Nadar Saraswathi College of Engineering & Technology

NSCET E-LEARNING PRESENTATION

LISTEN … LEARN… LEAD…

Nadar Saraswathi College of Engineering & Technology

COMPUTER SCIENCE AND ENGINEERING

IV YEAR / VII SEMESTER

CS8791 CLOUD COMPUTING

A.DURAIMURUGAN , M.E, (Ph.d)

ASSISTANT PROFESSOR

Nadar Saraswathi College of Engineering & Technology,

Vadapudupatti, Annanji (po), Theni – 625531.

Nadar Saraswathi College of Engineering & Technology

UNIT IV

RESOURCE MANAGEMENT AND SECURITY IN CLOUD

Nadar Saraswathi College of Engineering & Technology

Objectives

- ✓ Provides a simple and unambiguous taxonomy of three service models - Software as a service (SaaS) - Platform as a service (PaaS) - Infrastructure as a service (IaaS) (Private cloud, Community cloud, Public cloud, and Hybrid cloud)

Features of cloud computing

- ✓ The goal is to accelerate the federal government's adoption of secure and effective cloud computing to reduce costs and improve services.
- ✓ On demand-self service
- ✓ Broad Network access
- ✓ Resource pooling
- ✓ Rapid elasticity
- ✓ Measured service
- ✓ pricing

Data Related Security

Data Breach:

1.Confidentiality

2. Integrity

Data Lock in: Users may lose data if they migrate from one vendor to another vendor.

Data Remanence: It is the residual representation of data that have been nominally erased or removed in some way.

Data Related Security

- ✓ Data Recovery: Sometimes server may break down and cause damage or loss to users data. To avoid this, data should be backed up to be recovered in future

- ✓ Data Locality: In SaaS model of cloud environment, the user doesn't know where the data is stored which may be an issue. The issue can be solved by creating secure SaaS model which can provide reliability to the customer on the location of the data of the user.

Application related security issues

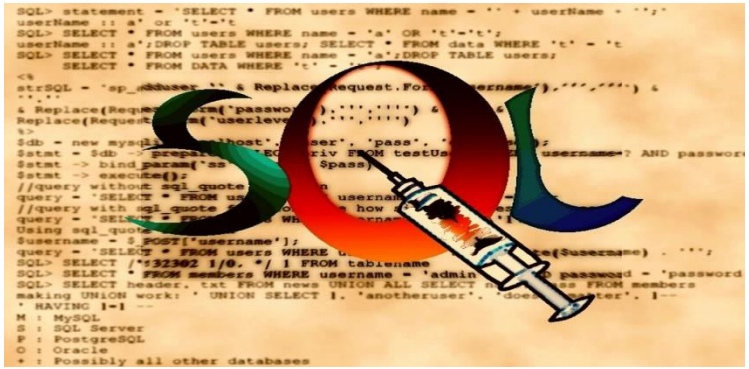
- ✓ Cloud malware injection attack: In this attack a malicious virtual machine or a service implementation is injected into the cloud system. one solution to prevent this is to perform the integrity check to the service instance.
- ✓ Cookie poisoning: In this an unauthorized access is made into the application by modifying the contents of the cookie. One solution is to clean up the cookie or encrypt the cookie data.

Application related security issues

- ✓ Backdoor and Debug Option: Debug option is for the developers who use it to implement any changes requested at later stage in a website since these debug option provides back entry for the developers, sometimes these debug options are left enabled unnoticed, they may provide easy access to the hackers and allow them to make changes in the website.
- ✓ Hidden Field Manipulation: Certain fields are hidden in the web-site and is used by the developers. Hacker can easily modify on the web page.

CSP level attacks

- ✓ Guest hopping attack: An attacker will try get access to one virtual machine by penetrating another virtual machine hosted in the same hardware.
- ✓ SQL injection: It can be done by injecting the SQL commands into the database of an application to crash the database.



