



SNIA[®] STORAGE
SECURITY SUMMIT
Wednesday, May 11, 2022 • Virtual

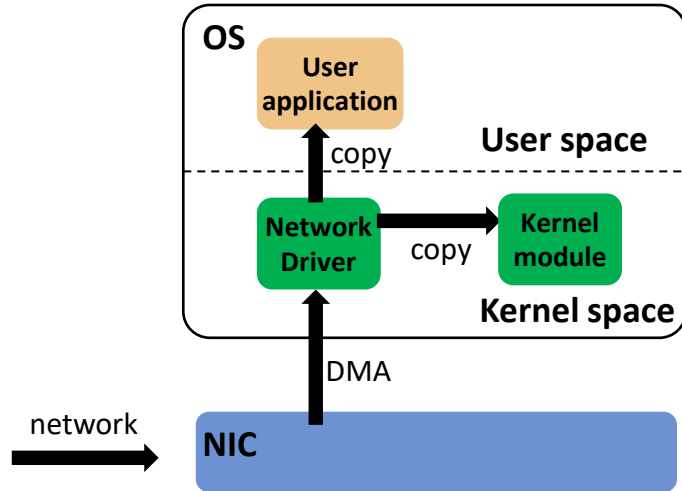
NeVerMore: Exploiting RDMA Mistakes in NVMe-oF Storage Applications

Presented by Konstantin Taranov (ETH Zurich)

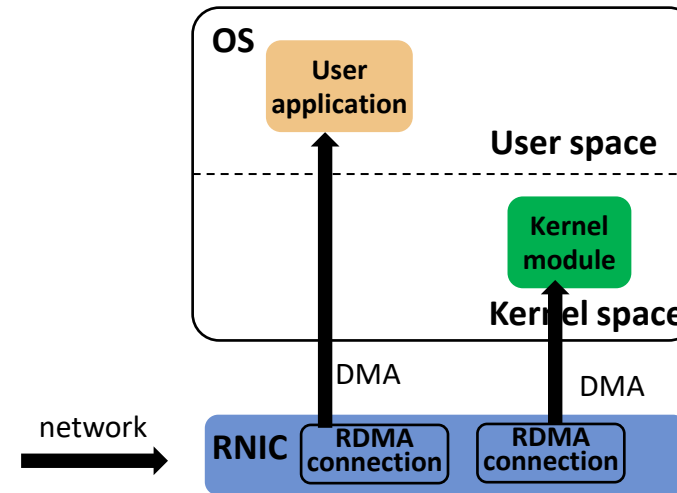


What is RDMA networking?

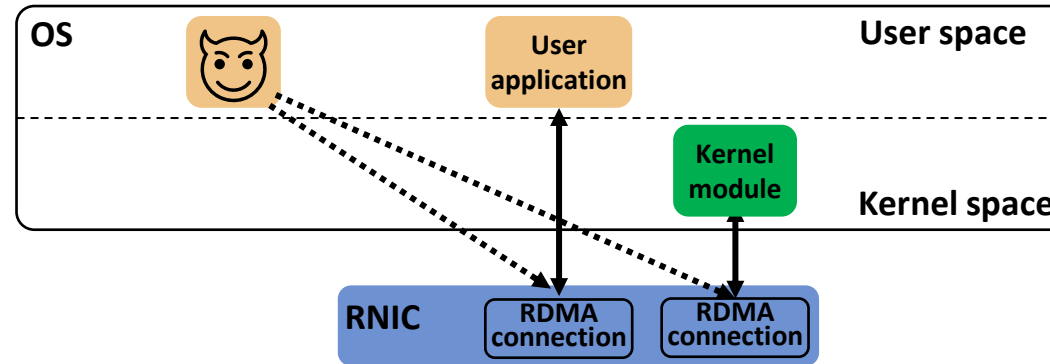
Socket-based networking



RDMA networking



Agenda



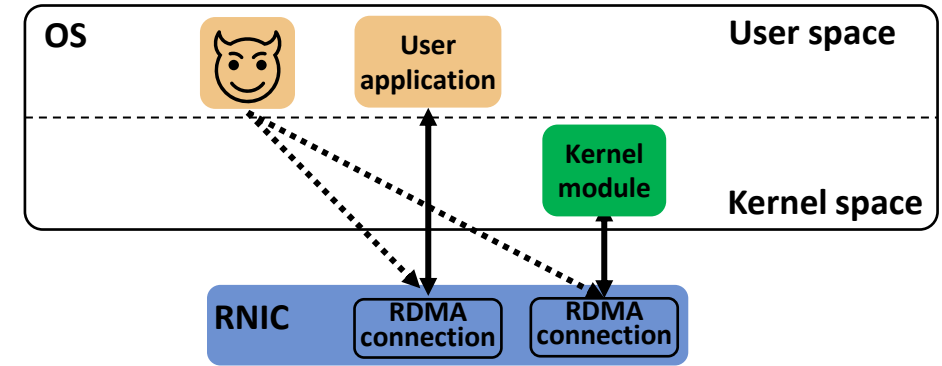
Injection without administrative privileges

Injection into any local RDMA connection

Injection into all IB-based protocols (including RoCE)

