Cloud Security

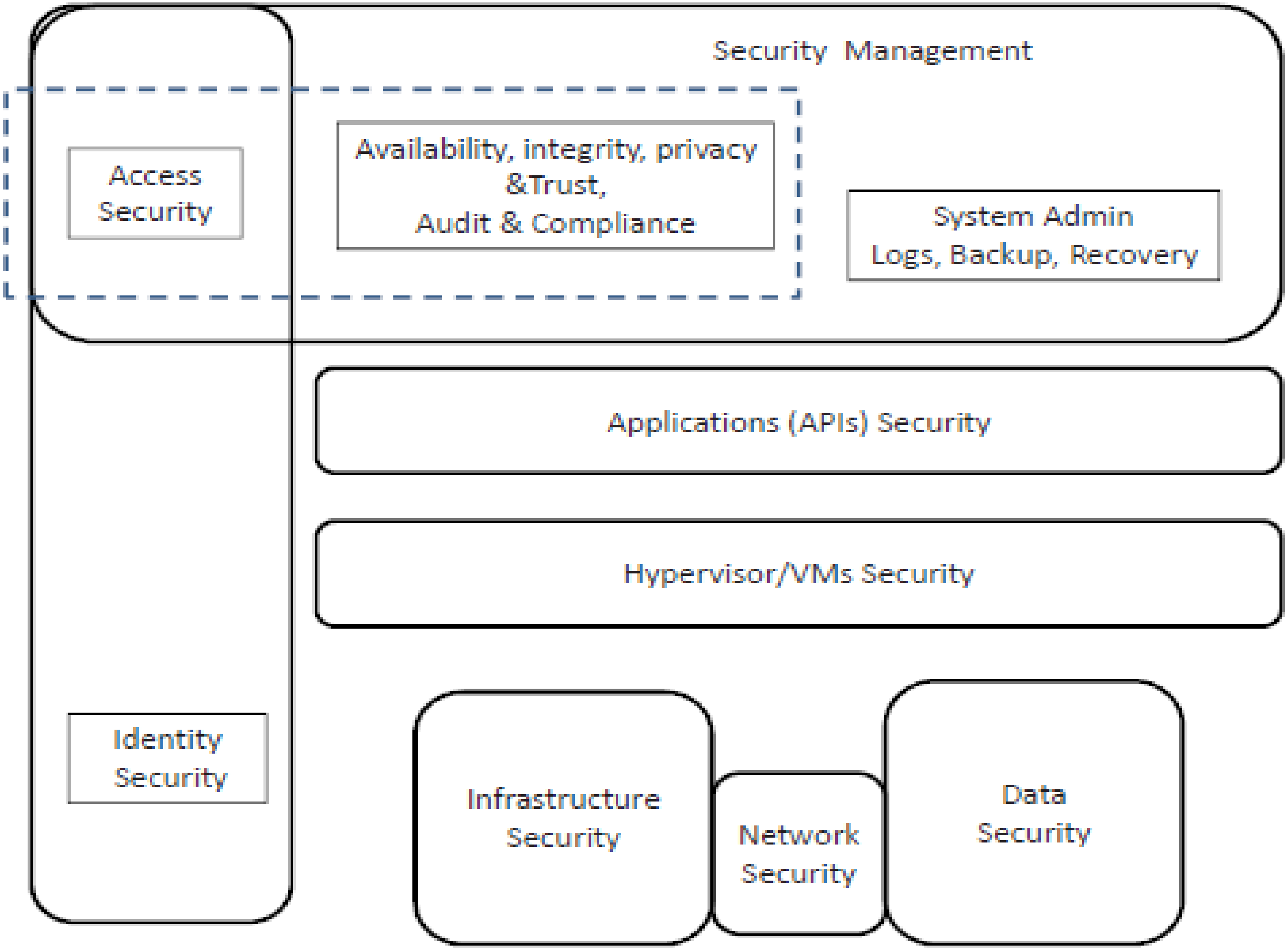
ACKNOWLEDGEMENTS

- This presentation has been made from various sources with minimum modifications from the presenter.
- The presenter is grateful to the authors of those various sources.
- The presenter acknowledge the efforts of those authors and thank them wholeheartedly.

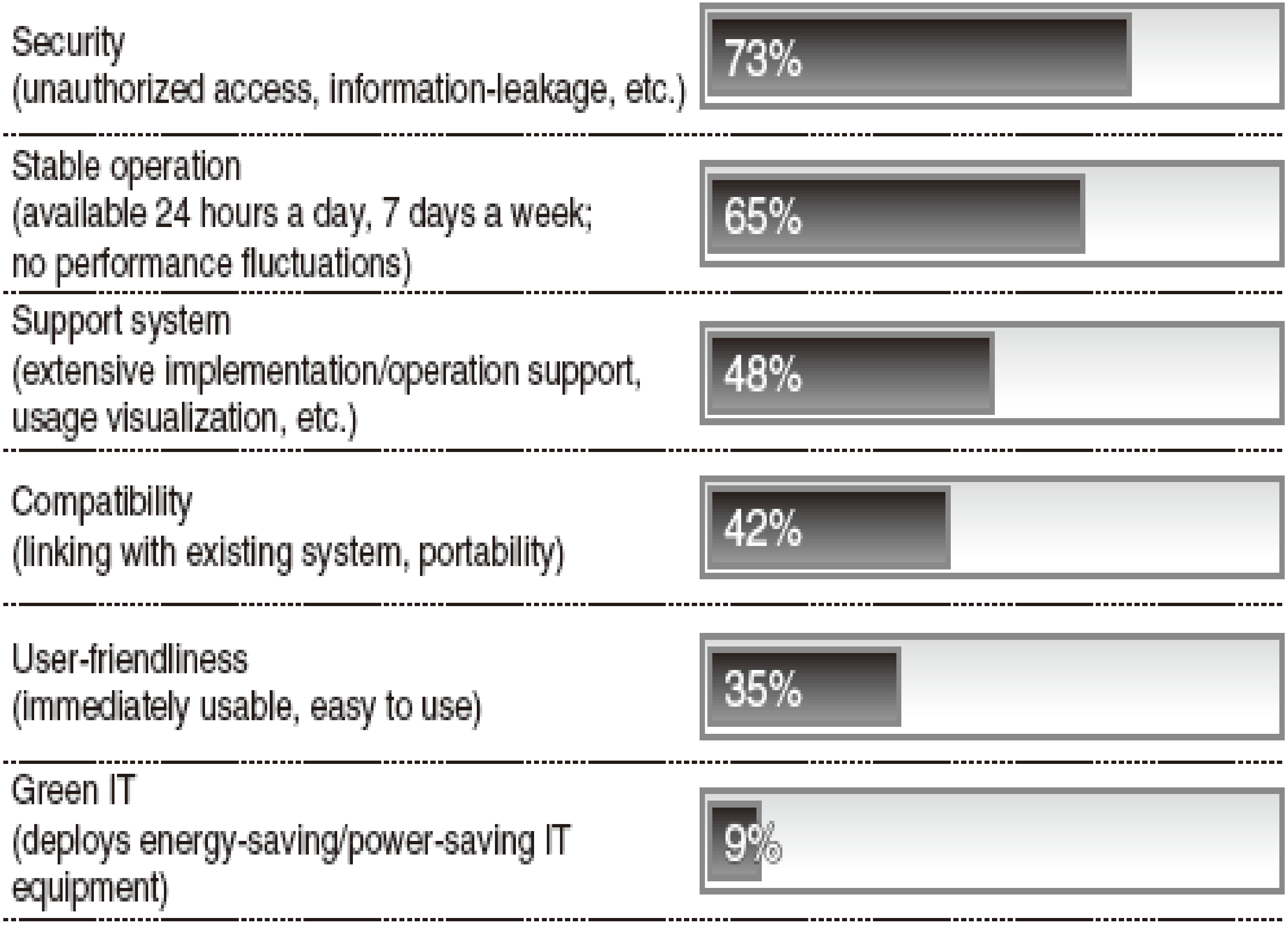
Cloud security

- Target-rich environment for malicious individuals and criminal organizations
- Major concern for existing users and for potential new users of cloud computing services.
- Standards, regulations, and laws governing the activities of organizations supporting cloud computing have yet to be adopted
  - There is the need for international regulations
- Service Level Agreements (SLAs) do not provide adequate legal protection

