

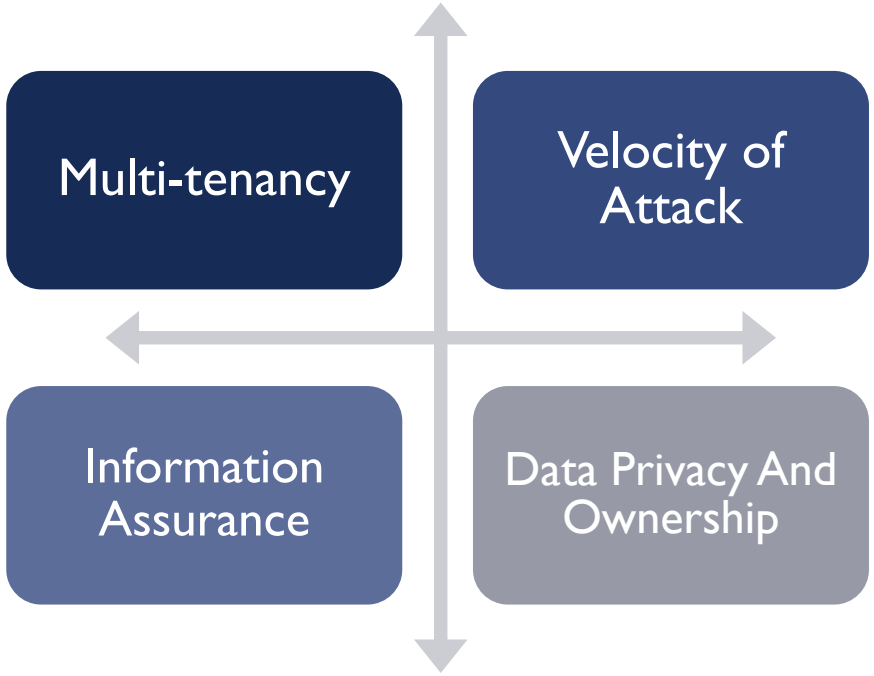


# CLOUD SECURITY : THREATS AND ATTACKS

SAMITHA SOMATHILAKA

Department of Computing & Mathematics, WIT

# CLOUD SECURITY - CONCERNS



# MULTI-TENANCY ISSUES IN THE CLOUD

- Conflict between tenants' opposing goals
  - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
  - Can tenants get along together and 'play nicely' ?
  - If they can't, can we isolate them?
- How to provide separation between tenants?
- Cloud Computing brings new threats
  - Multiple independent users share the same physical infrastructure
  - Thus an attacker can legitimately be in the same physical machine as the target

# SECURITY CONCERN: VELOCITY OF ATTACK

- Security threats amplify and spread quickly in a Cloud-known as “Velocity-of-Attack”
  - Effect of high VOA
    - Potential loss due to an attack is comparatively higher
- It is Comparatively difficult to mitigate the spread of the attack
- To counter this Challenge of VOA CSPs need to adopt robust security enforcement mechanisms

# SECURITY CONCERN: INFORMATION ASSURANCE AND DATA

- Information assurance concerns for cloud users involve
  - CIA
  - Authentication
  - Authorization use
- Data ownership concerns for cloud clients
  - In cloud, data belonging to a Cloud Client is maintained by a CSP, who has access to the data, but is not the legitimate owner of it
    - This raises concern of potential unauthorized data access and misuse
- Data should be protected using encryption and access control mechanisms

# SECURITY CONCERN: DATA PRIVACY

- Potential for unauthorized disclosure of private of a cloud client
- Private data may include
  - Individual identity of the client
  - Detail of the service requested by the client
  - Proprietary data of the client
- A CSP needs to ensure that private data of its client is protected from unauthorized disclosure
  - Both collections and dissemination of the private data requires protection
  - A CSP needs to deploy data privacy mechanisms, which are compliant with regional legal regulations

# NEW THREATS & ATTACKS

# SECURITY THREAT

**VM Theft:** A vulnerability that ensures an attacker to copy or move a VM in an unauthorized manner

- Is a result of inadequate controls on VM files allowing unauthorized copies or move operations

**Hyper-jacking:** It enables an attacker to install a rogue hypervisor or VM Monitor(VMM) that can take control of the underlying server resources

- An attacker can run unauthorized application on guest without the OS realizing it

**Data Leakage:** Confidential data stored on a third party Cloud is potentially vulnerable to unauthorized access or manipulation.