Implications of the attack

- A local user can manipulate any local RDMA connection
- A local user can manipulate RDMA-enabled kernel modules
- A local user can bypass security mechanisms of the OS and directly access the affected kernel module
- It is especially dangerous for the NVMe-oF protocol, relying on RDMA to access remote NVMe SSD

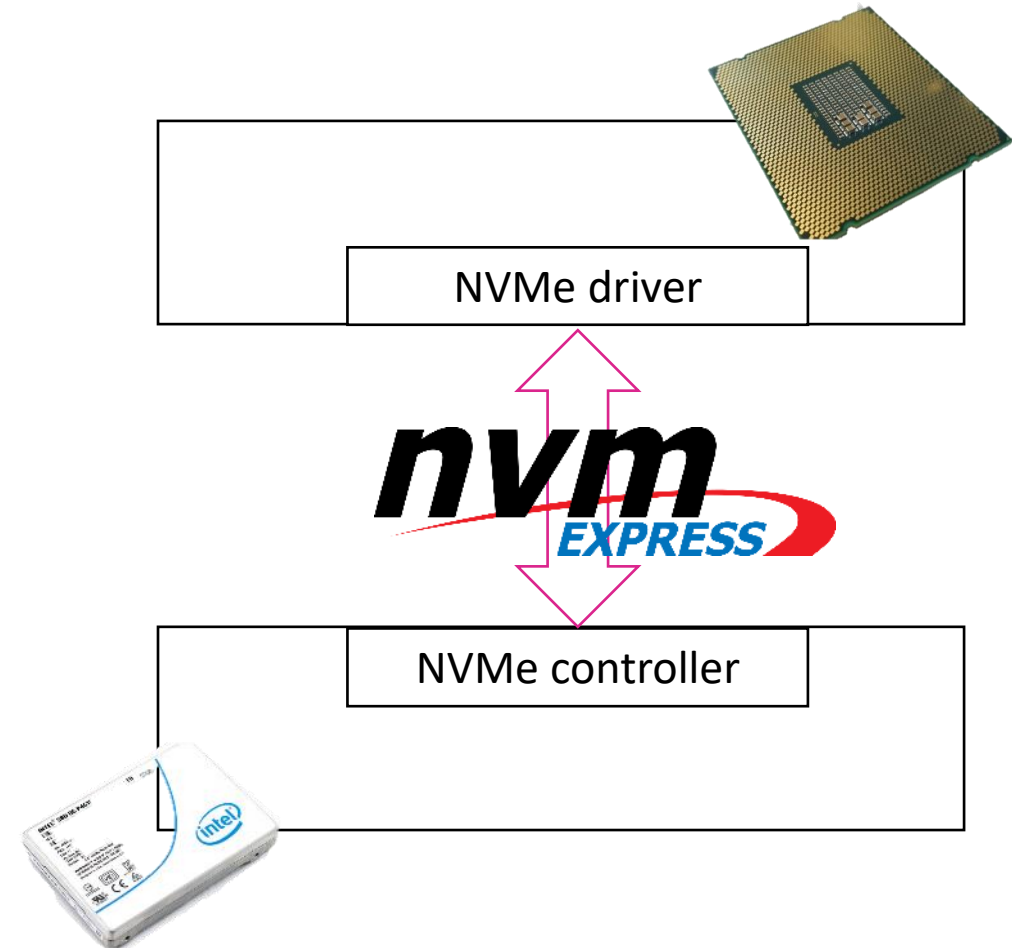
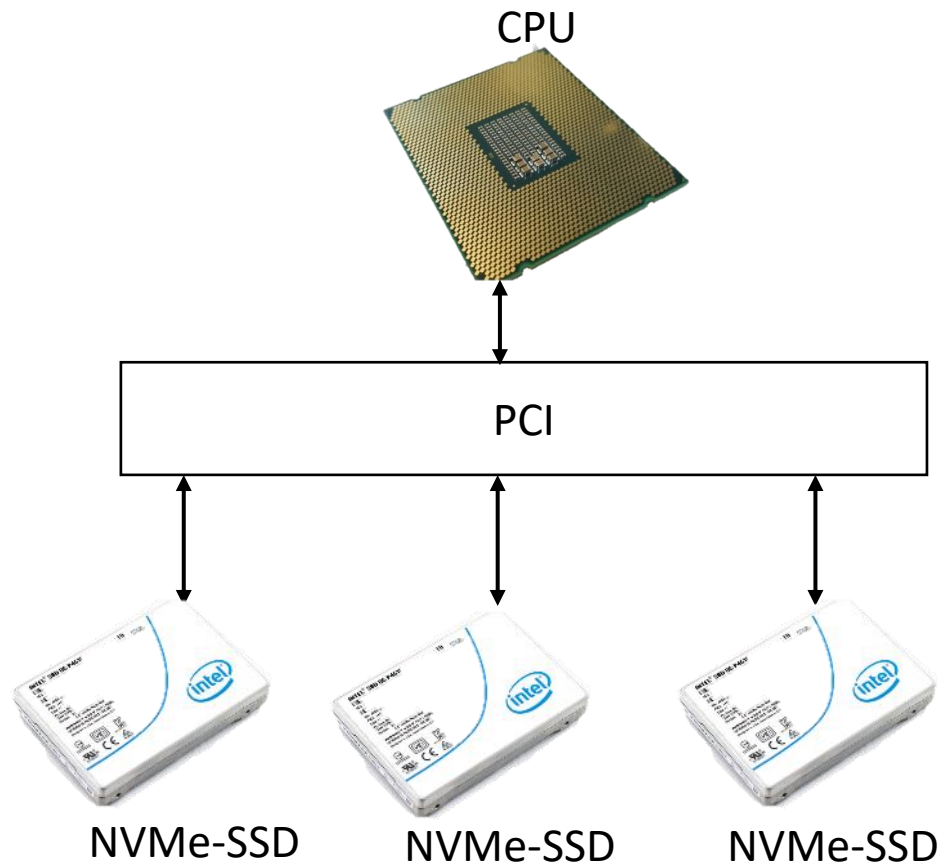




