Approach to The Secure Global Live Migration

Hidenobu Watanabe

Cybersecurity Center

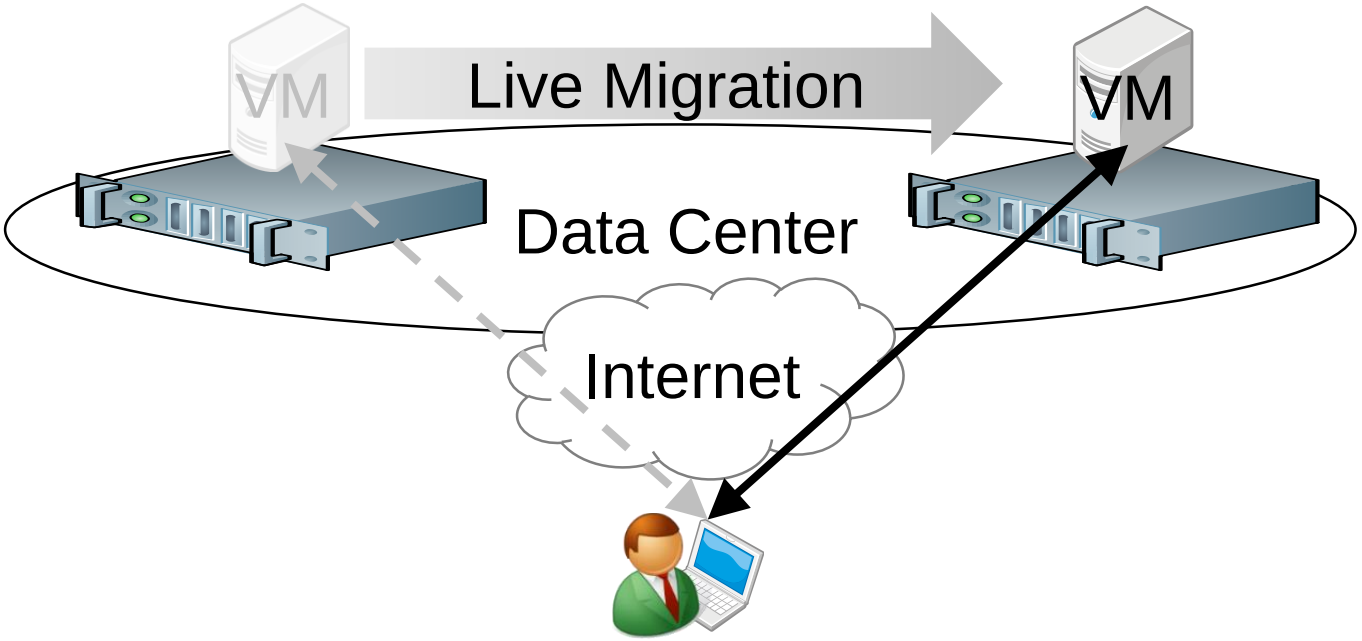
KYUSHU
UNIVERSITY

Outline

- **Background and objective**
- **Attack case and required security function**
- **Related work and my approach**

