

# Cloud Security and Privacy

# Infrastructure Security

- Network Level
- Host Level
- Application Level

# The Network Level

- Ensuring confidentiality and integrity of your organization's data-in-transit to and from your public cloud provider
- Ensuring proper access control (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider
- Ensuring availability of the Internet-facing resources in a public cloud that are being used by your organization, or have been assigned to your organization by your public cloud providers
- Replacing the established model of network zones and tiers with domains

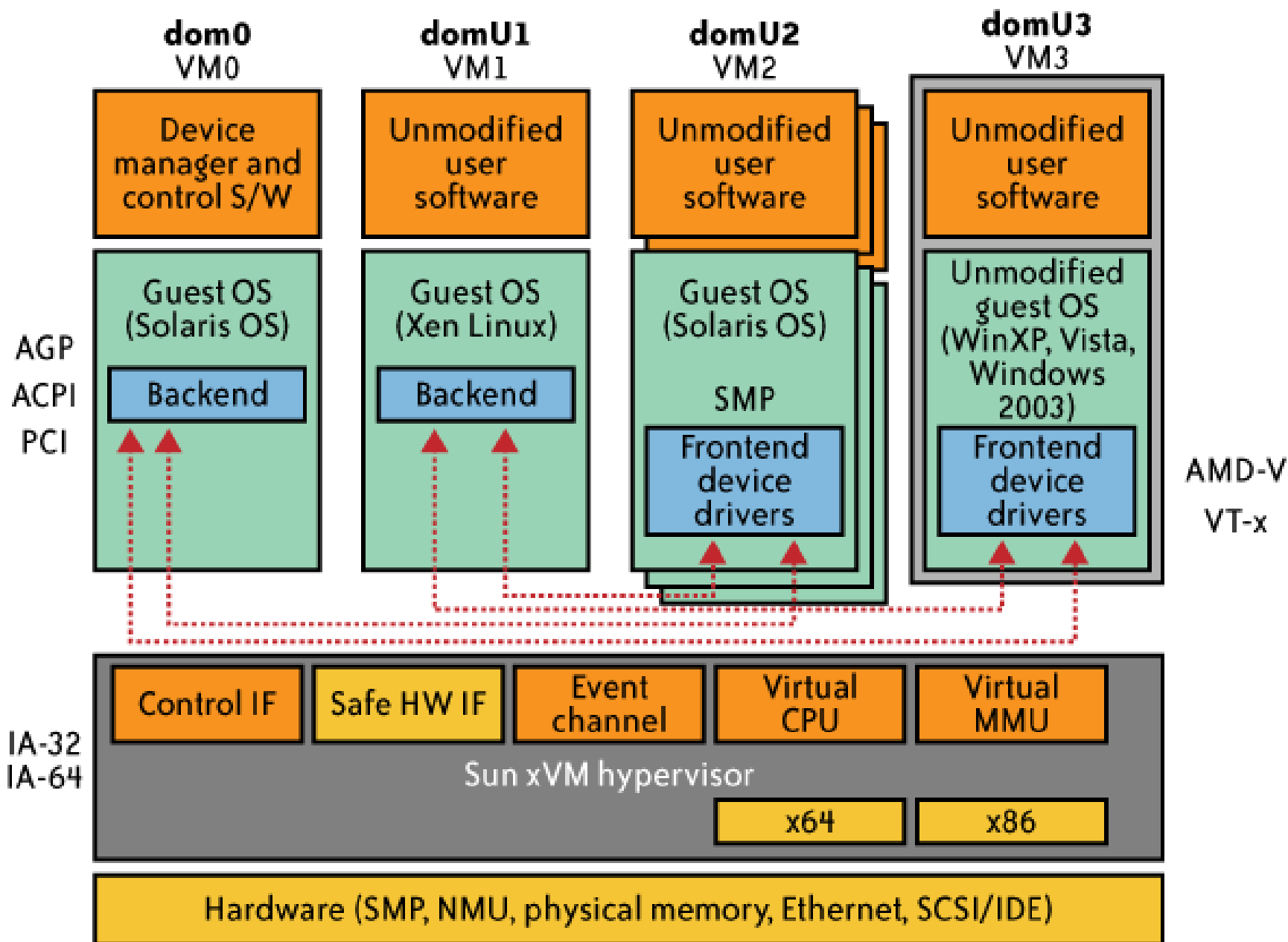
## The Network Level - Mitigation

- Note that network-level risks exist regardless of what aspects of “cloud computing” services are being used
- The primary determination of risk level is therefore not which IaaS/PaaS/SaaS is being used
- But rather whether your organization intends to use or is using a public, private, or hybrid cloud.