Injection into NVMe-oF

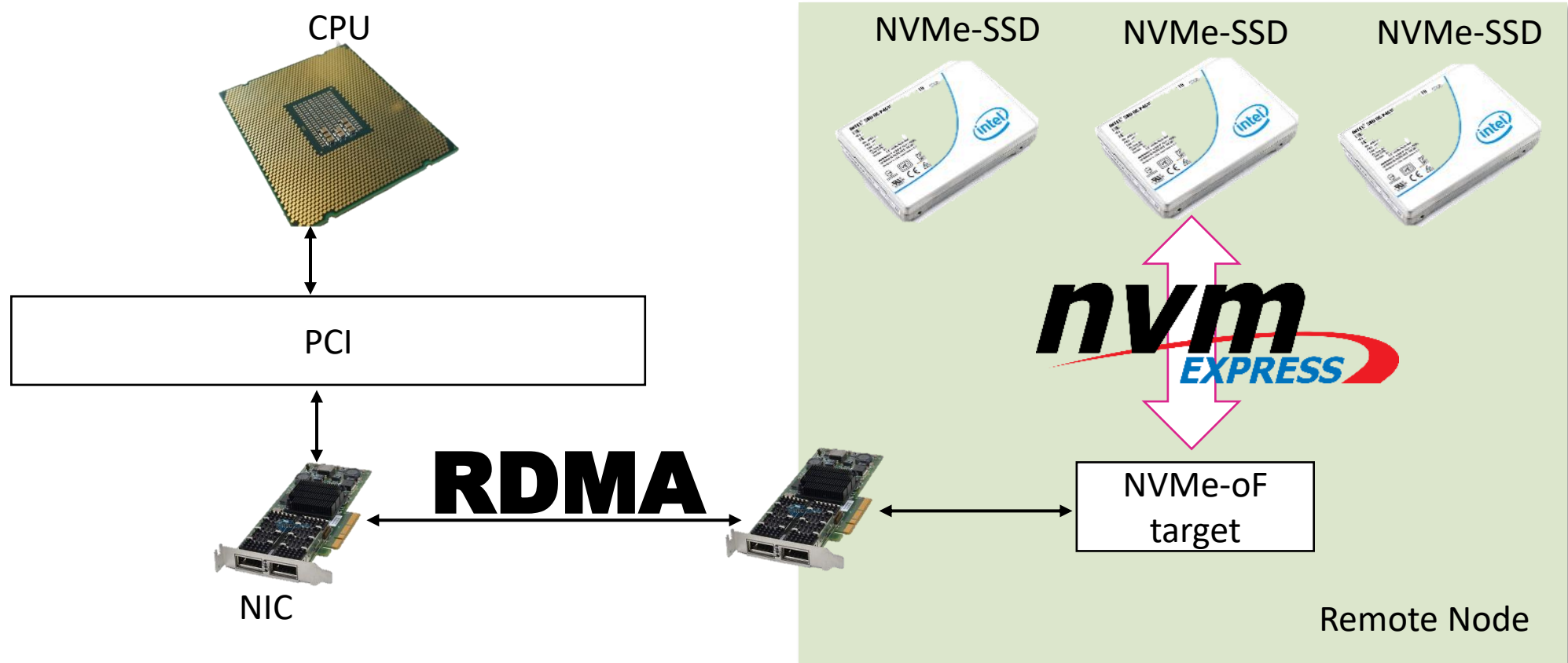
Acquiring block access

Non-Volatile Memory Express (NVMe)



designed for performance – lower latency, higher bandwidth, lower CPU utilization etc.