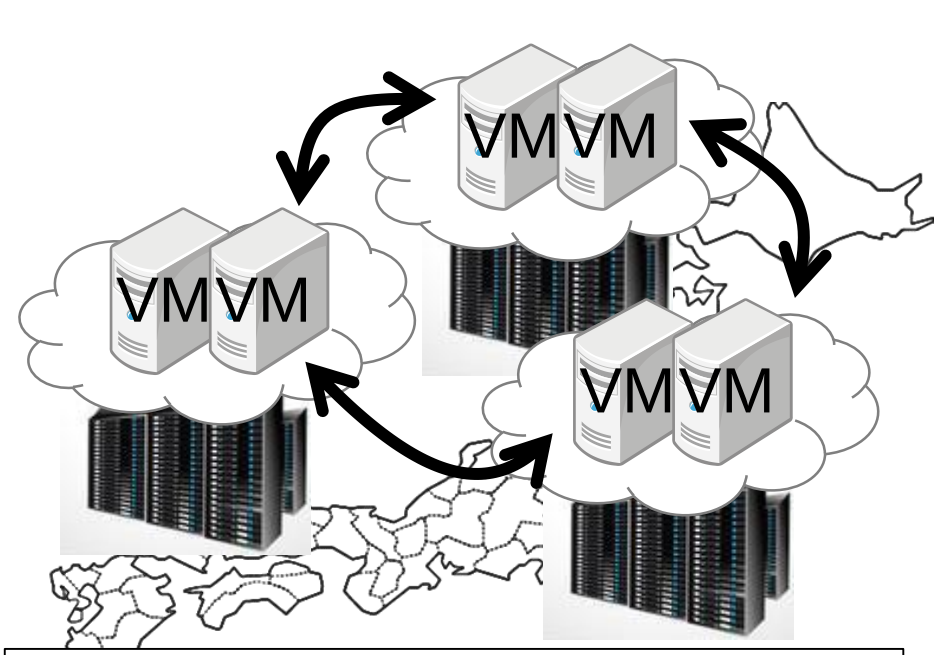
Background: Live Migration

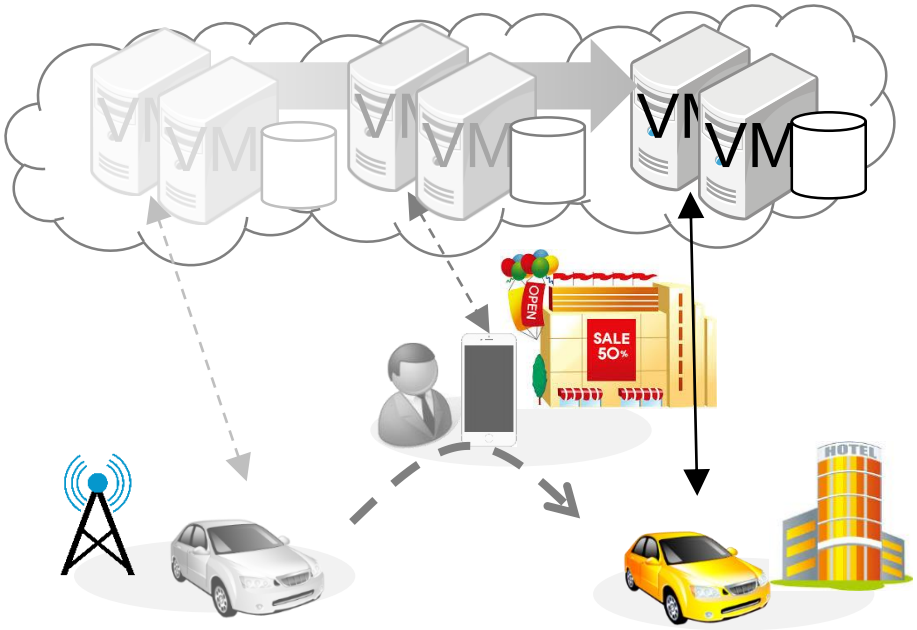
- **Virtual machine (VM) management function**
  - A running VM is transferred from one physical server to another without disconnection of VM and client.
- **Issues**
  - Network limitation (LAN only)
  - Security



Existing solution for Network limitation

- **Global live migration**
  - Live migration with the ability to over the Internet.
  - Combination with seamless network technology
    - L2 VPN, IP mobility, SDN etc.





Use case1
Disaster recovery

Use case2
Mobility Cloud Service

Objective

- **Research objective**
  - Realize the secure global live migration.

