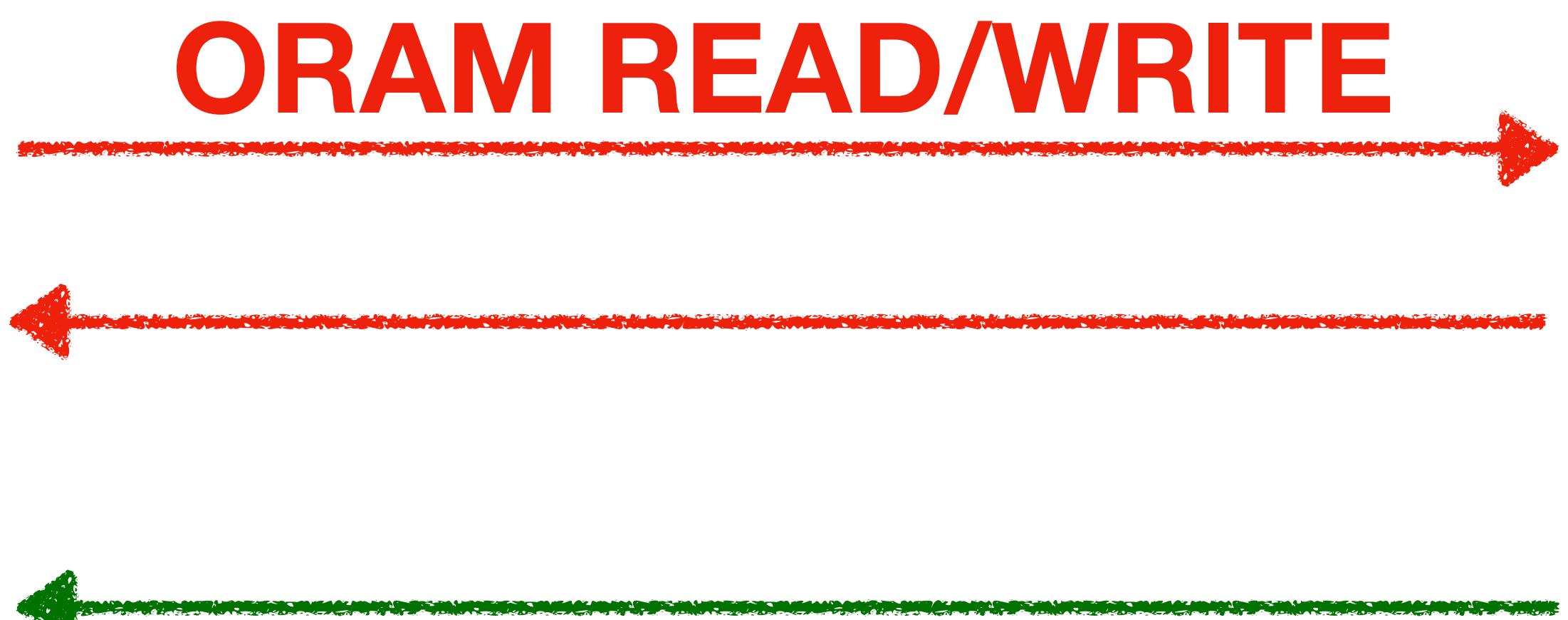
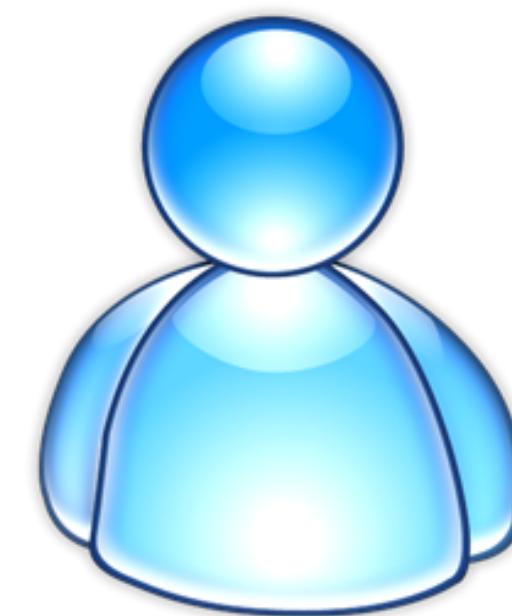