NVMe over Fabrics (NVMe-oF)

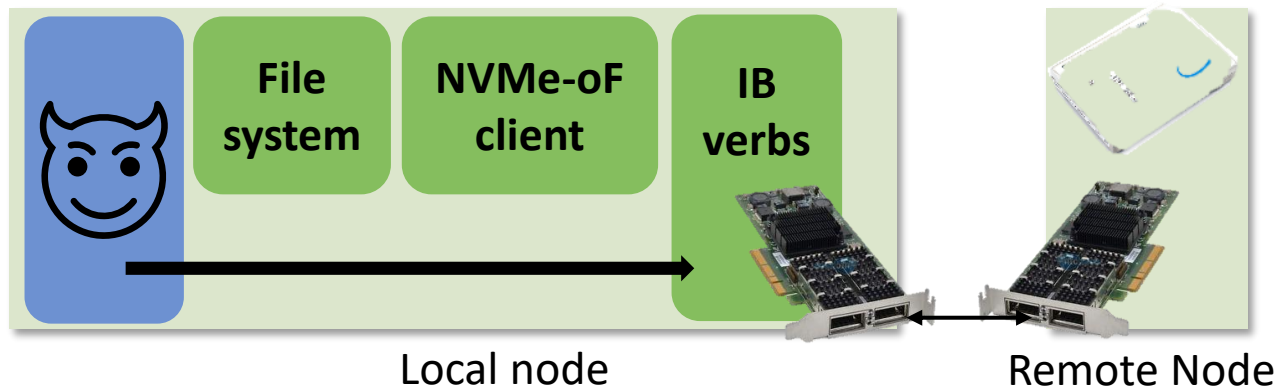


Threat model

- Model TLU – The attacker is at a local node. It does not have root privileges.