CSP level attacks

- ✓ Malicious Insider: In private cloud, its employee is granted access to the sensitive data of some or all customer administrators. Such privileges may expose information to security threats.

- ✓ Side channel attack: It occurs when an attacker places a malicious virtual machine on the same physical machine as the victim machine so that he can access all the confidential information on the victims machine.

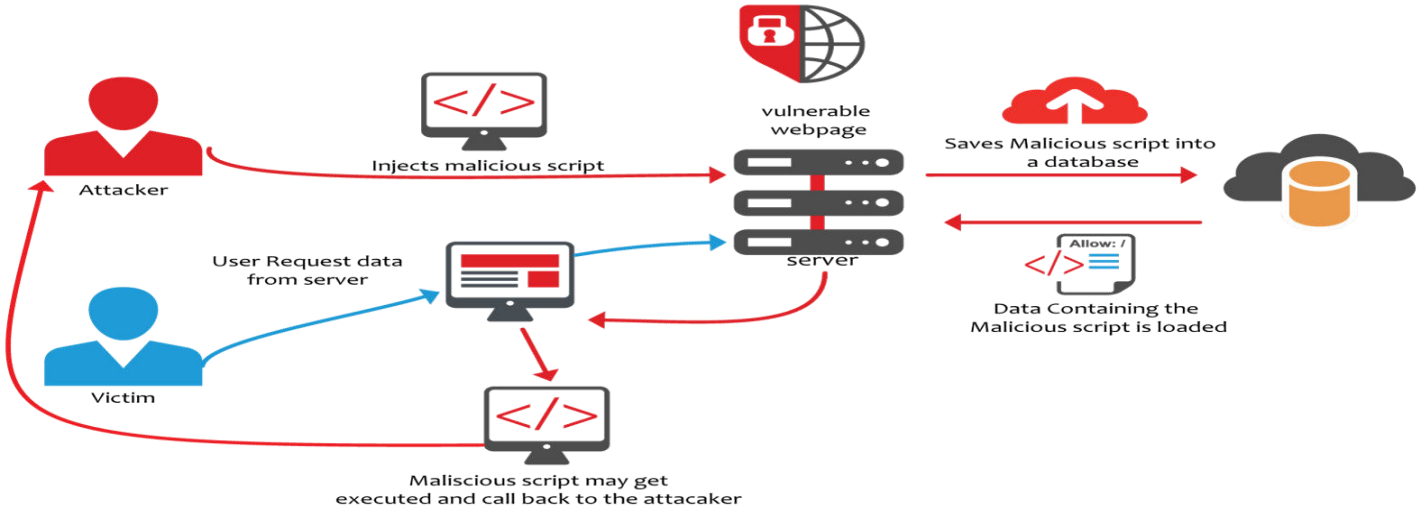
Network level attacks

DNS attacks:

- ✓ Domain hijacking: Domain hijacking is defined as changing the name of a domain without the knowledge or permission from the domain's owner or creator. This enable the intruders to access the sensitive information.
- ✓ Cross site scripting: It is a type of attack in which user enters right URL of a website and hacker on the other site redirect the user to its own website and hack its credentials.

Application related security issues

- ✓ Backdoor and Debug Option: Debug option is for the developers who use it to implement any changes requested at later stage in a website since these debug option provides back entry for the developers, sometimes these debug options are left enabled unnoticed, they may provide easy access to the hackers and allow them to make changes in the website.
- ✓ Hidden Field Manipulation: Certain fields are hidden in the web-site and is used by the developers. Hacker can easily modify on the web page.



