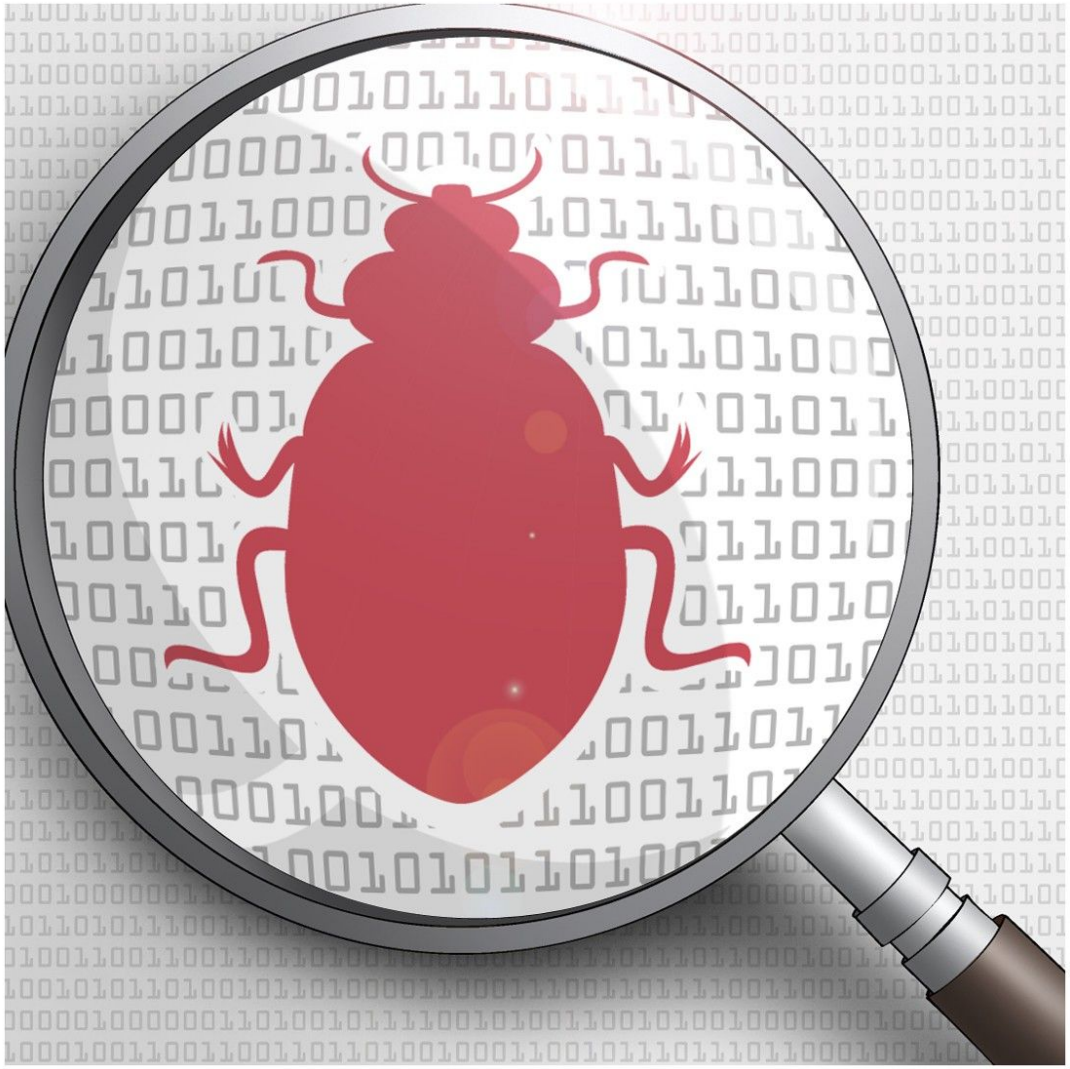


Agentless Bare-Metal Introspection

Apoorve Mohan
(PhD Candidate)

MOC

IBM


“Absolute Security”
is a Must...

The ONLY Rule of "Security Club"

Be Proactive or Lose $$$

Software Introspection is SUPER Important

Software is Constantly Evolving: NEVER Bug-Free

Software Updates

Software Upgrades

Software is Constantly Evolving: NEVER Bug-Free

Softwa

Software Upgrades

How to perform Software Introspection?

Agent-based Introspection

- Databases of Common Software Vulnerabilities and Weakness
  - e.g., CVE, CVSS, CWE, etc.

- Periodic System Introspection
  - client (agent) running on the system
  - compare deployed software/configurations against vulnerability databases
  - e.g., Amazon Inspector

Agent-based Introspection: Disadvantages

- Can the Agent be Trusted?
  - agent running on a potentially compromised system???
- Periodic Introspection Consumes Resources
  - performance impact on co-located applications
  - could result in SLA violations
    (for time-critical applications)
- Requires Privileged Access on Every System
  - but, cloud provider has no access in case of bare-metal instances

Agent-based Introspection: Disadvantages

- Can the Agent be Trusted?
  - agent running on a potentially compromised system???
- Periodic Introspection Consumes Resources
  - performance impact on c
  - could result in SLA viol
    (for time-critical applications)
- Privileged Access on Every System
  - but, cloud provider has no access in case of bare-metal instances

Solution?