Cloud Security Architecture

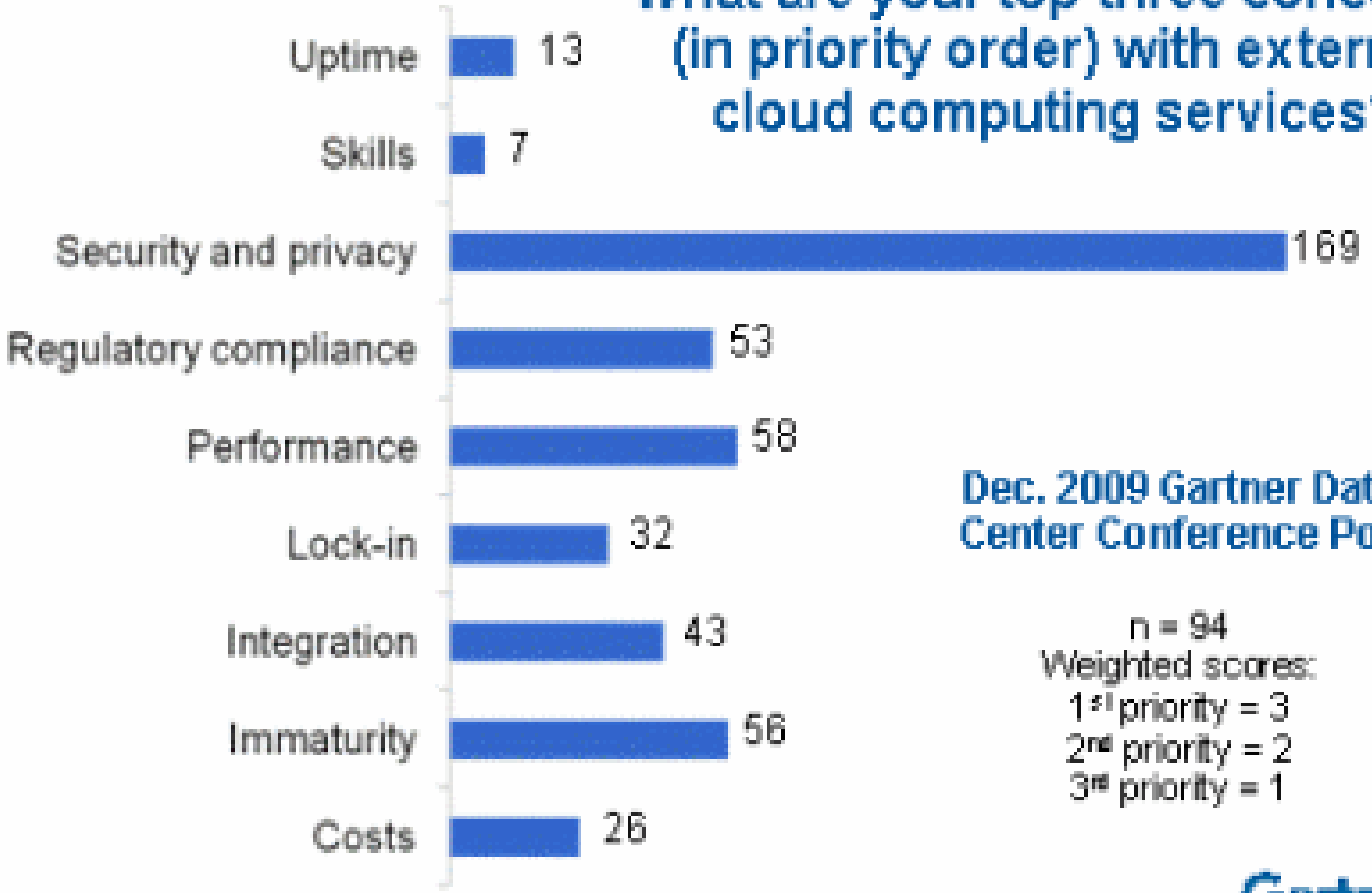


Cloud Computing Concerns (fujitsu-2009)



Concerns With Public Cloud Computing

What are your top three concerns (in priority order) with external cloud computing services?

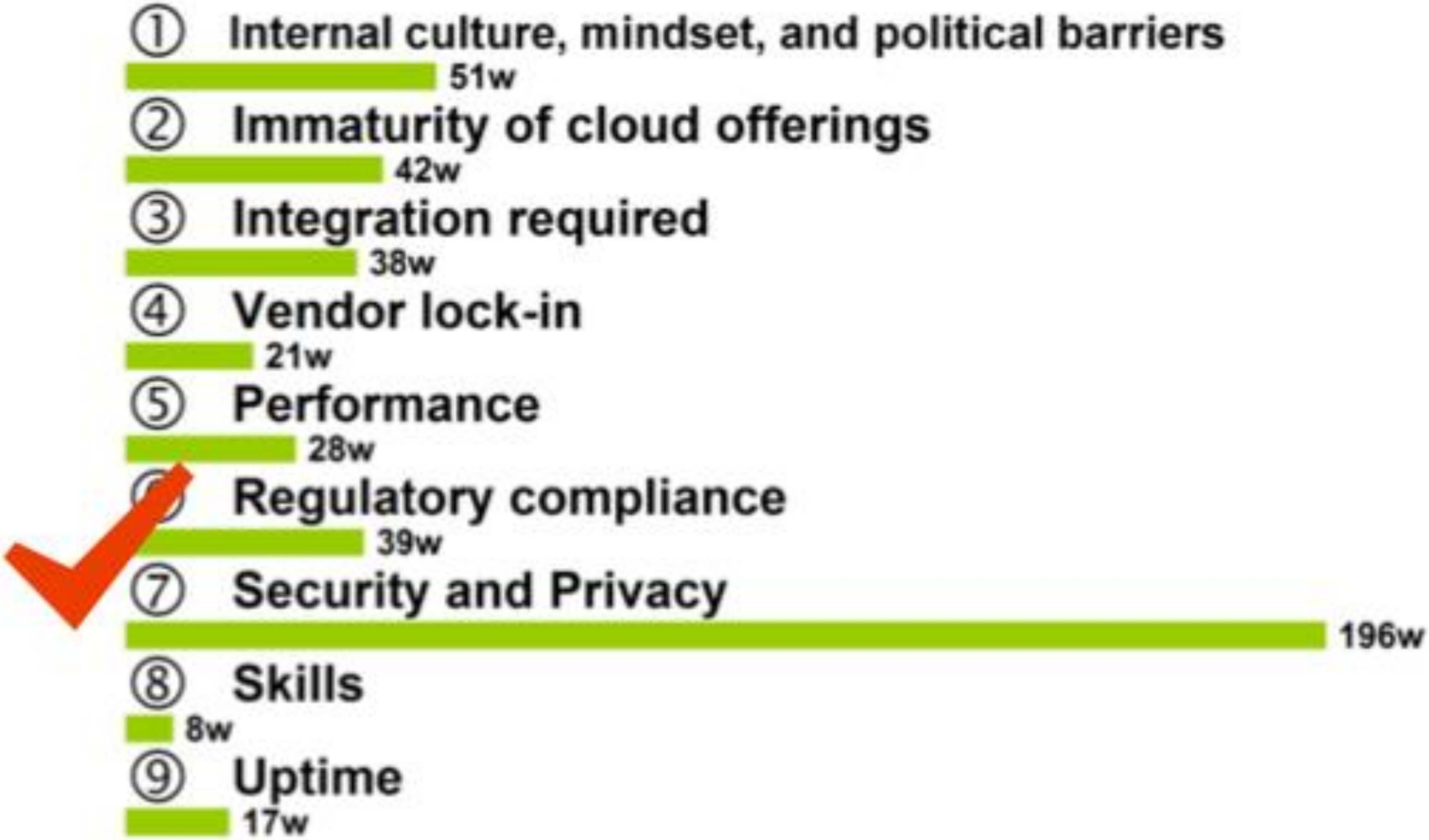


Dec. 2009 Gartner Data Center Conference Poll

n = 94
Weighted scores:
1st priority = 3
2nd priority = 2
3rd priority = 1

Gartner.

