Security in the cloud

The concerns, threats and risks

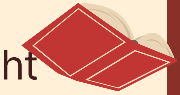
Abhishek Bhattacherjee

Security in the cloud

Companies planning to use cloud services *must be assured of tight, well-defined security services*. Many levels of security are required within a cloud environment:

✓ Identity management: For example, so that any application service or even hardware component can be authorized on a personal or group role basis.

✓ Access control: There also needs to be the right level of access control within the cloud environment to protect the security of resources.



✓ Authorization and authentication: There must be a mechanism so the right people can change applications and data.

A comprehensive security infrastructure must be provided at all levels and types of cloud services. Developers also need tools that allow them to secure the services they design to be delivered in the cloud. Organizations need consistent security across their own data center environments that intersect with a cloud service.

Raising questions...

01

Does the cloud provider use a third party to assess its own security risks?

02

Does the cloud provider understand your data preservation and protection needs?

03

Where does your data physically live? Do you have the cloud provider’s assurance that it will remain private?

04

Can the cloud provider keep security information such as private keys private?

05

Does your cloud provider have well implemented patch management policies and procedures?

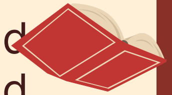
06

Does the cloud provider have a well-defined, well-executed identity and access management architecture?

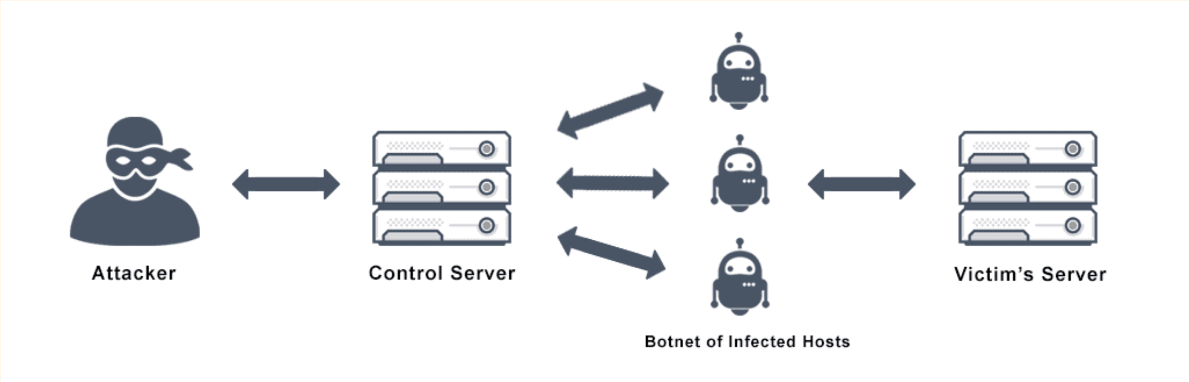
01

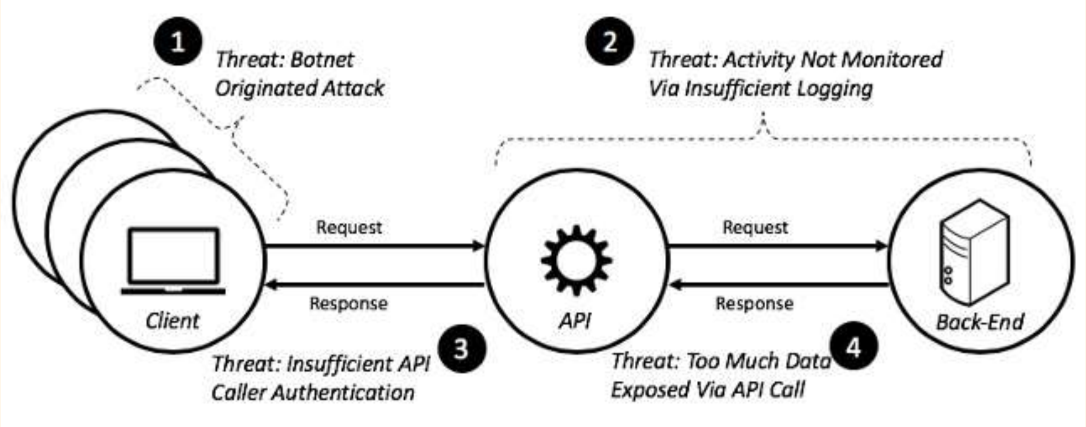
TYPES OF RISKS IN CLOUD COMPUTING

Threat #1—Misuse and illicit use of cloud computing: Lawless individuals may take advantage of the befitting registration, straightforward methods and somewhat anonymous access to cloud services to launch diverse attacks. Examples of such attacks include: password and key breaking, DDOS, malicious data hosting, commencing dynamic strike points, botnet command/control and CAPTCHA-solving farms. Targets are IaaS, PaaS.