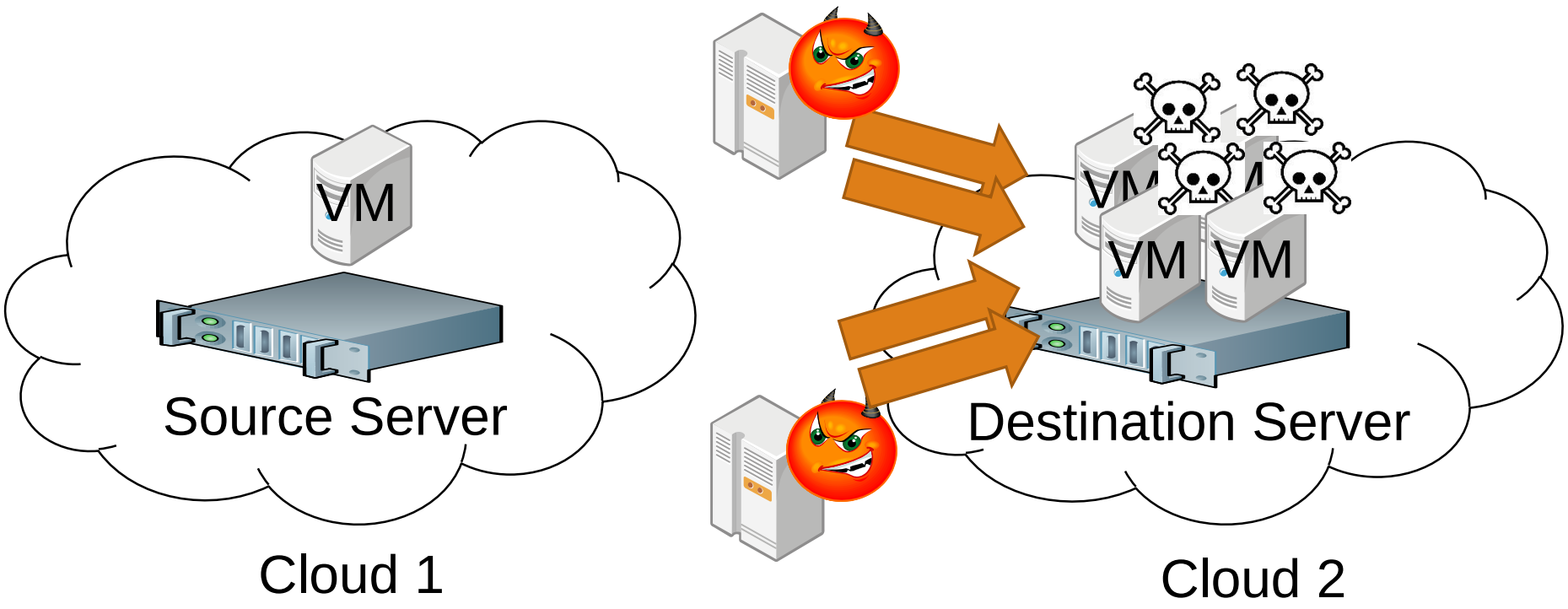
- **Our contributions**
  - Global live migration supports the following security requirements:
    - Reliability of platform (server, VM, NW etc)
    - Confidentiality of communication during live migration
    - Integrity of migration data

Attack Case

- **Attack on the servers**
- **Attack on the migration data**

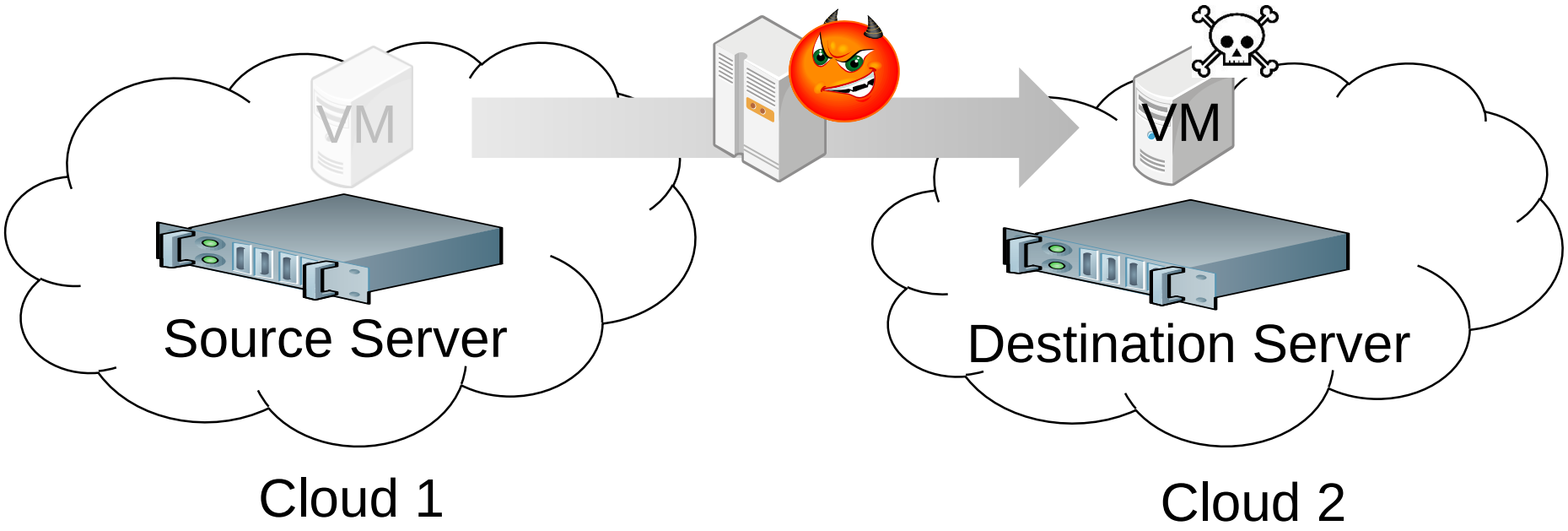
Attack on servers

- Live migration does not check trustworthy of servers and operation.
- Attacker can transfer malicious VMs to destination server by spoofing, replay attack and DoS/DDoS etc.