Solution: Remote Agentless Introspection

- Easy for Virtual Infrastructure
  - virtual machines and containers
  - disk remotely accessible
  - snapshot current state and introspect
    - e.g., IBM Vulnerability Advisor

But what about
Remote Introspection
of Bare-Metal systems?

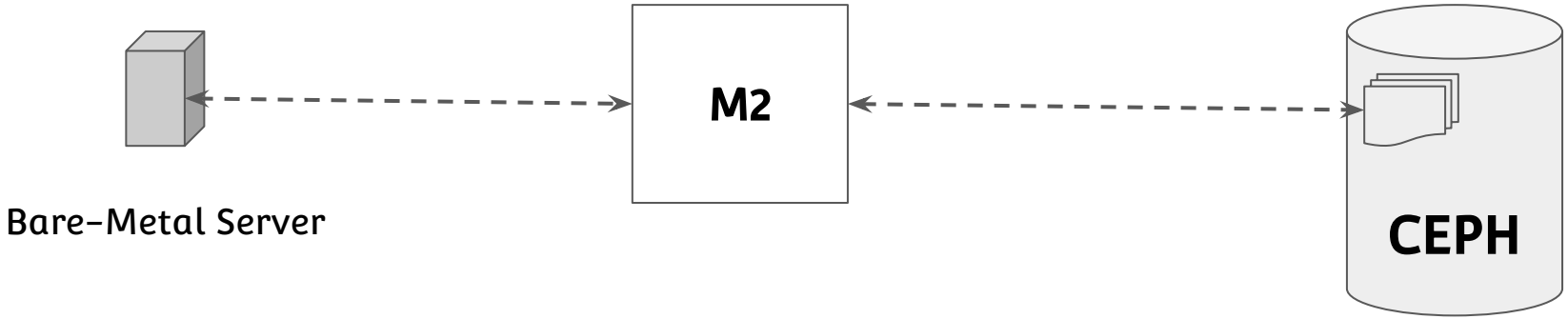
M2 to the Rescue

"Remote Introspection" of Bare-Metal Systems is Possible

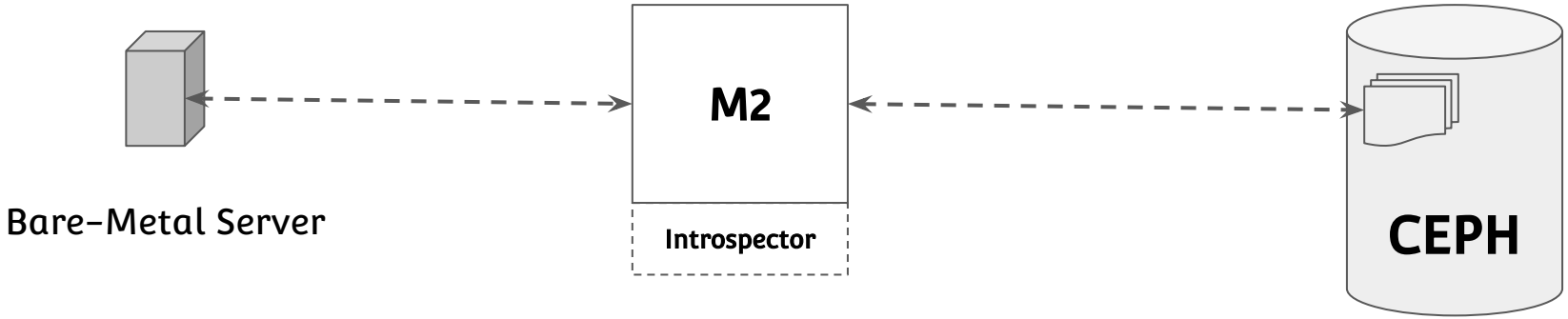
M2: **M**alleable **M**etal as a Service

- provisions bare-metal instances to remote disk (like Virtual Machines)
- creates shallow copies of remote disks
- introspects a remote disk from its shallow copy

