Security Issues at Network Level, Host Level and Application Level

Y. V. Lokeswari
AP / CSE
SSN College of Engineering

Security Threats

- Top security threats in cloud computing is classified as
  - Network level,
  - Host level and
  - Application level.

Network level security issues

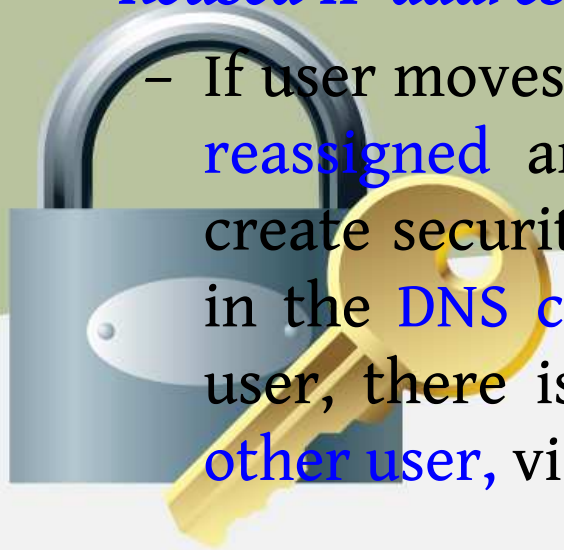
- In public cloud architecture the data moves to or from the organization.
- The network level security risk is classified as three types such as ensuring the
  - »Data confidentiality,
  - »Data Availability and
  - »Data Integrity.

Network level security issues

- ***Eavesdropping***
  - The unauthorized user access the data due to interception of network traffic, it results in failure of confidentiality. The Eavesdropper secretly listen the private conversation of others. This attack may done over email, instant messaging, etc. [2]
- ***Replay attack***
  - Its a network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. The attacker intercepts and save the old messages and later it is send to one of participants to gain access to unauthorized resources.

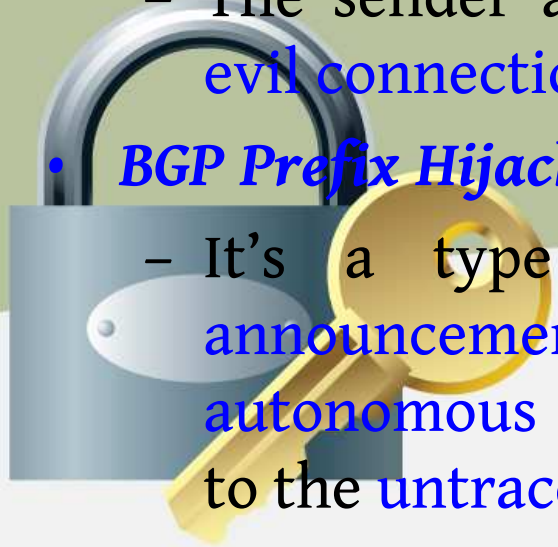
Network level security issues

- ***In Sybil attack***
  - The malicious user pretends to be distinct users after acquiring multiple identities and tries to create relationship with honest user. If malicious user is successful to compromise one of the honest users then attacker gains unauthorized privileges that helps in attacking process.
- ***Reused IP address***
  - If user moves out of the network then same IP address is reassigned and reused by other customer, so it will create security risk to new user. The address still exists in the DNS cache. If old IP address is assigned to new user, there is a chance of accessing the data by some other user, violating the privacy of the original user.



