CLOUD SECURITY

DR. MANJUNATH V HEGDE AND DR. VIDYA RAO

L34-36

CLOUD BREACHES OF 2021

Accenture. In August of 2021, Accenture fell prey to a LockBit ransomware attack. The culprits claimed to have stolen 6TB worth of data, for which they requested a ransom of $50 million.

Kaseya. In July of 2021, IT solutions provider Kaseya identified an attack on their unified remote monitoring and network perimeter security tool. The attackers aimed to steal administrative control for Kaseya services; from managed service providers to downstream customers.

Cognyte. In May of 2021, the cyber analytics firm Cognyte left a database unsecured without authentication protocols. In turn, hackers managed to expose 5 billion records. Information such as names, email addresses, passwords, and vulnerability data points within their system were leaked.

Facebook. In April of 2021, Facebook reported a breach affecting hundreds of millions of user records, which were publicly exposed on Amazon's cloud computing service. Although Facebook confirmed that it identified and resolved the issue immediately, the attack managed to impact founder Mark Zuckerberg.

Raychat. In February of 2021, Raychat, an online chat application, survived a large-scale cyber attack. A cloud database configuration breach gave hackers free access to 267 million usernames, emails, passwords, metadata and encrypted chats.

Source: https://www.cybertalk.org/2022/04/26/top-5-cloud-security-breaches-and-lessons/

THREE BASIC COMPONENTS OF SECURITY

Confidentiality

Keep data and Resources hidden

Integrity

Data Integrity (Integrity)

Origin integrity (Authentication)

Availability

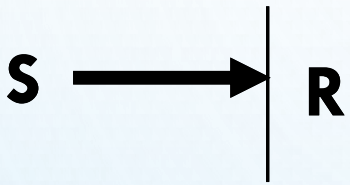
Enabling access to data and resources

SECURITY ATTACKS

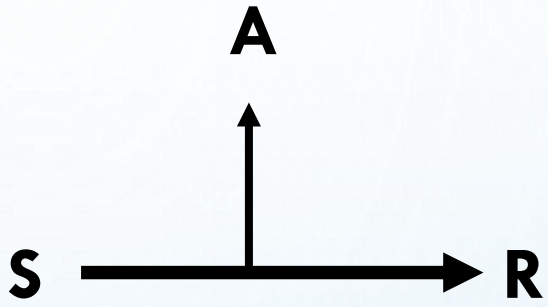
- Any action that compromises the security of information
- Four types of attack
  - **Interruption** - Obstruction during the communication process between the systems.
  - **Interception** - The data or message which is sent by the sender is stolen by an unauthorized individual where the message will be changed to the different form or it will be used by the malicious process
  - **Modification** - Message which is sent by the sender is modified and sent to the destination by an unauthorized user.
  - **Fabrication** - A fake message is inserted into the network by an unauthorized user as if it is a valid user.

BASIC MODEL

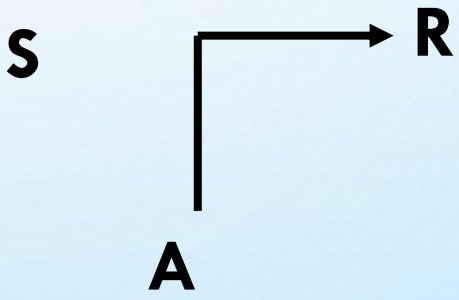
Interruption – Attack on availability



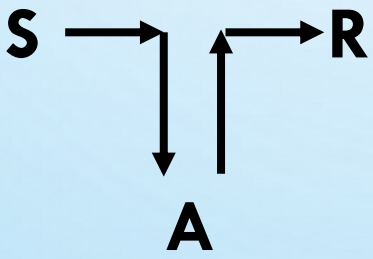
Interception – Attack on Confidentiality



Fabrication – Attack on Authenticity



Modification – Attack on Integrity



KEY TERMS

- **Threat** – is any potential occurrence, malicious or otherwise, that could harm an asset. In other words, a threat is any bad thing that can happen to your assets.
- **Vulnerability** – is a weakness that makes a threat possible. This may be because of poor design, configuration mistakes, or inappropriate and insecure coding techniques.
- **Attack** – is an action that exploits a vulnerability or enacts a threat. Examples of attacks include sending malicious input to an application or flooding a network in an attempt to deny service.

What are the differences between Attack and Threat?