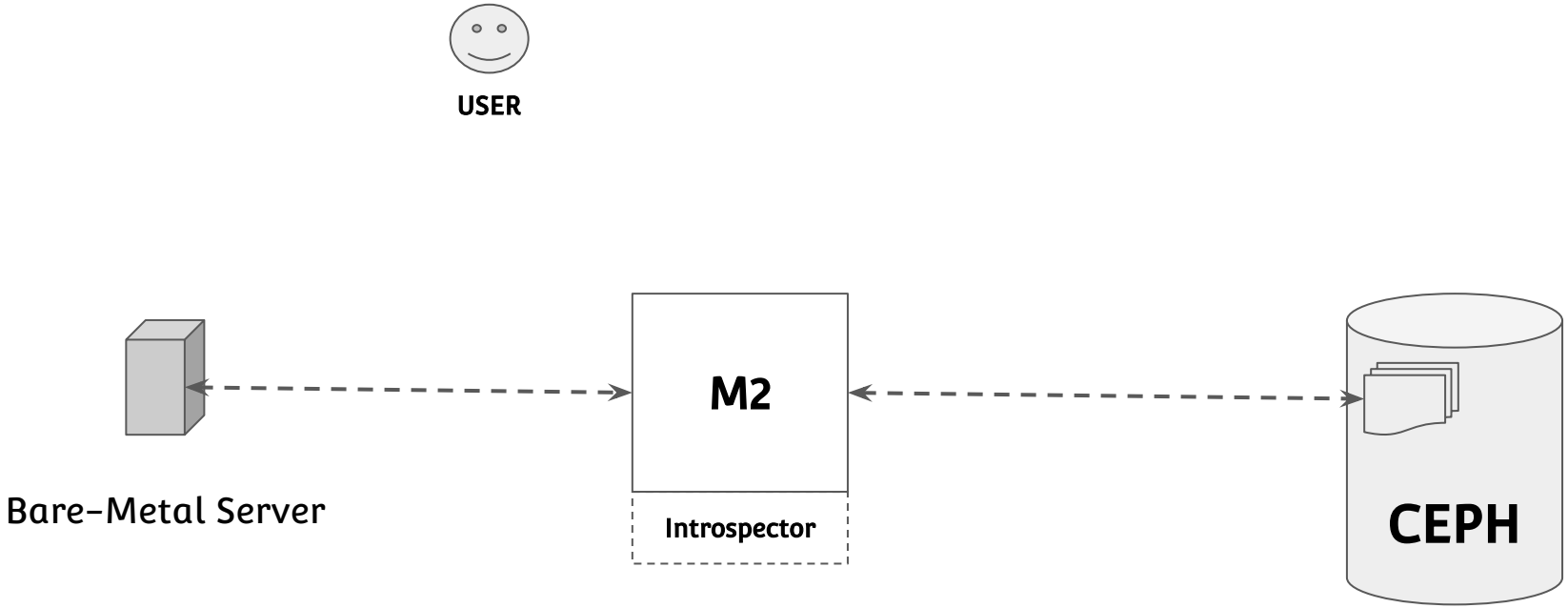
M2: Malleable Metal as a Service



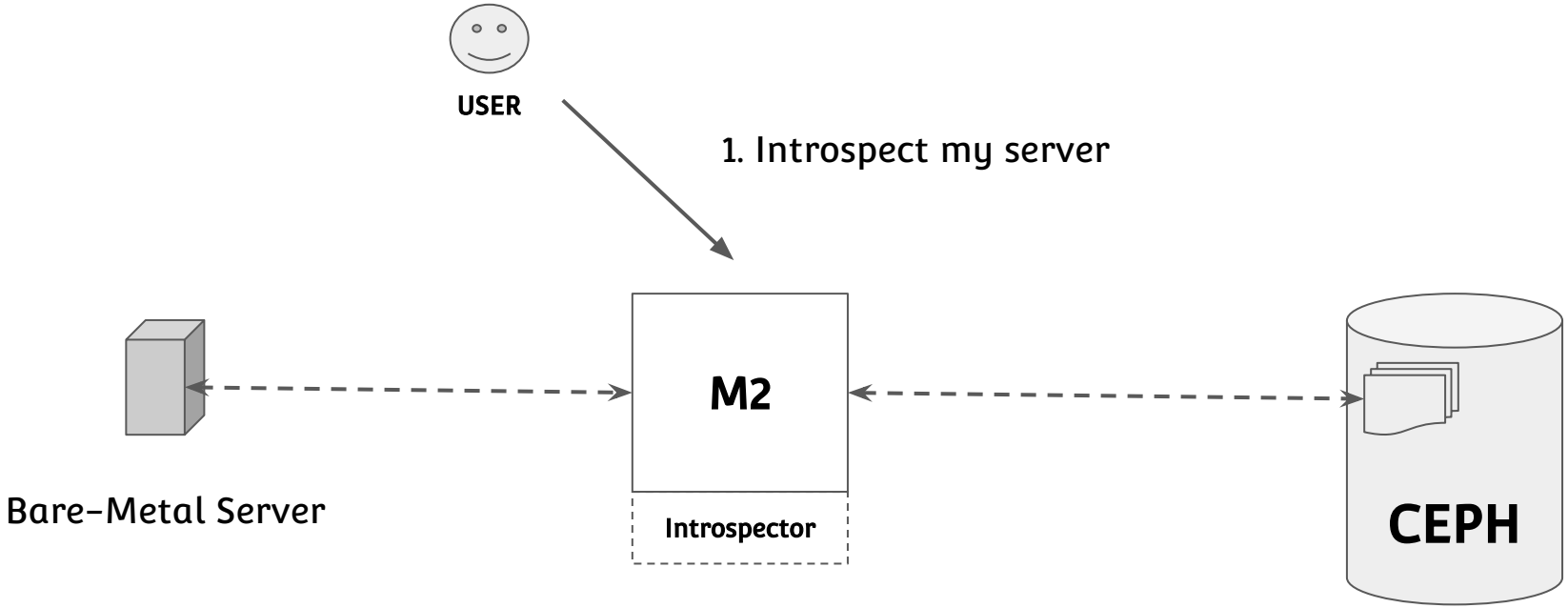
Agentless Bare-Metal Introspection using M2



