Cloud Computing and Web Service (IT4221)

Cloud Security

Course Instructor: Binanda Sengupta (Assistant Prof. @IT)
Email: binanda.it@faculty.iiests.ac.in
Webpage: https://sites.google.com/view/binanda

Introduction to Cloud Security

- One of the items that critics of clouds repeatedly hammer on is cloud security
- It also introduces real regulatory and standards compliance issues that needs to be considered
- In reality, the cloud can be made as secure as – or even more secure than – a traditional data center
- Ways of approach towards achieving information security may be radically different

Introduction to Cloud Security

- A move into the cloud requires consideration of a number of critical security issues:
  - Legal implications, regulatory compliance, and standards compliance issues are different in the cloud
  - There is no perimeter in the Amazon cloud; a security policy focused on perimeter security will not work with Amazon and should not be your focus, even with clouds that support traditional perimeter security
  - Although there have been no publicized exploits, cloud data storage should assume a high-risk profile
  - Virtualization technologies may have their own vulnerabilities and thus may introduce new attack vectors

Legal, Regulatory, and Standards Implications

- Unfortunately, the law and standards bodies are a bit behind the times when it comes to virtualization

- Many laws and standards assume that any given server is a physically distinct entity

- Most of the time, the difference between a physical server and a virtual server is not important to the spirit of a given law or standard, but the law or standard may nevertheless specify a physical server because the concept of virtual servers was not common when the specification was being written

Legal, Regulatory, and Standards Implications

- Before moving into the cloud, one must fully understand all of the relevant laws and standards to which your applications and infrastructure are bound
- In all probability, a cloud equivalent will support the spirit of those regulations and standards, but a client may have to talk to experts in its specific requirements to find a definitive answer as to whether the cloud can be considered conformant
- In cases where a pure cloud infrastructure won’t support client’s needs, it can craft a mixed infrastructure that will still provide many of the benefits of the cloud while still clearly complying with standards and regulations

Legal, Regulatory, and Standards Implications

- Beyond compliance issues, the cloud also introduces legal issues related to where client's data is stored:
  - Data may be exposed to subpoenas and other legal procedures that cite client’s cloud provider instead of citing the client, and that may invoke different rights than procedures involving the client directly
  - Some nations have strict regulations governing the physical location of private data

Disaster Recovery

- Disaster recovery is the art of being able to resume normal systems operations when faced with a disaster scenario
- In general, a disaster is an anomalous event that causes the interruption of normal operations
- In a traditional data center, for example, the loss of a hard drive is not a disaster scenario, because it is more or less an expected event
- A fire in the data center, on the other hand, is an abnormal event likely to cause an interruption of normal operations
- Disaster recovery is not simply an option – it is a requirement

Disaster Recovery

- What makes disaster recovery so problematic in a physical environment is the amount of manual labor required to prepare for and execute a disaster recovery plan

- Furthermore, fully testing the processes and procedures is often very difficult

- Too many organizations have a disaster recovery plan that has never actually been tested in an environment that sufficiently replicates real-world conditions to give them the confidence that the plan will work

Disaster Recovery

- Disaster recovery in the cloud can be much more automatic (in fact, some cloud infrastructure management tools will even automatically execute a disaster recovery plan without human intervention)
- What would happen if one lost the entire data center under a traditional IT infrastructure? (hopefully, one has a great off-site backup strategy that would enable to get going in another data center in a few weeks)
- On the other hand, cloud may enable one to move an entire infrastructure from one cloud provider to another and even have that move occur automatically in response to a catastrophic event

Disaster Recovery

- Another advantage for the cloud here is the cost associated with a response to a disaster of that level

- Recovery costs in the cloud are almost negligible beyond normal operations (with a traditional data center, one must shell out new capital costs for a new infrastructure and then make insurance claims)

- In addition, one can actually test out different disaster scenarios in the cloud in ways that are simply unimaginable in a traditional environment

Cloud Security

- Data security
- Network security
- Host security

Data Security

- Physical security defines how you control physical access to the servers that support your infrastructure
- The cloud still has physical security constraints
- After all, there are actual servers running somewhere
- When selecting a cloud provider, you should understand their physical security protocols and the things you need to do on your end to secure your systems against physical vulnerabilities

Data Security: Data Control

- Difference between traditional data centers and the cloud is the location of your data on someone else's servers
- If you, as a client, have outsourced your data centers to a managed services provider, what cloud services add is the inability to see or touch the servers on which your data is hosted
- It presents some real business challenges
- The main practical problem is that factors, which have nothing to do with your business, can compromise your operations and your data