# The Host Level

- SaaS/PaaS

- Both the PaaS and SaaS platforms abstract and hide the host OS from end users
- Host security responsibilities are transferred to the CSP (Cloud Service Provider)
  - You do not have to worry about protecting hosts
- However, as a customer, you still own the risk of managing information hosted in the cloud services.



# Case study: Amazon's EC2 infrastructure

- “Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds”
  - Multiple VMs of different organizations with virtual boundaries separating each VM can run within one physical server
  - "virtual machines" still have internet protocol, or IP, addresses, visible to anyone within the cloud.
  - VMs located on the same physical server tend to have IP addresses that are close to each other and are assigned at the same time
  - An attacker can set up lots of his own virtual machines, look at their IP addresses, and figure out which one shares the same physical resources as an intended target
  - Once the malicious virtual machine is placed on the same server as its target, it is possible to carefully monitor how access to resources fluctuates and thereby potentially glean sensitive information about the victim

# Local Host Security

- Are local host machines part of the cloud infrastructure?
  - Outside the security perimeter
  - While cloud consumers worry about the security on the cloud provider's site, they may easily forget to harden their own machines
- The lack of security of local devices can
  - Provide a way for malicious services on the cloud to attack local networks through these terminal devices
  - Compromise the cloud and its resources for other users



# Local Host Security (Cont.)

- With mobile devices, the threat may be even stronger
  - Users misplace or have the device stolen from them
  - Security mechanisms on handheld gadgets are often times insufficient compared to say, a desktop computer
  - Provides a potential attacker an easy avenue into a cloud system.
  - If a user relies mainly on a mobile device to access cloud data, the threat to availability is also increased as mobile devices malfunction or are lost
- Devices that access the cloud should have
  - Strong authentication mechanisms
  - Tamper-resistant mechanisms
  - Strong isolation between applications
  - Methods to trust the OS
  - Cryptographic functionality when traffic confidentiality is required

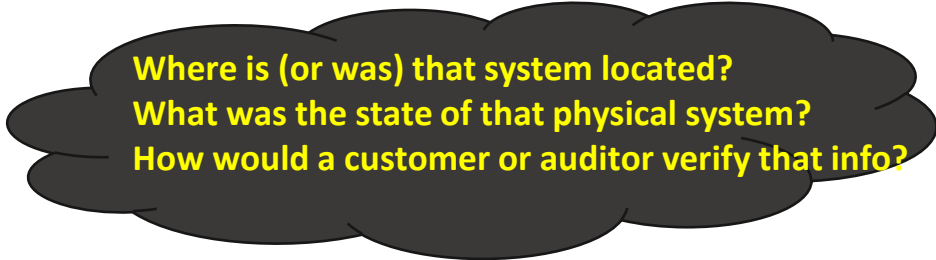
# The Application Level

- DoS
- EDoS(Economic Denial of Service)
  - An attack against the billing model that underlies the cost of providing a service with the goal of bankrupting the service itself.
- End user security
- Who is responsible for Web application security in the cloud?
- SaaS/PaaS/IaaS application security
- Customer-deployed application security

# Data Security and Storage

- Several aspects of data security, including:
  - Data-in-transit
    - Confidentiality + integrity using secured protocol
    - Confidentiality with non-secured protocol and encryption
  - Data-at-rest
    - Generally, not encrypted , since data is commingled with other users' data
    - Encryption if it is not associated with applications?
      - But how about indexing and searching?
      - Then homomorphic encryption vs. predicate encryption?
  - Processing of data, including multitenancy
    - For any application to process data, not encrypted

# Data Security and Storage (cont.)



Where is (or was) that system located?  
What was the state of that physical system?  
How would a customer or auditor verify that info?