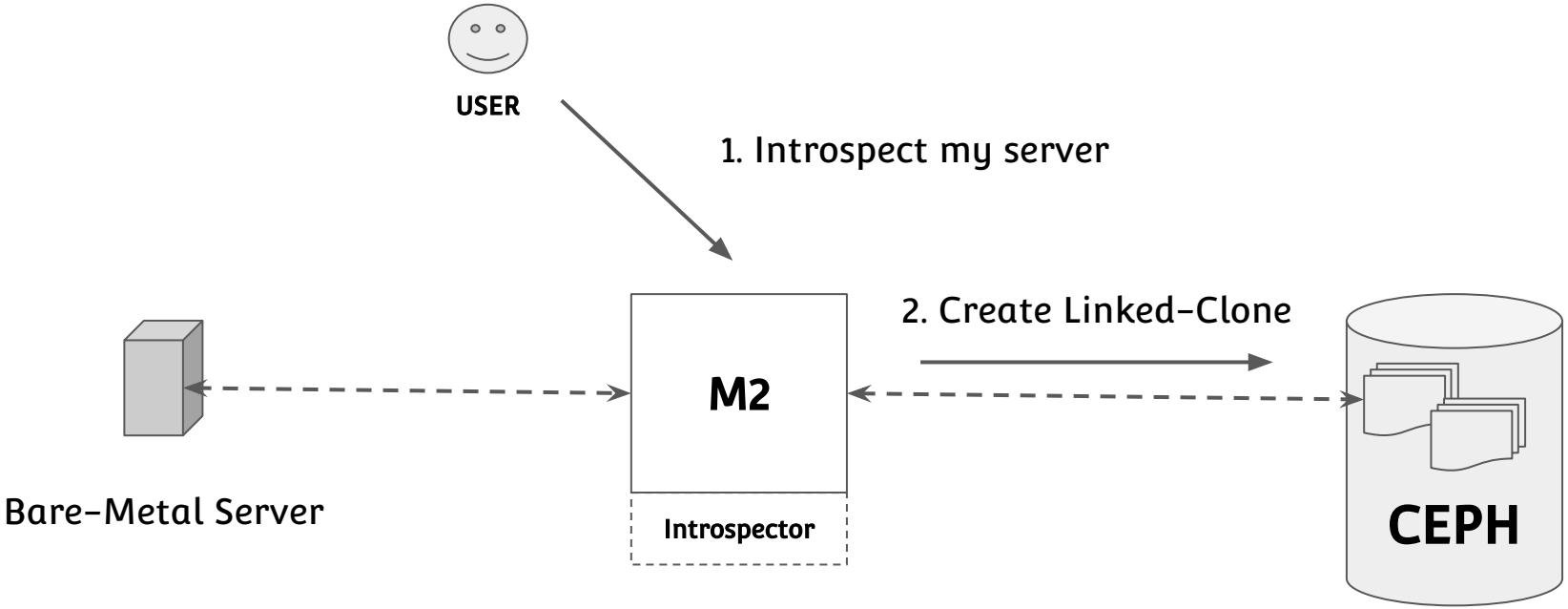
Agentless Bare-Metal Introspection using M2



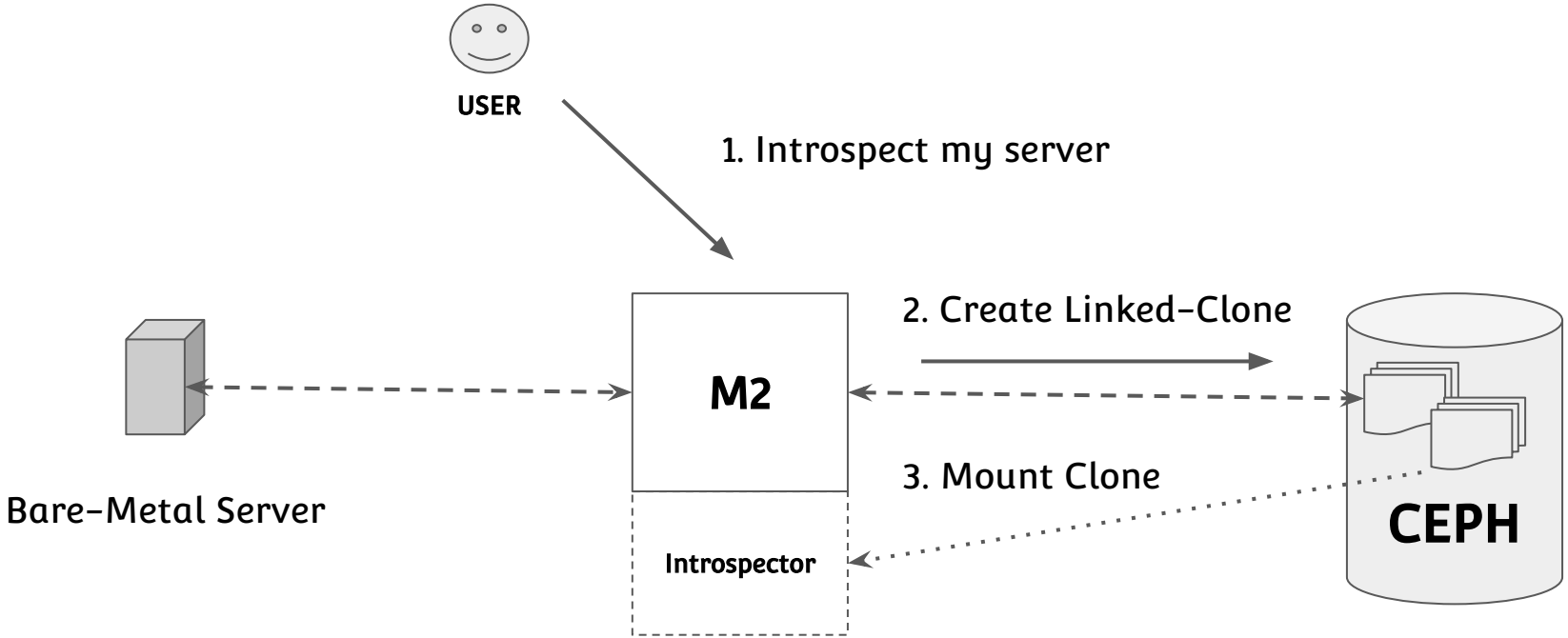
Agentless Bare-Metal Introspection using M2



