Cloud Security: The Malicious Insider Threat

Francisco Rocha

School of Computing Science
Newcastle University

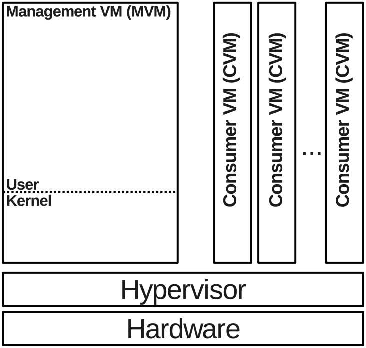
January 18, 2013

Outline

Outline

Terminology

- Consumer – cloud user, e.g., VM owner or cloud application developer.
- Hypervisor – virtualization layer, e.g., Xen Hypervisor.
- Management Virtual Machine (MVM) – administration tools (launch/destroy VMs), e.g., Xen's Dom0.
- Consumer Virtual Machine (CVM) – cloud consumer owned VM.



Outline

Malicious Insider Threat (1/2)

- **#3** in the Cloud Security Alliance (CSA) top threats list.
- Current studies focus on **consumer-side** and **co-residency** attacks.
- Biggest shift is having data processing/storage **entrusted** to a cloud provider.
- Companies holding **critical data** (e.g., medical data) want to use the cloud for data processing.
- What is the security impact of a malicious insider?

JULY 18, 2008

Why San Francisco's network admin went rogue

An inside source reveals details of missteps and misunderstandings in the curious case of Terry Childs, network kidnapper

By Paul Venezia | InfoWorld   Follow @infoworld

Malicious Insider Threat (2/2)

- Data processed in a cloud infrastructure is **not protected**, e.g., malicious insider can **compromise private keys**. (Rocha and Correia)
- Other attacks can be performed using virtual machine introspection. (Rocha, Gross, Van Moorsel)
- Cryptography on its own **is not enough**.
- Applicability of Fully Homomorphic Encryption (FHE).

Outline

Methodology

- Work environment using Xen 4.2 unstable source code and two consumer virtual machines.
- Verify if a VM's memory dump contains security sensitive data.
- Explore virtual machine introspection (VMI) (e.g., *libVMI* library).
- Use VMI as a malicious insider's attack tool against virtual machines' memory areas.
- Attack Xen's inter-virtual machine communication library (*libvchan*).
- Develop prevention techniques against known attacks.
- Verify if known attacks are no longer feasible.

Outline

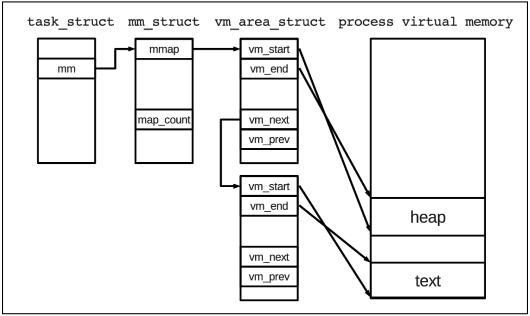
Access to Security Sensitive Data

- Recall *coldboot* attack (Princeton University).
- Plaintext passwords in memory (can be used in dictionary attacks).
- Compromised private keys in memory dump.
- It is as simply as running **two commands**.
- Used key search mechanism from *coldboot* attack.
- Obtained all the data stored in virtual disks.

Outline

VMI as an Attack Tool

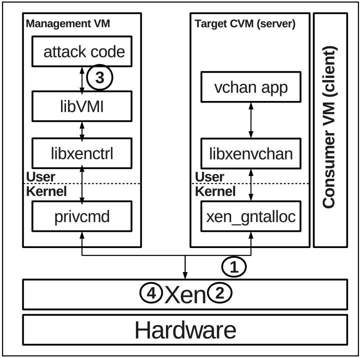
- Two consumer VMs (VMServer and VMClient) exchanging messages over an inter-VM channel.
- As root in the MVM, attack VMServer's memory to pinpoint *libvchan*'s data structure.
- Extract and monitor the shared memory location addresses.
- Result: compromised data confidentiality.



Outline

Secure Inter-VM Communication

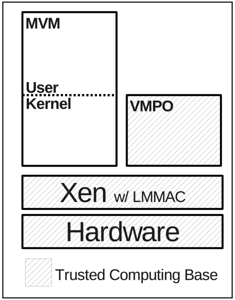
- Proof of concept for a more generic solution.
- (1) Change the kernel to send to Xen the used memory page.
- (2) Flag the memory page as inaccessible to MVM.
- (3) and (4) The attack code previously used receives a permission denied response from Xen.



Outline

LMMAC: Lightweight Mandatory Memory Access Control

- Generalize the secure inter-VM approach.
- Combines trusted computing base reduction with MAC.
- Access to a VM's special purpose pages required (e.g., load virtual firmware for HVM guests).
- Use the reference count in the memory pages to identify the special purpose pages.
- Flag all memory pages free for VM's usage as inaccessible to MVM.



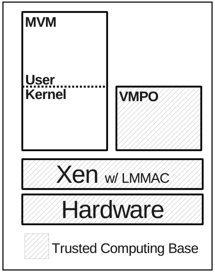
Outline

Discussion – LMMAC (1/2)

- Guarantees data **confidentiality** and **integrity** for consumer VM's memory.
- Uses two layers of protection TCB reduction and LMMAC.
- No need to load extra modules that might originate multiple executable files for Xen (FLASK/sHype).
- No mutable executable file, beneficial for use with trustworthy computing.
- No key management issues or overhead from encrypting memory pages before passing them to MVM (Chunxiao Li et al).

Discussion – LMMAC (2/2)

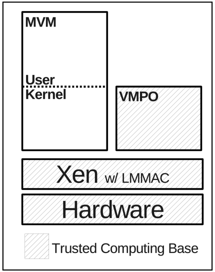
- Using special purpose VM to execute privileged operations.
- Reduced TCB when compared with previous work (Murray et al).
- Why? Xen is used as the policy decision and enforcement point.
- It will need a "micro TPM" similar to the one used by TrustVisor (McCune et al).
- vTPM (IBM) is vulnerable to TOCTOU attacks and it bloats the TCB.



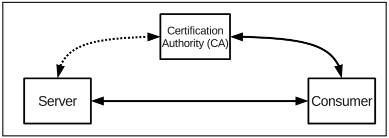
Outline

Secure Cloud Architecture (1/2)

- The architecture in the figure represents a single cloud server.
- Goals:
  - have all the servers with trustworthy computing support using the suggested architecture.
  - use remote attestation to verify a server's software integrity.
  - improve the granularity of components that can be measured.



Secure Cloud Architecture (1/2)



- 1. Server's TPM generates a AIK key pair and registers a certificate for the public AIK with a CA.
- 2. The consumer requests certificate from CA.
- 3. The consumer initiates remote attestation. Server's TPM signs a vector of PCRs with the private AIK and sends it to the consumer.
- 4. The consumer verifies if the signature is valid, and if the values in the PCRs match a trusted configurantion.

Outline

Conclusions

- Guarantees data **confidentiality** and **integrity** for a VM's memory space.
- Transparency for the consumer, i.e., attest remote operations.
- Brings the risk level closer to what is acceptable today for commodity systems.
- The consumer is left with trusting that the TCB is as free of vulnerabilities as it can be.

Thank you!

Questions?