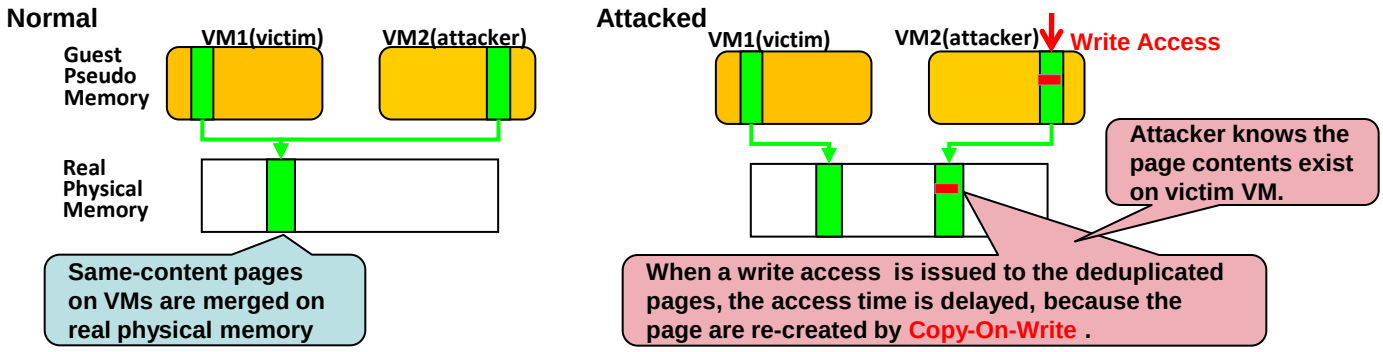
Software Side Channel Attack on Memory Deduplication

National Institute of Advanced Industrial Science and Technology AIST

Kuniyasu Suzaki, Kengo Iijima, Toshiki Yagi, Cyrille Artho
National Institute of Advanced Industrial Science and Technology (AIST)

Research Center for Information Security

Threat: Memory deduplication is vulnerable to software side channel attacks.



Challenge for the attacker

- Alignment of matching data
- Self-reflection (explained to the right)
- Runtime modification
  (swap-out, ASLR, anonymous page, preloading, self-modifying code)

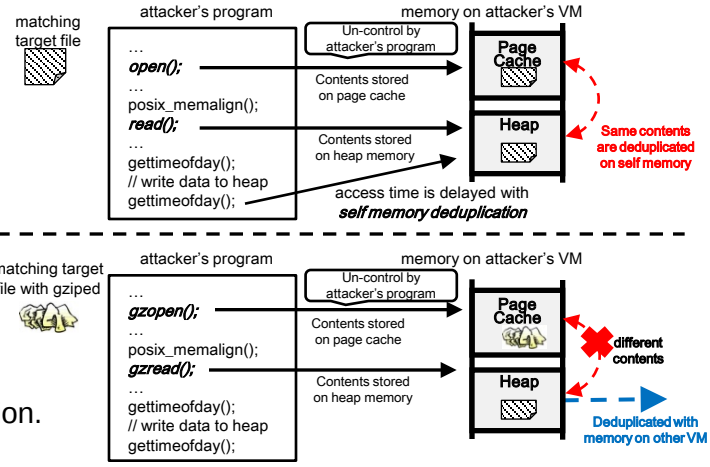
Attack Limitation

- 4KB page exact matching
- Time for being deduplicated
  (our experience on KSM of KVM is 5 min)

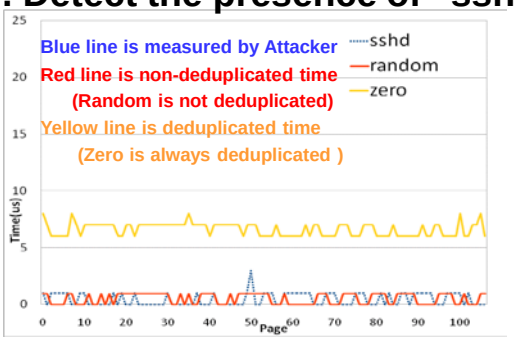
Countermeasures

- Whole memory encryption ruins deduplication.
- Sandbox with memory encryption is better.

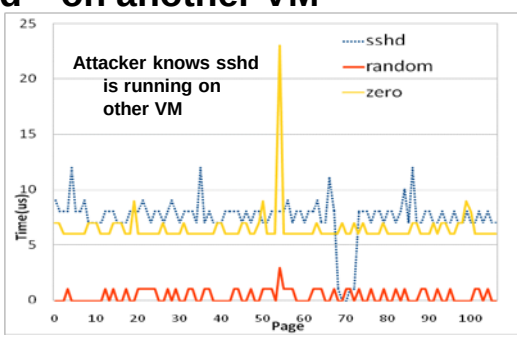
How to solve self-reflection problem



Example: Detect the presence of "sshd" on another VM



"sshd" is not running on victim VM



"sshd" is running on victim VM

Applications on multi-tenant cloud computing

Applicable by normal user or administrator.

1. Secret communication to other virtual machine for user-level optimization.
   - To prevent a conflict of interest on a processor, or to allocate VMs on same processor.
2. Detection of forbidden applications or unsecure applications.
3. To confirm erasure of important data from memory.