Chapter 9 – Cloud Security

Contents

- Security in an interconnected world, cloud security risks.
- Attacks in a cloud environment, top threats.
- Security, a major concern for cloud users.
- Privacy.
- Trust.
- Operating systems security.
- Virtual machine security.
- Security of virtualization.
- Security risks posed by shared images.
- Security risks posed by a management OS.
- XOAR - breaking the monolithic design of TCB.
- Terra a trusted virtual machine monitor.

Computer security in the new millennium

- In an interconnected world, various embodiments of malware can migrate easily from one system to another, cross national borders and infect systems all over the globe.
- The security of computing and communication systems takes a new urgency as the society becomes increasingly more dependent on the information infrastructure. Even the critical infrastructure of a nation can be attacked by exploiting flaws in computer security.
- Recently, the term cyberwarfare has enter the dictionary meaning "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption"

Cloud security

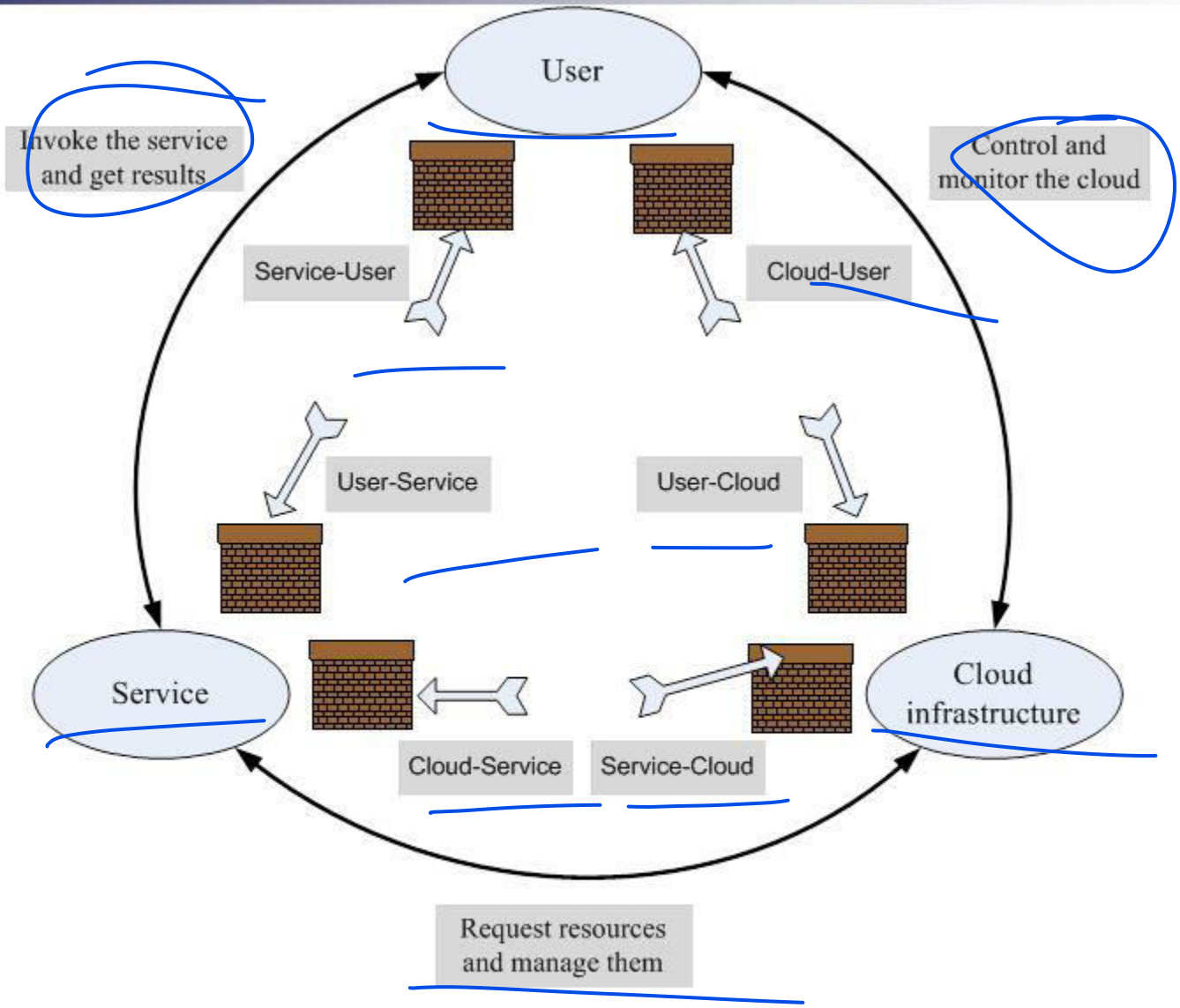
- A computer cloud is a target-rich environment for malicious individuals and criminal organizations.
- Major concern for existing users and for potential new users of cloud computing services. Outsourcing computing to a cloud generates new security and privacy concerns.
- Standards, regulations, and laws governing the activities of organizations supporting cloud computing have yet to be adopted. Many issues related to privacy, security, and trust in cloud computing are far from being settled.
- There is the need for international regulations adopted by the countries where data centers of cloud computing providers are located.
- Service Level Agreements (SLAs) do not provide adequate legal protection for cloud computer users, often left to deal with events beyond their control.