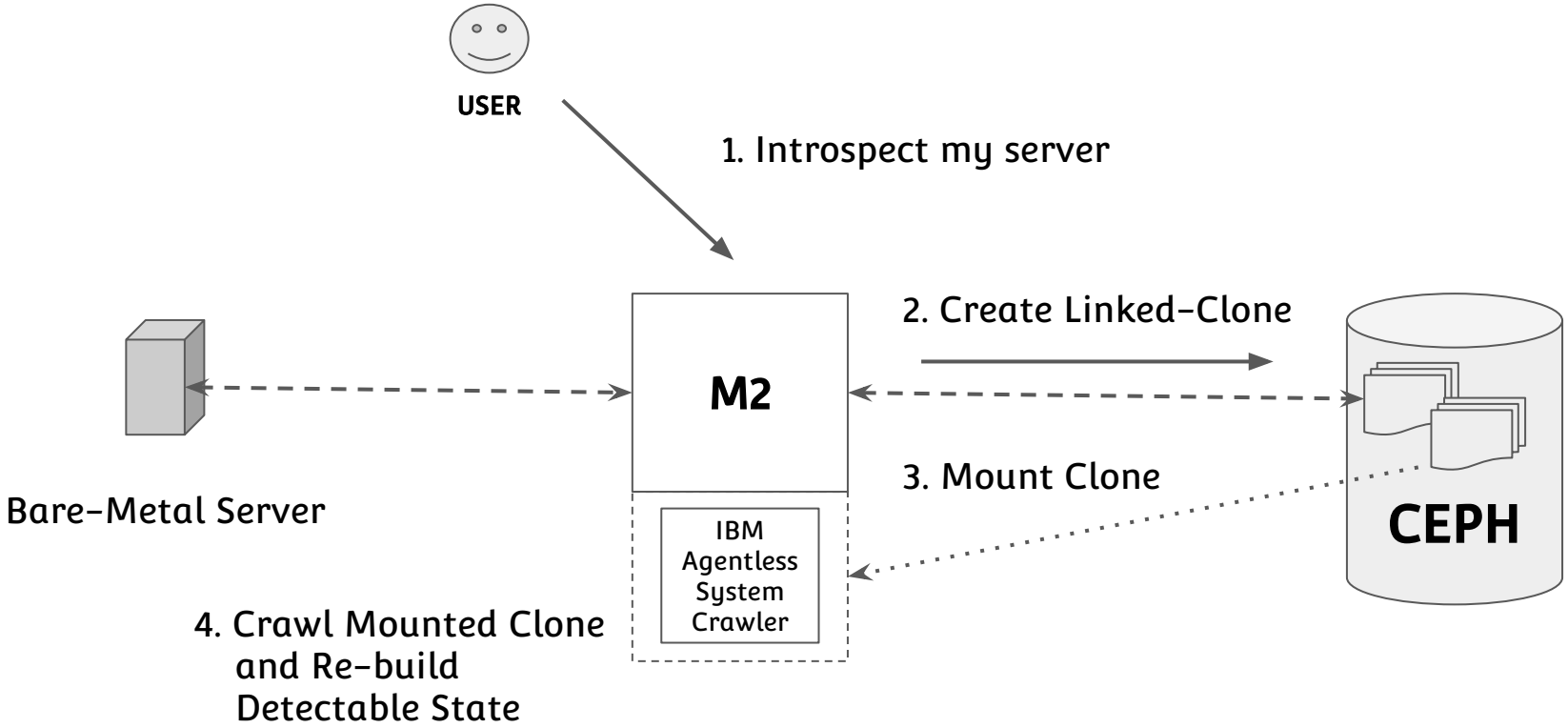
Agentless Bare-Metal Introspection using M2