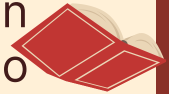


Threat #2—Insecure interfaces and APIs: Customers organize and combine with cloud services through interfaces or APIs. Providers should double-check that security is incorporated into their service forms, while users should be cognizant of security risks in the use, implementation, and administration and monitoring of such services. API dependencies, logging capabilities, inflexible access to controls, anonymous access, reusable passwords, clear-text authentication, transmission of content and improper authorizations are the example of such risks. Targets are IaaS, PaaS, SaaS.


Attacker
Control Server
Botnet of Infected Hosts
Victim's Server

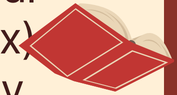

1
Threat: Botnet Originated Attack
2
Threat: Activity Not Monitored Via Insufficient Logging
Request
Response
Request
Response
Client
API
Back-End
3
Threat: Insufficient API Caller Authentication
4
Threat: Too Much Data Exposed Via API Call

Threat #3—Vicious insiders: Vicious insiders represent a larger risk in a cloud computing environment, since clients manage not have a clear outlook of provider principles and procedures.Vicious insiders can gain unauthorized access into organizations and their assets. Some risks encompass impairment, economic influence and decrease of productivity. Targets are IaaS, PaaS, SaaS.



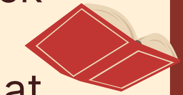
Threat #4—Issues-related technology sharing: IaaS is based on distributed infrastructure, which is often not conceived to accommodate a multi-tenant architecture. Overlooked flaws have authorized visitors to gain unauthorized rights and/or leverage on the platform. Targets are IaaS.

Threat #5—Data loss or leakage: Compromised data may encompass (i) deleted or changed data without producing a backup, (ii) unlinking a record, (iii) decrease of an encoding key and (iv) unauthorized access to perceptive data. The likelihood of data compromise considerably rises in cloud computing, due to the architecture and operations. Examples of data loss/ leakage include: (i) insufficient authentication, (ii) authorization, (iii) review (AAA) controls, (iv) inconsistent encryption, (v) inconsistent programs keys, (vi) operational flops, (vii) disposal challenges, (viii) risk of association, (xi) jurisdiction/political issues, (x) persistence and trials, (xi) datacentre reliability and catastrophe recovery. Targets are IaaS, PaaS, SaaS.