Cloud security risks

- Traditional threats → impact amplified due to the vast amount of cloud resources and the large user population that can be affected. The fuzzy bounds of responsibility between the providers of cloud services and users and the difficulties to accurately identify the cause.
- New threats → cloud servers host multiple VMs; multiple applications may run under each VM. Multi-tenancy and VMM vulnerabilities open new attack channels for malicious users. Identifying the path followed by an attacker more difficult in a cloud environment.
- Authentication and authorization → the procedures in place for one individual does not extend to an enterprise.
- Third-party control → generates a spectrum of concerns caused by the lack of transparency and limited user control.
- Availability of cloud services → system failures, power outages, and other catastrophic events could shutdown services for extended periods of time.

Attacks in a cloud computing environment

- Three actors involved; six types of attacks possible.
  - The user can be attacked by:
    - Service → SSL certificate spoofing, attacks on browser caches, or phishing attacks.
    - The cloud infrastructure → attacks that either originates at the cloud or spoofs to originate from the cloud infrastructure.
  - The service can be attacked by:
    - A user→ buffer overflow, SQL injection, and privilege escalation are the common types of attacks.
    - The cloud infrastructure → the most serious line of attack. Limiting access to resources, privilege-related attacks, data distortion, injecting additional operations.
  - The cloud infrastructure can be attacked by:
    - A user → targets the cloud control system.
    - A service → requesting an excessive amount of resources and causing the exhaustion of the resources.



Surfaces of attacks in a cloud computing environment.

Top threats to cloud computing

- Identified by a 2010 Cloud Security Alliance (CSA) report:
  - The abusive use of the cloud - the ability to conduct nefarious activities from the cloud.
  - APIs that are not fully secure - may not protect the users during a range of activities starting with authentication and access control to monitoring and control of the application during runtime.
  - Malicious insiders - cloud service providers do not disclose their hiring standards and policies, so this can be a serious threat.
  - Shared technology.
  - Account hijacking.
  - Data loss or leakage - if the only copy of the data is stored on the cloud, then sensitive data is permanently lost when cloud data replication fails followed by a storage media failure.
  - Unknown risk profile - exposure to the ignorance or underestimation of the risks of cloud computing.

Auditability of cloud activities

- The lack of transparency makes auditability a very difficult proposition for cloud computing.
- Auditing guidelines elaborated by the National Institute of Standards (NIST) are mandatory for US Government agencies:
  - the Federal Information Processing Standard (FIPS).
  - the Federal Information Security Management Act (FISMA).

Security - the top concern for cloud users

- The unauthorized access to confidential information and the data theft top the list of user concerns.
  - Data is more vulnerable in storage, as it is kept in storage for extended periods of time.
  - Threats during processing cannot be ignored; such threats can originate from flaws in the VMM, rogue VMs, or a VMBR.
- There is the risk of unauthorized access and data theft posed by rogue employees of a Cloud Service Provider (CSP).
- Lack of standardization is also a major concern.
- Users are concerned about the legal framework for enforcing cloud computing security.
- Multi-tenancy is the root cause of many user concerns. Nevertheless, multi-tenancy enables a higher server utilization, thus lower costs.
- The threats caused by multi-tenancy differ from one cloud delivery model to another.

Legal protection of cloud users

- The contract between the user and the Cloud Service Provider (CSP) should spell out explicitly:
  - CSP obligations to handle securely sensitive information and its obligation to comply to privacy laws.
  - CSP liabilities for mishandling sensitive information.
  - CSP liabilities for data loss.
  - The rules governing ownership of the data.
  - The geographical regions where information and backups can be stored.

Privacy

- Privacy ➔ the right of an individual, a group of individuals, or an organization to keep information of personal nature or proprietary information from being disclosed.
- Privacy is protected by law; sometimes laws limit privacy.
- The main aspects of privacy are: the lack of user control, potential unauthorized secondary use, data proliferation, and dynamic provisioning.
- Digital age has confronted legislators with significant challenges related to privacy as new threats have emerged. For example, personal information voluntarily shared, but stolen from sites granted access to it or misused can lead to identity theft.
- Privacy concerns are different for the three cloud delivery models and also depend on the actual context.

Federal Trading Commission Rules

- Web sites that collect personal identifying information from or about consumers online required to comply with four fair information practices:
  - Notice - provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it, how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.
  - Choice - offer consumers choices as to how their personal identifying information is used. Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).
  - Access - offer consumers reasonable access to the information a web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.
  - Security - take reasonable steps to protect the security of the information they collect from consumers.