Network level security issues

- ***DNS Attacks***
  - It translate the domain name to an IP address, Since domain name is easier to remember rather than IP address.
  - The user using IP address in not feasible because he /she has been routed to some other cloud instead of the one he/ she asked.
  - The sender and a receiver get rerouted through some evil connection.
- ***BGP Prefix Hijacking***
  - It's a type of network attack in which wrong announcement on IP address associated with a autonomous system (AS), so malicious parties get access to the untraceable IP address

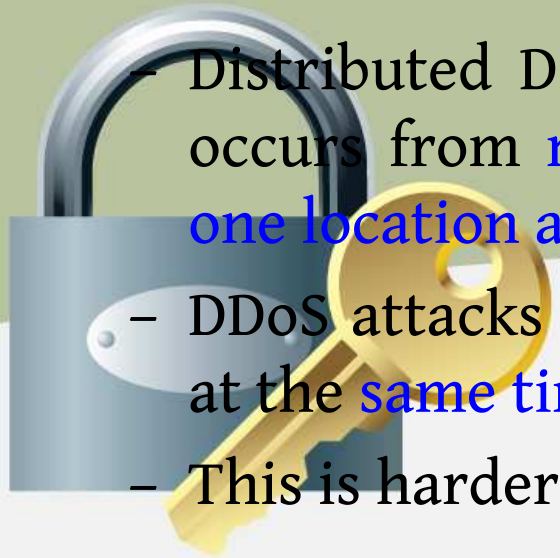


Network level security issues

- ***Sniffer Attack***
  - Data is flowing in network, and there is a chance to read the vital information, it can be traced and captured.
  - Sniffer program records the data/traffic linked to other systems through the NIC (network Interface Card).
- ***Port Scanning***
  - If customer configures the security group to allow traffic from any source to a specific port, then that specific port will be vulnerable to a port scan.

Network level security issues

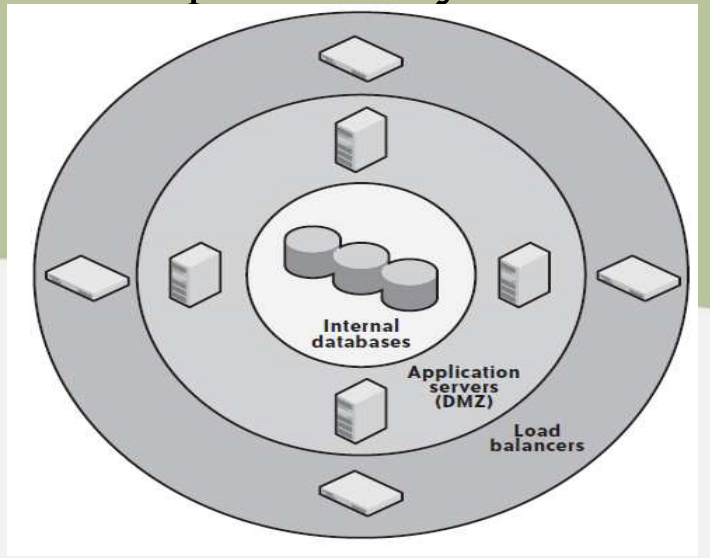
- ***Dos Attack***
  - Dos attack is an attack which forces the system component to limit, or even halt, normal services. The network is unavailable by flooding it , disrupting it, jamming it, or crashing it.
  - DoS attacks can be prevented with a firewall but they have to be configured properly
- ***Distributed Denial of Service Attack***
  - Distributed Denial of Service attack is a DoS attack that occurs from more than one source, and from more than one location at the same time.
  - DDoS attacks that comes from many "dummy" computers at the same time to flood the server.
  - This is harder to trace and they can use more bandwidth.



Network level security solutions

Firewall Rules

- Typically, a firewall protects the perimeter of one or more network segments. [1]
  - A main firewall protects the outermost perimeter, allowing in only HTTP, HTTPS, and (sometimes) FTP* traffic.
  - Within that network segment are border systems, such as load balancers, that route traffic into a DMZ protected by another firewall.
  - Finally, within the DMZ are application servers that make database and other requests across a third firewall into protected systems on a highly sensitive internal network.