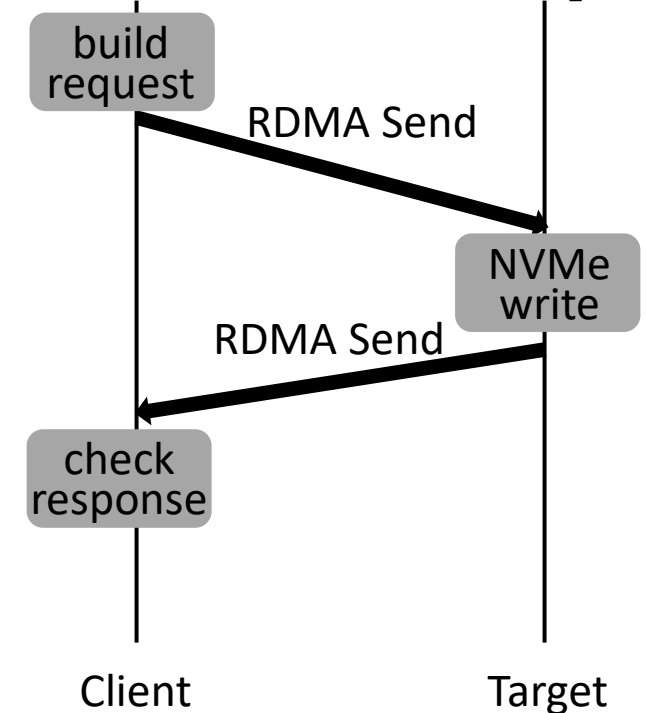


Towards injection of NVMe-oF write

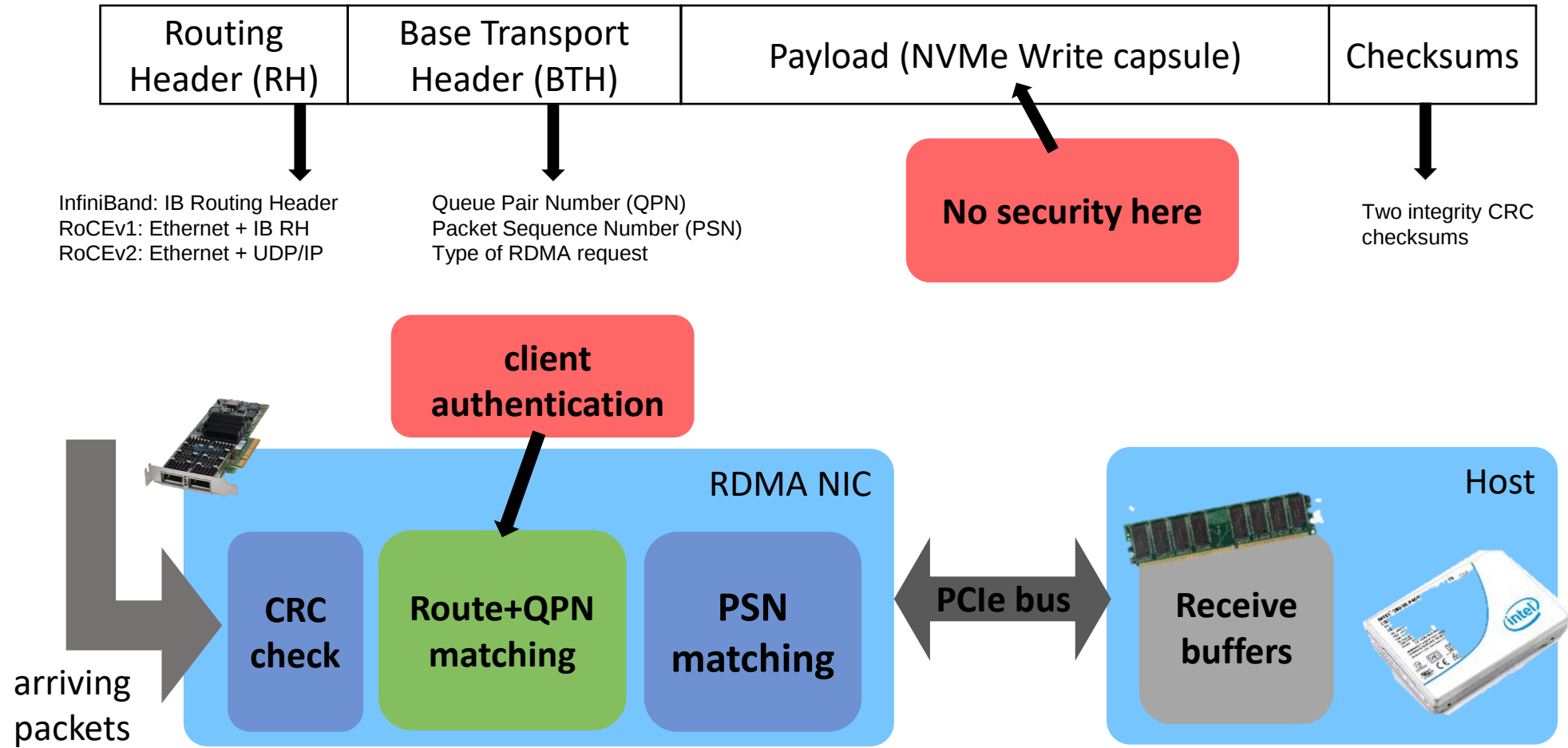


- Setting TLU:
 - The kernel mounts a remote NVMe SSD and installs a file system on it
 - The attacker is a user of the machine which uses the NVMe-oF client

NVMe-oF write in-capsule