Privacy Impact Assessment (PIA)

- The need for tools capable to identify privacy issues in information systems.
- There are no international standards for such a process, though different countries and organization require PIA reports.
- The centerpiece of A proposed PIA tool is based on a SaaS service.
  - The users of the SaaS service providing access to the PIA tool must fill in a questionnaire.
  - The system used a knowledge base (KB) created and maintained by domain experts.
  - The system uses templates to generate additional questions necessary and to fill in the PIA report.
  - An expert system infers which rules are satisfied by the facts in the database and provided by the users and executes the rule with the highest priority.

Trust

- Trust → assured reliance on the character, ability, strength, or truth of someone or something.
- Complex phenomena: enable cooperative behavior, promote adaptive organizational forms, reduce harmful conflict, decrease transaction costs, promote effective responses to crisis.
- Two conditions must exist for trust to develop.
  - Risk → the perceived probability of loss; trust not necessary if there is no risk involved, if there is a certainty that an action can succeed.
  - Interdependence → the interests of one entity cannot be archived without reliance on other entities.
- A trust relationship goes though three phases:
  1. Building phase, when trust is formed.
  2. Stability phase, when trust exists.
  3. Dissolution phase, when trust declines.
- An entity must work very hard to build trust, but may lose the trust very easily.

Internet trust

- Obscures or lacks entirely the dimensions of character and personality, nature of relationship, and institutional character of the traditional trust.
- Offers individuals the ability to obscure or conceal their identity. The anonymity reduces the cues normally used in judgments of trust.
- Identity is critical for developing trust relations, it allows us to base our trust on the past history of interactions with an entity. Anonymity causes mistrust because identity is associated with accountability and in absence of identity accountability cannot be enforced.
- The opacity extends identity to personal characteristics. It is impossible to infer if the entity or individual we transact with is who it pretends to be, as the transactions occur between entities separated in time and distance.
- There are no guarantees that the entities we transact with fully understand the role they have assumed.

How to determine trust

- Policies and reputation are two ways of determining trust.
  - Policies reveal the conditions to obtain trust, and the actions when some of the conditions are met. Policies require the verification of credentials; credentials are issued by a trusted authority and describe the qualities of the entity using the credential.
  - Reputation is a quality attributed to an entity based on a relatively long history of interactions or possibly observations of the entity. Recommendations are based on trust decisions made by others and filtered through the perspective of the entity assessing the trust.
- In a computer science context : trust of a party A to a party B for a service X is the measurable belief of A in that B behaves dependably for a specified period within a specified context (in relation to service X).

Operating system security

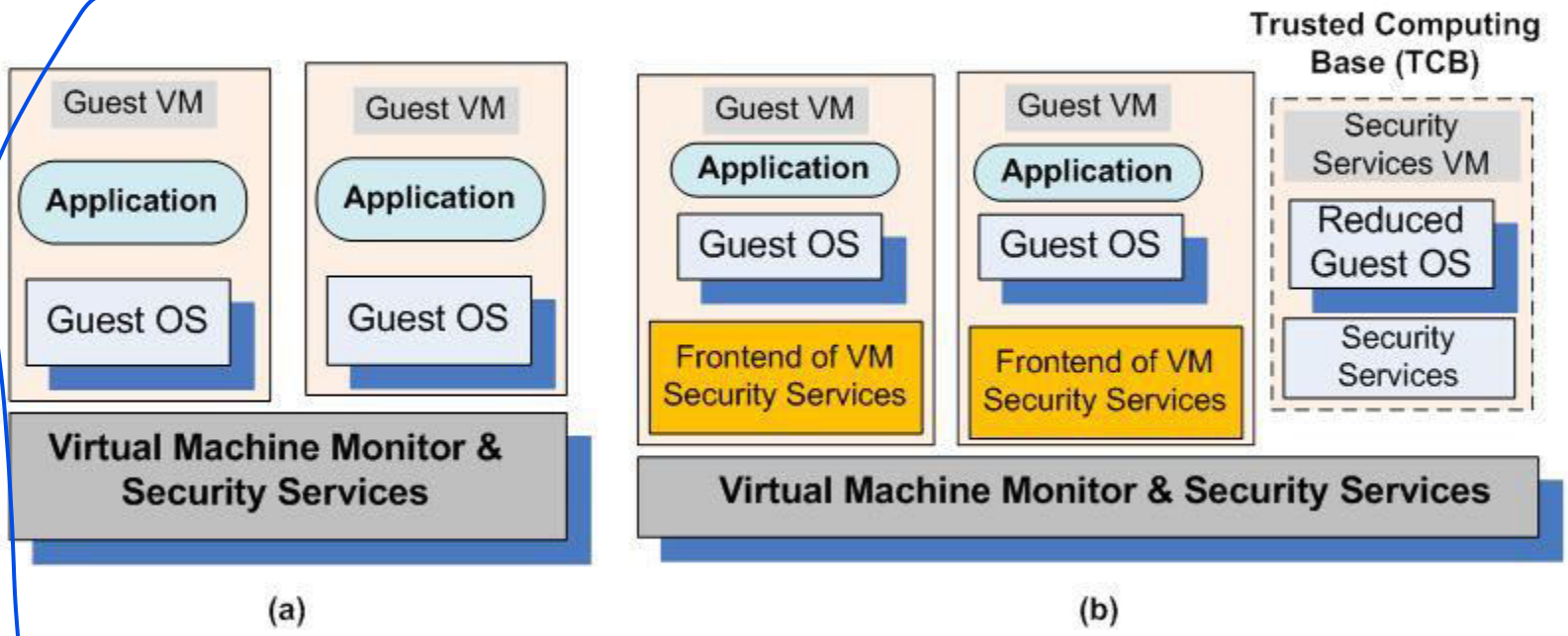
- A critical function of an OS is to protect applications against a wide range of malicious attacks, e.g., unauthorized access to privileged information, tempering with executable code, and spoofing.
- The elements of the mandatory OS security:
  - Access control → mechanisms to control the access to system objects.
  - Authentication usage → mechanisms to authenticate a principal.
  - Cryptographic usage policies → mechanisms used to protect the data
- Commercial OS do not support a multi-layered security; only distinguish between a completely privileged security domain and a completely unprivileged one.
- Trusted paths mechanisms → support user interactions with trusted software. Critical for system security; if such mechanisms do not exist, then malicious software can impersonate trusted software. Some systems provide trust paths for a few functions, such as login authentication and password changing, and allow servers to authenticate their clients.