Few best practices for network security

- Run only one network service (plus necessary administrative services) on each virtual server.
- Do not open up direct access to your most sensitive data
- Open only the ports absolutely necessary to support a server's service and nothing more
- Limit access to your services to clients who need to access them
- Even if you are not doing load balancing, use a reverse proxy
- Use the dynamic nature of the cloud to automate your security embarrassments

Network Intrusion Detection

- **Perimeter security** often involves network intrusion detection systems (NIDS), such as Snort, which monitor local traffic for anything that looks irregular.
- Examples of irregular traffic include:
  - Port scans
  - Denial-of-service attacks
  - Known vulnerability exploit attempts
- One can perform network intrusion detection either by routing all traffic through a system that analyzes it or by doing passive monitoring from one box on local traffic on your network

Host Security

- Host security describes how your server is set up for the following tasks:
  - Preventing attacks.
  - Minimizing the impact of a successful attack on the overall system.
  - Responding to attacks when they occur.

Host Level Security issues

- Cloud service provider do not publicly share information related to their host platforms, host operating systems, and processes that are in place to secure the hosts, since hackers are trying to intrude into the cloud service.

Host Level Security issues

- ***Security concerns with the hypervisor***
  - Hypervisor is a controller called as Virtual machine manager (VMM) that allows multiple OS runs on single machine at a time. [2]
  - If number of Operating systems running on hardware platform increases, security issues also increases, because single hardware unit is difficult to monitor multiple operating systems.
  - eg.:- Guest system tries to run malicious code on the host system and get control of the system and block other guest OS, even it can make changes to any guest OS.

Host Level Security issues

- ***Security concerns with the hypervisor***
  - Virtualization platform is software. Major virtualization platform vendors are VMware, Xen and Microsoft.
  - Its important to secure the layer of software that sits between hardware and virtual servers.
  - The isolation of customer VMs from each other in a multitenant environment.
  - It is very important to protect the hypervisors from unauthorized users

Host Level Security issues

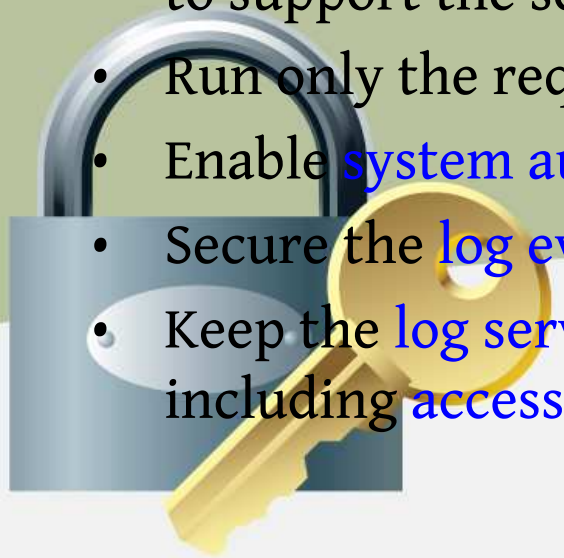
Virtual server Security

- Customers of IaaS have full access to the virtualized guest VMs that are hosted and isolated from each other by hypervisor technology.
- Virtual server may be accessible on the internet, so sufficient network access preventive steps should be taken to restrict access to virtual instances

Host Level Security practices

Virtual server Security practices

- Protect the integrity of the image from unauthorized users.
- Secure the private keys in the public cloud.
- Keep the decryption keys away from the cloud
- Do not allow password-based authentication for shell access.
- Require role-based access password
- Run a host firewall and open only the minimum ports necessary to support the services on an instance.
- Run only the required services and turn off the unused services
- Enable system auditing and event logging,
- Secure the log events to a dedicated log server.
- Keep the log server separate with higher security protection, including access controls.