- Data lineage
  - Knowing when and where the data was located w/i cloud is important for audit/compliance purposes
  - e.g., Amazon Web Service (AWS)
    - Store <d1, t1, ex1.s3.amazonaws.com>
    - Process <d2, t2, ec2.compute2.amazonaws.com>
    - Restore <d3, t3, ex2.s3.amazonaws.com>
- Data provenance
  - Computational accuracy (as well as data integrity)
  - E.g., financial calculation:  $\text{sum}(((2*3)*4)/6) - 2 = \$2.00$  ?
    - Correct : assuming US dollar
    - How about dollars of different countries?
    - Correct exchange rate?

# Data Security and Storage

- ❑ Data remanence
  - ❑ Inadvertent disclosure of sensitive information is possible
- ❑ Data security mitigation?
  - ❑ Do not place any sensitive data in a public cloud
  - ❑ Encrypted data is placed into the cloud?
- ❑ Provider data and its security: storage
- ❑ To the extent that quantities of data from many companies are centralized, this collection can become an attractive target for criminals
- ❑ Moreover, the physical security of the data centre and the trustworthiness of system administrators take on new importance.

# Why is Identity and Access Management (IAM)?

- Organization's trust boundary will become dynamic and will move beyond the control and will extend into the service provider domain.
- Managing access for diverse user populations (employees, contractors, partners, etc.)
- Increased demand for authentication
  - personal, financial, medical data will now be hosted in the cloud
  - S/W applications hosted in the cloud requires access control
- Need for higher-assurance authentication
  - authentication in the cloud may mean authentication outside firmware
  - Limits of password authentication
- Need for authentication from mobile devices

Early this morning, at 3:30am PST, we started seeing elevated levels of authenticated requests from multiple users in one of our locations. While we carefully monitor our overall request volumes and these remained within normal ranges, we had not been monitoring the proportion of authenticated requests. Importantly, these cryptographic requests consume more resources per call than other request types.

Shortly before 4:00am PST, we began to see several other users significantly increase their volume of authenticated calls. The last of these pushed the authentication service over its maximum capacity before we could complete putting new capacity in place. In addition to processing authenticated requests, the authentication service also performs account validation on every request Amazon S3 handles. This caused Amazon S3 to be unable to process any requests in that location, beginning at 4:31am PST. By 6:48am PST, we had moved enough capacity online to resolve the issue.