Closed-box versus open-box platforms

- Closed-box platforms , e.g., cellular phones, game consoles and ATM could have embedded cryptographic keys to reveal their true identity to remote systems and authenticate the software running on them.
- Such facilities are not available to open-box platforms, the traditional hardware for commodity operating systems.
- Commodity operating system offer low assurance. An OS is a complex software system consisting of millions of lines of code and it is vulnerable to a wide range of malicious attacks.
- An OS provides weak mechanisms for applications to authenticate to one another and create a trusted path between users and applications.
- An OS poorly isolates one application from another; once an application is compromised, the entire physical platform and all applications running on it can be affected. The platform security level is reduced to the security level of the most vulnerable application running on the platform.

Virtual machine security

- Hybrid and hosted VMs, expose the entire system to the vulnerability of the host OS.
- In a traditional VM the Virtual Machine Monitor (VMM) controls the access to the hardware and provides a stricter isolation of VMs from one another than the isolation of processes in a traditional OS.
  - A VMM controls the execution of privileged operations and can enforce memory isolation as well as disk and network access.
  - The VMMs are considerably less complex and better structured than traditional operating systems thus, in a better position to respond to security attacks.
  - A major challenge → a VMM sees only raw data regarding the state of a guest operating system while security services typically operate at a higher logical level, e.g., at the level of a file rather than a disk block.
- A secure TCB (Trusted Computing Base) is a necessary condition for security in a virtual machine environment; if the TCB is compromised then the security of the entire system is affected.



(a) Virtual security services provided by the VMM; (b) A dedicated security VM.

VMM-based threats

- Starvation of resources and denial of service for some VMs. Probable causes:
  - (a) badly configured resource limits for some VMs.
  - (b) a rogue VM with the capability to bypass resource limits set in VMM.
- VM side-channel attacks: malicious attack on one or more VMs by a rogue VM under the same VMM. Probable causes:
  - (a) lack of proper isolation of inter-VM traffic due to misconfiguration of the virtual network residing in the VMM.
  - (b) limitation of packet inspection devices to handle high speed traffic, e.g., video traffic.
  - (c) presence of VM instances built from insecure VM images, e.g., a VM image having a guest OS without the latest patches.
- Buffer overflow attacks.

VM-based threats

- Deployment of rogue or insecure VM. Unauthorized users may create insecure instances from images or may perform unauthorized administrative actions on existing VMs.
  Probable cause:
  - improper configuration of access controls on VM administrative tasks such as instance creation, launching, suspension, re-activation and so on.
- Presence of insecure and tampered VM images in the VM image repository. Probable causes:
  - (a) lack of access control to the VM image repository.
  - (b) lack of mechanisms to verify the integrity of the images, e.g., digitally signed image.

Security of virtualization

- The complete state of an operating system running under a virtual machine is captured by the VM; this state can be saved in a file and then the file can be copied and shared. Implications:
  - Ability to support the IaaS delivery model. In this model a user selects an image matching the local environment used by the application and then uploads and runs the application on the cloud using this image.
  - Increased reliability. An operating system with all the applications running under it can be replicated and switched to a hot standby.
  - Improved intrusion prevention and detection. A clone can look for known patterns in system activity and detect intrusion. The operator can switch to a hot standby when suspicious events are detected.
  - More efficient and flexible software testing. Instead of a very large number of dedicated systems running under different OS, different version of each OS, and different patches for each version, virtualization allows the multitude of OS instances to share a small number of physical systems.