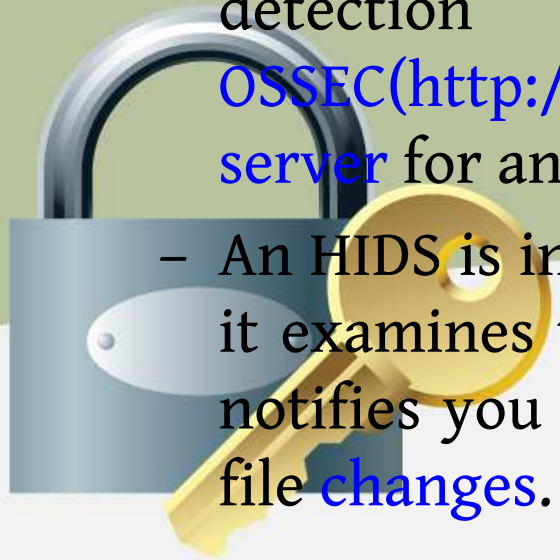


Host Level Security solutions

- ***System Hardening***
  - Prevention begins when you set up your machine image. As you get going, you will experiment with different configurations and constantly rebuild images.
  - Once you have found a configuration that works for a particular service profile, you should harden the system before creating your image. [1]
- ***Server hardening***
  - It is the process of disabling or removing unnecessary services and eliminating unimportant user accounts.
  - Tools such as Bastille Linux can make the process of hardening your machine images much more efficient.

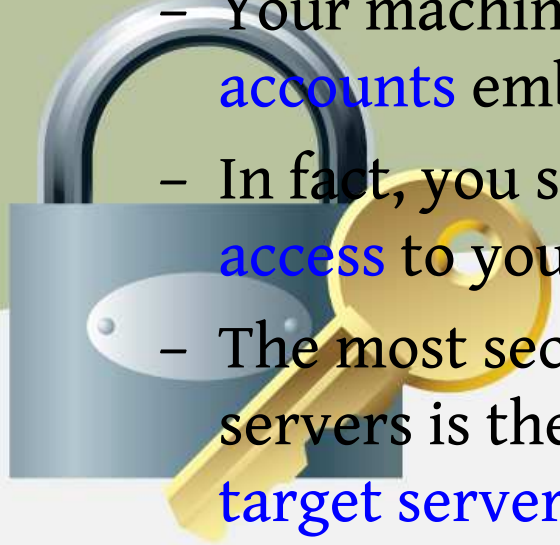
Host Level Security solutions

- ***Antivirus Protection***
  - Some regulations and standards require the implementation of an antivirus (AV) system on your servers
- ***Host Intrusion Detection***
  - Whereas a network intrusion detection system monitors network traffic for suspicious activity, a host intrusion detection system (HIDS) such as OSSEC(http://www.ossec.net) monitors the state of your server for anything unusual.
  - An HIDS is in some ways similar to an AV system, except it examines the system for all signs of compromise and notifies you when any core operating system or service file changes.



Host Level Security solutions

- ***Data Segmentation***
  - The segmentation of data based on differing levels of sensitivity is your first tool in minimizing the impact of a successful attack.
  - Eg: Data segmentation involves separation of credit card data from customer data.
- ***Credential Management***
  - Your machine images OSSEC profile should have no user accounts embedded in them.
  - In fact, you should never allow password-based shell access to your virtual servers.
  - The most secure approach of providing access to virtual servers is the dynamic delivery of public SSH keys to target servers

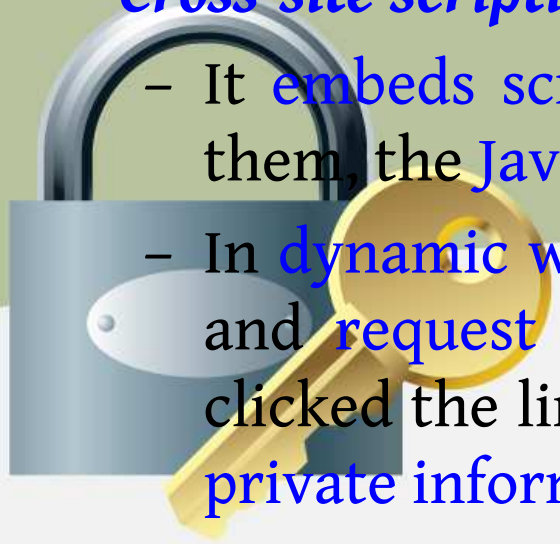


Application Level Security issues

- Some company host applications in internet
- Many user use without considering about
- Where, how, by whom the services are provided, so proper security mechanism should be adapted.