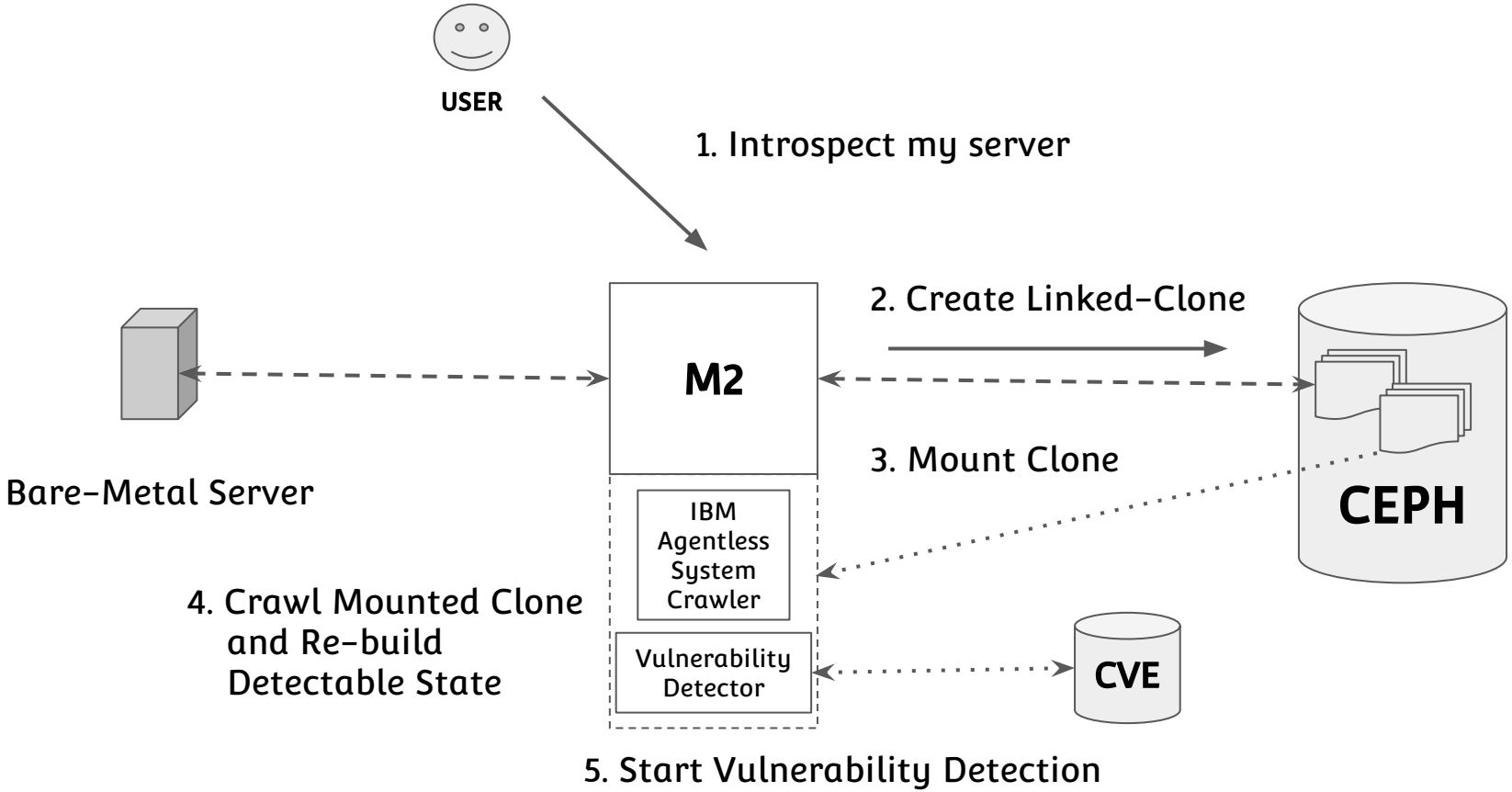
Agentless Bare-Metal Introspection using M2



