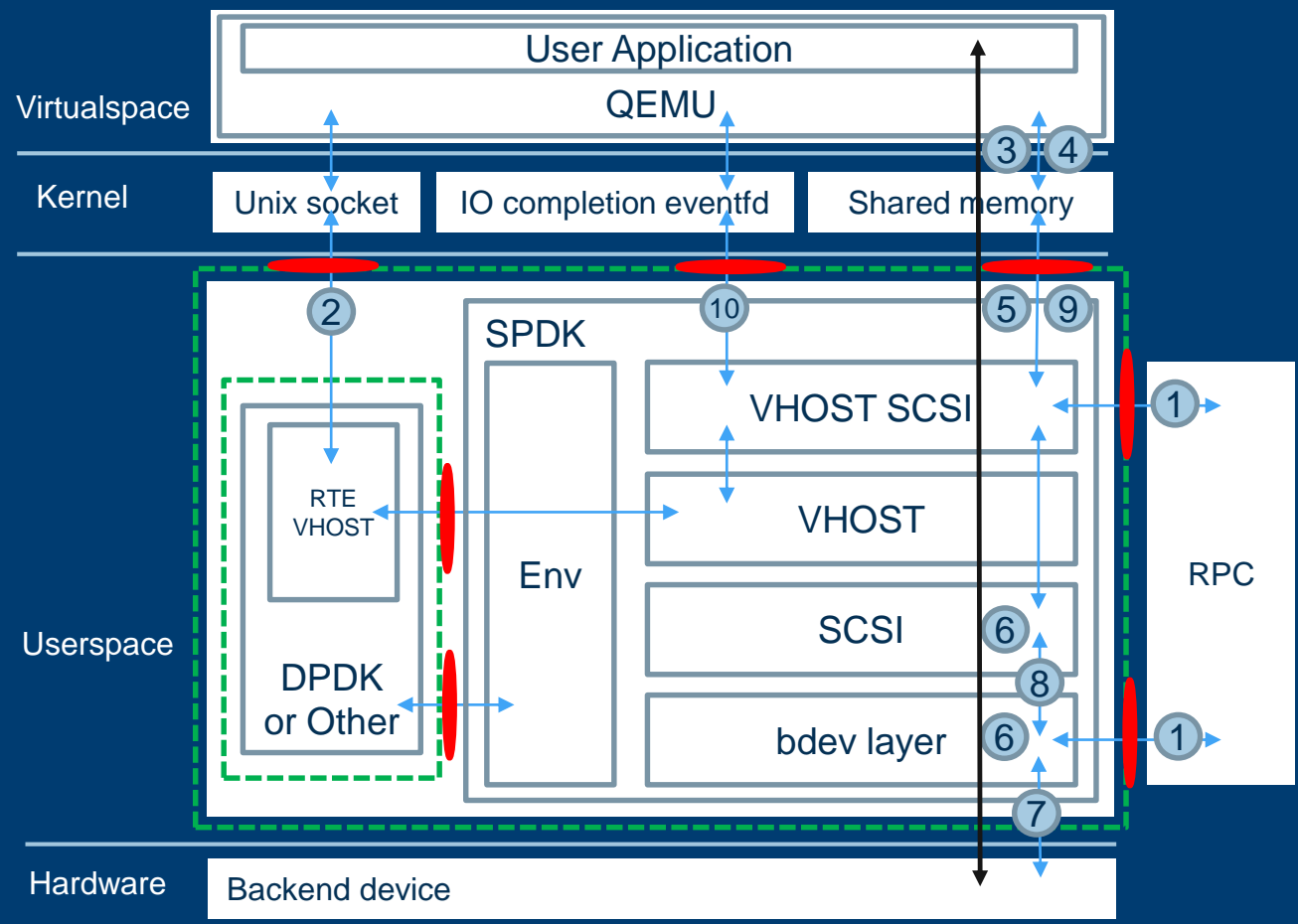


USE CASE: VHOST INTEGRATION

- User has decided to integrate SPDK vhost stack into his existing virtualization solution
- Related hardware and software components (including bdev interface) were configured correctly so they are assumed to be safe in this use case

SYSTEM DIAGRAM



Assets:

- A. Data
- B. Shared memory
- C. Sockets
- D. Env
- E. QEMU
- F. RTE_VHOST

High Level Flow:

- 1) SPDK gets configured with RPC
- 2) SPDK creates a unix socket and establishes connection with QEMU
- 3) QEMU shares memory and I/O queues
- 4) User application sends I/O request
- 5) SPDK detects request by continuously polling shared I/O queues
- 6) SPDK processes the request, first in lib/scsi then in bdev layer
- 7) Request is sent to backend device
- 8) Callback is called from bdev layer
- 9) Vhost updates the request status by modifying shared queues
- 10) Vhost notifies the application about completion by writing to completion eventfd

Control/Function Calls

Data

Attack Surfaces

Trust Boundaries

ATTACK SURFACES

System Element	Compromise Type(s)	Assets exposed	Attack Method
QEMU socket interface	Invalid input	RTE_VHOST, Shared memory, QEMU	Malformed vhost-user commands
Completion eventfd	Invalid initialization	Sockets, RTE_VHOST	Bad target address, Cause loop
Shared memory	Invalid input	Data, RTE_VHOST	Malformed IO descriptors
ENV/RTE VHOST interface	DLL Injection	Env, RTE_VHOST, Data, QEMU, Sockets, Shared Memory	Replaced Env library calls
RPC interface	Invalid input	Sockets, RTE_VHOST	Malformed/invalid json-rpc requests

THREAT MATRIX

Assets Surface	Data	Shared memory	Sockets	Env	QEMU	RTE_VHOST
QEMU socket interface	No	No	Yes	No	Yes	Yes
Completion eventfd	No	No	No	No	No	Yes
Shared memory	Yes	Yes	No	No	No	Yes
ENV/RTE VHOST interface	Yes	Yes	Yes	Yes	Yes	Yes
RPC interface	No	No	Yes	No	No	Yes

ADVERSARIES IN SCOPE

Persona	Motivation	Attacker Type	Starting Privilege Level	Skill and Potential Effort level
Malicious VM User	Wants to snoop data/disrupt users on system	Software Adversary in a VM	None	Unskilled, gives up easily
Malicious Hypervisor	Wants to snoop data/disrupt users on system	Hypervisor Software Adversary	None	Proficient level of skill, does not give up easily
Malicious RPC Admin	Denial Of Service	Network Adversary	None	Proficient level of skill, does not give up easily

* host system software adversary is out of scope because such adversaries have permissions to defeat all mitigations. User needs to ensure appropriate deployment policies are in place to prevent system level software adversaries

THREATS

Protec t-ions							
ID	Threat	Assets	Req'd	Adversary	Attack Point	Technique	Mitigation
1							
2							
3							
4							
Protec t-ions							
ID	Threat	Assets	Req'd	Adversary	Attack Point	Technique	Mitigation