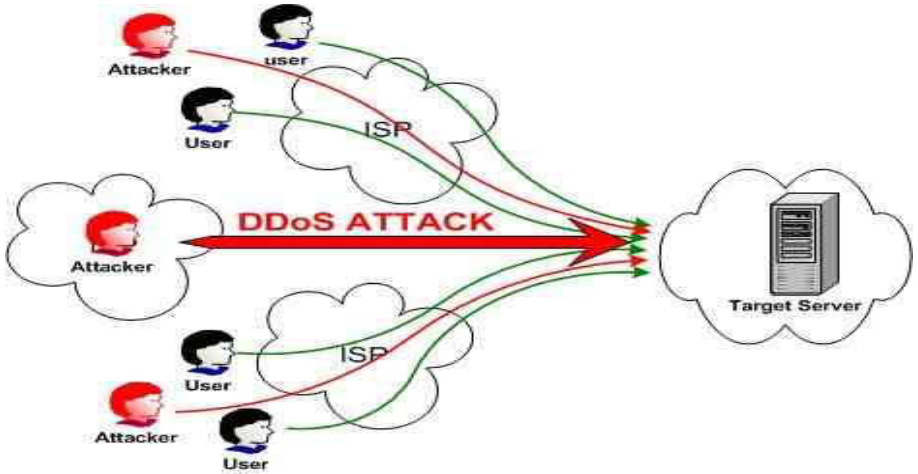
Nadar Saraswathi College of Engineering & Technology

Topic

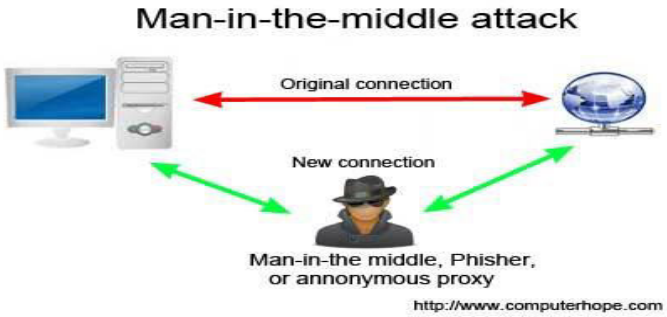
IP spoofing

Nadar Saraswathi College of
Engineering & Technology

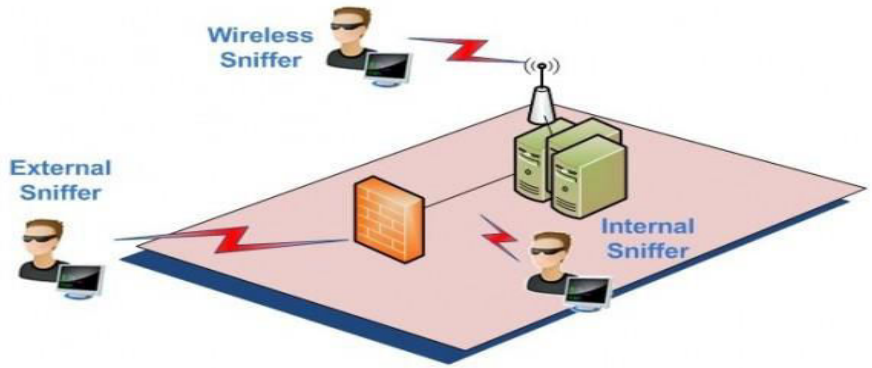
DOS attack: When hackers overflows a network server or web server with frequent request of services to damage the network, the denial of service cannot keep up with them, server could not legitimate client regular requests.



Man in the middle attack: This is another issue of network security that will happen if secure socket layer (SSL) is not properly configured.



Network Sniffing: Another type of attack is network sniffer, it is a more critical issue of network security in which unencrypted data are hacked through network.



Security requirements for cloud computing.

- Identification and Authenticity:
- Authorization
- Non-repudiation
- Availability

Challenges in cloud computing

- Security
- Costing model
- Charging model
- Service level agreement
- Cloud interoperability issue

Topic

CLOUD SECURITY GOVERNANCE

Nadar Saraswathi College of Engineering & Technology

CLOUD SECURITY

•Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data, and infrastructure.

• These security measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices.

Cloud security

•Cloud security is effective and efficient security management and operations in the cloud environment so that an enterprise's business targets are achieved.