Data Security: Data Control

- For example, any of the following events could create trouble for the infrastructure:
  - The cloud provider declares bankruptcy and its servers are seized or it ceases operations
  - A third party with no relationship to you (or, worse, a competitor) sues your cloud provider and obtains a blanket subpoena granting access to all servers owned by the cloud provider
  - Failure of your cloud provider to properly secure portions of its infrastructure – especially in the maintenance of physical access controls – results in the compromise of your systems

Data Security: Data Control

- The solution is to do two things: encrypt everything and keep off-site backups
  - Encrypt sensitive data in your database and in memory. Decrypt it only in memory for the duration of the need for the data (encrypt your backups and encrypt all network communications)
  - Choose a second provider and use automated, regular backups (for which many open source and commercial solutions exist) to make sure any current and historical data can be recovered even if your cloud provider were to disappear from the face of the earth

Data Security: Data Control

- When you select a cloud provider, you absolutely must understand how they treat physical, network, and host security
- Though it may sound counterintuitive, the most secure cloud provider is one in which you never know where the physical server behind your virtual instance is running
- Chances are that, if you cannot figure it out, a determined hacker who is specifically targeting your organization is going to have a much harder time breaching the physical environment in which your data is hosted

Data Security: Encrypt Everything

- Encrypt network traffic
  - One must have network traffic encrypted – at least for the most part
  - A nice feature of the Amazon cloud is that virtual servers cannot sniff the traffic of other virtual servers
  - May not reliable: It may not be true of other providers
  - Furthermore, Amazon might roll out a future feature that renders this protection measure obsolete
  - One must therefore encrypt all network traffic

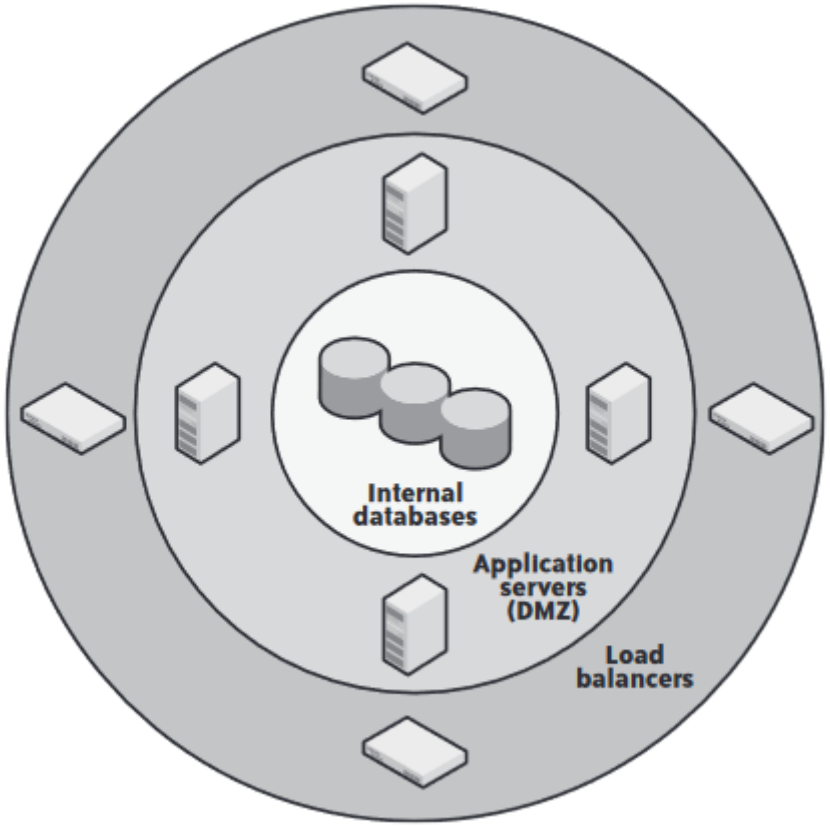
Data Security: Encrypt Everything

- Encrypt backups
  - When you bundle your data for backups, you should be encrypting it using some kind of strong cryptography, such as PGP
  - You can then safely store it in a moderately secure cloud storage environment like Amazon S3, or even in a completely insecure environment
  - Encryption eats up CPU – it is recommended to first copy your files in plain text over to a temporary backup server whose job it is to perform encryption, and then uploading the backups into your cloud storage system
  - Not only does the use of a backup server avoid taxing your application server and database server CPUs, it also enables you to have a single higher-security system holding your cloud storage access credentials rather than giving those credentials to every system that needs to perform a backup

