Cloud Security and Privacy

Causes of Problems

- Most security problems stem from:
  - Loss of control
  - Lack of trust (mechanisms)
  - Multi-tenancy

- These problems exist mainly in 3rd party management models
  - Self-managed clouds still have security issues, but not related to above

Loss of Control in the Cloud

- Consumer's loss of control
  - Data, applications, resources are located with provider
  - User identity management is handled by the cloud
  - User access control rules, security policies and enforcement are managed by the cloud provider
  - Consumer relies on provider to ensure
    - Data security and privacy
    - Resource availability
    - Monitoring and repairing of services/resources

Lack of Trust in the Cloud

- Trusting a third party requires taking risks

- Defining trust and risk
  - Opposite sides of the same coin
  - People only trust when it pays (Economist’s view)
  - Need for trust arises only in risky situations

- Hard to balance trust and risk

Multi-tenancy Issues in the Cloud

- Conflict between tenants opposing goals
  - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
  - Can tenants get along together and ‘play nicely’ ?
  - If they can’t, can we isolate them?
- How to provide separation between tenants?

- Cloud Computing brings new threats
  - Multiple independent users share the same physical infrastructure
  - Thus an attacker can legitimately be in the same physical machine as the target

Taxonomy of Fear

- **Confidentiality**
  - Fear of loss of control over data
    - Will the sensitive data stored on a cloud remain confidential?
    - Will cloud compromises leak confidential client data
  - Will the cloud provider itself be honest and won’t peek into the data?
- **Integrity**
  - How do I know that the cloud provider is doing the computations correctly?
  - How do I ensure that the cloud provider really stored my data without tampering with it?

Taxonomy of Fear (cont.)

- **Availability**
  - Will critical systems go down at the client, if the provider is attacked in a DoS attack?
  - What happens if cloud provider goes out of business?
  - Would cloud scale well-enough?
  - Often-voiced concern
    - Although cloud providers argue their downtime compares well with cloud user’s own data centers

Taxonomy of Fear (cont.)

- Privacy issues raised via massive data mining
  - Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients
- Increased attack surface
  - Entity outside the organization now stores and computes data
  - Attackers can now target the communication link between cloud provider and client
  - Cloud provider employees can be phished

Taxonomy of Fear (cont.)

- Auditability and forensics (out of control of data)
  - Difficult to audit data held outside organization in a cloud
  - Forensics also made difficult since now clients don’t maintain data locally

- Legal dilemma and transitive trust issues
  - Who is responsible for complying with regulations?
  - If cloud provider subcontracts to third party clouds, will the data still be secure?

Taxonomy of Fear (cont.)

- Security is one of the most difficult task to implement in cloud computing.
  - Different forms of attacks in the application side and in the hardware components
- Attacks with catastrophic effects only **needs one security flaw**

Threat Model

- A threat model helps in analyzing a security problem, design mitigation strategies, and evaluate solutions
- Steps:
  - Identify attackers, assets, threats and other components
  - Rank the threats
  - Choose mitigation strategies
  - Build solutions based on the strategies

Threat Model

- Basic components
  - Attacker modeling
    - Choose what attacker to consider
      - insider vs. outsider?
      - single vs. collaborator?
    - Attacker capabilities
  - Attacker goals
    - motivation
    - Disruption, damage, profit, revenge, …
  - Vulnerabilities / threats

What is the issue?

- The core issue here is the levels of trust
  - Many cloud computing providers trust their customers
  - Each customer is physically mixing its data with data from anybody else using the cloud while logically and virtually you have your own space
  - The way that the cloud provider implements security is typically focused on the fact that those outside of their cloud are evil, and those inside are good.
- But what if those inside are also evil?

Attacker Capability: Malicious Insiders

- At client
  - Learn passwords/authentication information
  - Gain control of the VMs
- At cloud provider
  - Log client communication
  - Can read unencrypted data
  - Can possibly peek into VMs, or make copies of VMs
  - Can monitor network communication, application patterns
  - Why?
    - Gain information about client data
    - Gain information on client behavior
    - Sell the information or use itself

Attacker Capability: Outside attacker

- What?
  - Listen to network traffic (passive)
  - Insert malicious traffic (active)
  - Probe cloud structure (active)
  - Launch DoS
- Goal?
  - Intrusion
  - Network analysis
  - Man in the middle

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 mixed with other users' data
    - Encryption if it is not associated with applications?
      - But how about indexing and searching?
  - **Processing of data, including multitenancy**
    - For any application to process data

Data Security and Storage (cont.)

- Data lineage
  - Knowing when and where the data was located within cloud is important for audit/compliance purposes
  - e.g., Amazon 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: sum ((((2*3)*4)/6) -2) = 2.00 ?

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;
- Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data
- Privacy is about the accountability of organizations to data subjects, as well as the transparency to an organization’s practice around personal information.

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?

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)
  - **Multi-tenancy**
    - Private cloud
    - Strong separation

Third Party Cloud Computing

- 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 refinement of how physical resources can be transparently shared between VMs
- Such attacks are based on placement and extraction
- A customer VM and its opponent can be assigned to the same physical server
- Adversary can penetrate the VM and violate customer confidentiality

Minimize Loss of Control: Monitoring

- Provide mechanisms that enable the provider to act on attacks he can handle.
  - infrastructure remapping
    - create new or move existing fault domains
  - shutting down offending components or targets
    - and assisting tenants with porting if necessary
  - Repairs
- Provide mechanisms that enable the consumer to act on attacks that he can handle
  - application-level monitoring
  - RAdAC (Risk-adaptable Access Control)
  - VM porting with remote attestation of target physical host
  - Provide ability to move the user’s application to another cloud

Conclusion

- Cloud computing is sometimes viewed as a reincarnation of the classic mainframe client-server model
  - However, resources are ubiquitous, scalable, highly virtualized
  - Contains all the traditional threats, as well as new ones

- In developing solutions to cloud computing, security issues may identify the problems and approaches in terms of
  - Loss of control
  - Lack of trust
  - Multi-tenancy problems