Attack on migration data

- Migration data does not encrypted.
- Migrated data does not verified.
- Attacker can wiretap and tamper migration data during live migration by man-in-the-middle attack etc.



Required Security Function

- **Federated authentication and authorization**
  - The trusted source/destination servers, VMs, NW and users are protected from unauthorized access and operation.
- **Encrypted end-to-end communication**
  - The migration data is secret.
- **Migration data live verification**
  - The migrated data is verified as same as source data before resuming the migrated VM.

Virtualization Security

- **Trusted Platform Module (TPM)**
  - A secure crypto-processor built-in a motherboard chip in computer.
  - This offers facilities for the secure generation of cryptographic keys and random number generator.
    - Platform integrity
    - Disk encryption
    - Password protection
    - Digital rights management
    - Software license protection & enforcement

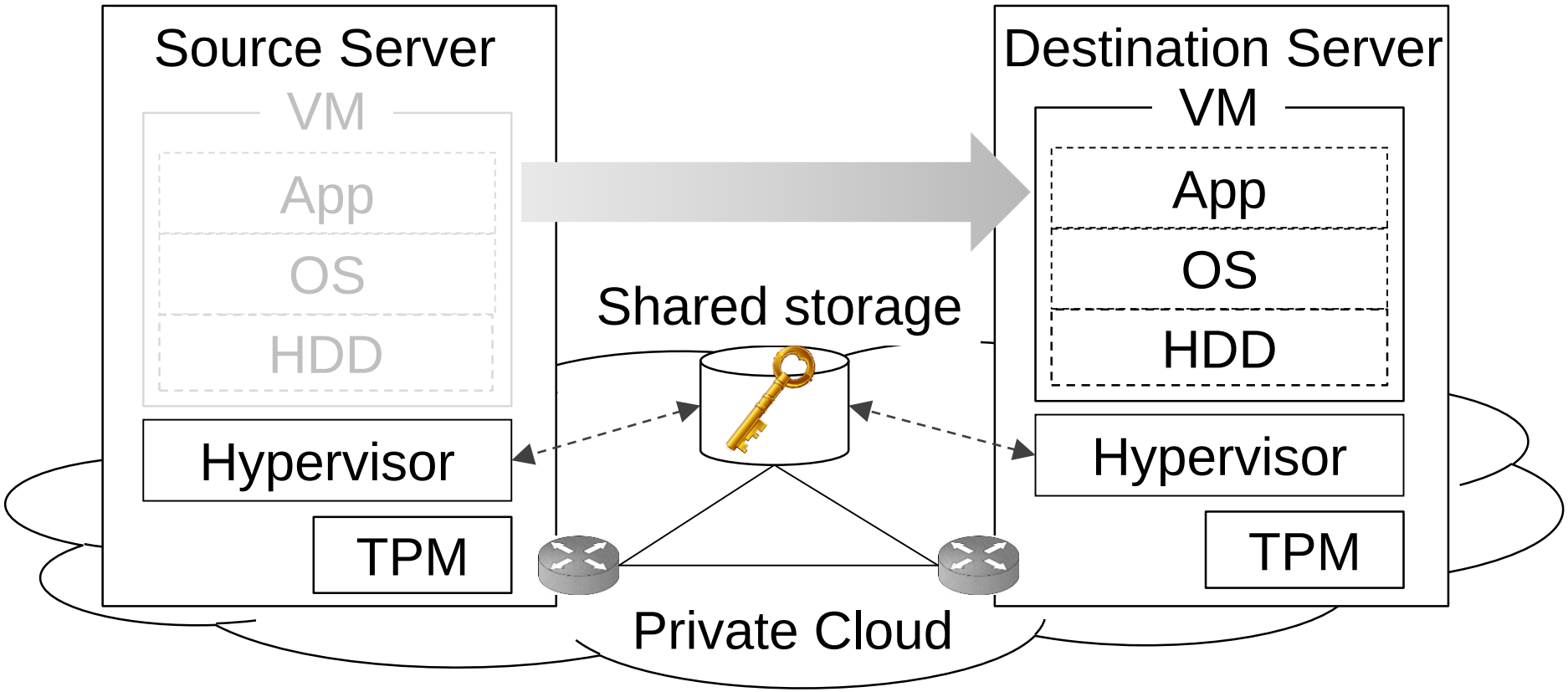
- **Virtual TPM (vTPM)**
  - This allows VM to get interaction with a unique, emulated, software TPM in the same way they interact with a TPM on the physical system.
  - Xen hypervisor supports it now.