CLASSES OF THREATS

- **Disclosure**
  - Snooping*
- **Deception**
  - Modification, Spoofing**, Repudiation of origin, Denial of receipt
- **Disruption**
  - Modification
- **Usurpation*****
  - Modification, Spoofing, Delay, Denial of service

*snooping is unauthorized access to another person's or company's data
**Spoofing is pretends to be something else in an attempt to gain the confidence to access the system/service
***Unauthorized control of some part of a system

GOALS OF SECURITY

- **Prevention**
  - Prevention attack from violating the security policies
- **Detection**
  - Prevention attackers who violating the security policies
- **Recovery**
  - Stop attack, asses and repair damage
  - Continue to function correctly even if attack succeeds

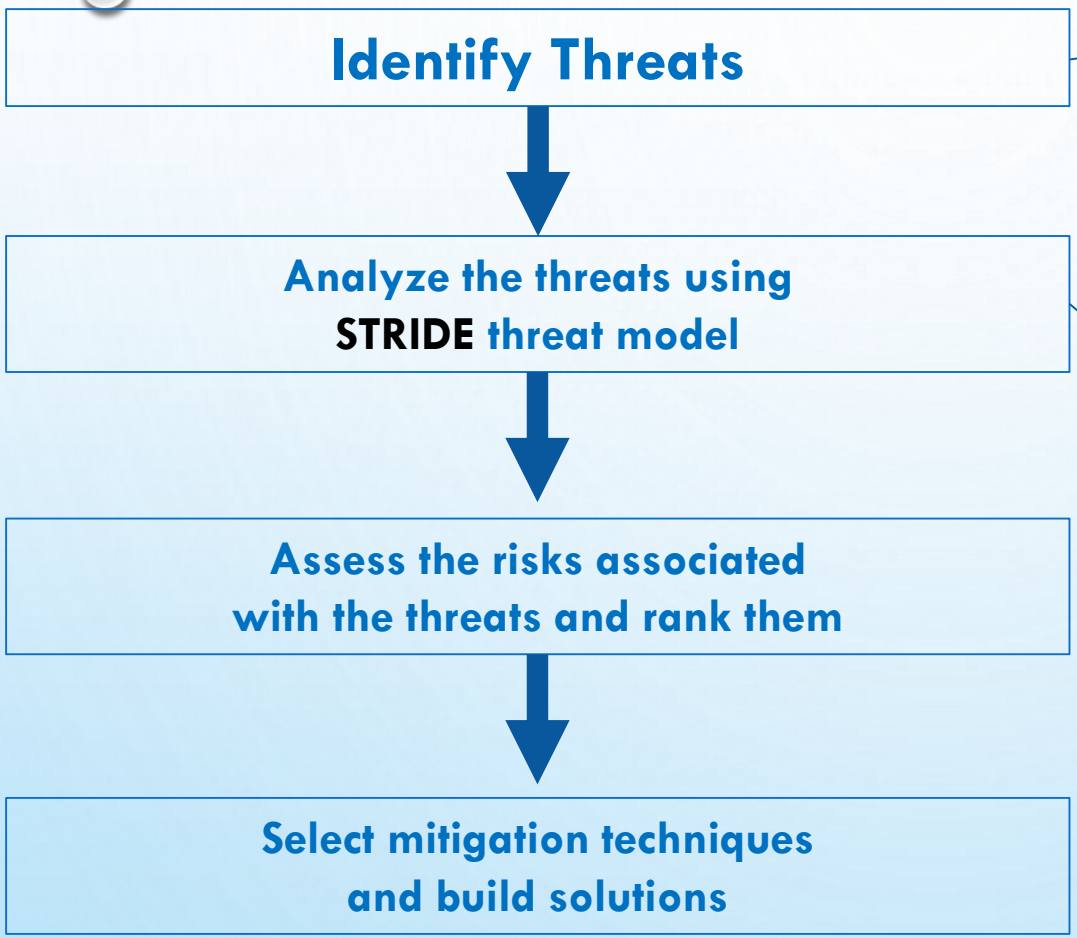
WHAT IS CLOUD SECURITY?

- Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion.
- Methods of providing cloud security include
  - Firewalls
  - Penetration testing
  - Tokenization, virtual private networks (VPN)
  - Avoiding public internet connections.
- Cloud security is a form of cybersecurity.