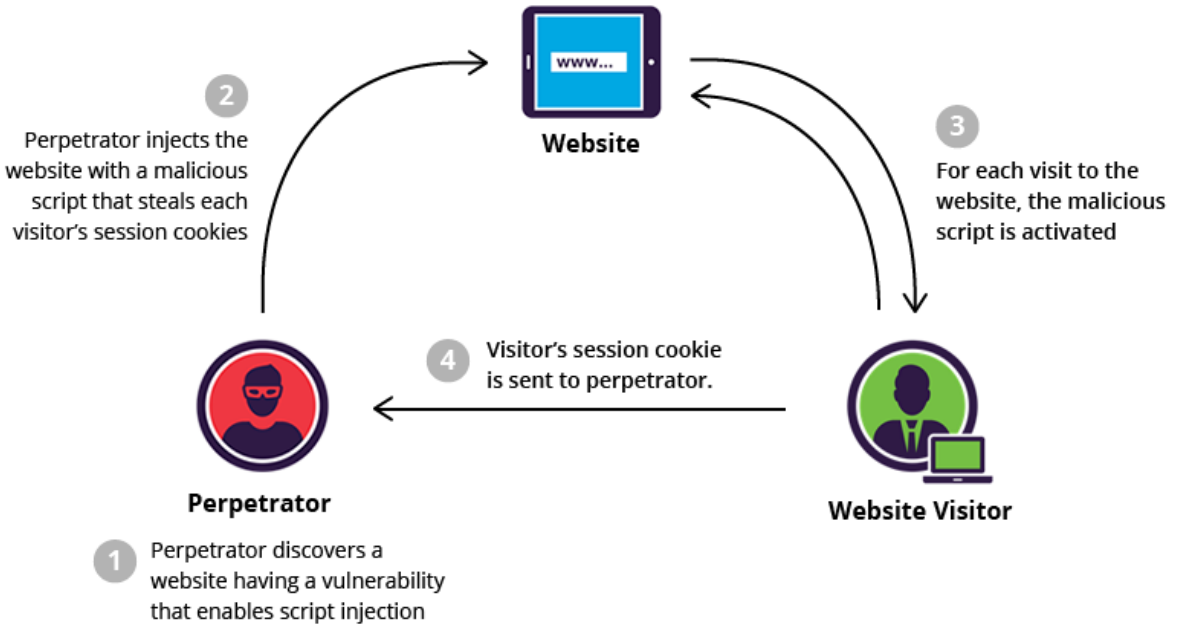
- Attacks n service provider's control systems(for example password lists) could make all the client's data vulnerable.

# 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.
- **Backdoor and Debug Option:** Debug option is for the developers who use it to implement any changes requested at later stage in an implementation 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.
- **Guest hopping attack:** An attacker will try get access to one virtual machine by penetrating another virtual machine hosted in the same hardware.

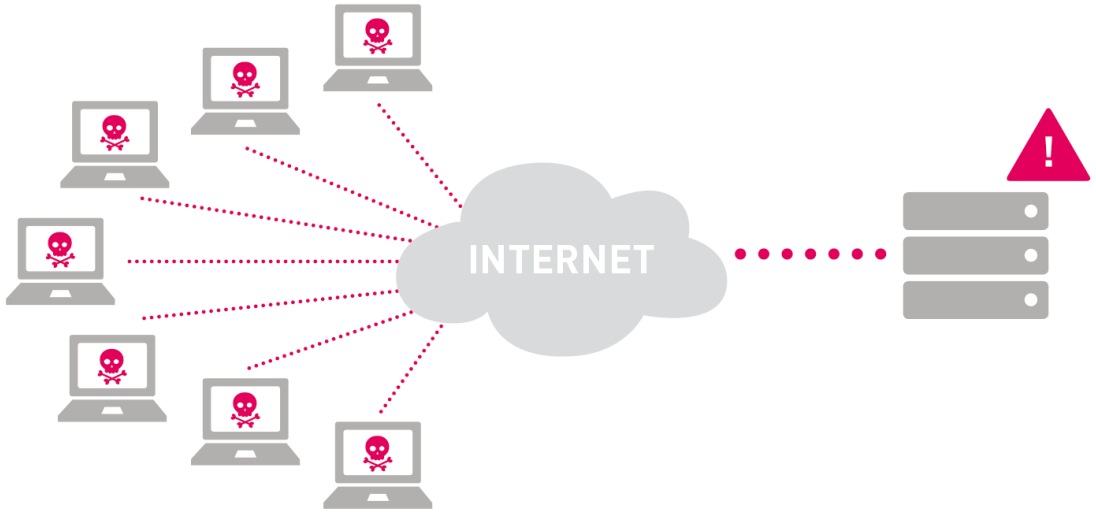
# NETWORK LEVEL ATTACKS

- **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.



# NETWORK LEVEL ATTACKS

- **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.



# NETWORK LEVEL ATTACKS

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