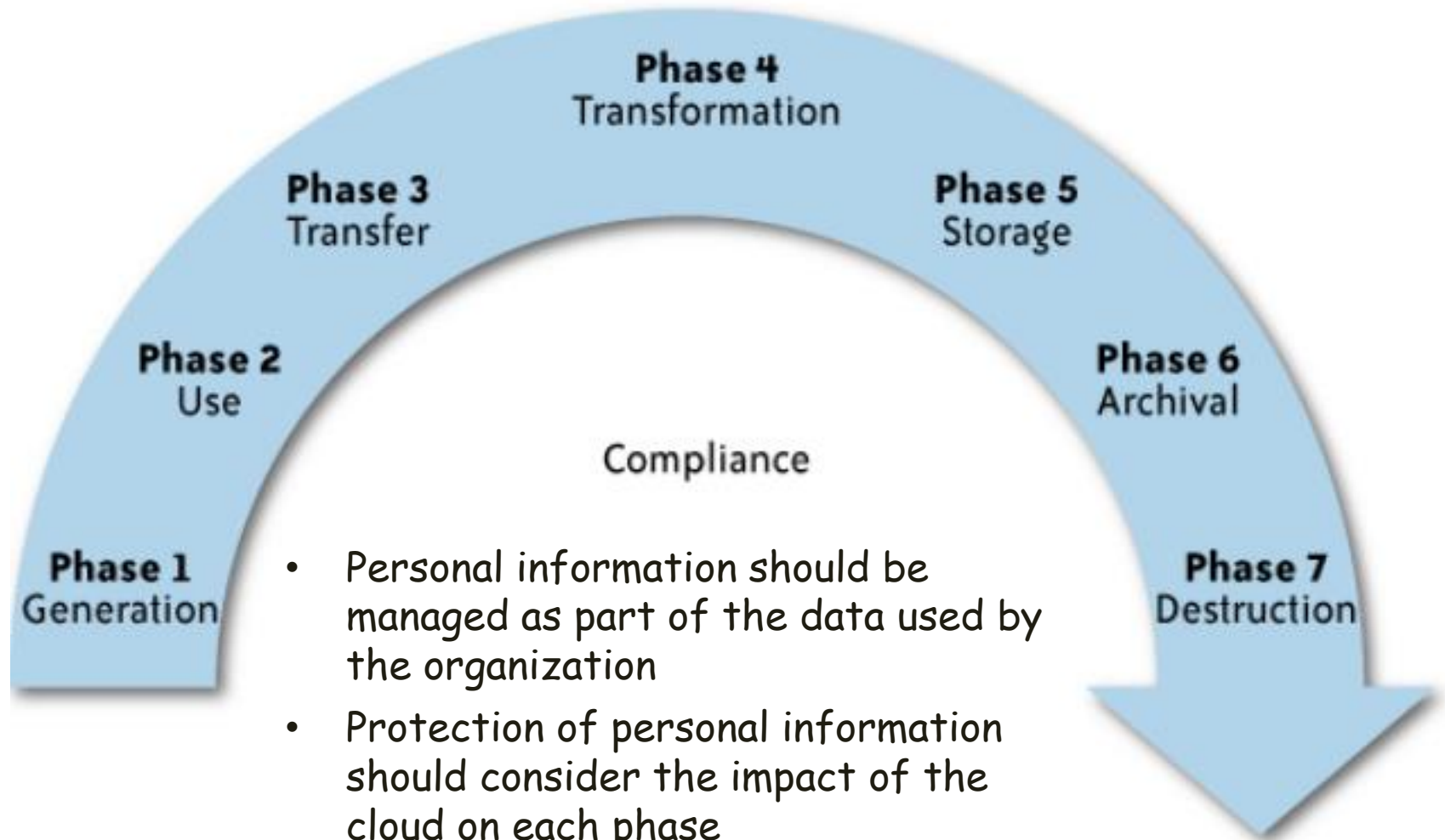
As we said earlier today, though we're proud of our uptime track record over the past two years with this service, any amount of downtime is unacceptable. As part of the post mortem for this event, we have identified a set of short-term actions as well as longer term improvements. We are taking immediate action on the following: (a) improving our monitoring of the proportion of authenticated requests; (b) further increasing our authentication service capacity; and (c) adding additional defensive measures around the authenticated calls. Additionally, we've begun work on a service health dashboard, and expect to release that shortly.

# What is Privacy?

- The concept of privacy varies widely among (and sometimes within) countries, cultures, and jurisdictions.
- It is shaped by public expectations and legal interpretations; as such, a concise definition is elusive if not impossible.
- Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data (or Personally Identifiable Information—PII).
- At the end of the day, privacy is about the accountability of organizations to data subjects, as well as the transparency to an organization's practice around personal information.



# What is the data life cycle?



# What Are the Key Privacy Concerns?

- Typically mix security and privacy
- Some considerations to be aware of:
  - Storage
  - Retention
  - Destruction
  - Auditing, monitoring and risk management
  - Privacy breaches
  - Who is responsible for protecting privacy?

# Storage

- Is it blended with information from other organizations that use the same Content Security Policy (CSP)?
- The aggregation of data raises new privacy issues
  - Some governments may decide to search through data without necessarily notifying the data owner, depending on where the data resides
- Whether the cloud provider itself has any right to see and access customer data?
- Some services today track user behaviour for a range of purposes, from sending targeted advertising to improving services

# Retention

- How long is personal information (that is transferred to the cloud) retained?
- Which retention policy governs the data?
- Does the organization own the data, or the CSP?
- Who enforces the retention policy in the cloud, and how are exceptions to this policy (such as litigation holds) managed?