More advantages of virtualization

- Straightforward mechanisms to implement resource management policies:
  - To balance the load of a system, a VMM can move an OS and the applications running under it to another server when the load on the current server exceeds a high water mark.
  - To reduce power consumption, the load of lightly loaded servers can be moved to other servers and then, turn off or set on standby mode the lightly loaded servers.
- When secure logging and intrusion protection are implemented at the VMM layer, the services cannot be disabled or modified. Intrusion detection can be disabled and logging can be modified by an intruder when implemented at the OS level. A VMM may be able to log only events of interest for a post-attack analysis.

Undesirable effects of virtualization

- Diminished ability to manage the systems and track their status.
  - The number of physical systems in the inventory of an organization is limited by cost, space, energy consumption, and human support. Creating a virtual machine (VM) reduces ultimately to copying a file, therefore the explosion of the number of VMs. The only limitation for the number of VMs is the amount of storage space available.
  - Qualitative aspect of the explosion of the number of VMs → traditionally, organizations install and maintain the same version of system software. In a virtual environment the number of different operating systems, their versions, and the patch status of each version will be very diverse. Heterogeneity will tax the support team.
  - The software lifecycle has serious implication on security. The traditional assumption → the software lifecycle is a straight line, hence the patch management is based on a monotonic forward progress. The virtual execution model maps to a tree structure rather than a line; indeed, at any point in time multiple instances of the VM can be created and then, each one of them can be updated, different patches installed, and so on.

Implications of virtualization on security

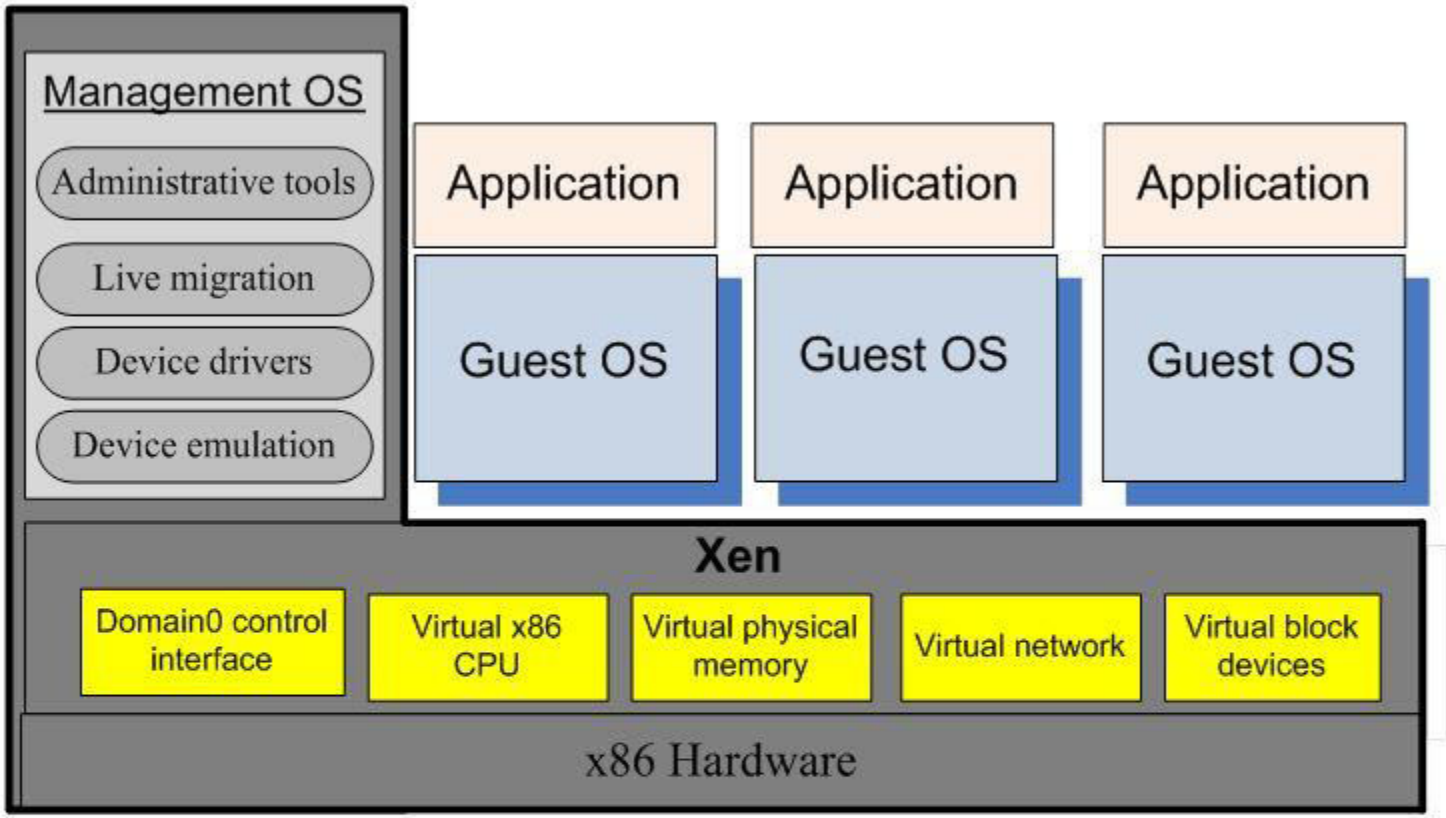
- Infection may last indefinitely → some of the infected VMs may be dormant at the time when the measures to clean up the systems are taken and then, at a later time, wake up and infect other systems; the scenario can repeat itself.
- In a traditional computing environment a steady state can be reached. In this steady state all systems are brought up to a desirable state. This desirable state is reached by installing the latest version of the system software and then applying to all systems the latest patches. Due to the lack of control, a virtual environment may never reach such a steady state.
- A side effect of the ability to record in a file the complete state of a VM is the possibility to roll back a VM. This allows a new type of vulnerability caused by events recorded in the memory of an attacker.
- Virtualization undermines the basic principle that time sensitive data stored on any system should be reduced to a minimum.

