Cloud Computing

Module 5

Cloud Computing Computing – Text Books

- **Modules 1 to 4** - Kai Hwang , Geoffrey C Fox, Jack J Dongarra : “Distributed and Cloud Computing – From Parallel Processing to the Internet of Things” , Morgan Kaufmann Publishers – 2012.
- **Module 5** – John W Rittinghouse and James F Ransome , “Cloud Computing: Implementation – Management – and Security”, CRC Press, 2010.
- **Module 6** - Michael Miller, “Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online”, Pearson Education, 2009.

Security Overview

- Although there is a **significant benefit to leveraging cloud computing**, **security concerns** have led organizations to **hesitate to move critical resources** to the cloud.
- Corporations and individuals are often concerned about how **security and compliance integrity** can be maintained in this new environment.
- Even more worrying, however, may be those corporations that are jumping into cloud computing that may be **oblivious to the implications of putting critical applications and data in the cloud**.
- **Moving critical applications and sensitive data to public and shared cloud** environments is of great concern for those corporations that are **moving beyond their data center's network perimeter defense**.
- To alleviate these concerns, a cloud solution provider
  - must ensure that customers will continue to have the **same security and privacy controls** over their applications and services,
  - **provide evidence to customers** that their organization and customers are secure and they can **meet their service-level agreements**,
  - and that they can **prove compliance to auditors**.

Cloud Security Challenges

- With the cloud model, you **lose control over physical security**.
  - In a public cloud, you are sharing computing resources with other companies.
  - In a shared pool outside the enterprise, you don’t have any knowledge or control of where the resources run.
  - Exposing your data in an environment shared with other companies could give the government “reasonable cause” to seize your assets because another company has violated the law.
  - Simply because you share the environment in the cloud, may put your data at risk of seizure.
- Storage services provided by **one cloud vendor may with another vendor’s** services should you decide to move from one be incompatible to the other.
  - Vendors are known for creating what the hosting world calls **“sticky services”—**services that an end user may have difficulty transporting from one cloud vendor to another.
  - (e.g., Amazon’s “Simple Storage Service” [S3] is incompatible with IBM’s Blue Cloud, or Google, or Dell).

Cloud Security Challenges

- If information is encrypted while passing through the cloud, **who controls the encryption/decryption keys? Is it the customer or the cloud vendor?**
  - Most customers probably want their data encrypted both ways across the Internet using SSL (Secure Sockets Layer protocol).
  - They also most likely want their data encrypted while it is at rest in the cloud vendor’s storage pool.
- **Data integrity** means ensuring that data is identically maintained during any operation (such as transfer, storage, or retrieval).
  - Put simply, data integrity is assurance that the data is consistent and correct.
  - **Ensuring the integrity** of the data really means that it changes only in response to **authorized transactions**.
  - This sounds good, but you must remember that **a common standard to ensure data integrity does not yet exist**.

Cloud Security Challenges

- Using **SaaS offerings** in the cloud means that there is much less need for software development.
  - For example, using a web-based customer relationship management (CRM) offering **eliminates the necessity to write code** and “customize” a vendor’s application.
  - If we plan to use internally developed code in the cloud, it is even more important to have a **formal secure software development life cycle (SDLC)**.
  - The **immature use of mashup technology** (combinations of web services), which is fundamental to cloud applications, is inevitably going to cause unwitting security vulnerabilities in those applications.
  - The development tool of choice should have a **security model embedded** in it to guide developers during the development phase and **restrict users only to their authorized data** when the system is deployed into production.
  - **Someone has to be responsible for monitoring for security and compliance**, and unless the application and data are under the control of end users, they will not be able to.
  - Since the **SaaS provider’s logs are internal** and not necessarily accessible externally or by clients or investigators, monitoring is difficult.
  - Since **access to logs** is required for **Payment Card Industry Data Security Standard (PCI DSS)** compliance and may be requested by **auditors and regulators, security managers** need to make sure to negotiate access to the provider’s logs as part of any service agreement.

Cloud Security Challenges

- Cloud applications **undergo constant feature additions**, and **user**s must **keep up to date** with application improvements to be **sure they are protected**.
  - The speed at which applications will change in the cloud **will affect both SDLC and security**.
  - For example, **Microsoft's SDLC** assumes that mission-critical software will have a **three- to five-year period** in which it will not change substantially, but the **cloud** may require a change in the application **every few weeks**.
  - **Users** must **constantly upgrade**, because an older version may not function, or protect the data.
- Having **proper fail-over technology** is a component of securing the cloud that is often overlooked.
  - The company can survive if a non-missioncritical application goes offline, but this may not be true for mission-critical applications.
  - Security needs to move to the data level, so that enterprises can be sure their data is protected wherever it goes.
  - Sensitive data is the domain of the enterprise, not the cloud computing provider.