Related Work

- **Roll-based live migration with TPM**
- **VM migration with vTPM**

Roll-based live migration with TPM

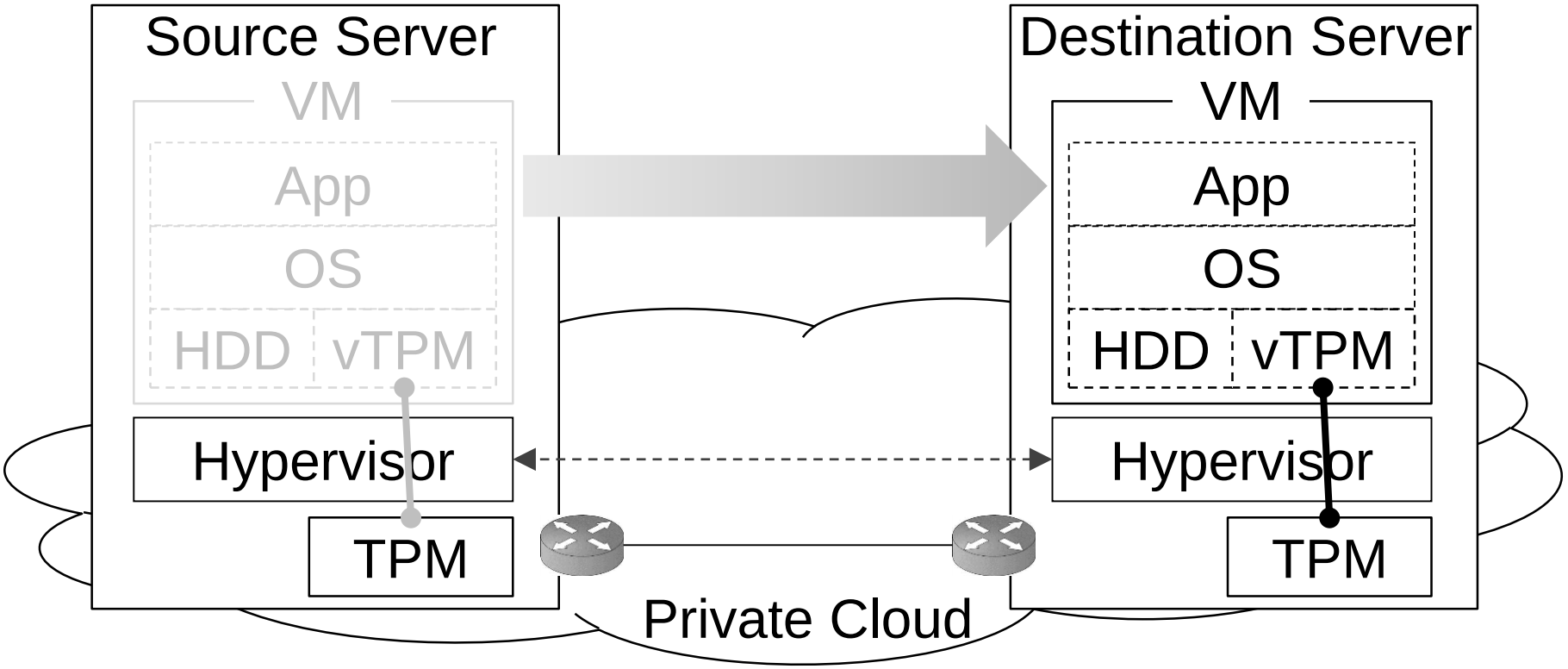
- Hypervisors share security data such as private key of TPM, roll-based policy, certification using the shared storage.
- A scope of this paper is limited to **a private cloud.**