Network Security: Firewalls

- Typically, a firewall protects the perimeter of one or more network segments
- 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

Network Security: Firewalls



Network Security: Firewalls

- This structure requires you to move through several layers – or perimeters – of network protection in the form of firewalls to gain access to increasingly sensitive data
- Outer layer services tend to be more hardened against Internet vulnerabilities, whereas interior services tend to be less Internet-aware
- The weakness of this infrastructure is that a compromise of any individual server inside any given segment provides full access to all servers in that network segment

Network Security: Network Intrusion Detection

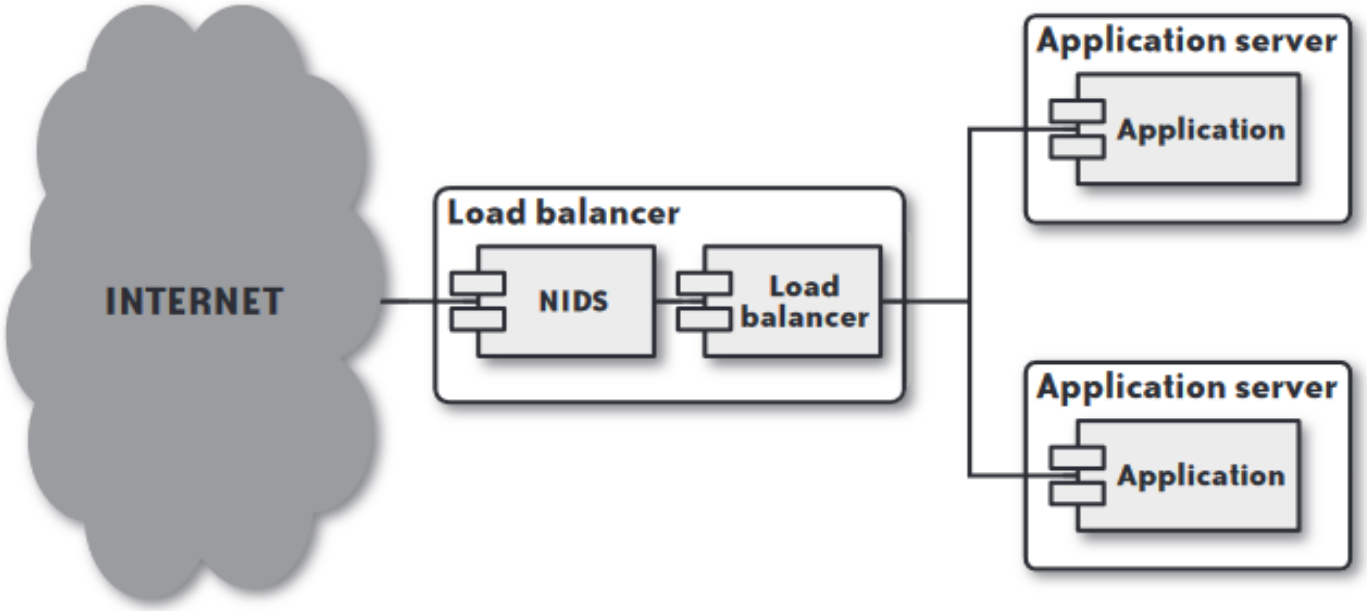
- Perimeter security often involves network intrusion detection systems (NIDS), such as Snort, which monitor local traffic for anything that looks irregular

- Examples of irregular traffic include: Port scans, denial-of-service attacks, known vulnerability exploit attempts

- Routing all traffic through a system that analyzes it

Network Security: Network Intrusion Detection

- The simplest approach to implement NIDS is to have a dedicated NIDS server in front of the network as a whole that watches all incoming traffic and acts accordingly



Network Security: Network Intrusion Detection

- Because the only software running on the load balancer is the NIDS software and Apache, it maintains a very low attack profile

- Compromising the NIDS server requires a vulnerability in the NIDS software or Apache – assuming the rest of the system is properly hardened and no actual services are listening to any other ports open to the Web as a whole

Network Security: Network Intrusion Detection

- The load balancer approach creates a single point of failure for your network intrusion detection system because, in general, the load balancer is the most exposed component in your infrastructure