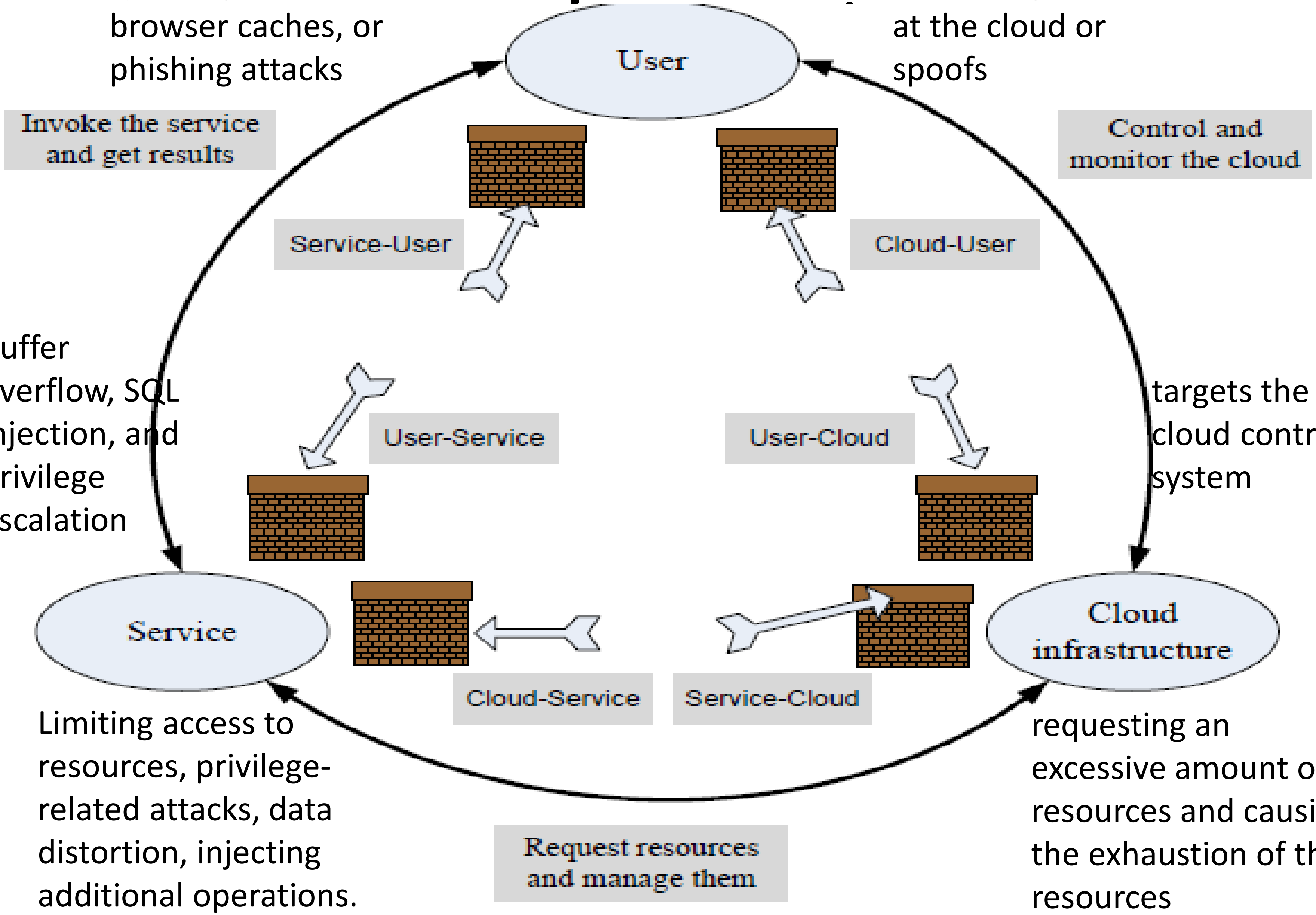
What Are Your Top Three Issues With Public Cloud Computing in Rank Order?



Cloud Security Risks

- Traditional threats
- New threats
- Authentication and authorization
- Third-party control
- Availability of cloud services

Attacks in a cloud computing



SSL certificate spoofing, attacks on browser caches, or phishing attacks

attacks that either originates at the cloud or spoofs

buffer overflow, SQL injection, and privilege escalation

targets the cloud control system

Limiting access to resources, privilege-related attacks, data distortion, injecting additional operations.

requesting an excessive amount of resources and causing the exhaustion of the resources

Cloud Security Alliance: Top Threats

- Abuse and nefarious use of cloud computing
- Insecure interfaces and APIs
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Account or service hijacking
- Unknown risk profile

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).

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.

Security Challenges – User Perspective

- Privileged user access
- Regulatory compliance.
- Data location
- Data segregation
- Investigative support
- Long-term viability