Application Level Security issues

- ***SQL Injection attack***
  - Attackers insert a malicious code into a standard SQL code and it allow unauthorized person to download the entire database or interact it in other illicit ways.
  - So Unauthorized user can access the sensitive data.
  - This can be avoided by usage of dynamically generated SQL in the code. [2]
- ***Cross-site scripting [XSS]***
  - It embeds script tags in URLs and when user clicks on them, the JavaScript get executed on machine.
  - In dynamic websites, some pop ups windows get opened and request the user to click on that link, once user clicked the link the hacker get control and access all our private information

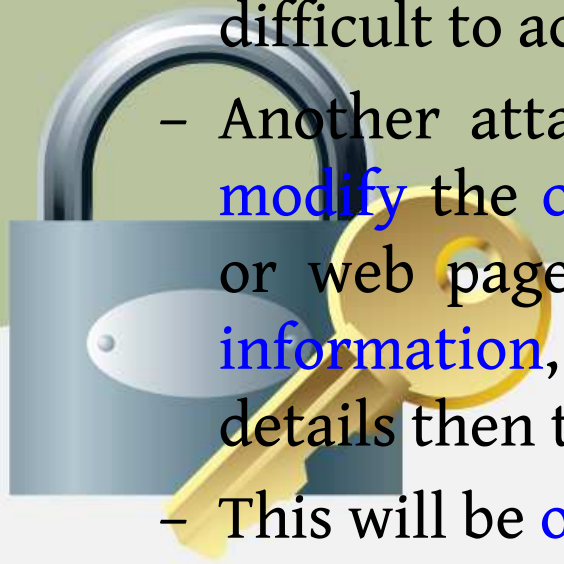


Application Level Security issues

- ***EDoS* - Economic Denial of Sustainability**
  - An attack against the billing model that underlies the cost of providing a service with the goal of bankrupting the service itself.
  - DoS attacks on pay-as-you-go cloud applications will result dramatic increase in your cloud utility bill, increased use of network bandwidth, CPU, and storage consumption.

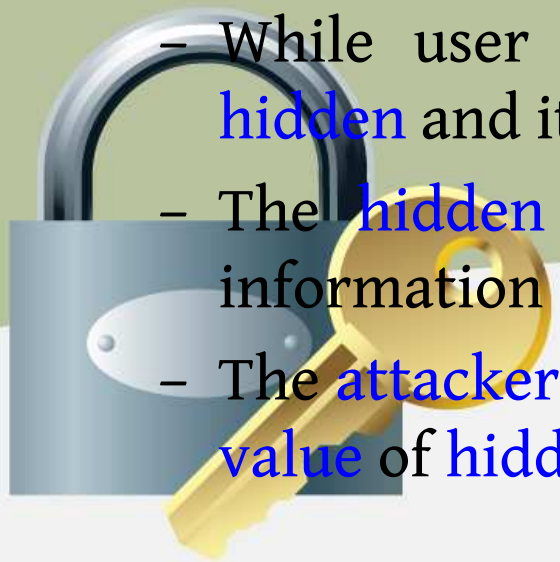
Application Level Security issues

- ***Cookie Poisoning***
  - Cookies used to store User IDs. The two types of cookies are: persistent and non-persistent.
  - Persistent cookie is stored on the client hard-drive, hacker who can access the client machine and easily access the cookies
  - Non-Persistent cookie is stored in memory and more difficult to access.
  - Another attack is unauthorized person can change or modify the content of cookies to access the application or web page. Cookies contain user identity credential information, one unauthorized person access these details then they can able to forge as an authorized user.
  - This will be overcome by regular cookie cleanup.



