Security and Privacy in Cloud Computing

Molnár Bálint(GKK4ZF)
Biztonságos e-kereskedelemben alapjai
Content

• What is Cloud Computing?
  – Type of service offered through cloud

• Infrastructure Security
  – Network level
  – Host level
  – Application level
Content cont.

• Data Security
  – Confidentiality
  – Integrity
  – Availability

• Privacy
  – Key Privacy Concerns
  – Privacy Principles
Evolution of Cloud Computing
Cloud Definition

• Five main attributes:
  – Multitenancy (shared resources)
  – Massive scalability
  – Elasticity
  – Pay as you go
  – Self-provisioning of resources
SPI Framework
**Cloud Services Delivery Model**

<table>
<thead>
<tr>
<th>Level</th>
<th>Definition</th>
<th>Examples</th>
</tr>
</thead>
</table>
| **Infrastructure** *(servers, storage, databases)* | A highly scaled redundant and shared computing infrastructure accessible using Internet technologies Consists of servers, storage, security, databases, and other peripherals | • Amazon EC2, S3, etc.  
• Rackspace Mosso offering  
• Sun’s cloud services  
• Terremark cloud offering |
| **Platform**  | A platform that enables developers to write applications that run on the cloud A platform would usually have several application services available for quick deployment | • Microsoft Azure  
• Google App Engine  
• Force.com |
| **Software**  | Applications that are enabled for the cloud Supports an architecture that can run multiple instances of itself regardless of location Stateless application architecture Monthly subscription-based pricing model | • Google Docs  
• MobileMe  
• Zoho |

*While cloud-based software services are maturing, cloud platform and infrastructure offerings are still in their early stages.*
SaaS

• User rents the software for use
• Software can be accessed through any authorized device
• Companies can outsource the hosting and the management of application to third party.
• Just basic hardware required to use
• Cannot be completely customized
PaaS

• Vendor offers development environment
• Vendor toolkit
• Developers can develop application without installing any tool in the computer
• Browser based
• Supports multi users
• Multitenant deployment architecture
<table>
<thead>
<tr>
<th>Supported area</th>
<th>In-house development platform</th>
<th>PaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoints: desktops, browsers, mobile devices</td>
<td>Most endpoints and clients are supported</td>
<td>Mostly browser-based</td>
</tr>
<tr>
<td>Business logic</td>
<td>Multiple vendors are supported</td>
<td>Restricted by PaaS model</td>
</tr>
<tr>
<td>Application development framework</td>
<td>Java Platform, Enterprise Edition (Java EE), .NET, etc.</td>
<td>Restricted by PaaS model</td>
</tr>
<tr>
<td>Application servers</td>
<td>Multiple vendors are supported</td>
<td>Provided by PaaS</td>
</tr>
<tr>
<td>Databases</td>
<td>Multiple vendors are supported</td>
<td>Provided by PaaS</td>
</tr>
<tr>
<td>Servers and VMs</td>
<td>Multiple vendors are supported</td>
<td>Provided by PaaS</td>
</tr>
<tr>
<td>Storage</td>
<td>Multiple vendors are supported</td>
<td>Provided by PaaS</td>
</tr>
</tbody>
</table>
IaaS

• The vendor provides the entire infrastructure
• Scalability
• Pay as you go
Cloud Deployment Models

• Public
  – Third party vendor tasks
    • Shares resources
    • Security management

• Private
  – Emulate cloud on private network
  – Organization do everything
Cloud Deployment Models Cont.
Why adopt to Cloud?

• No infrastructure
• Billed actual use only
• Flexibility
• High availability
• Lower Costs
Why not adopt to Cloud?

- Security
- Privacy
- Interoperability
Infrastructure Security
Network Level

• Private Cloud
  – No changes required

• Public Cloud
  – Changes required
    • Ensuring the confidentiality and integrity
    • Ensuring proper access control
    • Ensuring the availability of the internet-facing resources
Data Confidentiality, Integrity

• Data previously confined to a private network are now exposed to the Internet

• Example: 2008 (Amazon Simple DB) flaw in digital signature algorithm
Proper Access Control

• Costumers have limited access to
  – Relevant network-level logs
  – Data

• IP Reusable problem
  – Somebody can reach your resources
  – Amazon Elastic IP

• Problem exist in the internal network too
Availability of Internet-facing resources

• Any attack on the internet can deny your cloud access
  – DNS attack
  – Network misconfiguration
    • 2008 Pakistan Telecom
  – DoS
    • Not only in the external network (IaaS)
Network Level Mitigation