- By finding a way to compromise your load balancer, the intruder not only takes control of the load balancer, but also has the ability to silence detection of further attacks against your cloud environment

Network Security: Network Intrusion Detection

- You can alternately implement intrusion detection on a server behind the load balancer that acts as an intermediate point between the load balancer and the rest of the system

- This design is generally superior to the previously described design, except that it leaves the load balancer exposed (only traffic passed by the load balancer is examined) and reduces the overall availability of the system

Network Security: Network Intrusion Detection

- Another approach is to implement network intrusion detection on each server in the network
- This approach creates a very slight increase in the attack profile of the system as a whole because you end up with common software on all servers
- A vulnerability in your NIDS would result in a vulnerability on each server in your cloud architecture

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
- In the real world, the best approach for preventing attacks is to assume your software has security holes
- Each service run on a host presents a distinct attack vector into host
- More attack vectors, more likely an attacker will find a security exploit
- So, you must minimize different kinds of software running on a server

Host Security: 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

Host Security: System Hardening

- Server hardening is the process of disabling or removing unnecessary services and eliminating unimportant user accounts
  - No network services are running except those necessary to support the server's function
  - No user accounts are enabled on the server except those necessary to support the services running on the server or to provide access for users who need it
  - All configuration files for common server software are configured to the most secure settings
  - All necessary services run under a nonprivileged role user account (e.g., run MySQL as the mysql user, not root)
  - When possible, run services in a restricted filesystem

Host Security: Antivirus Protection

- Some regulations and standards require the implementation of an antivirus (AV) system on your servers
- Controversial issue: an AV system with an exploit is itself an attack vector and, on some operating systems, the percentage of AV exploits to known viruses is relatively high
- You first should understand what your requirements are
- If you are required to implement AV, then you should look for two critical features in your AV software
  - How wide is the protection it provides? (% of known exploits it covers)
  - Average time when a virus is released and AV provides protection against it?

Host Security: Antivirus Protection

- Once you have selected an AV vendor and implemented it on your servers, you absolutely must keep your signatures up to date

- You are probably *better* off with no AV system than one with outdated versions of some AV

Host Security: Host Intrusion Detection

- Whereas a network intrusion detection system monitors network traffic for suspicious activity, a host intrusion detection system (HIDS) 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
- In the cloud, you should always opt for the centralized configuration. It centralizes your rules and analysis so that it is much easier to keep your HIDS infrastructure up to date
- Furthermore, it enables you to craft a higher security profile for your HIDS processing than the individual services might allow for

Host Security: Host Intrusion Detection

- As with an AV solution, you must keep your HIDS servers up to date constantly, but you do not need to update your individual servers as often

- The downside of an HIDS is that it requires CPU power to operate, and thus can eat up resources on your server

- By going with a centralized deployment model, however, you can push a lot of that processing onto a specialized intrusion detection server

Host Security: Data Segmentation

- Failure/compromise is inevitable (the best infrastructure assumes the compromise of any individual node)

- This tolerance is not meant to encourage lax security for individual servers, but is meant to minimize the impact of the compromise of specific nodes

Host Security: Data Segmentation

- Making this assumption provides you with a system that has the following advantages:
  - Access to your most sensitive data requires a full system breach
  - The compromise of the entire system requires multiple attack vectors with potentially different skill sets
  - The downtime associated with the compromise of an individual node is negligible or nonexistent

Host Security: Data Segmentation

- The segmentation of data based on differing levels of sensitivity is your first tool in minimizing the impact of a successful attack
- Here the approach of one server/one service helps out
- This is because each type of server in the chain offers a different attack vector, an attacker will need to exploit multiple attack vectors to compromise the system as a whole

Host Security: Credential Management

- If someone needs access to a server, cloud should provide her credentials to the server when it starts up or via an administrative interface instead of embedding information in the machine image
- You should pass in user credentials as part of the process of launching your virtual server
- At boot time, the virtual server has access to all of the parameters you pass in and can thus set up user accounts for each specified user
- It’s simple because it requires no tools other than those that cloud already provides
- However, adding/removing access later becomes a manual task

Host Security: Credential Management

- Another approach is to use existing cloud infrastructure management tools or build your own that enable you to store user credentials outside the cloud and dynamically add/remove users to your cloud servers at runtime

- This approach, however, requires an administrative service running on each host and thus represents an extra attack vector against your server