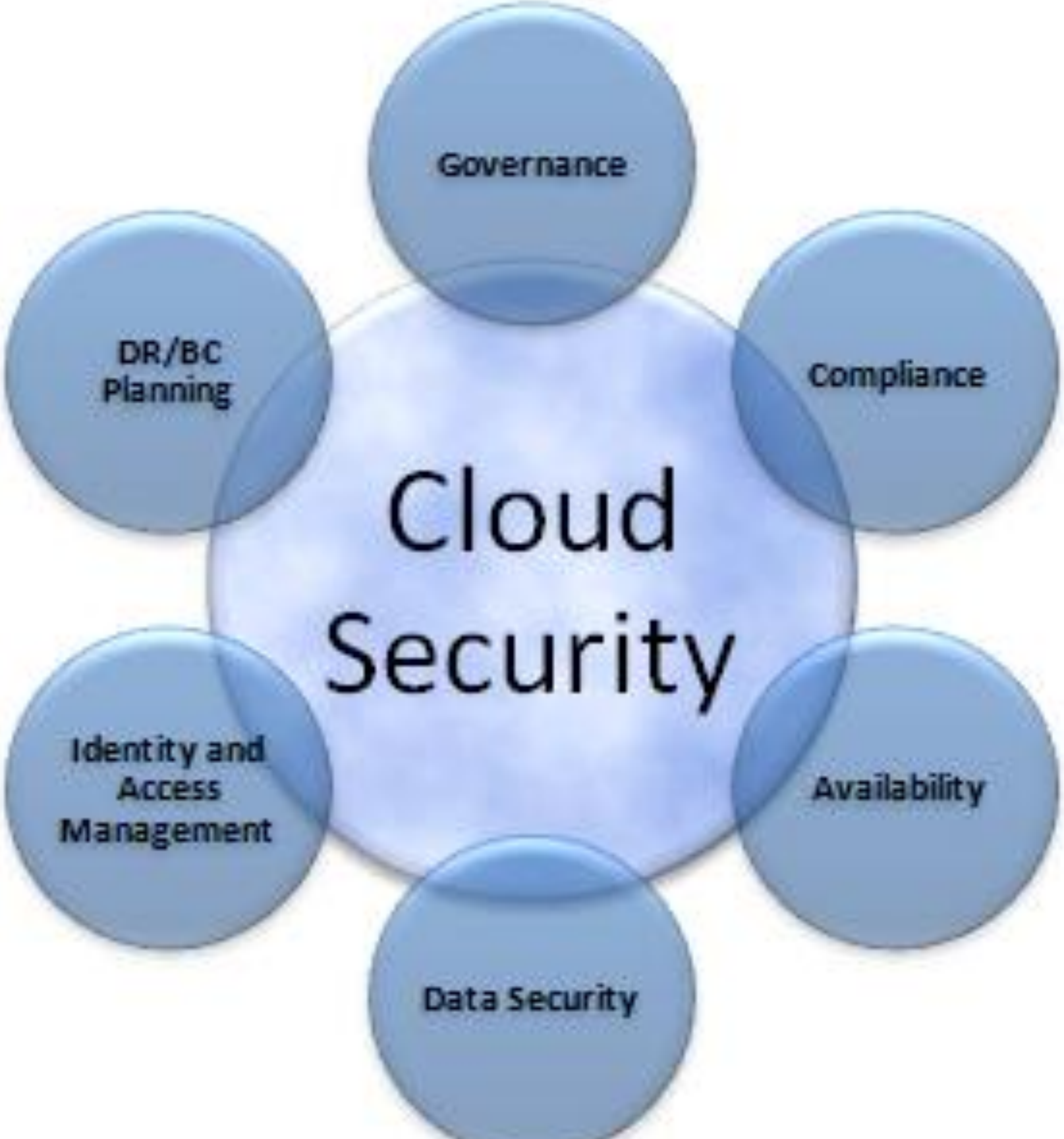
Privacy

- 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, p
  - 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
  - Choice
  - Access
  - Security

Secured Cloud



http://maintec.com/blog/find-your-way-to-secure-cloud-part-2/

Governance

- Jurisdiction and regulatory requirements
- Complying with Export/Import controls
- Compliance of the infrastructure
- Audit and reporting

Data

- Data location and segregation
- Data footprints
- Backup and recovery
- Administration

Architecture

- Protection
- Hypervisor vulnerabilities
- Multi-tenant environments
- Security policies
- Identity Management

Application

- Software Vulnerabilities
- Patch management
- Application devices

Assurance

- Assurance
- Operational oversight
- Audit and assurance
- Investigating an incident
- Experience of new cloud providers

Cloud Security Requirements

- Confidentiality
- Integrity
- Availability
- Privacy
- Trust
- Audit and Compliance

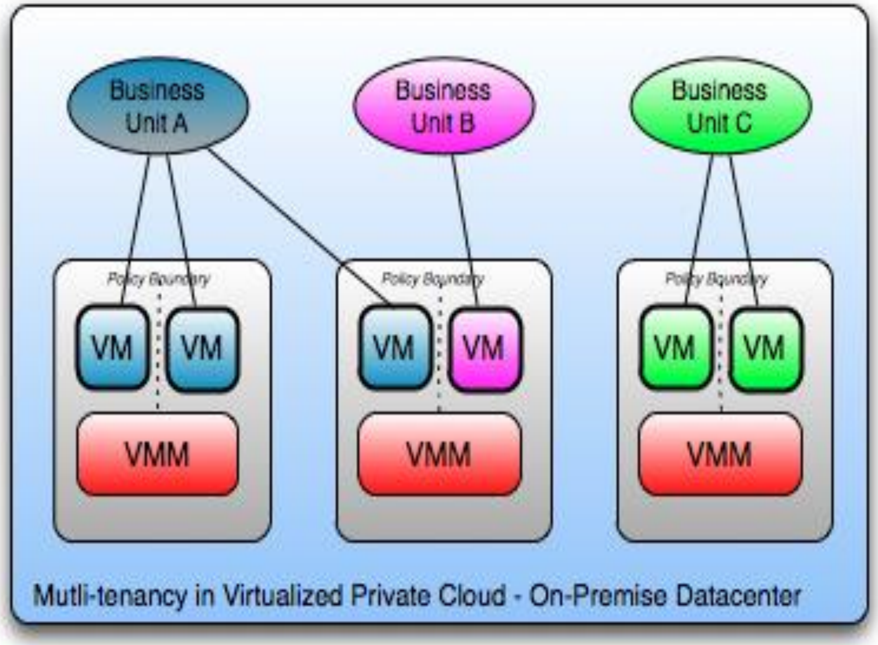
CLOUD CHARACTERISTICS & SECURITY

- Multi-tenancy
- Extensibility and Shared Responsibility
- Multiple Stakeholders
- *Third-Party Control*
- Resource location
  - Outsourcing Data and Applications
- Service Level Agreements (SLAs)
- Heterogeneity
- Elasticity
- Virtualization

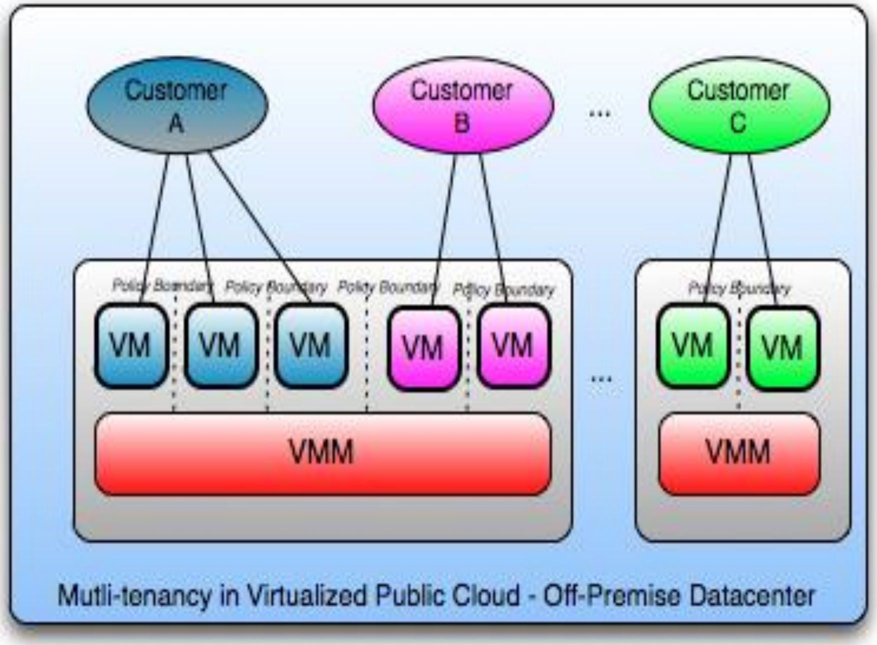
Resource Location

- Location, Relocation, Availability, Security
- Loss of Control Problem:
  - Data and apps may still need to be on the cloud
  - But can they be managed in some way by the consumer?
- Lack of trust
  - Increase trust (mechanisms)
    - Technology
    - Policy, regulation
    - Contracts (incentives)
    - SLAs