Application Level Security issues

- ***Backdoor and debug options***
  - Normally developers will enable the debugging option while publishing the web site. So hacker can easily enter into the web-site and make some changes.
  - To prevent this attack developer should disable the debugging option.
- ***Hidden field manipulation***
  - While user accessing the web page some fields are hidden and its used by developer.
  - The hidden fields in HTML forms convey important information such as price, user ID etc.
  - The attacker can save the catalogue page and change the value of hidden field and posted on web page



Application Level Security issues

- ***Google Hacking***
  - Google search engine is the best option for the hacker to access the sensitive information.
  - Even the hacker hacks the user's account.
  - Generally they try to find out the security loopholes on Google and after having gathered the necessary information of the concerned system, they hack the account information.

Application Level Security issues

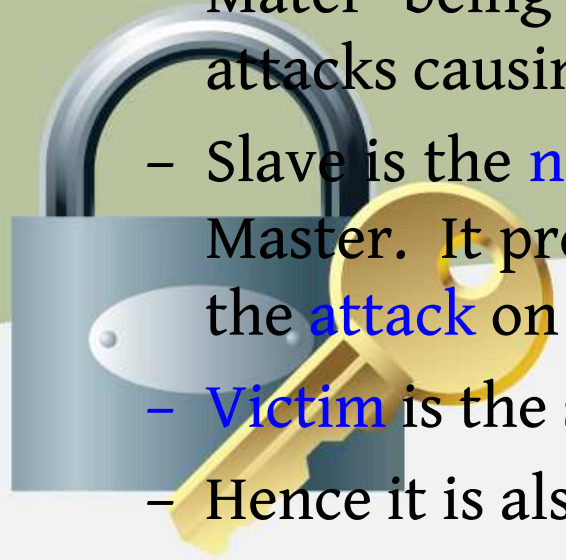
- ***Man in the middle attack***
  - This attack is also a category of eavesdropping.
  - The attacker set up the connection between two users and tries to hear the conversation or it provide false information between them.
  - Tools like Dsniff, Cain, Ettercap, Wsniff, Airjack etc have developed to protect from this attack

Application Level Security issues

- ***Dos Attack***
  - Dos attack the services assigned to the authorized users unable to use by them. When the large number of services request handled by the server exceeds, the service becomes unavailable to the authorized user.
  - DoS attack increases bandwidth consumption besides causing congestion
  - Intrusion detection system (IDS) is the most popular method of defense against this type of attacks

Application Level Security issues

- ***Distributed Denial of services***
  - DDos is advanced version of DoS in terms of denying the services running on a server. Many dummy computers generate request to single server from many locations at same time.
  - Three functional units of DDos attacks: A Master, A Slave and A Victim.
  - Mater being the attack launcher is behind all these attacks causing DDoS,
  - Slave is the network which acts like a launch pad for the Master. It provides the platform to the Master to launch the attack on the Victim.
  - Victim is the system being compromised.
  - Hence it is also called as coordinated attack.



Application Level Security Solutions

- ***Identity based access***
  - In identity based access a username and password is provided by the user and if they matches with the records in the database then only the access is provided otherwise the access is denied.
- ***Role based access***
  - In role based identity a role is associated with the user like administrator, developer etc and the application changes the view according to the role of that user.

Application Level Security Solutions

- ***Key based access***
  - In key based identity the end user is provided a key and by using that key only the end user can access the services.
  - This key is also stored in the database for verification.
  - This key is encrypted and is generally very long such that no one can guess it.
- ***Claim based access***
  - In claim based identity a live id is created for a particular brand and all other services provided by that particular brand are accessed by that id. [3]

References

- Leese, Goerge. “Cloud Application Architecture”, Building applications and Infrastructure in the cloud (2010). O’Reilly publication.
- Charanya, R., M. Aramudhan, K. Mohan, and S. Nithya. "Levels of Security Issues in Cloud Computing." *International Journal of Engineering and Technology (2013)* Vol 5 (2).
- Ankur Pandey et al, “Application Level Security in Cloud Computing” , (IJCSIT) International Journal of Computer Science and Information Technologies, (2012) Vol. 3 (6),