W. Wang, et.al., “Secured VM Live Migration in Personal Clouds”, 2009.

VM migration with vTPM

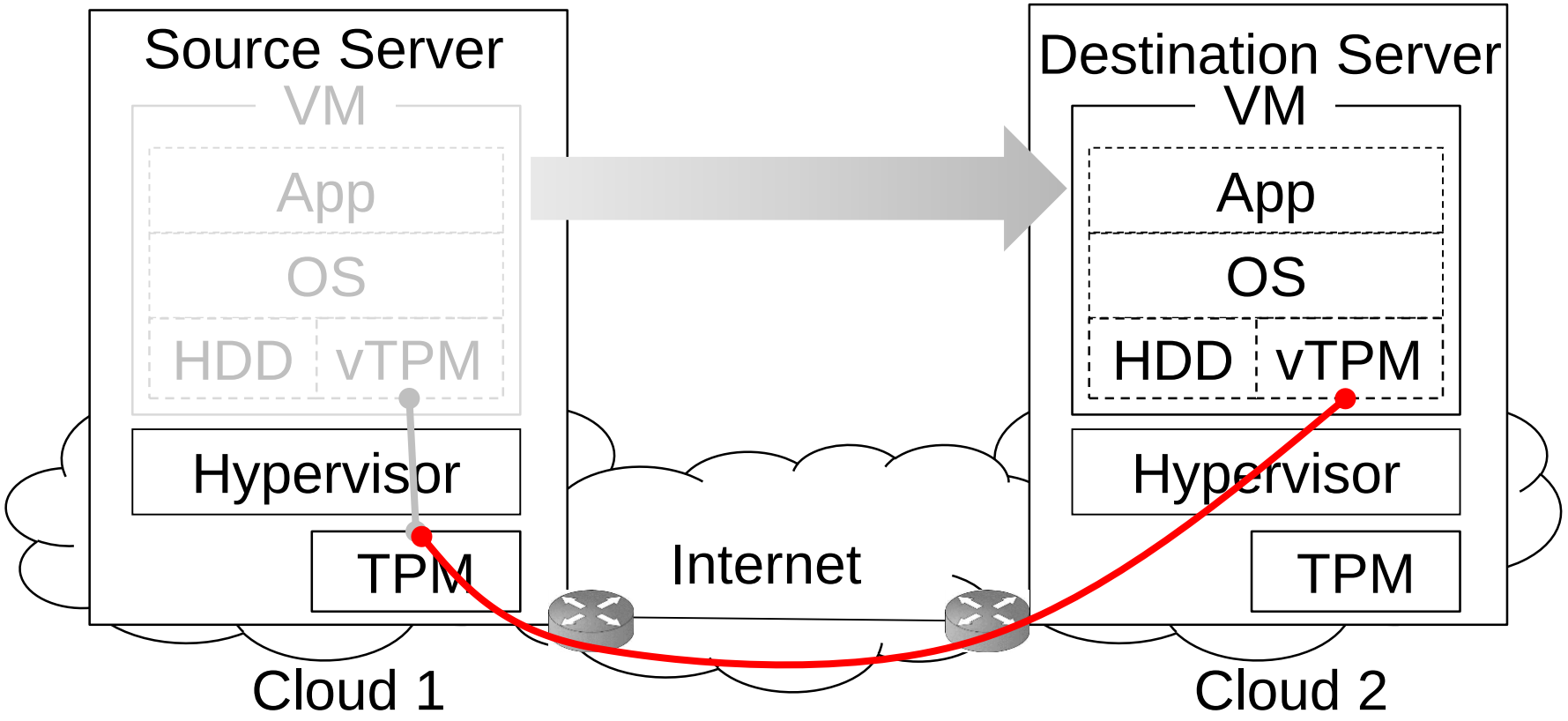
- Source hypervisor transfers vTPM status to destination after VM migration, then destination hypervisor establishes connection of vTPM and destination TPM.
- A scope of this paper is limited to **private cloud and VM migration (not live migration).**