RDMA packet format and packet processing

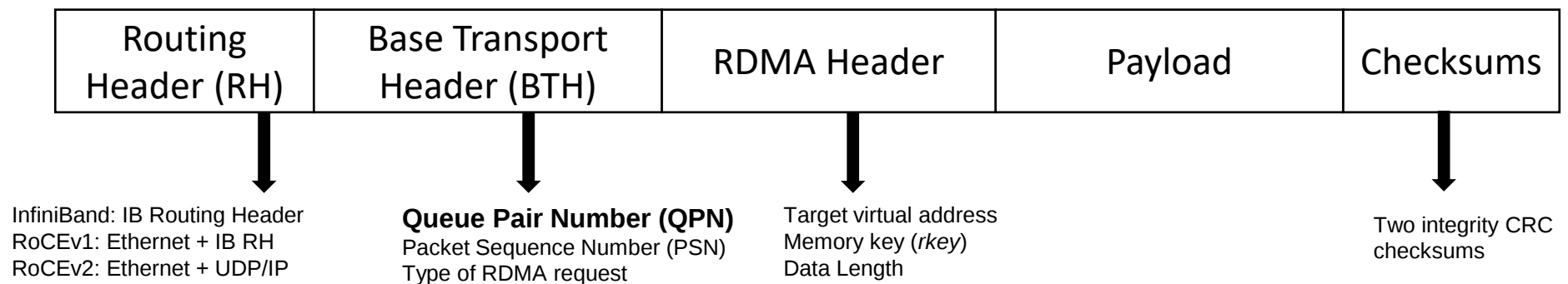


Vulnerabilities in InfiniBand-based protocols

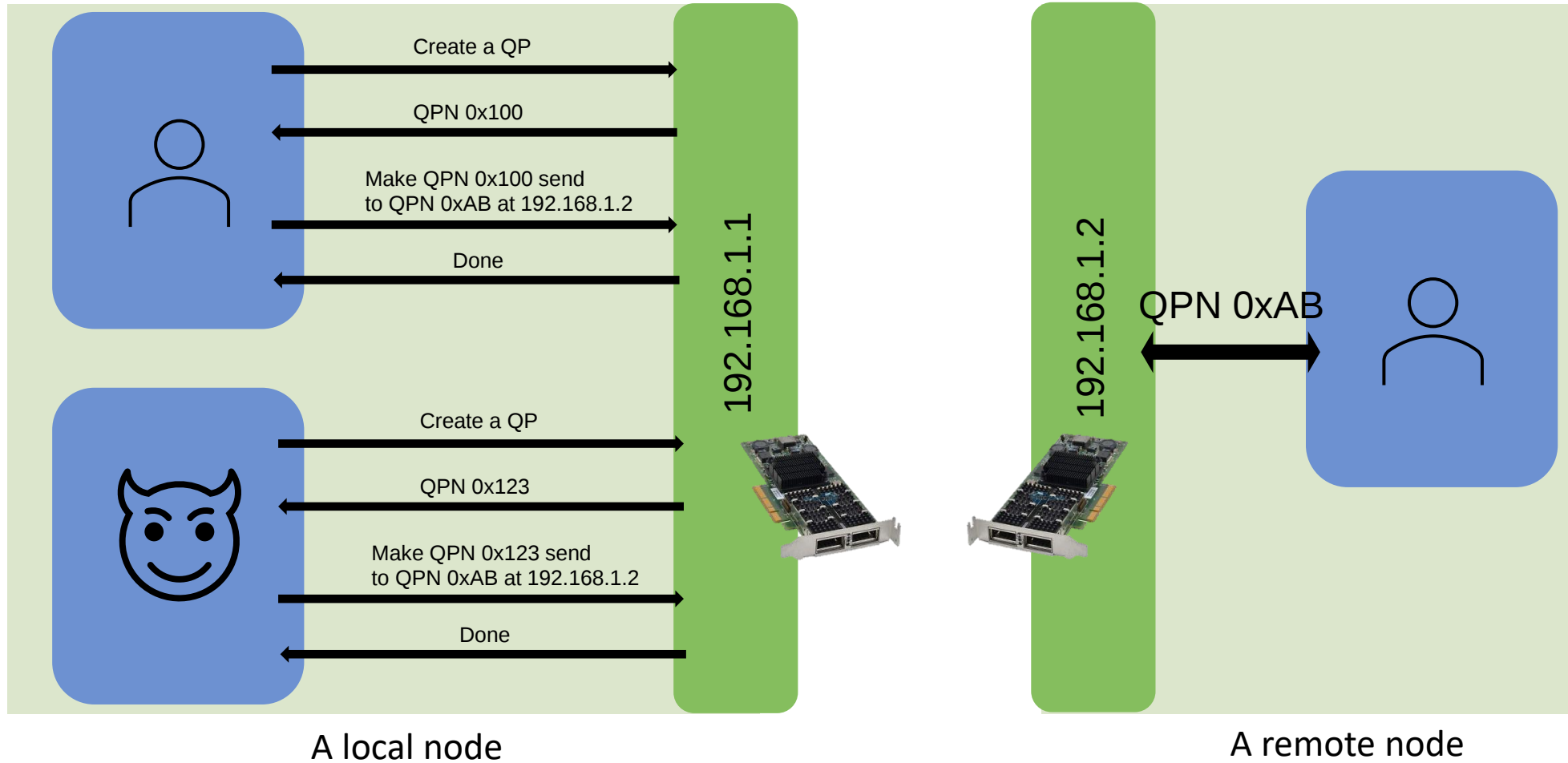
- 1) The IBV user space library allows to create any RDMA connection with no sudo:
 - A user can manually create a QP and add to it routing, PSNs, destination QPN