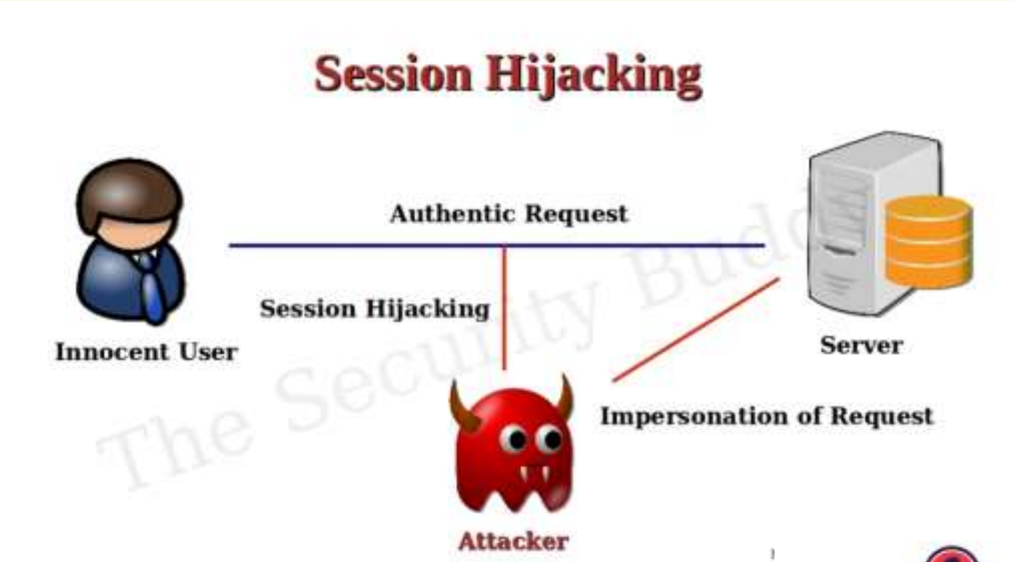


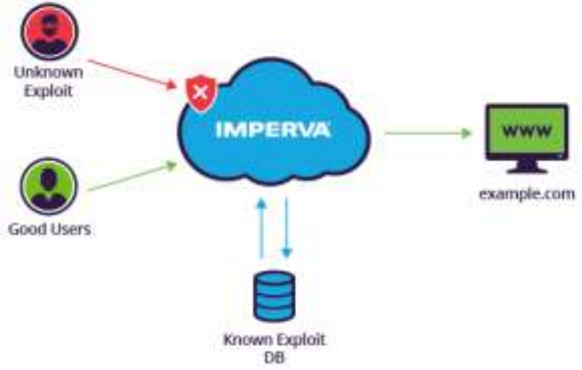
RANSOMWARE
ATTACK OPTIONS
RESTORE, PAY, OR LOSE
PATIENT DATA
PAY

Threat #6—Hijacking (Account/Service): Account or service hijacking is generally carried out with pilfered credentials. Such attacks encompass phishing, deception and exploitation of programs vulnerabilities. Using pilfered(to steal something in small quantity) credentials, attackers can access critical localities of cloud computing services and compromise the confidentiality, integrity and accessibility (CIA) of such services. Examples of such attacks include eavesdropping on transactions/sensitive undertakings, manipulation of data, coming back with falsified data, redirection to illegitimate sites.



Threat #7—Unknown Risk Profile: Cloud services signify that organizations are less engaged with hardware and software ownership and maintenance. Although this boasts important benefits, organizations should be cognizant that matters like internal security systems, security compliance, configuration hardening, patching, auditing and logging may be overlooked.


Session Hijacking
Authentic Request
Innocent User
Session Hijacking
Server
Impersonation of Request
Attacker
The Security Buddy


Unknown Exploit
IMPERVA
www
example.com
Good Users
Known Exploit DB

02

Security mechanisms

Step 1: Determine Security Policy

1. A security policy is a full security roadmap
   - ✓ Usage policy for networks, servers, etc.
   - ✓ User training about password sharing, password strength, social engineering, privacy, etc.
   - ✓ Privacy policy for all maintained data
2. A schedule for updates, audits, etc.
3. The network design should reflect this policy
   - ✓ The placement/protection of database/file servers
   - ✓ The location of demilitarized zones (DMZs)
   - ✓ The placement and rules of firewalls
   - ✓ The deployment of **intrusion detection systems (IDSs)**

Step 2: Implement Security Policy

1. Installing and configuring firewalls
   - ✓ Rules for incoming packets should be created
   - ✓ These rules should drop packets by default
   - ✓ Rules for outgoing packets *may be created*
2. Installing and configuring IDSes
   - ✓ *snort is a free and upgradeable IDS for several platforms*
   - ✓ Most IDSs send alerts to log files regularly
   - ✓ Serious events can trigger paging, E-Mail, telephone

Step 3: Reconnaissance / study

1. First, we learn about the network
   - ✓ IP addresses of hosts on the network
   - ✓ Identify key servers with critical data
   - ✓ Services running on those hosts/servers
   - ✓ Vulnerabilities on those services
2. Two forms: passive and active
   - ✓ Passive reconnaissance is undetectable
   - ✓ Active reconnaissance is often detectable by IDS

Step 4: Vulnerability Scanning

1. Steps to conduct vulnerability scanning on your cloud interface to check whether the system has any weaknesses

✓ Scan for a list of hosts and services

✓ Scan for targets on these services

✓ Many scanners will detect vulnerabilities (e.g. nessus)