•This model incorporates a hierarchy of executive mandates, performance expectations, operational practices, structures, and metrics that, when implemented, result in the optimization of business value for an enterprise

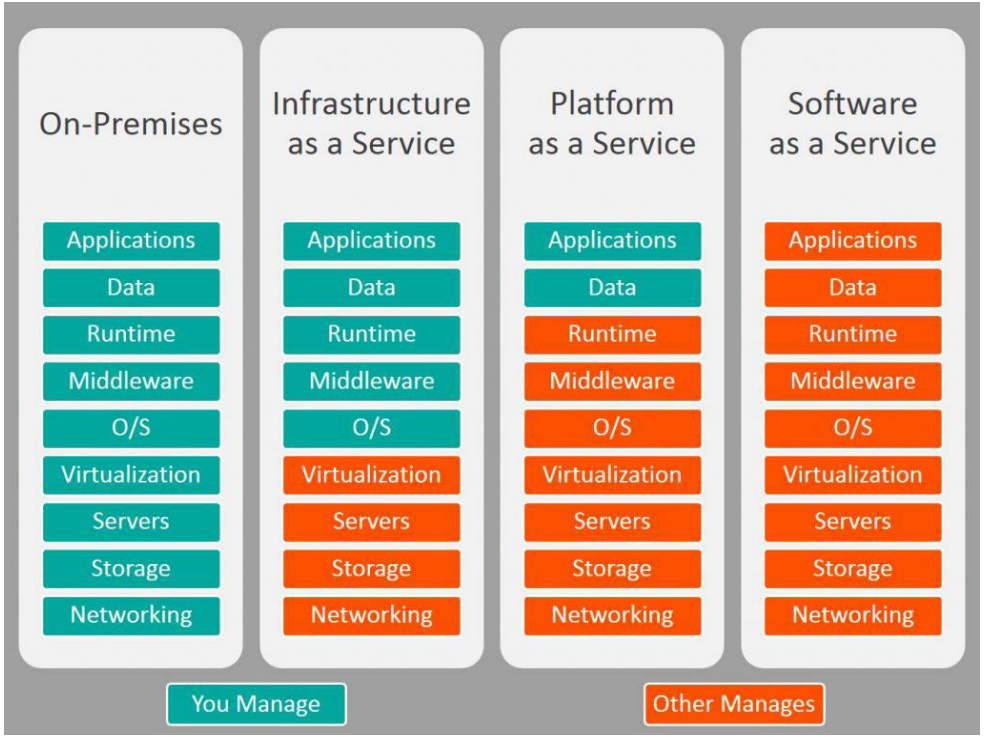
Why cloud security is required?

•Cloud security is important for both business and personal users. Everyone wants to know that their information is safe and secure and businesses have legal obligations to keep client data secure, with certain sectors having more stringent rules about data storage.

•Security is an essential element of your cloud service and you should always check that your service provider can provide the correct levels of security for your industry.

Cloud security

Cloud security



CLOUD SERVICE PROVIDER SECURITY

•The cloud shared responsibility model denotes that CSPs are responsible for the security of the cloud and customers are responsible for securing the data they put in the cloud.

•Depending on the type of deployment—IaaS, PaaS, or SaaS—customer responsibilities will be determined.

Cloud Security Guidance

•The Cloud Security Guidance aims to guide organisations including government, cloud service providers (CSP), and Information Security Registered Assessors Program (IRAP) assessors on how to perform a comprehensive assessment of a CSP and its cloud services so a risk-informed decision can be made about its suitability to handle an organisation's data.

CLOUD CONSUMER SECURITY

Through 2020, 80% of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, not cloud provider vulnerabilities

-Gartner

CONSUMER SECURITY RESPONSIBILITIES

- Security Configuration
- Redundancy(ISP/CSP)
- Access management
- Source Control/Drifting
- Network Segregation
- Monitoring
- Patch management