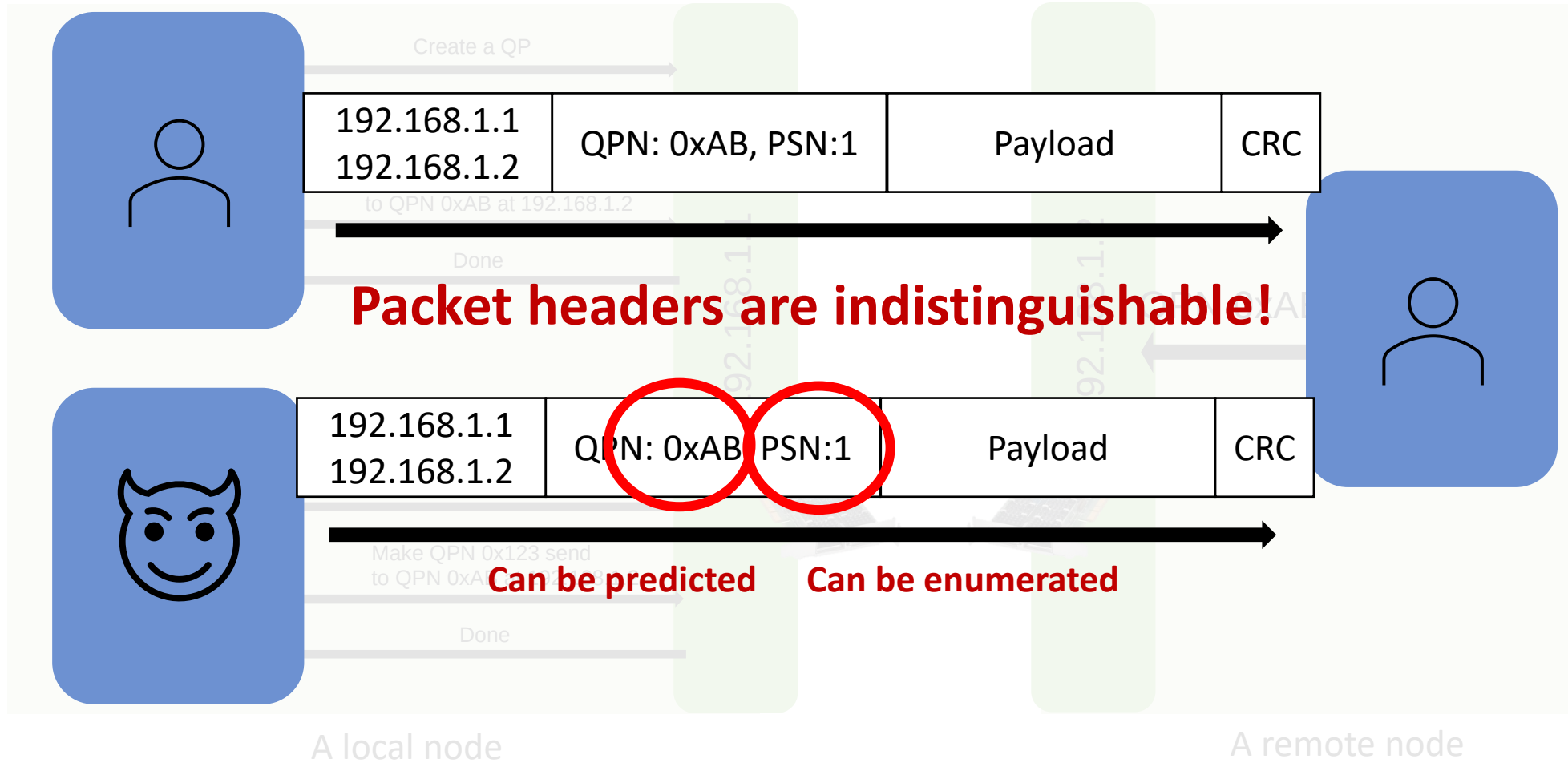
- 2) The Base Transport Header does not include source QPN