✓ These scanners produce a risk report

✓ Other scanners will allow you to exploit them (e.g. metasploit)

✓ These scanners find ways in, and allow you to choose the payload to use (e.g. obtain a root shell, download a package)

Step 5: Penetration Testing

1. After identifying vulnerabilities
2. An exploit attack is done to check the intensity of vulnerability
3. This involves writing code or testing functions accepting user input

Step 6: Post-Attack Investigation

1. Forensics of Attacks
2. Retain chain of evidence
   - ✓ The evidence in this case is the data on the host
   - ✓ The log files of the compromised host hold the footsteps and fingerprints of the attacker
   - ✓ Every minute with that host must be accounted for
3. For legal reasons, you should examine a low-level copy of the disk and not modify the original

03

Vulnerabilities

Vulnerabilities

These are flaws in a computer system that weakens the overall security of the device/system.

In spite of security features, cloud computing adds some key security issues. Some of these key security challenges are summarized as follows:

- Investigation: Investigating an illegal undertaking may be unrealistic in cloud environments. Cloud services are particularly hard to enquire, because data for multiple clients may be co-located and may also be dispersed over multiple datacentres. Users have little information about the mesh topology of the inherent environment. Service provider may also enforce limits on the network security of the users.
- Data segregation: Data in the cloud is normally in a distributed simultaneously with data from other customers. Encryption will not be presumed as the single solution for data segregation issues. Some clients may not desire to encrypt data because there may be a case when encryption misleads can decimate the data.

Vulnerabilities

- Long-term viability: Service providers should double-check the data security in altering enterprise positions, such as mergers and acquisitions. Customers should double-check data accessibility in these situations. Service provider should furthermore confirm data security in contradictory situations such as extended outage, etc.

- Compromised servers: In a cloud computing environment, users do not even have an alternative of utilizing personal acquisition toolkit. In a situation where a server is compromised, they require to shut their servers down until they get a backup of the data. This will further create source accessibility concerns.

Vulnerabilities

- Regulatory compliance: Traditional service providers are exempted from outside audits and security certifications. If a cloud service provider does not adhere to these security audits, then it directs to a conspicuous decline in clientele trust.
- Recovery: Cloud service providers should double-check the data security in natural and man-made disasters. Generally, data is duplicated over multiple sites. However, in the case of any such redundant happenings, provider should do an absolute and fast restoration.

04

Governance strategies

Centralization

Centralization refers to the practice of consolidating a set of security controls, processes, policies, and services and reducing the number of places where security needs to be managed and implemented. For example, a common set of services should be built for allowing users to be authenticated and authorized to use cloud services as opposed to having each application provide different solutions. All of the security controls related to the application stack should be administered from one place, as well.

Standardization

Standardization is the next important strategy. Security should be thought of as a core service that can be shared across the enterprise, not a solution for a specific application. Each application having its own unique security solutions is the equivalent of adding doors all over the side of the building in the grocery store analogy. Companies should look at implementing industry standards for accessing systems, such as OAuth and OpenID, when connecting to third parties. Leveraging standard application protocols like Lightweight Directory Access Protocol (LDAP) for querying and modifying directory services like Active Directory or ApacheDS is highly recommended, as well.

Automation

The third strategy is automation. A great example of the need for automation comes from the book called The Phoenix Project. This book tells a fictional, yet relevant, story of a company whose IT department was always missing dates and never finding time to implement technical requirements such as a large number of security tasks. Over time, they started figuring out what steps were repeatable so that they could automate them. Once they automated the process for creating environments and deploying software, they were able to implement the proper security controls and process within the automation steps.

