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

Shin-Yeh Tsai
Yiying Zhang
Traditional (Two-sided communication)

User A

CPU

Memory

Server
Traditional (Two-sided communication)

User A

GET Key-50

Send

CPU

Memory

Server
Traditional (Two-sided communication)

User A

GET Key-50

Send

CPU

Key-50

Memory

Server
Traditional (Two-sided communication)

User A

GET Key-50

Server

CPU

← Reply

Memory

Key-50

GET Key-50
Traditional (Two-sided communication)

User A
GET Key-50
Set Key-100

User B
Send →

Server
CPU
Memory

Key-50
Traditional (Two-sided communication)

User A
GET Key-50

User B
SET Key-100

Send →

CPU

Memory

Server

GET Key-50

SET Key-100

Key-50

Key-100
Traditional (Two-sided communication)

User A
GET Key-50
SET Key-100

User B

← Reply

Server

CPU

Memory

Key-50
Key-100
Traditional (Two-sided communication)

User A
GET Key-50
SET Key-100

User B

CPU
Memory

Server

One-sided communication
Traditional (Two-sided communication)

User A
GET Key-50
SET Key-100

User B

GET Key-50
SET Key-100

CPU
Memory

Server

One-sided communication
Traditional (Two-sided communication)

User A
GET Key-50
SET Key-100

User A

CPU

Memory

Server

Key-50
Key-100

One-sided communication
Traditional (Two-sided communication)

GET Key-50
SET Key-100

One-sided communication

GET Key-50
Traditional (Two-sided communication)

GET Key-50

SET Key-100

One-sided communication
Traditional (Two-sided communication)

User A
GET Key-50
SET Key-100

User B
GET Key-50
SET Key-100

One-sided communication

User A
GET Key-50

User B
GET Key-50

Server
GET Key-50
SET Key-100

CPU
Memory
CPU
Memory
RDMA
Omni-Path
Gen-Z
NVMeOF
GPUDirect
Performance

RDMA
Omni-Path
Gen-Z
NVMeOF
GPUDirect

Scalability

Hotpot [SoCC '17]
Wukong [OSDI '16]
DrTM+R [SOSP '15]
RSI [VLDB '16]
NAM-DB [OSDI '16]
DRTM+H [SOSP '17]

Usability

FaRM [NSDI '14]
FaRM + Xact [SOSP '15]
Mojim [ATC '14]
HERD [SIGCOMM '14]
NAM-DB [VLDB '17]

What about Security?

Omni-Path [NSDI '14]
Octopus [ATC '17]
APUS [SOSP '15]
DrTM [VLDB '17]

Orion [FAST '19]
KV-Direct [SOSP '17]
RSI [VLDB '16]
FaSST [OSDI '16]
LITE [SOSP '17]

RDMA
Omni-Path
Gen-Z
NVMeOF
GPUDirect

GPUDirect
Gen-Z
NVMeOF
Omni-Path
RDMA

Performance

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
Vulnerability 1: Lack of Accountability

- WRITE accountability
Vulnerability 1: Lack of Accountability

- WRITE accountability

Server: Who SET the (corrupted) record?
Vulnerability 1: Lack of Accountability

- WRITE accountability
- READ accountability

Server: Who SET the (corrupted) record?
Vulnerability 1: Lack of Accountability

- WRITE accountability
- READ accountability

User A
- SET Key-50

User B
- GET Key-100

CPU

Memory

Server: Who SET the (corrupted) record?
Vulnerability 1: Lack of Accountability

- WRITE accountability
- READ accountability

Server: Who SET the (corrupted) record?

Server: Who GET the (corrupted) record?
Vulnerability 2: Denial of Service

- Hard to trace attackers
- Can overload NICs easily
Vulnerability 2: Denial of Service

- Hard to trace attackers
- Can overload NICs easily
Vulnerability 2: Denial of Service

- Hard to trace attackers
- Can overload NICs easily
Vulnerability 2: Denial of Service

- Hard to trace attackers
- Can overload NICs easily
Discussion and Defense

- Adding intermediate layer at the sender side
Discussion and Defense

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

CPU
- User
- Kernel
- Memory

Two-Sided
One- and Two-Sided Hardware
One- and Two-Sided Hardware

1. Address mapping
2. Permission checking
3. Resource isolation
One- and Two-Sided Hardware

1. Address mapping
2. Permission checking
3. Resource isolation
One- and Two-Sided Hardware

1. Address mapping
2. Permission checking
3. Resource isolation
One- and Two-Sided Hardware

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

Memory Region
1. rkey/lkey
2. Address
Vulnerability 3 - Predictable Hardware Managed Keys

Virtual addr + rkey

PTE Translation

Physical addr

rkey/lkey Value

ConnectX-3
ConnectX-4
ConnectX-5
Vulnerability 3 - Predictable Hardware Managed Keys

Virtual addr + rkey

PTE Translation

Physical addr

ConnectX-3
ConnectX-4
ConnectX-5
Vulnerability 3 - Predictable Hardware Managed Keys

Virtual addr + rkey

PTE Translation

Physical addr

ConnectX-3
ConnectX-4
ConnectX-5

nth-MemoryRegion Registered

rkey/lkey Value

0
1M
2M
3M
Vulnerability 3 - Predictable Hardware Managed Keys

Virtual addr + rkey

PTE Translation

Physical addr

rkey/lkey Value

ConnectX-3
ConnectX-4
ConnectX-5

nth-MemoryRegion Registered
Vulnerability 4 - Side Channel in NICs

ConnectX-5, 1KB READ request latency

Virtual addr + rkey

PTE Translation

Physical addr
Vulnerability 4 - Side Channel in NICs

ConnectX-5, 1KB READ request latency

Virtual addr + rkey

PTE Translation

Physical addr

Latency (us)

Percentile

Hit
Miss-PageTableEntries
Miss-MemoryRegionInfo
Vulnerability 4 - Side Channel in NICs

ConnectX-5, 1KB READ request latency

Virtual addr + rkey

PTE Translation

Physical addr

Latency (us)

Percentile

Hit

Miss-PageTableEntries

Miss-MemoryRegionInfo
Side-Channel Attacks in RDMA (Pythia, USENIX Sec ‘19)

Timeline (ms)

Access Probability (%)
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
Discussion and Defense

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

Server
Opportunity of One-sided Communication

ORAM Access

ORAM READ/WRITE

One-sided READ

Server
Opportunity of One-sided Communication

ORAM Access

ORAM READ/WRITE

One-sided READ

Server
Opportunity of One-sided Communication

ORAM Access

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

K% One-sided READ
Opportunity of One-sided Communication

Throughput (KOPS)

K% of One-Sided READ Operations
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?

WukLab
wuklab.io

Purdue University