# Destruction

- How does the cloud provider destroy PII at the end of the retention period?
- How do organizations ensure that their PII is destroyed by the CSP at the right point and is not available to other cloud users?
- Cloud storage providers usually replicate the data across multiple systems and sites—increased availability is one of the benefits they provide.
  - How do you know that the CSP didn't retain additional copies?
  - Did the CSP really destroy the data, or just make it inaccessible to the organization?
  - Is the CSP keeping the information longer than necessary so that it can mine the data for its own use?

# Auditing, monitoring and risk management

- How can organizations monitor their CSP and provide assurance to relevant stakeholders that privacy requirements are met when their PII is in the cloud?
- Are they regularly audited?
- What happens in the event of an incident?
- If business-critical processes are migrated to a cloud computing model, internal security processes need to evolve to allow multiple cloud providers to participate in those processes, as needed.
  - These include processes such as security monitoring, auditing, forensics, incident response, and business continuity

# Privacy breaches

- How do you know that a breach has occurred?
- How do you ensure that the CSP notifies you when a breach occurs?
- Who is responsible for managing the breach notification process (and costs associated with the process)?
- If contracts include liability for breaches resulting from negligence of the CSP?
  - How is the contract enforced?
  - How is it determined who is at fault?

# Who is responsible for protecting privacy?

e.g., Suppose a hacker breaks into Cloud Provider A and steals data from Company X. Assume that the compromised server also contained data from Companies Y and Z.

- Who investigates this crime?
- Is it the Cloud Provider, even though Company X may fear that the provider will try to absolve itself from responsibility?
- Is it Company X and, if so, does it have the right to see other data on that server, including logs that may show access to the data of Companies Y and Z?

- Data breaches have a cascading effect
- Full reliance on a third party to protect personal data?
- In-depth understanding of responsible data stewardship
- Organizations can transfer liability, but not accountability
- Risk assessment and mitigation throughout the data life cycle is critical.
- Many new risks and unknowns
  - The overall complexity of privacy protection in the cloud represents a bigger challenge.



# Part III. Possible Solutions

- Minimize Lack of Trust
  - Policy Language
  - Certification
- Minimize Loss of Control
  - Monitoring
  - Utilizing different clouds
  - Access control management
  - Identity Management (IDM)
- Minimize Multi-tenancy

# Security Issues in the Cloud

- In theory, minimizing any of the issues would help:
  - Third Party Cloud Computing
  - Loss of Control
    - Take back control
      - 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): topic of a future talk
  - Multi-tenancy
    - Private cloud
      - Takes away the reasons to use a cloud in the first place
    - VPC: its still not a separate system
    - Strong separation

# Third Party Cloud Computing

Like Amazon's EC2, Microsoft's Azure

- Allow users to instantiate Virtual Machines
- Allow users to purchase required quantity when required
- Allow service providers to maximize the utilization of sunk capital costs
- Confidentiality is very important

# Known issues: Already exist

- Confidentiality issues
- Malicious behavior by cloud provider
- Known risks exist in any industry practicing outsourcing
- Provider and its infrastructure needs to be trusted

# New Vulnerabilities & Attacks

- Threats arise from other consumers
- Due to the subtleties of how physical resources can be transparently shared between VMs
- Such attacks are based on placement and extraction
- A customer VM and its adversary can be assigned to the same physical server
- Adversary can penetrate the VM and violate customer confidentiality

## More on attacks...

- Collaborative attacks
- Mapping of internal cloud infrastructure
- Identifying likely residence of a target VM
- Instantiating new VMs until one gets co-resident with the target
- Cross-VM side-channel attacks
- Extract information from target VM on the same machine

## More on attacks...

- Can one determine where in the cloud infrastructure an instance is located?
- Can one easily determine if two instances are co-resident on the same physical machine?
- Can an adversary launch instances that will be co-resident with other user instances?
- Can an adversary exploit cross-VM information leakage once co-resident?

Answer: Yes to all