One-sided READ

Opportunity of One-sided Communication

ORAM Access

Server

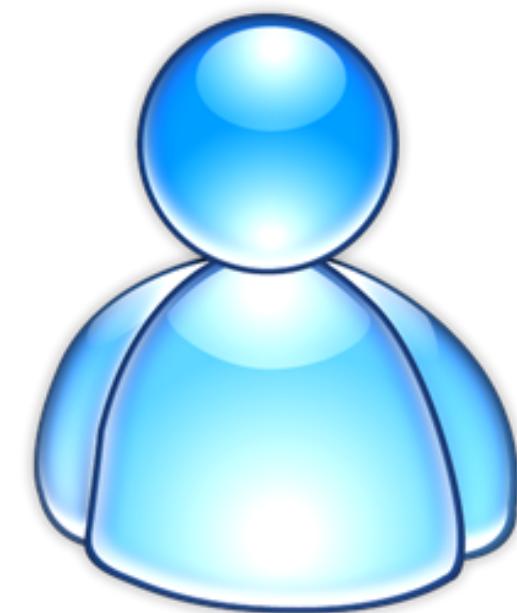


One-sided READ

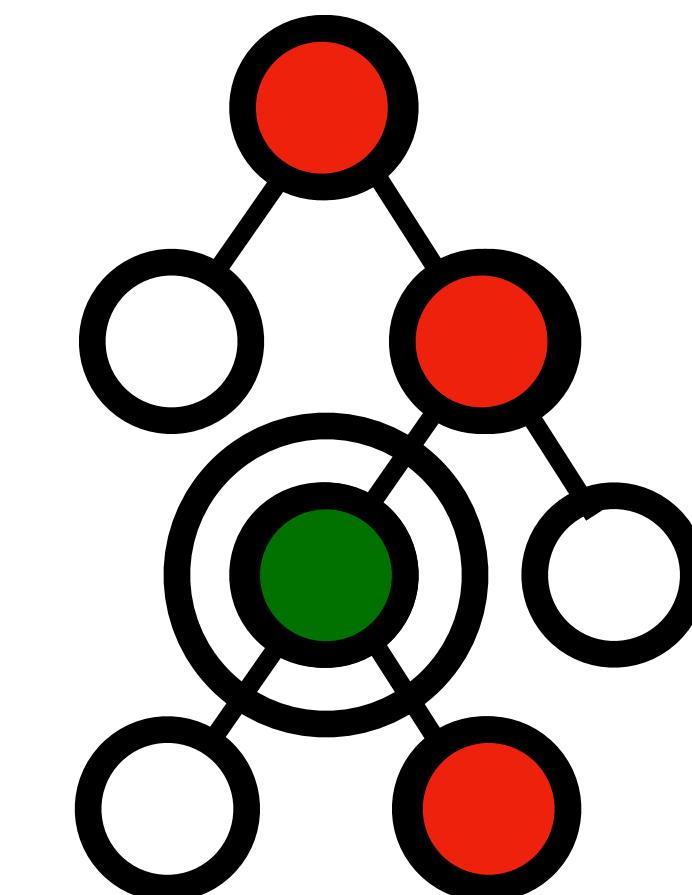
Opportunity of One-sided Communication

ORAM Access

**(1-K)% ORAM READ
100% ORAM WRITE**

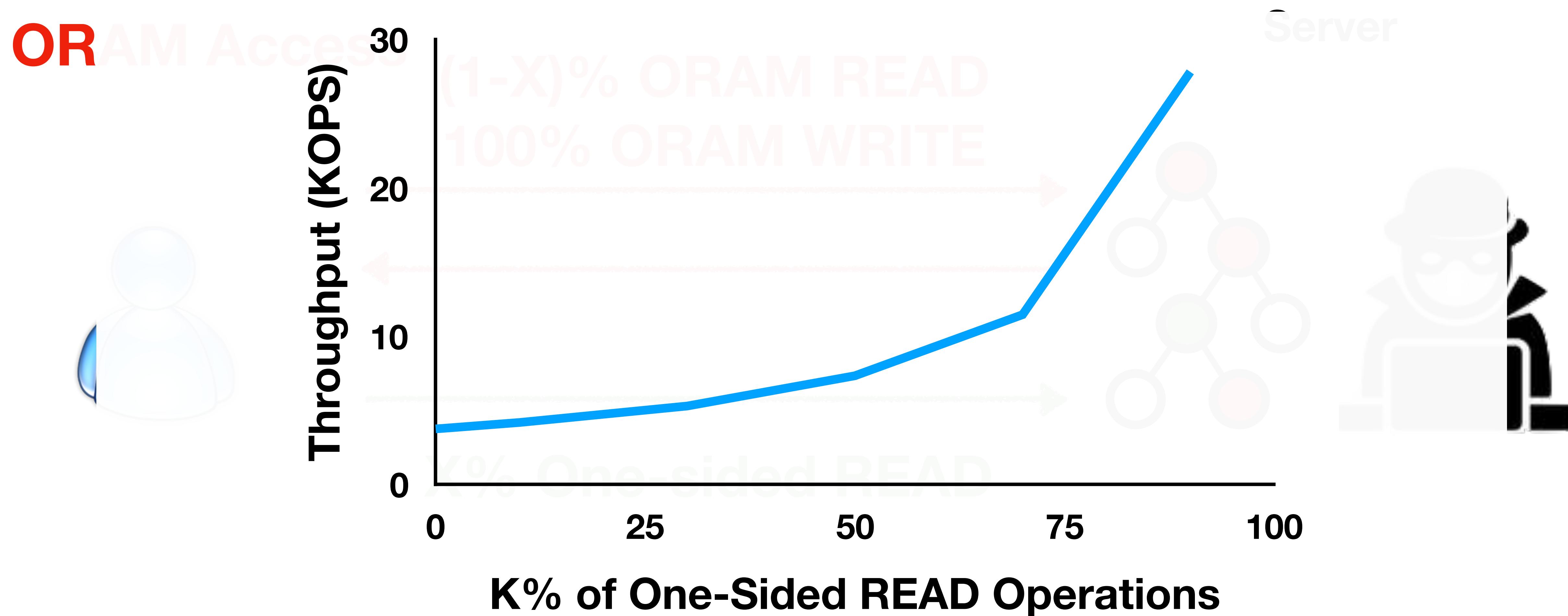


Server



K% One-sided READ

Opportunity of One-sided Communication



