Rocky: Replicating Block Devices for Tamper and Failure Resistant Edge-based Virtualized Desktop Infrastructure

Beom Heyn Kim
University of Toronto

Hyoungshick Kim
Sungkyunkwan University
Background

- Various VDI solutions exist and widely deployed.
- The VDI market size is expected to reach 38.41 billion US Dollars by 2027 (Fior Market ’21).

**VDI on Cloud may entail perceivable latency**
Emergence of EdgeVDI

Edge VDI (Cloudlet)  Cloud  Edge VDI (Cloudlet)

VM  5G  State Replication  5G

RDP  Traveling  RDP
Problems with EdgeVDI

Edge VDI (Cloudlet)

Failure

Cloud

State Replication

Edge VDI (Cloudlet)

Heterogenous Cloudlets

5G

RDP

5G

VM

RDP

Traveling

Tampering
Related Works

• Ransomware detection methods.
  • But, those works do not explore how to recover tampered data.

• Tamper-resistant storage systems to protect user data against ransomware.
  • However, those works require modification on hardware architecture or need a special hardware device.

• Existing solutions against tampering attacks do not work when a cloudlet on which the VM runs fails.
Heterogenous Cloudlets

Replication Protocol

Synchronous
Push-based
Rocky: Pub/Sub Style Replication

Asynchronous Pull-based Replication Broker (Connector-Cloudlet)

- Periodic Mutation Snapshot Update
- Asynchronous Pull-based
- Periodic Prefetch & Snapshot Merging
Tampering Attacks on Block Device States

T1: \( \text{Write(\text{Block 1}, X)}, \text{Write(\text{Block 2}, Y)}, \text{Write(\text{Block 3}, Z)} \)
Rocky: Replay Non-Tampering Writes Only

Write(Block 1, X), Write(Block 2, Y), Write(Block 3, Z)

Ransomware Encrypts Disk Blocks

T1:

T2: Ransomware Encrypts

Anti-malware can detect tampering attacks and inform

T3: Write(Block 1, E(X)), Write(Block 2, E(Y)), Write(Block 3, E(Z))

Replay to recover

Don’t Replay
Coherency Problem

Contiguous Write Sequence: W1, W2, W3, W4

‘W3’ is permanently lost!
Coherency Problem

Contiguous Write Sequence: **W1, W2, W3, W4**
Discard W4 and Replay W1 and W2 only

Cloudlet A
- T1: W1, W2
- T4: W3
- T6: Failed

Cloudlet B
- T2: W1, W2
- T5: W3
- T8: Failed

Connector-Cloudlet
- T3: W1, W2
- T7: W4
- Coherent
- Incoherent
Rocky Cloudlet

Rocky Endpoint

Virtual Machine

Rocky Controller

(NBD Server)

Rocky Block Device

(NBD Block Device)

Rocky Storage

User

Kernel

Connector-Cloudlet

Rocky Cloudlets
Performance Overhead

• If up-to-date blocks are replicated timely, only 8.4% and 11.9% additional throughput overheads are required for write and read, respectively.
Conclusion

- Pub/Sub Style Replication Protocol
- Replaying Non-Tampering Writes
- Replaying Contiguous Writes

Rocky Shows that Overcoming All These Three Problems is Possible