Multi-Tenancy

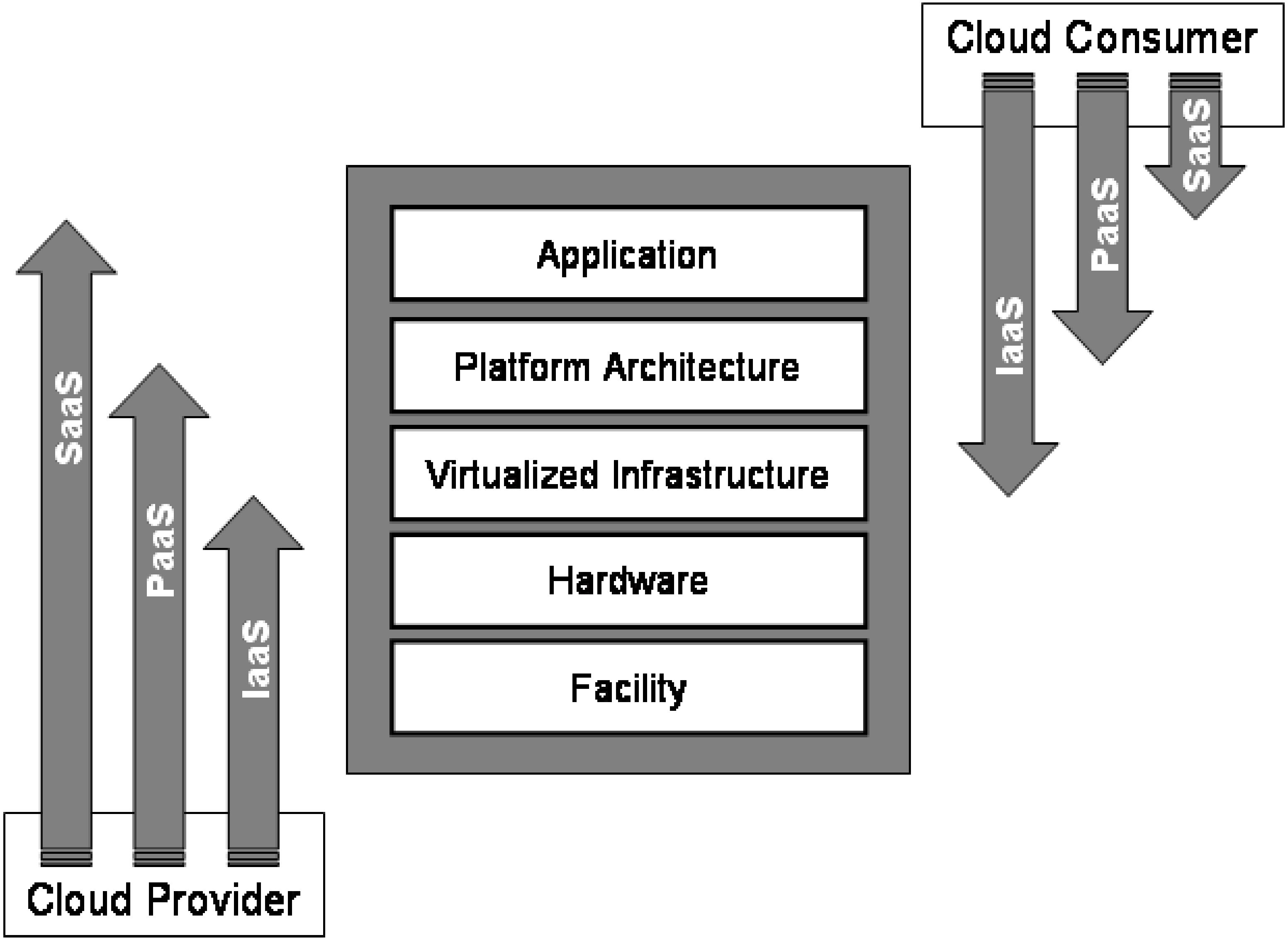


Private Cloud of Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure



Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

Differences in scope and control

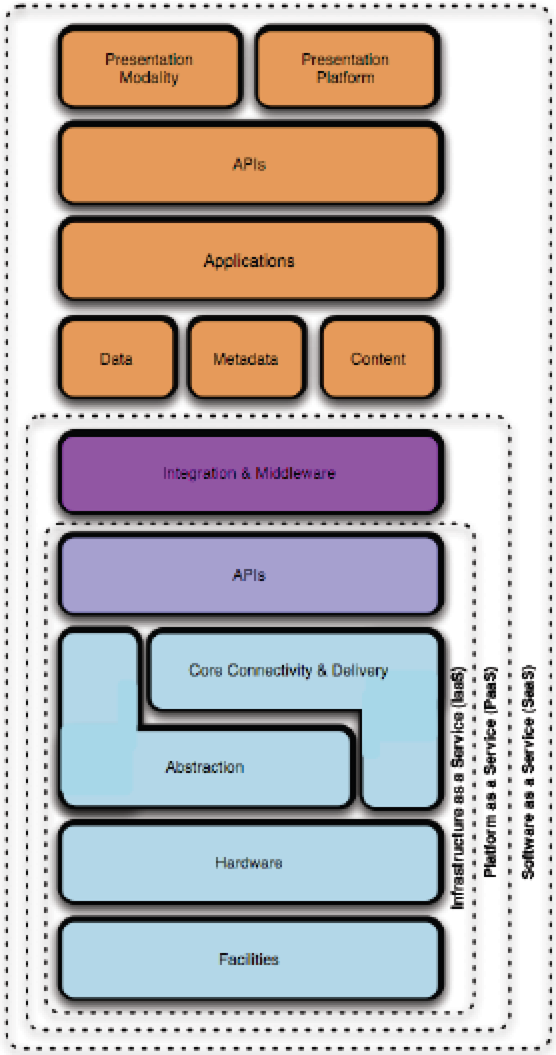


Security Considerations of Each Type of Cloud

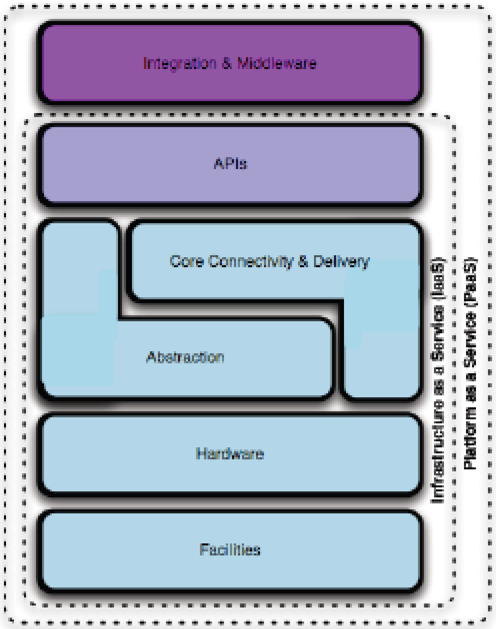
- Software (SaaS)
  - Least extensibility and greatest amount of security responsibility taken on by the cloud provider
- Infrastructure (IaaS)
  - Greatest extensibility and least amount of security responsibility taken on by the cloud provider
- Platform (PaaS)
  - Lies somewhere in the middle, with extensibility and security features which must be leveraged by the customer

The lower down the stack the Cloud provider stops, the more security **you** are tactically responsible for implementing & managing yourself.