Security risks posed by shared images

- Image sharing is critical for the IaaS cloud delivery model. For example, a user of AWS has the option to choose between
  - Amazon Machine Images (AMIs) accessible through the Quick Start.
  - Community AMI menus of the EC2 service.
- Many of the images analyzed by a recent report allowed a user to undelete files, recover credentials, private keys, or other types of sensitive information with little effort and using standard tools.
- A software vulnerability audit revealed that 98% of the Windows AMIs and 58% of Linux AMIs audited had critical vulnerabilities.
- Security risks:
  - Backdoors and leftover credentials.
  - Unsolicited connections.
  - Malware.

Security risks posed by a management OS

- A virtual machine monitor, or hypervisor, is considerably smaller than an operating system, e.g., the Xen VMM has ~ 60,000 lines of code.
- The Trusted Computer Base (TCB) of a cloud computing environment includes not only the hypervisor but also the management OS.
- The management OS supports administrative tools, live migration, device drivers, and device emulators.
- In Xen the management operating system runs in Dom0; it manages the building of all user domains, a process consisting of several steps:
  - Allocate memory in the Dom0 address space and load the kernel of the guest operating system from the secondary storage.
  - Allocate memory for the new VM and use foreign mapping to load the kernel to the new VM.
  - Set up the initial page tables for the new VM.
  - Release the foreign mapping on the new VM memory, set up the virtual CPU registers and launch the new VM.



The trusted computing base of a Xen-based environment includes the hardware, Xen, and the management operating system running in Dom0. The management OS supports administrative tools, live migration, device drivers, and device emulators. A guest operating system and applications running under it reside in a DomU.

Possible actions of a malicious Dom0

- At the time it creates a DomU:
  - Refuse to carry out the steps necessary to start the new VM.
  - Modify the kernel of the guest OS to allow a third party to monitor and control the execution of applications running under the new VM.
  - Undermine the integrity of the new VM by setting the wrong page tables and/or setup wrong virtual CPU registers.
  - Refuse to release the foreign mapping and access the memory while the new VM is running.
- At run time:
  - Dom0 exposes a set of abstract devices to the guest operating systems using split drivers with the frontend of in a DomU and the backend in Dom0. We have to ensure that run time communication through Dom0 is encrypted. Transport Layer Security (TLS) does not guarantee that Dom0 cannot extract cryptographic keys from the memory of the OS and applications running in DomU

A major weakness of Xen

- The entire state of the system is maintained by XenStore.
- A malicious VM can deny to other VMs access to XenStore; it can also gain access to the memory of a DomU.