Agentless Bare-Metal Introspection using M2

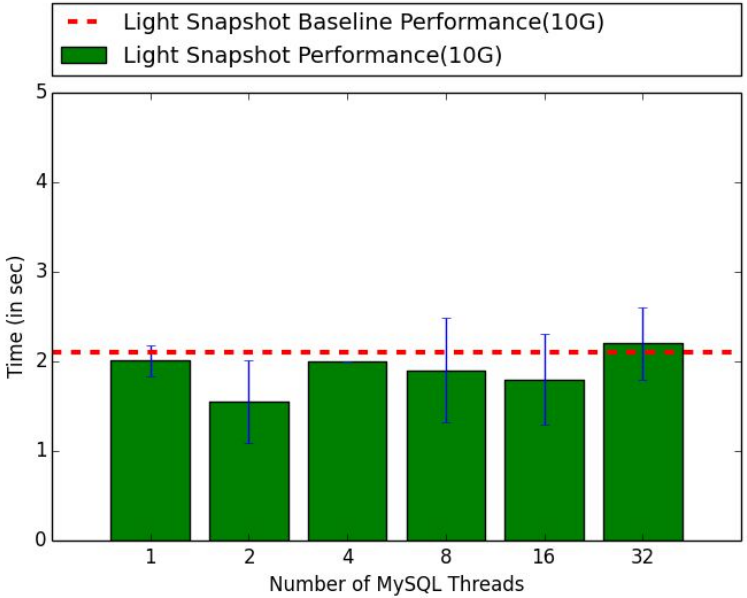


Agentless Bare-Metal Introspection using M2



Sneak-Peak: Results

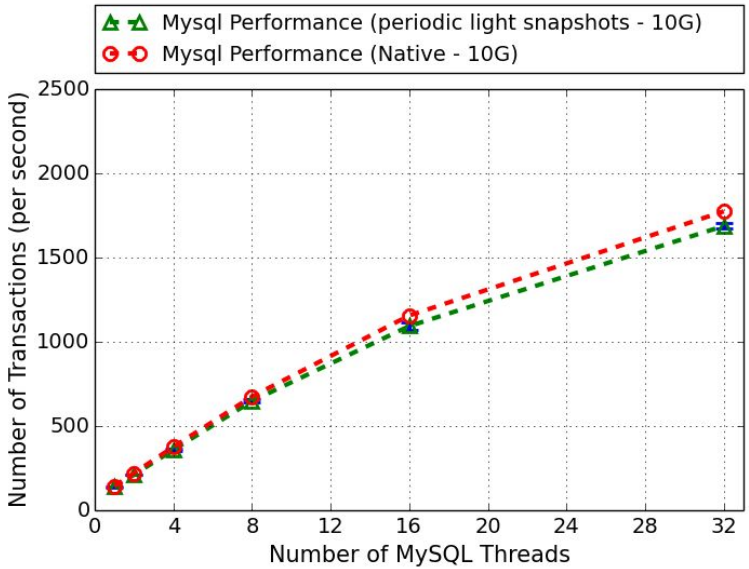
- System Running MySQL
  - I/O Intensive Application
  - periodically snapshotting system disk (boot-drive + software packages)
  - snapshot == COW clones
  - varying workload intensity (1-32 threads)
- Snapshotting Cost Unchanged
  - 5 snapshots per minute
- Negligible Impact on OLTP Performance



Sneak-Peak: Results

- System Running MySQL
  - I/O Intensive Application
  - periodically snapshotting system disk (boot-drive + software packages)
  - snapshot == COW clones
  - varying workload intensity (1-32 threads)
- Snapshotting Cost Unchanged
  - 5 snapshots per minute
- Negligible Impact on OLTP Performance

Application Performance



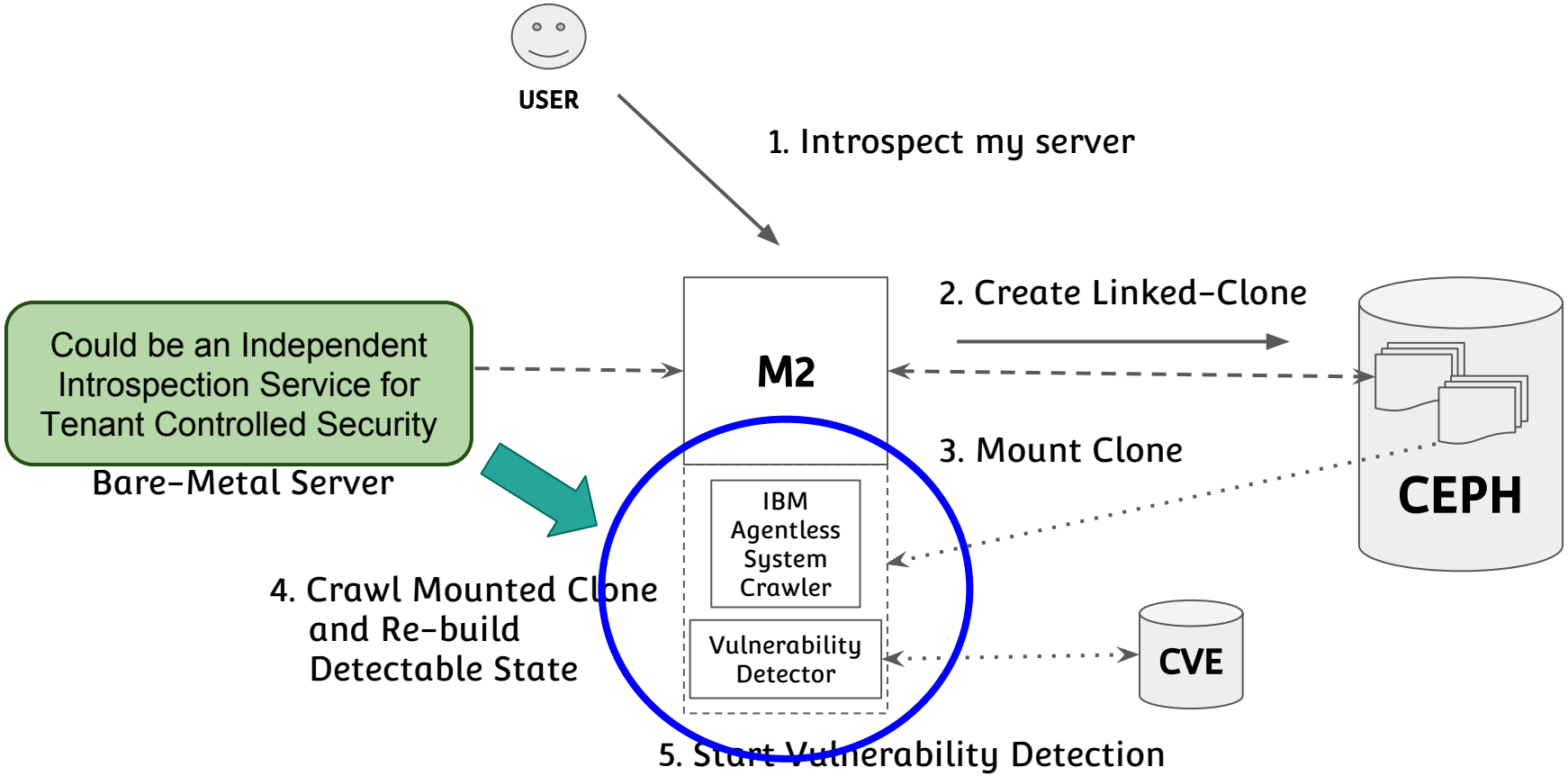
Project Status

- Summer 2017 : Discussion
- Spring 2018: Implementation - Cloud Computing Class
  - Integration between M2 and IBM Agentless System Crawler (both open-source)
  - Crawler code changes upstreamed
- Fall 2018: Working on a Research Paper