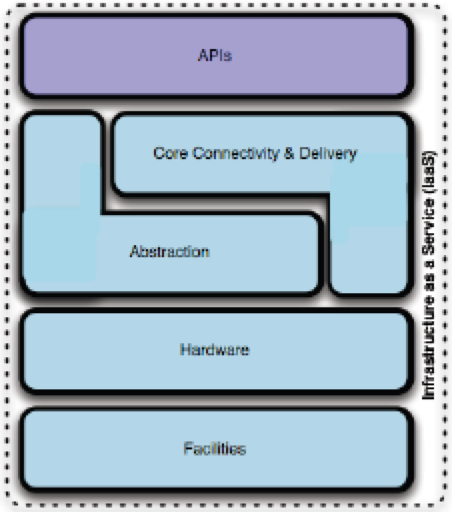
Salesforce - SaaS



Google AppEngine - PaaS

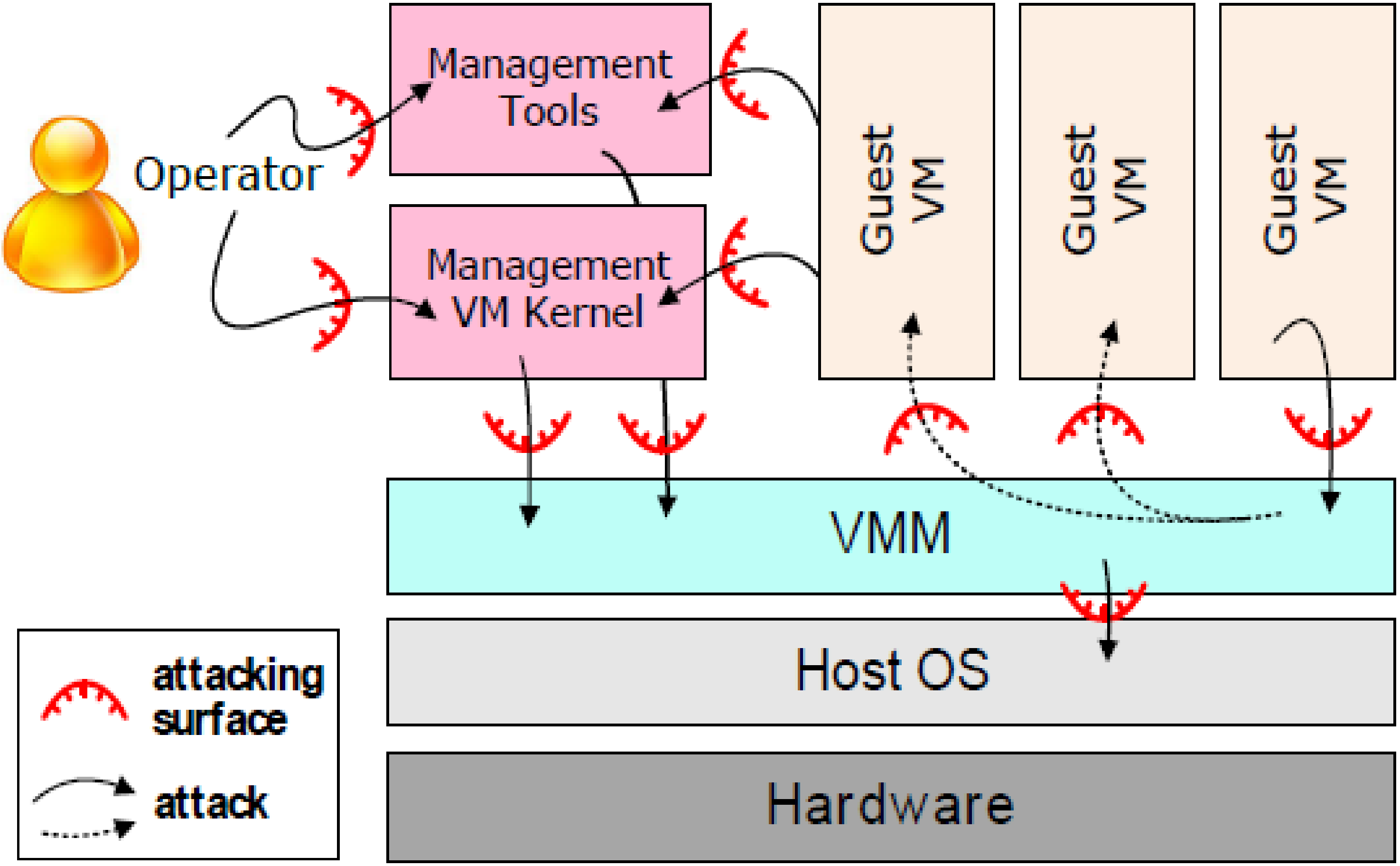

Integration & Middleware
APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)

Amazon EC2 - IaaS


APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)

Responsibilities on Cloud Security

Responsibility of	cloud provider	service provider	cloud customer
VM's Security			Responsible
Secured VM images repository	Responsible		
Securing VM boundaries	Responsible		
Hypervisor security	shared responsibility	shared responsibility	
SOA related security	shared responsibility		shared responsibility
API Security		Responsible	
SaaS security	shared responsibility	shared responsibility	
Web application security	Responsible		


Operator
Management Tools
Management VM Kernel
Guest VM
Guest VM
Guest VM
VMM
Host OS
Hardware
attacking surface
attack

Operating System Security

- Protect applications against a wide range of malicious attacks
  - 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.

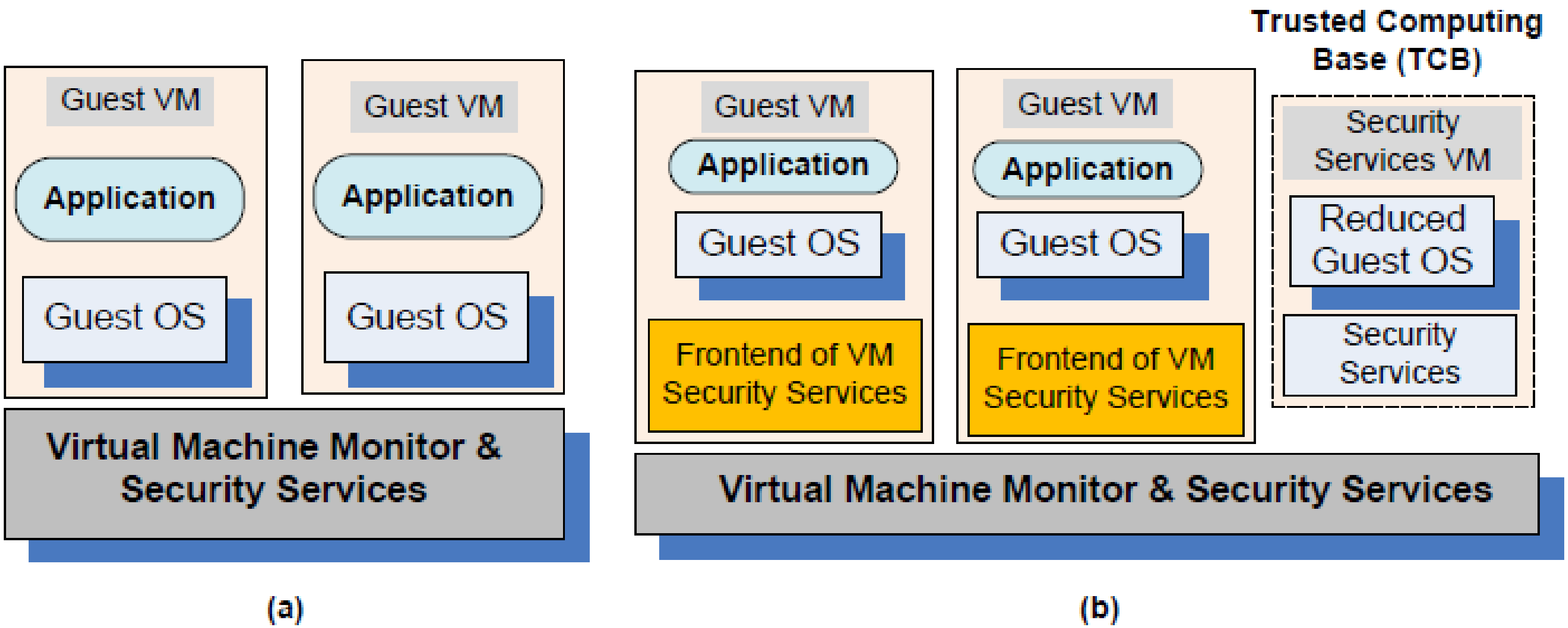
Closed-box versus open-box platforms

- Closed-box platforms
  - cellular phones, game consoles and ATM
  - Have embedded cryptographic keys to reveal their true identity to remote systems and authenticate the software running on them.
- Open-box platforms
  - Traditional hardware for commodity operating systems
  - Such (above) facilities are not available
- Commodity operating system offer low assurance.
  - it is vulnerable to wide range of 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
  - provides a stricter isolation of VMs from one another
    - than the isolation of processes in a traditional OS.
  - controls the execution of privileged operations and
  - can enforce memory isolation as well as disk and network access.
  - 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.