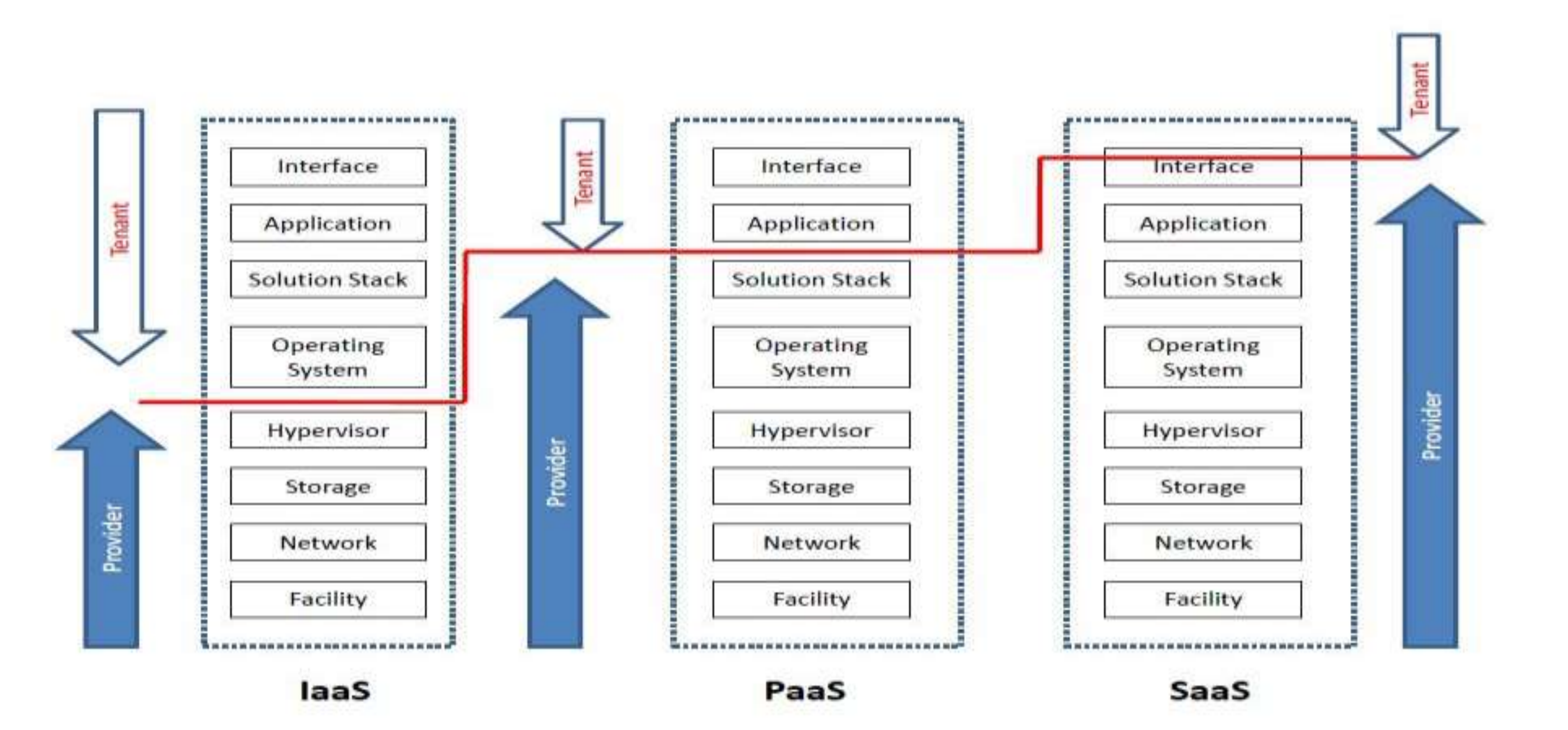
Classes of Threats

1. Disclosure (telling publically)
2. Snooping (look around secretly)
3. Deception (abc in real but shows 12)
4. Modification, spoofing, repudiation of origin, denial of receipt
5. Disruption (break chain)
6. Modification
7. Modification, spoofing, delay, denial of service

Security Issues in Cloud Computing

- Unique security features:
  - Co-tenancy(shared responsibility)
  - Lack of control on outsourced data and application
- General concerns among cloud customers:
  - Inadequate policies and practices
  - Insufficient security controls
- Customers use cloud services to serve their clients
- Need to establish trust relationships
- Beneficial to both stakeholders

Security responsibilities in cloud



Developing a Secure, Accountable, Reliable Cloud Environment

In order to secure cloud-based systems, there are a number of areas to focus the security controls on. Here are some of the most important areas:

- Policy enforcement
- Encryption
- Key management
- Web security
- API management
- Patch management
- Logging
- Monitoring
- Auditing