Cloud Security Challenges

- Most **compliance standards do not envision compliance** in a world **of cloud computing.**
  - There is a **huge body of standards** that apply for **IT security and compliance, governing** most business interactions that will, over time, have to be translated to the cloud.
  - **SaaS** makes the process of compliance **more complicated**, since it may be difficult for a customer to discern where its **data resides** on a network controlled by its **SaaS provider, or a partner of that provider**, which raises all sorts of **compliance issues of data privacy, segregation, and security.**
  - Eg:- Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA), and industry standards such as the PCI DSS
  - Many compliance regulations require that **data not be intermixed with other data**, such as on shared servers or databases.

Cloud Security Challenges

- **Government policy will need to change** in response to both the **opportunity and the threats that cloud computing brings**.
  - This will likely focus on the **off-shoring of personal data and protection of privacy**, whether it is data being controlled by a third party or off-shored to another country.
  - There will be a corresponding **drop in security as the traditional controls** such as VLANs (virtual local-area networks) and **firewalls prove less effective** during the transition to a virtualized environment.
  - Security managers will need to pay particular attention to systems that contain **critical data such as corporate financial information or source code** during the transition to server virtualization in production environments.
  - **Outsourcing means losing significant control over data**, and while this isn’t a good idea from a security perspective, the business ease and financial savings will continue to increase the usage of these services.
  - Security managers will **need to work with their company’s legal staff to ensure that appropriate contract terms** are in place to protect corporate data and provide for acceptable service-level agreements.

Cloud Security Challenges

- Cloud-based services will result in many **mobile IT users accessing business data and services without traversing the corporate network**.
  - This will increase the need for enterprises to **place security controls between mobile users and cloud-based services.**
  - Placing large amounts of **sensitive data** in a globally accessible cloud **leaves organizations open to large distributed threats—attackers** no longer have to come onto the premises to steal data, and they can find it all in the one “virtual” location.
  - Although **traditional data center security** still applies in the cloud environment, **physical segregation and hardware-based security** cannot protect against attacks between virtual machines on the same server.
  - The **dynamic and fluid nature of virtual machines** will make it difficult to maintain the **consistency of security and ensure the auditability of records**.
  - The ease of **cloning and distribution between physical servers** could result in the **propagation of configuration errors and other vulnerabilities**.

Cloud Security Challenges

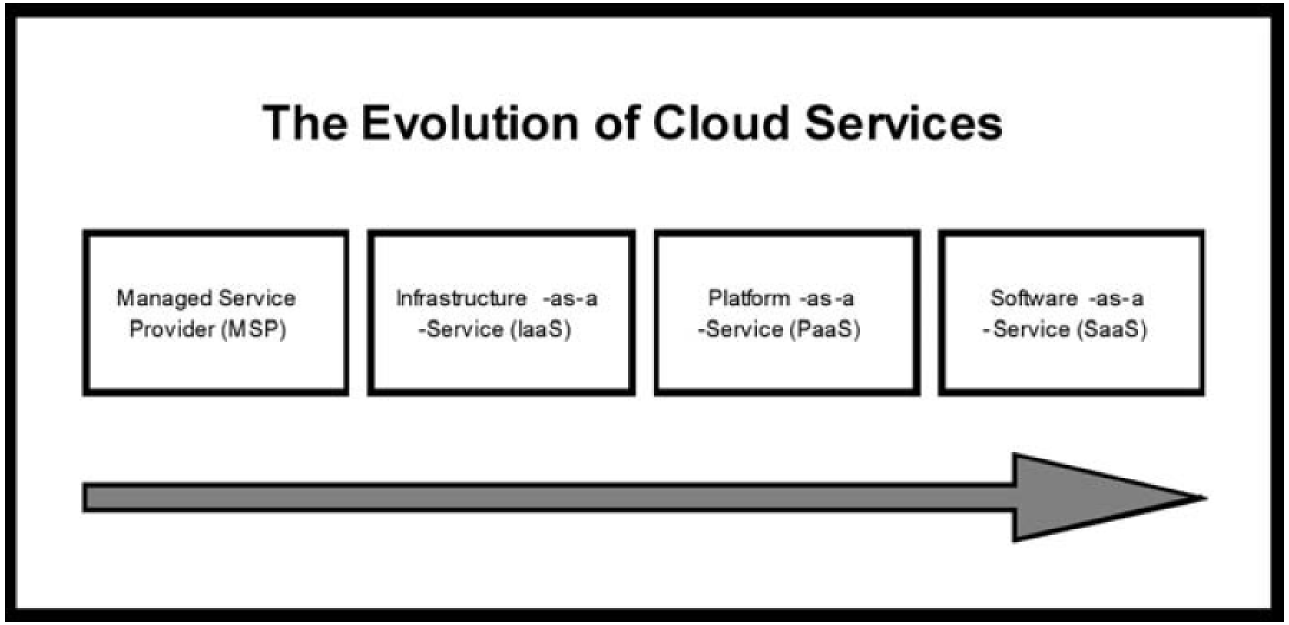
- Virtual machines are vulnerable as they move between the private cloud and the public cloud.
    - A fully or partially shared cloud environment is expected to have a greater attack surface and therefore can be considered to be at greater risk than a dedicated resources environment.
    - Localized virtual machines and physical servers use the same operating systems as well as enterprise and web applications in a cloud server environment, increasing the threat of an attacker or malware exploiting vulnerabilities in these systems and applications remotely.
- **Enterprises** are often required to prove that their **security compliance is in accord with regulations, standards, and auditing practices**, **regardless of the location** of the systems at which the data resides.

