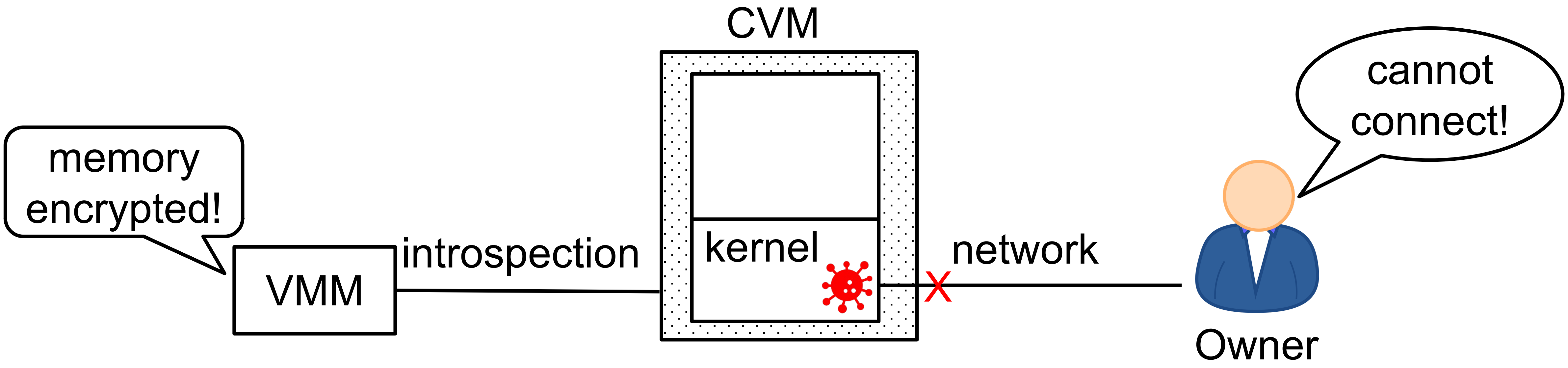
TETD: Trusted Execution in Trust Domains

Zhanbo Wang, Jiaxin Zhan, Xuhua Ding, Fengwei Zhang and Ning Hu

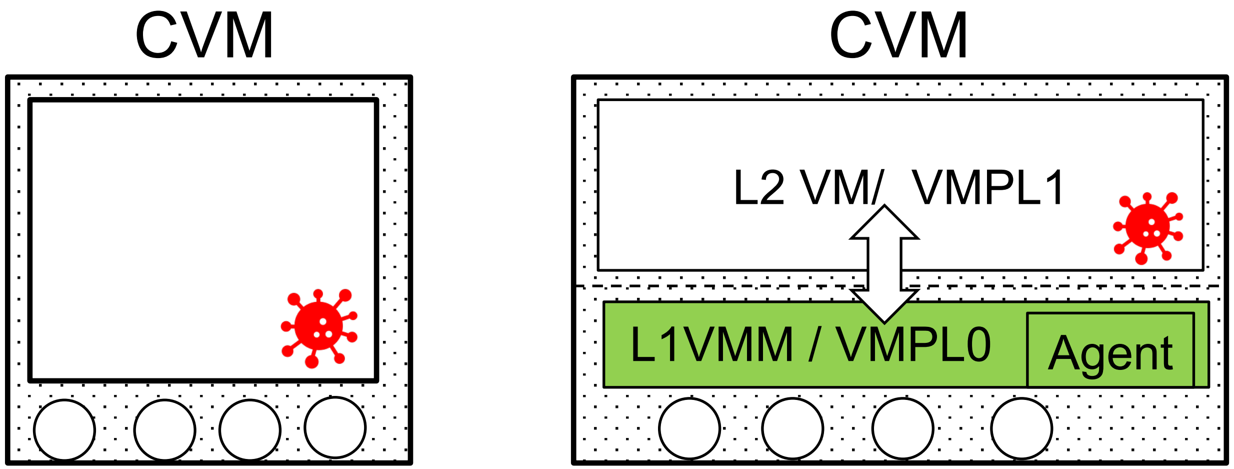
The Problem

- In the event of CVM kernel compromise or crash, the owner loses the foothold to take care of her CVM.



Existing Approach

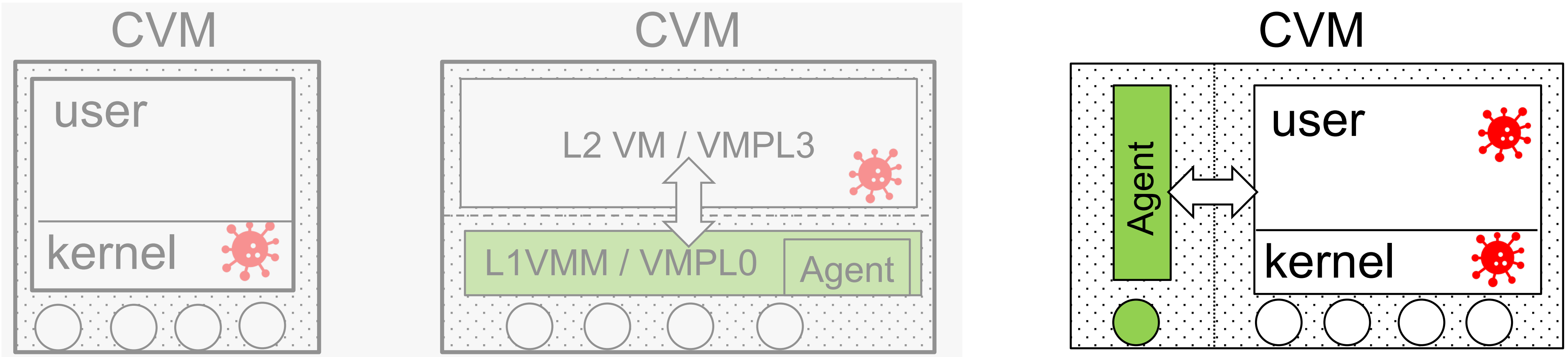
- **In-VM Privilege Layering**: to insert a more privileged and trusted layer under the CVM kernel.
  - used in HARDLOG[SP22], Hecate[CCS22], Veil[ASPLOS23], SVSM-vTPM[ACSAC23], 00SEVen [Sec24], NestedSGX [NDSS25] etc.



Privilege Layering

Our Approach

- **Resource Separation**:
  a) A CVM is split into a two (or more) sub-systems with separated physical memory and vCPUs.
  b) To protect a subsystem against another, the untrusted VMM withholds the former's resources when others are running.



No hardening

Privilege Layering

Resource Separation

Results

- **TETD**: a resource-separation based TD hardening scheme without modifying the Intel TDX Module.
- Two execution modes:
  - **exclusive mode** for system-level maintenance.
    - Example case: introspection
  - **collaborative mode** for secure execution against untrusted kernel.
    - Example case: kernel log hardening, enclave-like decryption.
- Pros and Cons:
  - + Secure against full-CVM compromise, including L1VMM or VMPL0 kernel.
  - + No architectural change to CVM; easy to deploy; highly flexible
  - - Trust the VMM to faithfully execute the scheme.