Security Issues in Cloud Computing

CSCI 454/554

Cloud Computing

▪ Definition based on NIST:
  “A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.”
Figure 16.7 Cloud Computing Elements

- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service
- On-Demand Self-Service

Service Models:
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Deployment Models:
- Public
- Private
- Hybrid
- Community

Figure 16.8 Cloud Computing Context
Cloud Computing Reference Architecture

- “what” cloud services provide, not a “how to” design solution and implementation.
- facilitate the understanding of the operational intricacies in cloud computing.
- It does not represent the system architecture of a specific cloud computing system; instead it is a tool for describing, discussing, and developing a system-specific architecture using a common framework of reference.

Figure 16.9 NIST Cloud Computing Reference Architecture
Cloud Provider

Cloud provider (CP)

Can provide one or more of the cloud services to meet IT and business requirements of cloud consumers

For each of the three service models (SaaS, PaaS, IaaS), the CP provides the storage and processing facilities needed to support that service model, together with a cloud interface for cloud service consumers

For SaaS, the CP deploys, configures, maintains, and updates the operation of the software applications on a cloud infrastructure so that the services are provisioned at the expected service levels to cloud consumers

For PaaS, the CP manages the computing infrastructure for the platform and runs the cloud software that provides the components of the platform, such as runtime software execution stack, databases, and other middleware components

For IaaS, the CP acquires the physical computing resources underlying the service, including the servers, networks, storage, and hosting infrastructure

Roles and Responsibilities

Cloud carrier
• A networking facility that provides connectivity and transport of cloud services between cloud consumers and CPs

Cloud broker
• Useful when cloud services are too complex for a cloud consumer to easily manage
• Three areas of support can be offered by a cloud broker:
  • Service intermediation
    • Value-added services such as identity management, performance reporting, and enhanced security
  • Service aggregation
    • The broker combines multiple cloud services to meet consumer needs not specifically addressed by a single CP, or to optimize performance or minimize cost
  • Service arbitrage
    • A broker has the flexibility to choose services from multiple agencies

Cloud auditor
• An independent entity that can assure that the CP conforms to a set of standards
Cloud Security Risks and Countermeasures

Abuse and nefarious use of cloud computing
- Countermeasures: stricter initial registration and validation processes; enhanced credit card fraud monitoring and coordination; comprehensive introspection of customer network traffic; monitoring public blacklists for one’s own network blocks

Malicious insiders
- Countermeasures: enforce strict supply chain management and conduct a comprehensive supplier assessment; specify human resource requirements as part of legal contract; require transparency into overall information security and management practices, as well as compliance reporting; determine security breach notification processes

Risks and Countermeasures (II)

Insecure interfaces and APIs
Countermeasures: analyzing the security model of CP interfaces; ensuring that strong authentication and access controls are implemented in concert with encryption machines; understanding the dependency chain associated with the API

Shared technology issues
Countermeasures: implement security best practices for installation/configuration; monitor environment for unauthorized changes/activity; promote strong authentication and access control for administrative access and operations; enforce SLAs for patching and vulnerability remediation; conduct vulnerability scanning and configuration audits

Data loss or leakage
Countermeasures: implement strong API access control; encrypt and protect integrity of data in transit; analyze data protection at both design and run time; implement strong key generation, storage and management, and destruction practices
Risks and Countermeasures (III)

- Account or service hijacking
  - Countermeasures: prohibit the sharing of account credentials between users and services; leverage strong two-factor authentication techniques where possible; employ proactive monitoring to detect unauthorized activity; understand CP security policies and SLAs

- Unknown risk profile
  - Countermeasures: disclosure of applicable logs and data; partial/full disclosure of infrastructure details; monitoring and alerting on necessary information

<table>
<thead>
<tr>
<th>Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that the service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identity and access management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software isolation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.</td>
</tr>
</tbody>
</table>

Table 16.3

NIST Guidelines on Security and Privacy Issues and Recommendations

(Table can be found on Pages 514 – 515 in textbook)
The threat of data compromise increases in the cloud

Database environments used in cloud computing can vary significantly

- **Multi-instance model**
  - Provides a unique DBMS running on a virtual machine instance for each cloud subscriber
  - This gives the subscriber complete control over role definition, user authorization, and other administrative tasks related to security

- **Multi-tenant model**
  - Provides a predefined environment for the cloud subscriber that is shared with other tenants, typically through tagging data with a subscriber identifier
  - Tagging gives the appearance of exclusive use of the instance, but relies on the CP to establish and maintain a sound secure database environment
The Cloud Security Alliance defines SecaaS as the provision of security applications and services via the cloud either to cloud-based infrastructure and software or from the cloud to the customers’ on-premise systems.

SecaaS security services:
- Identity and access management
- Data loss prevention
- Web security
- E-mail security
- Security assessments
- Intrusion management
- Security information and event management
- Encryption
- Business continuity and disaster recovery
- Network security

Figure 16.11 Elements of Cloud Security as a Service
Summary

- Cloud computing
  - Elements
  - Reference architecture
- Cloud security risks and countermeasures
- Data protection in the cloud
- Cloud Security as a Service