Cloud Security Challenges

- Things to note:
  - To establish zones of trust in the cloud, the **virtual machines must be self-defending**, effectively moving the **perimeter to the virtual machine itself**.
  - **Enterprise perimeter security** (i.e., firewalls, demilitarized zones [DMZs], network segmentation, intrusion detection and prevention systems [IDS/IPS], monitoring tools, and the associated security policies) **only controls the data that resides and transits behind the perimeter**.
  - In the cloud computing world, the cloud computing provider is in **charge of customer data security and privacy**.

Software-as-a-Service Security

- **New business models** being developed as a result of the move to cloud computing are **creating not only new technologies** and **business operational processes but also new security requirements and challenges** as described previously.
- As the most recent evolutionary step in the cloud service model (see Figure 6.2), **SaaS will likely remain the dominant cloud service model** for the foreseeable future and the area where the most critical need for **security practices and oversight** will reside.


The Evolution of Cloud Services
Managed Service Provider (MSP)
Infrastructure -as-a -Service (IaaS)
Platform -as-a -Service (PaaS)
Software -as-a -Service (SaaS)

Software-as-a-Service Security

- The technology analyst and consulting firm Gartner lists seven security issues which one should discuss with a cloud-computing vendor:
  1. **Privileged user access** —Inquire about who has specialized access to data, and about the hiring and management of such administrators.
  2. **Regulatory compliance** —Make sure that the vendor is willing to undergo external audits and/or security certifications.
  3. **Data location** —Does the provider allow for any control over the location of data?
  4. **Data segregation** —Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.
  5. **Recovery** —Find out what will happen to data in the case of a disaster. Do they offer complete restoration? If so, how long would that take?
  6. **Investigative support** —Does the vendor have the ability to investigate any inappropriate or illegal activity?
  7. **Long-term viability** —What will happen to data if the company goes out of business? How will data be returned, and in what format?

SaaS Environment – Baseline Security Practices.

- ***Security Governance***
  - A **security steering committee** should be developed whose objective is to focus on **providing guidance about security initiatives and alignment** with business and IT strategies.
  - This committee must clearly define **the roles and responsibilities of the security team** and other groups involved in performing information security functions.
  - **Lack of a formalized strategy** can lead to an **unsustainable operating model and security level** as it evolves.
  - In addition, lack of attention to security governance can result in key needs of the **business not being met, including but not limited to, risk management, security monitoring, application security, and sales support**.
  - Lack of proper governance and management of duties can also result in **potential security risks being left unaddressed and opportunities to improve the business being missed**.

SaaS Environment – Baseline Security Practices.

- ***Risk Management***
  - **Effective risk management** entails **identification of technology assets; identification of data and its links to business processes, applications, and data stores; and assignment of ownership and custodial responsibilities**.
  - Actions should also include **maintaining a repository of information assets**.
  - Owners have authority and accountability for **information assets including protection requirements, and custodians implement confidentiality, integrity, availability, and privacy controls.**
  - A formal risk assessment process should be created that **allocates security resources linked to business continuity.**

SaaS Environment – Baseline Security Practices.