How to deal with run-time vulnerability of Dom0

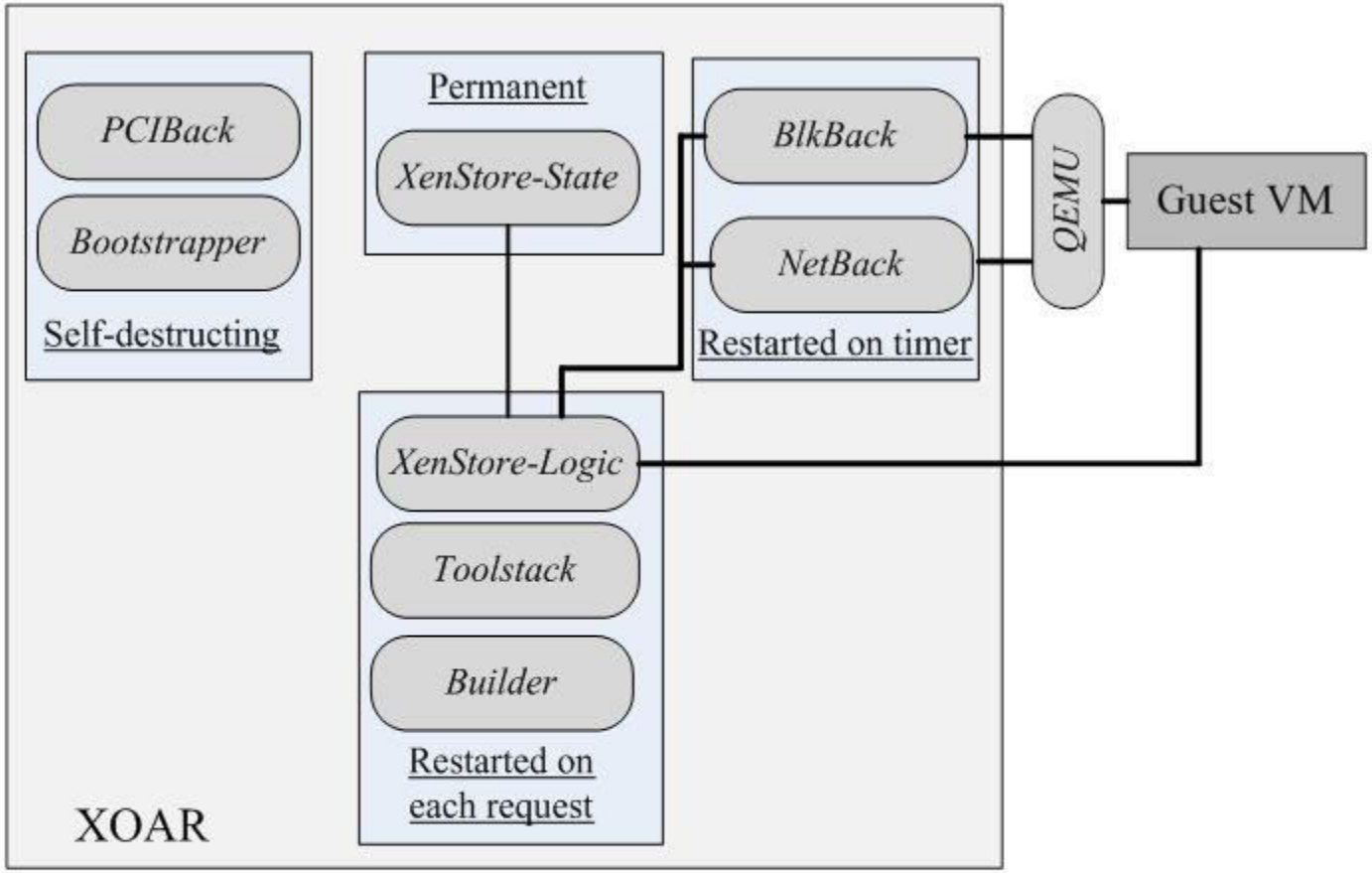
- To implement a secure run-time system, we have to intercept and control the hypercalls used for communication between a Dom0 that cannot be trusted and a DomU we want to protect.
- New hypercalls are necessary to protect:
  - The privacy and integrity of the virtual CPU of a VM. When Dom0 wants to save the state of the VM the hypercall should be intercepted and the contents of the virtual CPU registers should be encrypted. When DomU is restored, the virtual CPU context should be decrypted and then an integrity check should be carried out.
  - The privacy and integrity of the VM virtual memory. The page table update hypercall should be intercepted and the page should be encrypted so that Dom0 handles only encrypted pages of the VM. To guarantee the integrity, the hypervisor should calculate a hash of all the memory pages before they are saved by Dom0. An address translation is necessary as a restored DomU may be allocated a different memory region.
  - The freshness of the virtual CPU and the memory of the VM. The solution is to add to the hash a version number.