Packet forging with no root

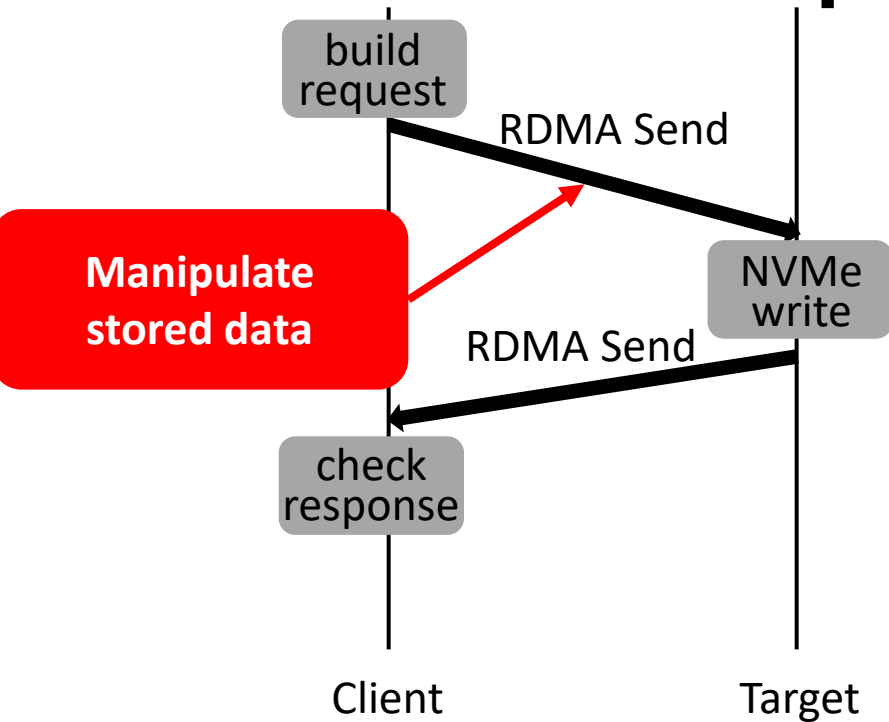


Packet forging with no root

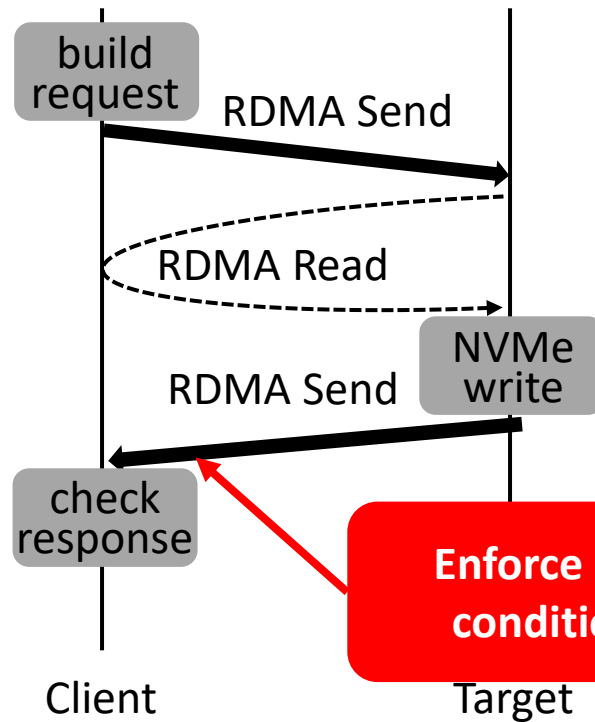


NVMe-oF data requests

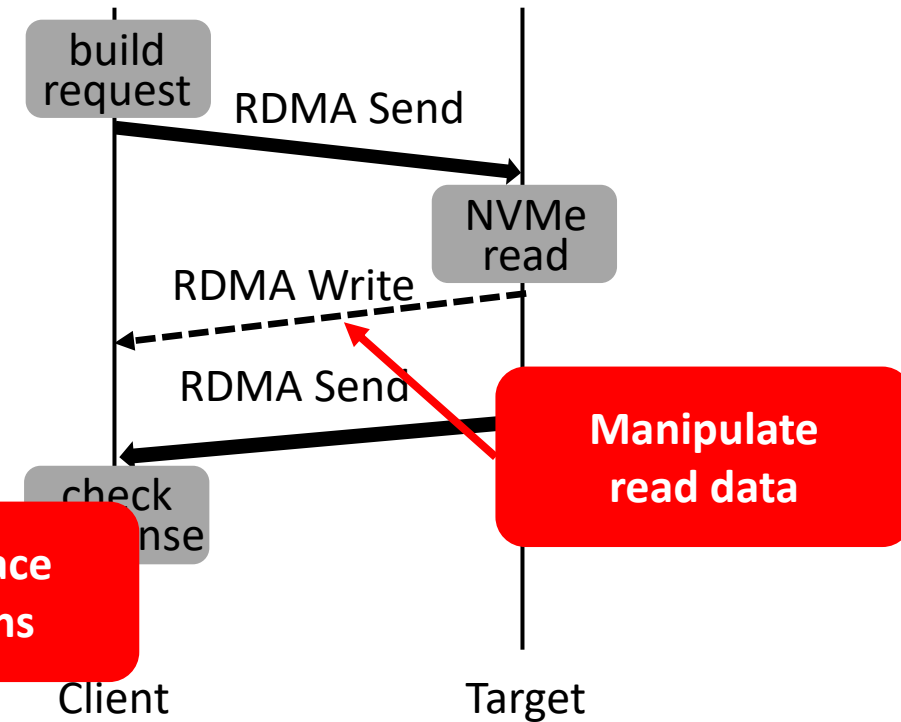
NVMe-oF write in-capsule



NVMe-oF write



NVMe-oF read



Security mechanisms in NVMe-oF

- Attacks tested for
 - *Storage Performance Development Kit (SPDK)*
 - Linux Kernel modules (nvme-rdma and nvmet-rdma)
- Existing security mechanisms in the NVMe-oF protocol:
 - In-band security – For client/target authentication at connection establishment
 - IPsec – To prevent injection into the secure link

Attack	Threat Model TLU			Threat Model TRA			Effect
	None	In-band	IPsec	None	In-band	IPsec	
Spoof NVMe-oF request	Yes	Yes	Yes	Yes	Yes	No	Execution of falsified request
Spoof NVMe-oF response	Yes	Yes	Yes	Yes	Yes	No	Early termination
Corrupt memory	Yes ¹	Yes ¹	Yes ¹	Yes ¹	Yes ¹	No	Use of falsified data

Mitigation for NVMe-oF - Message Authentication

- Challenge:

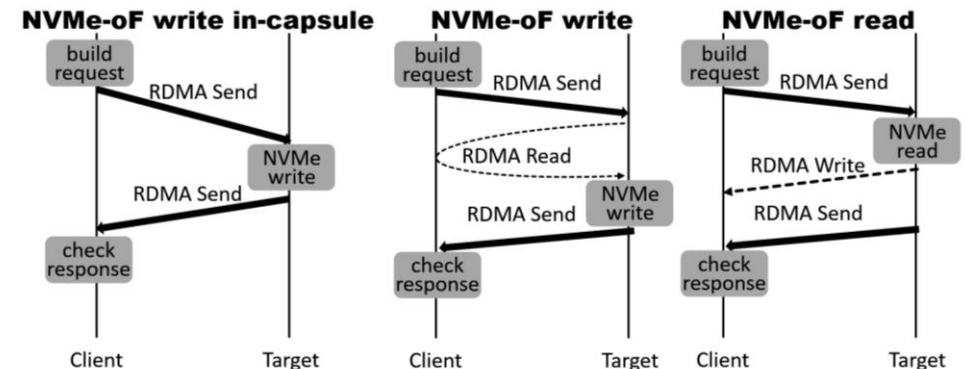
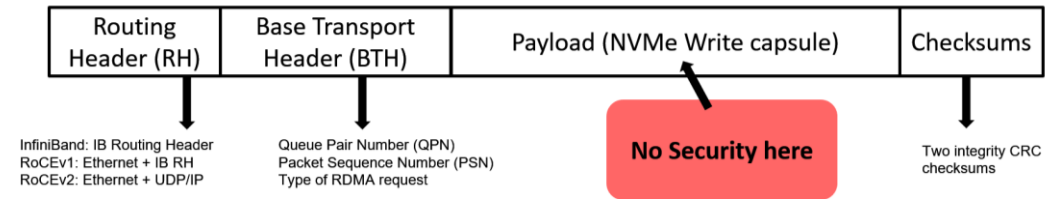
- One-sided requests can not be secured at application layer [1]

- We propose to add a MAC to authenticate NVMe packets

- MAC is verified before request processing
- MAC is sent with NVMe requests in RDMA sends

- Rules:

- All NVMe-oF requests and responses are authenticated
- The MAC may include data payload
- The MAC over data is verified once buffer is immutable



↗
All requests involve two sends

[1] Konstantin Taranov et al., sRDMA - Efficient NIC-based Authentication and Encryption for RDMA. Usenix ATC 2020

Takeaways

- Vulnerabilities in the packet format allows spoofing RDMA packets without root
- The injection allows to manipulate local RDMA-enabled kernel modules from the user space
- NVMe-oF security is not sufficient for insecure RDMA interconnects
- NVMe-oF requires an application layer security



Contact information:
Konstantin Taranov
konstantin.taranov@inf.ethz.ch



Please take a moment to rate this session.

Your feedback is important to us.