Future Work

- Agentless Bare-Metal Memory Introspection
- Tenant Controlled Introspection
  - Current Architecture
    - provider introspecting on behalf of tenant
  - Can the tenant introspect themself ???

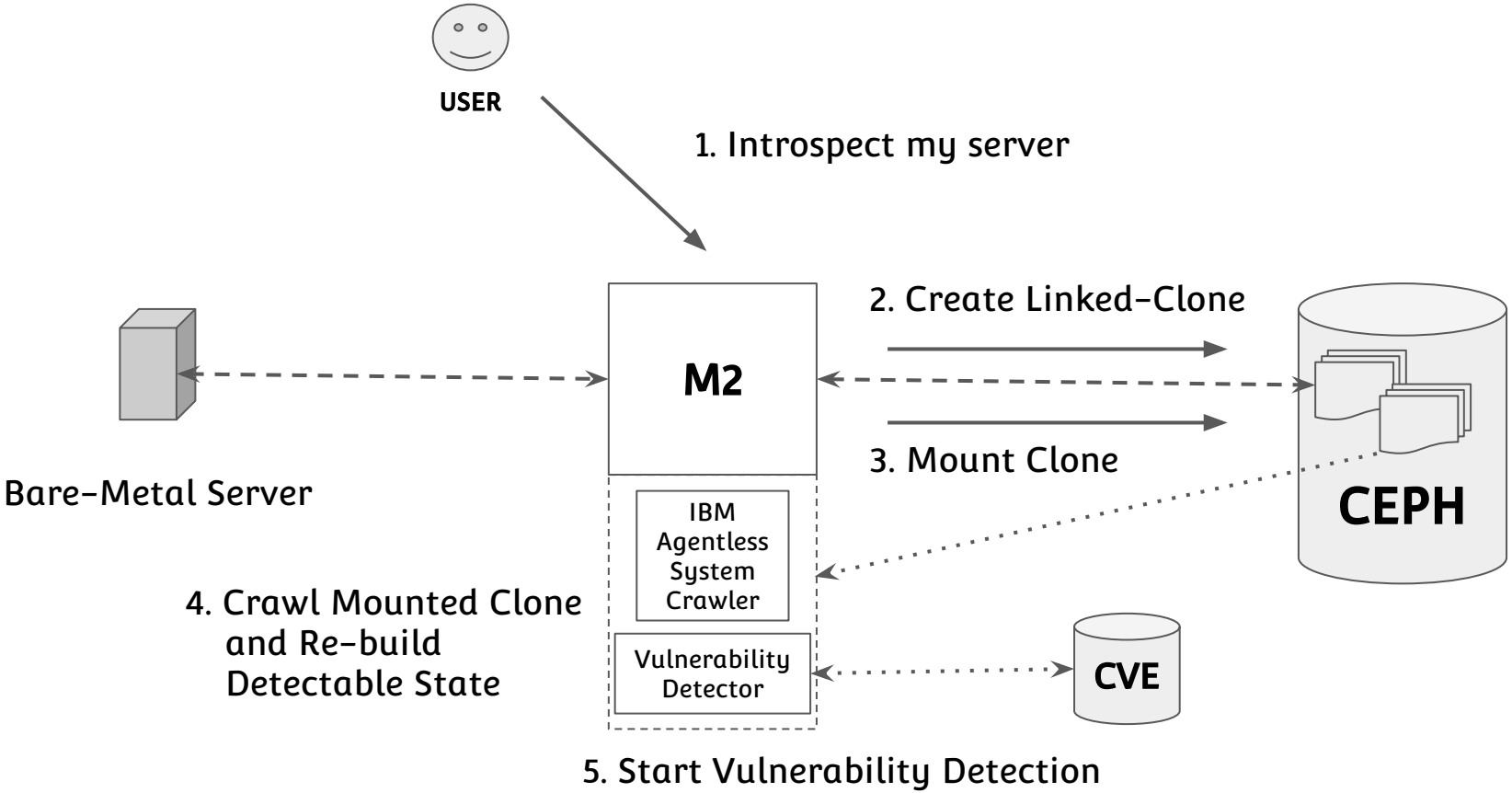
Agentless Bare-Metal Introspection using M2



Future Work

- Agentless Bare-Metal Memory Introspection
- Tenant Controlled Introspection
  - Current Architecture
    - Provider providing introspection infrastructure
  - Can the tenant introspect himself ???

Thank You


USER
1. Introspect my server
2. Create Linked-Clone
3. Mount Clone
M2
Bare-Metal Server
CEPH
IBM Agentless System Crawler
Vulnerability Detector
CVE
4. Crawl Mounted Clone and Re-build Detectable State
5. Start Vulnerability Detection