Xoar - breaking the monolithic design of TCB

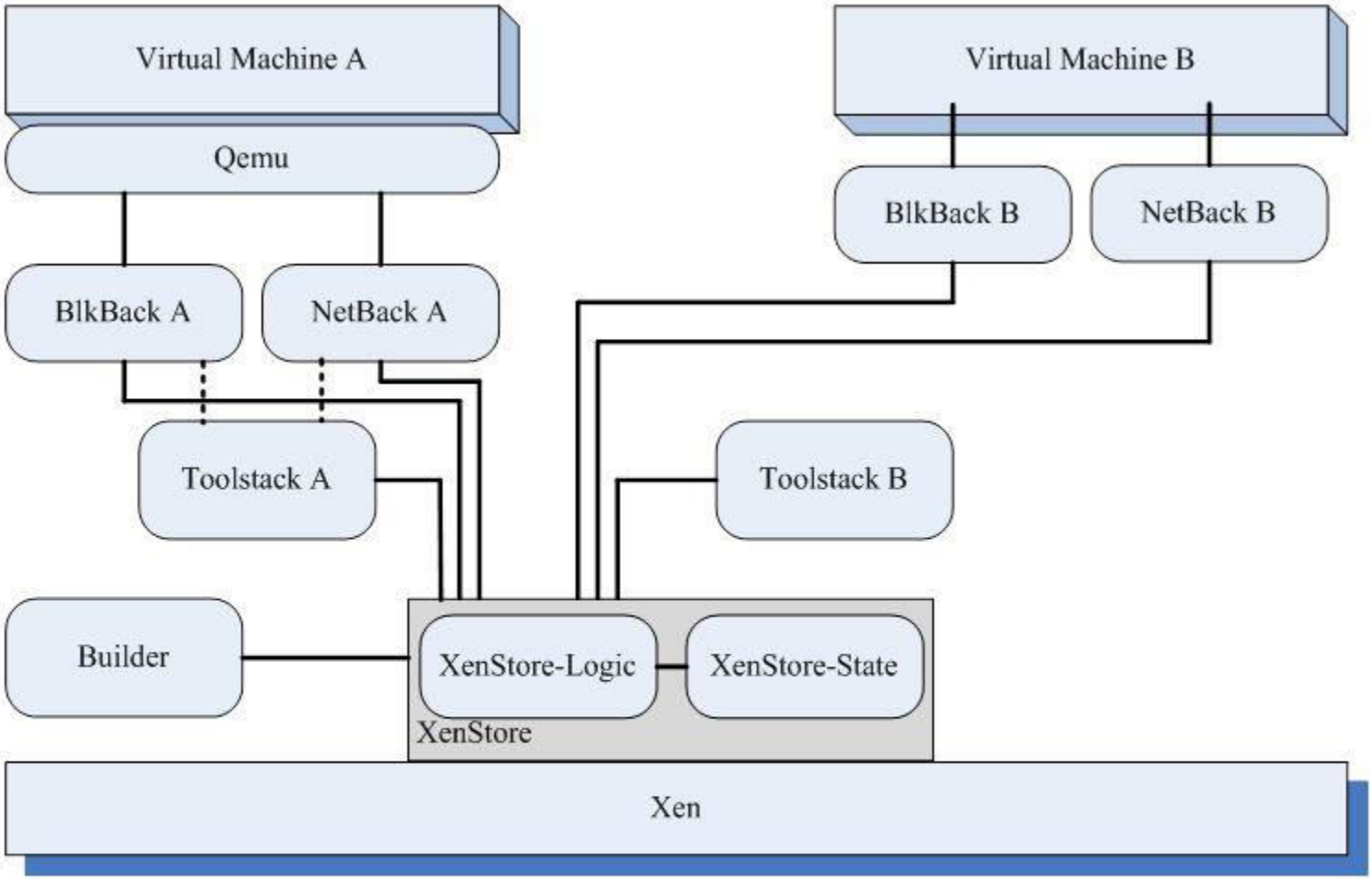
- Xoar is a version of Xen designed to boost system security; based on micro-kernel design principles. The design goals are:
  - Maintain the functionality provided by Xen.
  - Ensure transparency with existing management and VM interfaces.
  - Tight control of privileges, each component should only have the privileges required by its function.
  - Minimize the interfaces of all components to reduce the possibility that a component can be used by an attacker.
  - Eliminate sharing. Make sharing explicit whenever it cannot be eliminated to allow meaningful logging and auditing.
  - Reduce the opportunity of an attack targeting a system component by limiting the time window when the component runs.
- The security model of Xoar assumes that threats come from:
  - A guest VM attempting to violate data integrity or confidentiality of another guest VM on the same platform, or to exploit the code of the guest.
  - Bugs in the initialization code of the management virtual machine.

Xoar system components

- Permanent components → XenStore-State maintains all information regarding the state of the system.
- Components used to boot the system; they self-destruct before any user VM is started. They discover the hardware configuration of the server including the PCI drivers and then boot the system:
  - PCIBack - virtualizes access to PCI bus configuration.
  - Bootstrapper - coordinates booting of the system.
- Components restarted on each request:
  - XenStore-Logic.
  - Toolstack - handles VM management requests, e.g., it requests the Builder to create a new guest VM in response to a user request.
  - Builder - initiates user VMs.
- Components restarted on a timer; the two components export physical storage device drivers and the physical network driver to a guest VM.
  - Blk-Back - exports physical storage device drivers using udev rules.
  - NetBack - exports the physical network driver.



Xoar has nine classes of components of four types: permanent, self-destructing, restarted upon request, and restarted on timer. A guest VM is started using the by the Builder using the Toolstack; it is controlled by the XenStore-Logic. The devices used by the guest VM are emulated by the Qemu component. Qemu is responsible for device emulation



Component sharing between guest VMs in Xoar. Two VMs share only the XenStore components. Each one has a private version of the BlkBack, NetBack and Toolstack.

Terra - a trusted virtual machine monitor

- Novel ideas for a trusted virtual machine monitor (TVMM):
  - It should support not only traditional operating systems, by exporting the hardware abstraction for open-box platforms, but also the abstractions for closed-box platforms (do not allow the contents of the system to be either manipulated or inspected by the platform owner).
  - An application should be allowed to build its software stack based on its needs. Applications requiring a very high level of security should run under a very thin OS supporting only the functionality required by the application and the ability to boot. At the other end of the spectrum are applications demanding low assurance, but a rich set of OS features; such applications need a commodity operating system.
  - Provide trusted paths from a user to an application. Such a path allows a human user to determine with certainty the identity of the VM it is interacting with and allows the VM to verify the identity of the human user.
  - Deny the platform administrator the root access.
  - Support attestation, the ability of an application running in a closed-box to gain trust from a remote party, by cryptographically identifying itself.