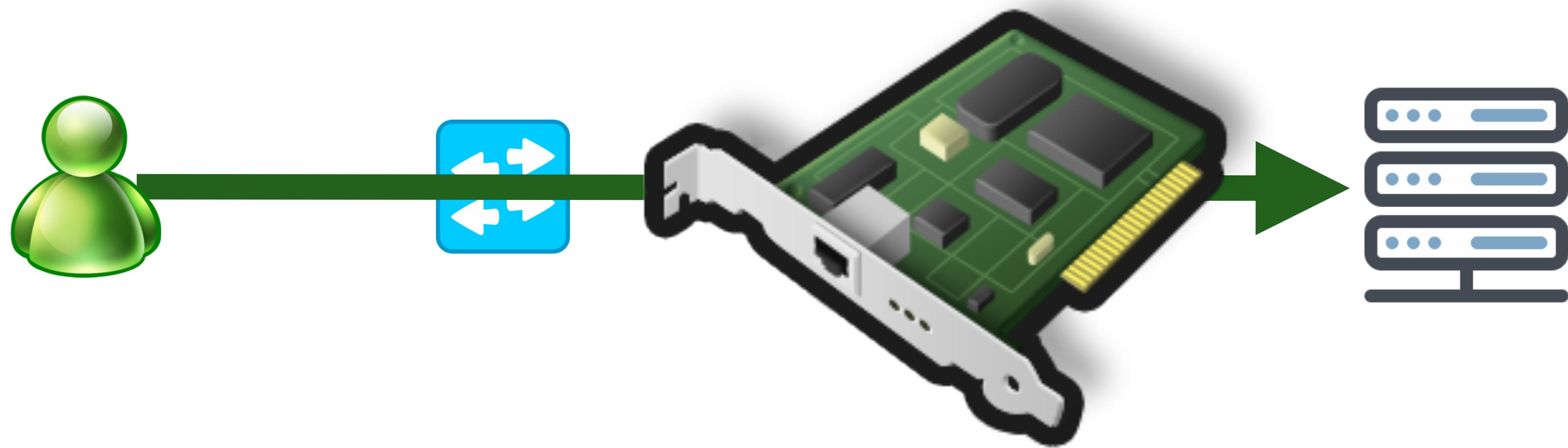
Conclusion

- **Security concerns** of one-sided communication
- Tradeoffs between **Performance** and **Security**
- **Hardware Vendor, Software Developers, and Datacenter**



Conclusion

- **Security concerns** of one-sided communication
- Tradeoffs between **Performance** and **Security**
- **Hardware Vendor, Software Developers, and Datacenter**



Thank you Questions?