Virtual Machine Security


Guest VM
Application
Guest OS
Guest VM
Application
Guest OS
Virtual Machine Monitor & Security Services
(a)
Trusted Computing Base (TCB)
Guest VM
Application
Guest OS
Frontend of VM Security Services
Guest VM
Application
Guest OS
Frontend of VM Security Services
Security Services VM
Reduced Guest OS
Security Services
Virtual Machine Monitor & Security Services
(b)

- (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.
- VM side-channel attacks: malicious attack on one or more VMs by a rogue VM under the same VMM.
- 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.
- Presence of insecure and tampered VM images in the VM image repository. Probable causes:

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.
    - Ability to support the IaaS delivery model.
    - increased reliability
    - Improved intrusion prevention and detection
    - More efficient and flexible software testing

Undesirable effects of virtualization

- Diminished ability to manage the systems and track their status
  - Quantitative aspect - Increase in the number of VMs.
  - Qualitative aspect of the explosion of the number of VMs
    - Heterogeneity, Versions, Patches… etc
  - The software lifecycle has serious implication on security

Implications of virtualization on security

- Infection may last indefinitely
- Due to the lack of control, a virtual environment may never reach such a steady state.
- 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.
- 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.

Virtualization and Vulnerabilities

- Detecting a virtualized environment.
- Identifying the hypervisor.
- Breach in the isolation.
  - Denial of service:
  - System halt:
  - VM escape:
- The concept of the network perimeter evaporates
  - no physical segregation across VMs

Virtualization and Vulnerabilities

- The public cloud provides user access via the Internet
  - Cloud subscribers conduct administrative activities
- Cyber attacker or malware can exploit the vulnerabilities remotely throughout physical and virtual enterprise
- Virtual Machine based rootkits
  - Blue Pill, subVert

Virtualization and Vulnerabilities

- Increases the risk of VM-to-VM vulnerability exploitation
  - Colocation of VMs
  - Remote user on one VM can access another dormant VM if both reside on the same physical server
    - Malware attacks can be generated as malware scans are not done on dormant machines
- Easy reconfiguration
  - Creates an environment to propagate vulnerabilities and unknown configuration errors
- These attacks can also affect other physical devices in the cloud

Critical Areas to Focus

- Governance Domain
  - Cloud computing architectural framework
  - Governance and enterprise risk management
  - Legal and electronic discovery
  - Compliance & Audit
  - Information Life Cycle Management
  - Portability & Interoperability

Critical Areas to Focus

- Operational Domain
  - Traditional Security, business continuity and disaster recovery
  - Data Centre Operations
  - Incident response, notification and remediation
  - Application Security
  - Encryption and Key Management
  - Identity and Access Management
  - Virtualization

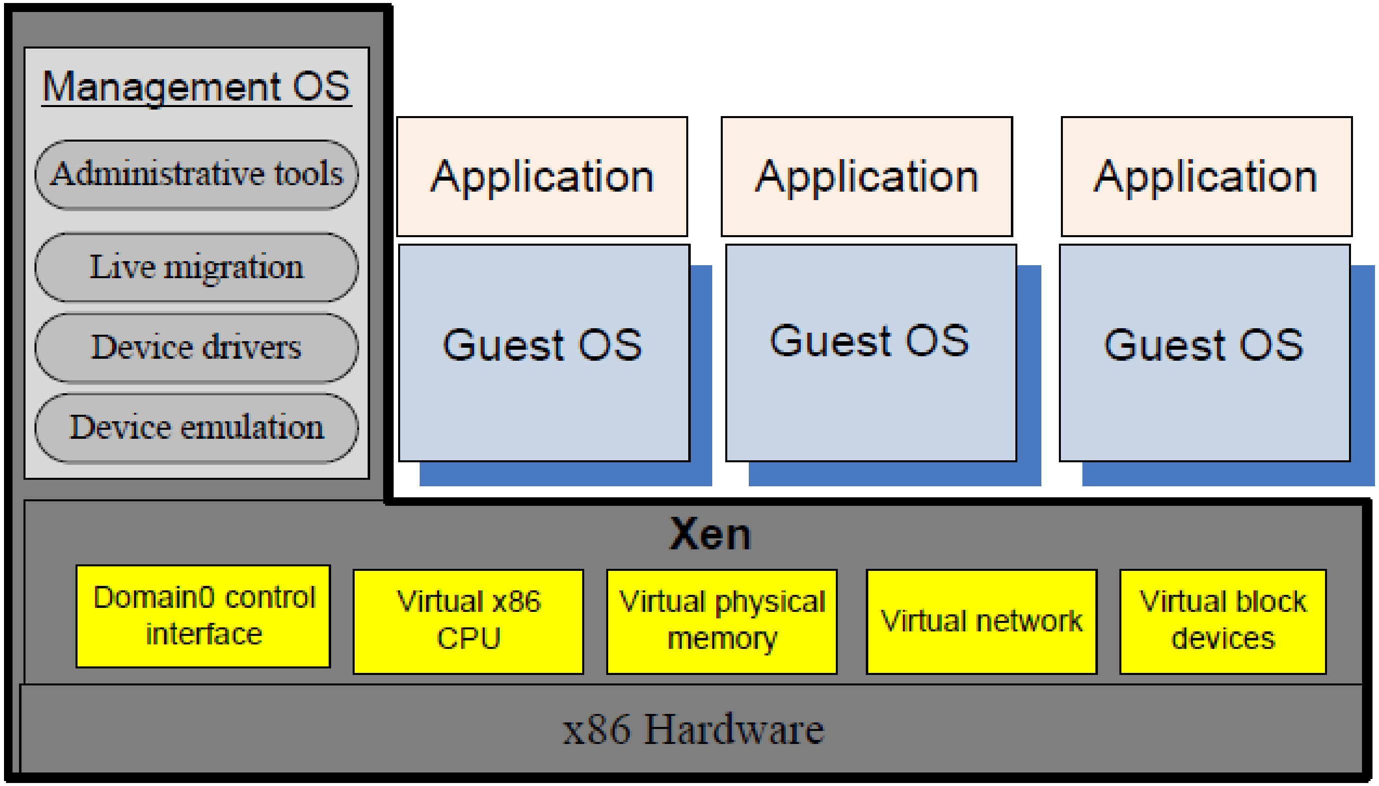
XEN CASE STUDY

Intro

- A virtual machine monitor, or hypervisor, is considerably smaller than an operating system,
  - 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

Security risks posed by a management OS

- 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: 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.