- The network-level risks exist in IaaS, SaaS, PaaS
- Use private cloud if you can afford
- Encrypt transmitted data
- Firewall
Infrastructure Security
Host Level

• Power of thousands of compute nodes, combined with the homogeneity of the operating system
• PaaS SaaS Security
• IaaS Security
PaaS SaaS Security

• Host operating systems, platforms, processes managed by the cloud operator
• ISO 27002 or SysTrust
• Abstraction layer
  – SaaS cannot be accessed by the user
  – PaaS can be accessed through API
IaaS Security

• Virtualization software security
  – Important to secure this layer
  – Managed by the CSP
  – Vulnerable hypervisor

• Virtual Server Security
  – Customers are responsible for the security
  – Threats
    • Stealing keys used to access and manage hosts (SSL)
    • Attacking vulnerable services (FTP)
    • Hijack Accounts (weak password)
    • Deploying trojans embedded in the software
Secure Virtual Servers

- Install custom build OS
- Install recommended OS
- Run Firewall and open only necessary ports
- Run only the required services
- Enable logging
Infrastructure Security
Application Level

- Web application security
- Browser security
- SaaS Application Security
- PaaS Application Security
- IaaS Application Security
SaaS application Security

• Provider manages the entire application
• Customers are responsible for operational security
• Privileges
  – Google Docs image problem
• Providers commingle customers data
  – No encryption(key management)
  – Tagged with unique customer tag
  – Could problem during update
PaaS application Security

- PaaS platform (runtime engine)
  - Sandbox

- Customer deployed application
  - Become familiar with the API
  - API with security features
  - Currently no standards
IaaS application Security

- Providers treat the customers application as a black box
- Customers are responsible for all aspects of the security
Data Security and Storage

• Primary risk is not using encryption during data transmit

• Use secure protocol(SCP, SFTP, HTTPS)

• Should encrypt data-at-rest
  – Data stored in big databases with other users data
  – For stored data only

• Processed data must be unencrypted
  – 2009 June fully homomorphic encryption(Stanford)
Data Security and Storage Cont.

• Useful to know where and when the data located
• Prove data provenance
  – \( \text{SUM}(((2*3)*4)/6)-2) = $2.00 \)
• Data remanence
• What metadata does your provider have from your data
  – System, Application logs
Data Confidentiality

• Access Control
  – Sadly the most common is the username password

• How the data stored in the cloud protected?
  – If Encrypted
    • Algorithm
    • Key Length
    • Who manages your keys?
      – CSP usually use one key for the whole data or worse one key for all customer
Data Integrity

• Encryption is for Confidentiality
• Hash
• Problems:
  – Explicitly knowledge of the whole data sets
  – Data sets are dynamic and frequently changing
Data Availability

• Availability of the CSP
• Examples
  – 2009 March: Carbonite Inc lost 7500 customers data
  – 2009 February: Coghead suddenly shut down
Privacy

• What is privacy:
  – “The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information.”
  – any information relating to an identified or identifiable individual (data subject)
Data Life Cycle

• Protection of personal information should consider the impact of the cloud on each of the following phases.
Key Privacy Concerns in the Cloud

• Access
  – Data subjects have rights to know what personal information is held. Can make a request to stop processing
  – Access to all personal information
  – Problem:
    • How can you ensure that all of your information deleted?
Key Privacy Concerns in the Cloud

• Compliance
  – What are the privacy compliance requirements in the cloud?
  – Who is responsible for maintaining the compliance?
    • Data may be stored in multiple countries
Key Privacy Concerns in the Cloud

• Storage
  – Where is the data in the cloud stored?
  – Privacy laws in various countries place limitations

• Retention
  – How long is personal information retained?
  – Who enforces the retention policy in the cloud?
Key Privacy Concerns in the Cloud

• Destruction
  – Can you truly destroy information once it is in the cloud?
  – Did the CSP really destroy the data?

• Privacy breaches
  – How do you know that a breach has occurred?
  – How is it determined who is at fault?
Privacy Principles

• Collection Limitation Principle
  – collection of personal data should be limited to the minimum amount of data required
  – Different data elements about individuals are collected and later merged

• Use Limitation Principle
  – personal data should not be disclosed, otherwise used for purposes other than those with the consent of the data subject
  – Critical because of the centralized database
  – Combine data from multiple sources
Privacy Principles

• Security Principle
  – Personal data should be protected by reasonable security safeguards

• Retention and Destruction Principle
  – data should not be retained for longer than needed
  – Data should be destroyed in a secure way
Privacy Principles

• Transfer Principle
  – data should not be transferred to countries that don’t provide the same level of privacy protection as the organization that collected the information
References:


Questions??