B. Danev, et.al., “Enabling Secure VM-vTPM Migration in Private Clouds”, 2011.

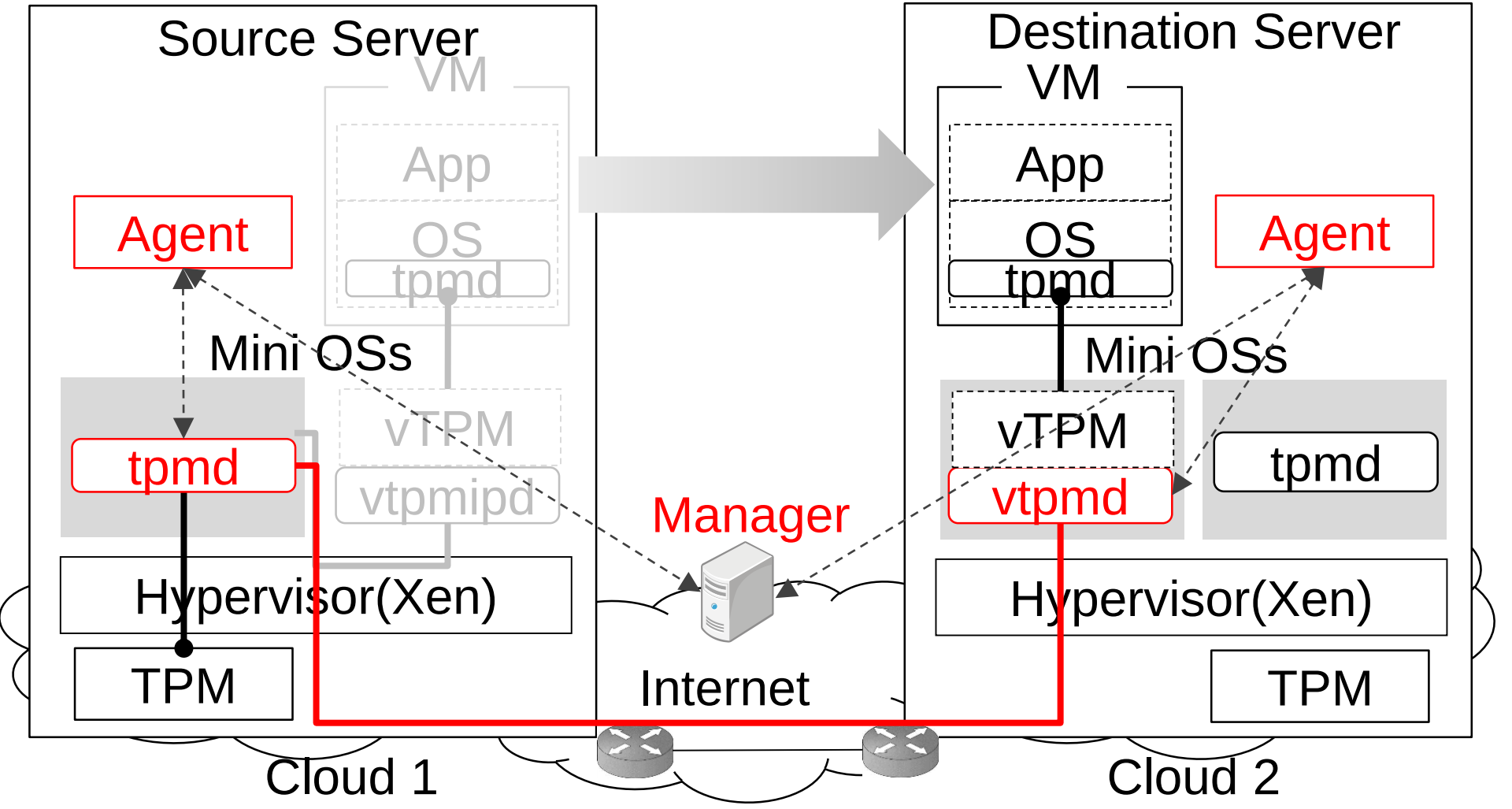
My Approach

- **Secure Global live migration with TPM over IP**
  - Accessing remote TPM over the Internet.
  - It's not necessary to transfer security data to destination server.
  - Available to live migration.



TPM over IP Platform Design

- Agent and manager manage connection of vTPM and TPM.
- Extended vTPM driver and TPM driver in mini OS encapsulates TPM I/O message to TCP/IP packets.



Conclusion

- **Required security functions of secure global live migration are:**
  - Federated authentication and authorization
  - Encrypted end-to-end communication
  - Migration data live verification

- **Approach to secure global live migration.**
  - TPM over IP
  - Each created TPM instance holds an association with a VM over the Internet throughout its lifetime on the platform.

- **Future work**
  - Implementation of agent, manager and extended vTPM driver and TPM driver