- *Security Monitoring and Incident Response*
  - **Centralized security information management** systems should be used to **provide notification of security vulnerabilities and to monitor systems continuously** through automated technologies to identify potential issues.
  - They should **be integrated with network and other systems monitoring** processes (e.g., security information management, security event management, security information and event management, and security operations centers that use these systems for dedicated 24/7/365 monitoring).
  - Management of **periodic, independent third-party security testing** should also be included.
  - Many of the security threats and issues in SaaS center around **application and data layers**, so the types and sophistication of threats and attacks for a SaaS organization require a different approach to security monitoring than traditional infrastructure and perimeter monitoring.
  - The organization may thus need to expand its **security monitoring capabilities to include application- and data-level activities**.
  - This may also require **subject matter experts in applications**security and the unique aspects of maintaining privacy in the cloud.

SaaS Environment – Baseline Security Practices.

- *Security Architecture Design*
  - A **security architecture framework** should be established with consideration of processes (enterprise authentication and authorization, access control, confidentiality, integrity, nonrepudiation, security management, etc.), operational procedures, technology specifications, people and organizational management, and security program compliance and reporting.
  - A **security architecture document** should be developed that **defines security and privacy principles** to meet business objectives.
  - **Documentation is required for management controls and metrics** specific to asset classification and control, physical security, system access controls, network and computer management, application development and maintenance, business continuity, and compliance.
  - A **design and implementation program** should also be integrated with the formal system development life cycle to include a business case, requirements definition, design, and implementation plans.

SaaS Environment – Baseline Security Practices.

- Technology and design methods should be included, as well as the **security processes** necessary to provide the following services across all technology layers:
  1. Authentication
  2. Authorization
  3. Availability
  4. Confidentiality
  5. Integrity
  6. Accountability
  7. Privacy
- The creation of a **secure architecture** provides the engineers, **data center operations personnel, and network operations personnel a common blueprint** to design, build, and test the security of the applications and systems.

SaaS Environment – Baseline Security Practices.

- ***Data Security***
- The ultimate challenge in cloud computing is **data-level security, and sensitive data** is the domain of the enterprise, not the cloud computing provider.
- Security will need to move to the **data level so that enterprises** can be sure their data is protected wherever it goes.
    - For example, with data-level security, the enterprise can specify that this data is not allowed to go outside of the United States.
- It can also **force encryption of certain types of data**, and permit only specified users to access the data.
- It can provide compliance with the **Payment Card Industry Data Security Standard (PCI DSS).**

SaaS Environment – Baseline Security Practices.

- ***Application Security***
  - Application security is one of the **critical success factors** for a **world-class SaaS company**.
  - This is where the **security features and requirements** are defined and application security test results are reviewed.
  - Application security processes, secure coding guidelines, training, and testing scripts and tools are typically a **collaborative effort between the security and the development teams**.
  - **External penetration testers** are used for application **source code reviews, and attack and penetration tests** provide an objective review of the security of the application as well as assurance to customers that attack and penetration tests are performed regularly.
  - **Fragmented and undefined collaboration** on application security can result in **lower-quality design, coding efforts, and testing results.**
  - **Open Web Application Security Project (OWASP)**15 **guidelines for secure application development** (mirroring Requirement 6.5 of the PCI DSS, which mandates compliance with OWASP coding practices) and locking down ports and unnecessary commands on Linux, Apache, MySQL, and PHP (LAMP) stacks in the cloud, just as you would on-premises.

SaaS Environment – Baseline Security Practices.

- ***Virtual Machine Security***
  - In the cloud environment, **physical servers are consolidated** to multiple virtual machine instances on virtualized servers.
  - **Firewalls, intrusion detection and prevention, integrity monitoring, and log inspection** can all be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premises to public cloud environments.
  - By deploying this traditional line of defense to the virtual machine itself, you can enable **critical applications and data to be moved to the cloud securely**.
  - To facilitate the **centralized management of a server firewall policy**, the security software loaded onto a virtual machine should include a **bidirectional stateful firewall** that enables **virtual machine isolation and location awareness**, thereby enabling a **tightened policy** and **the flexibility to move the virtual machine from on-premises to cloud resources**.
  - **Integrity monitoring and log inspection software** must be applied at the virtual machine level.

SaaS Environment – Baseline Security Practices.

- ***Advantages Virtual Machine Security***
- The approach to virtual machine security, which connects the machine back to the mother ship, has some advantages
  - The security software can be put into a single software agent that provides for consistent control and management throughout the cloud while integrating seamlessly back into existing security infrastructure investments,
  - Providing economies of scale, deployment,
  - And cost savings for both the service provider and the enterprise.