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

- 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.
  - The privacy and integrity of the VM virtual memory.
  - The freshness of the virtual CPU and the memory of the VM

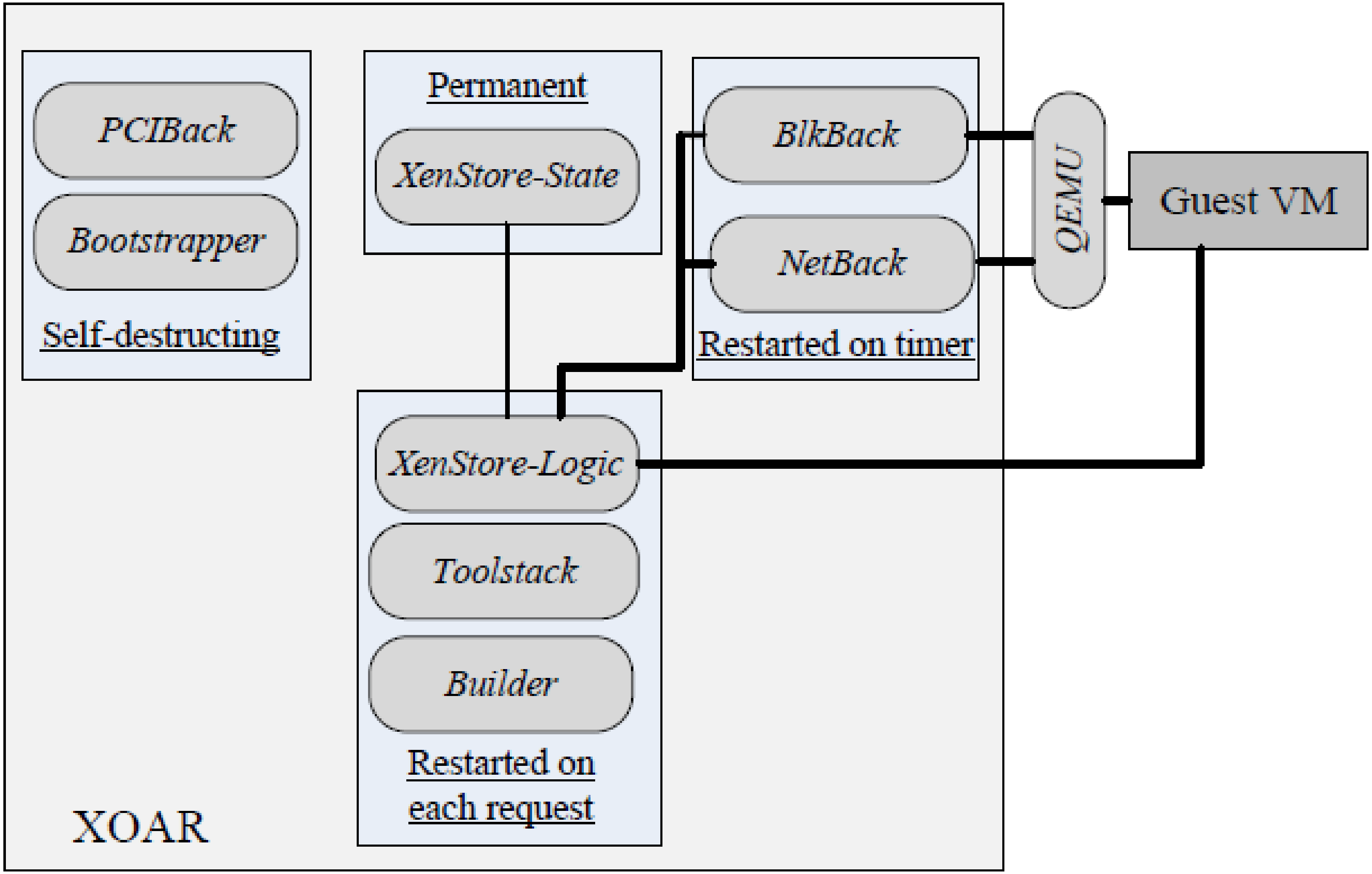
Xoar - breaking the monolithic design of TCB

- 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.

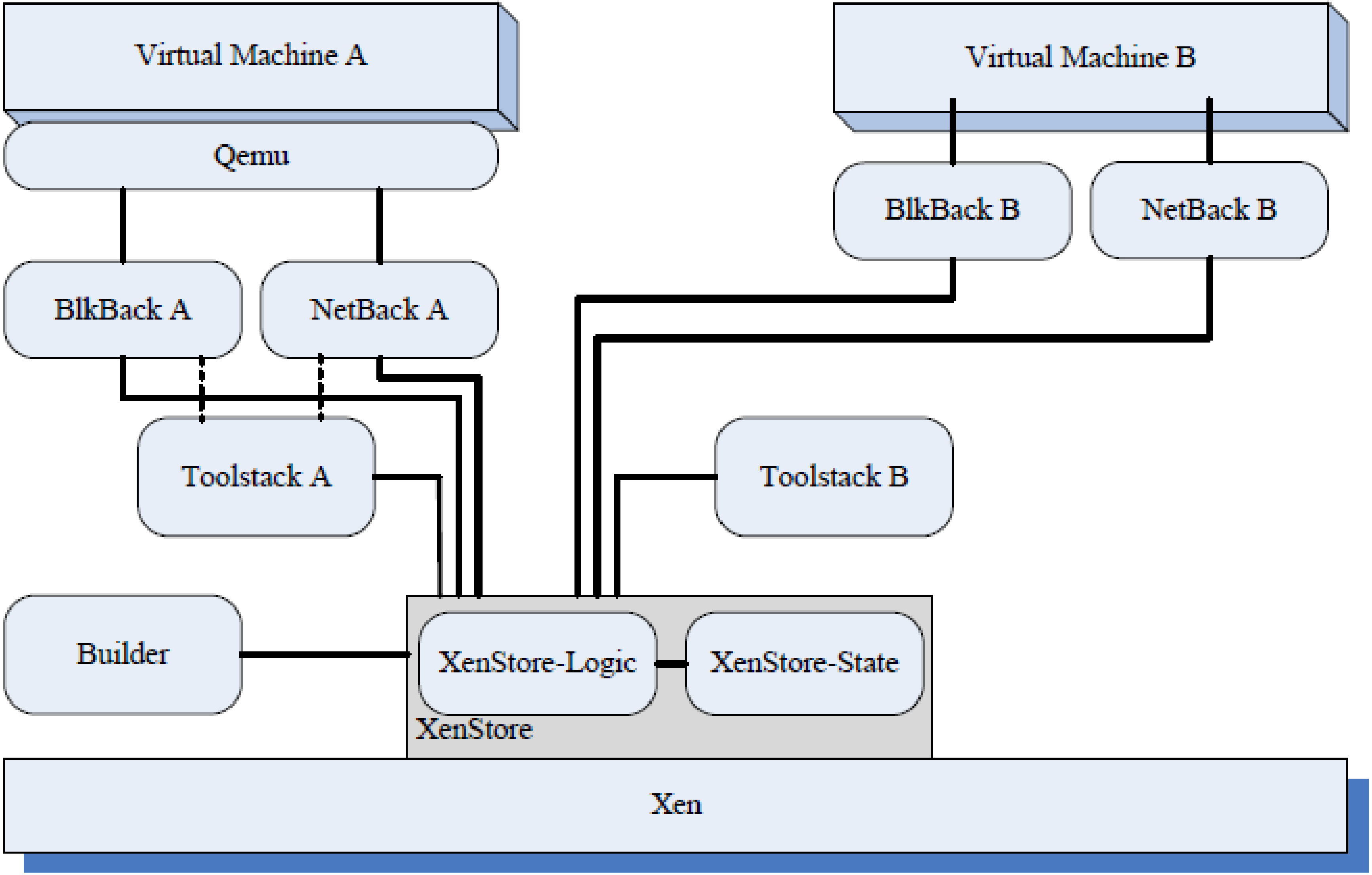
Xoar - breaking the monolithic design of TCB

- 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


PCIBack
Bootstrapper
Self-destructing
Permanent
XenStore-State
BlkBack
NetBack
Restarted on timer
QEMU
Guest VM
XenStore-Logic
Toolstack
Builder
Restarted on each request
XOAR

Xoar


Virtual Machine A
Virtual Machine B
Qemu
BlkBack B
NetBack B
BlkBack A
NetBack A
Toolstack A
Toolstack B
Builder
XenStore-Logic
XenStore-State
XenStore
Xen

Terra - a trusted virtual machine monitor

- Novel ideas for a trusted virtual machine monitor (TVMM):
  - support not only traditional operating systems,
    - by exporting the hardware abstraction for open-box platforms,
  - 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.

Terra - a trusted virtual machine monitor

- 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.

THANK YOU