MOTIVATION

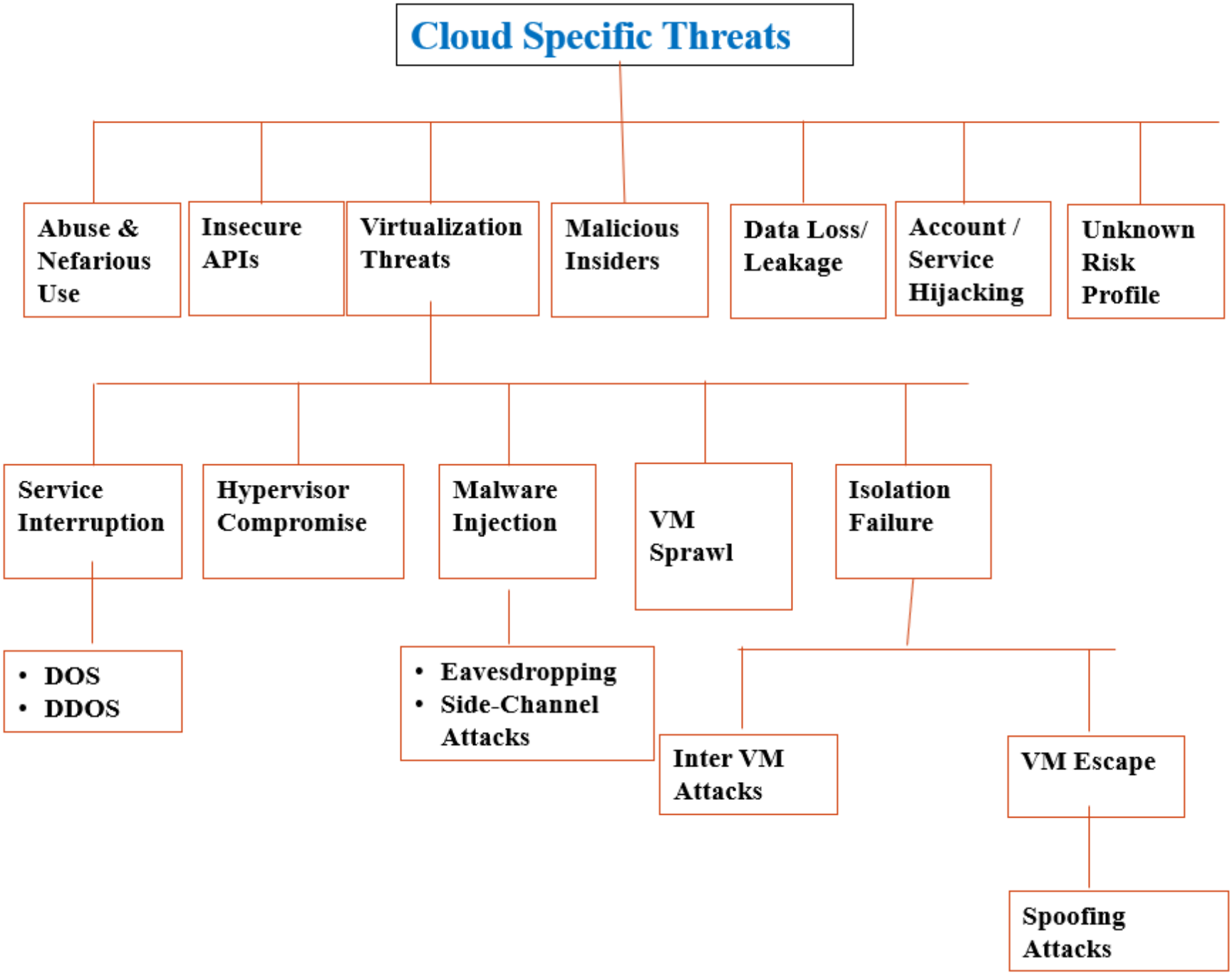
- **Cloud provider -** provides resources/services that can be accessed from anywhere in the world by the user.
- **Cloud user -** can be either a single person or any organization.
- Cloud computing has many benefits, but security is a big concern.
- Cloud provider should provide privacy and security to the user's data and applications.

THREAT MODEL



Examine Assets, Vulnerabilities, and Attackers

S – Spoofing Identity
T – Tampering With Data
R – Repudiation
I – Information Disclosure
D – Denial of Service
E – Elevation of Privilege


Cloud Specific Threats
Abuse & Nefarious Use
Insecure APIs
Virtualization Threats
Malicious Insiders
Data Loss/ Leakage
Account / Service Hijacking
Unknown Risk Profile
Service Interruption
Hypervisor Compromise
Malware Injection
VM Sprawl
Isolation Failure
• DOS
• DDOS
• Eavesdropping
• Side-Channel Attacks
Inter VM Attacks
VM Escape
Spoofing Attacks

THREE STAGES OF SECURITY

- **DATA SECURITY**
- **NETWORK SECURITY**
- **HOST SECURITY**

DATA SECURITY

- Physical storage security defines how you control physical access to the servers that support your infrastructure.
- The cloud still has physical security constraints as there are actual servers running somewhere.
- When selecting a cloud provider, you should understand their physical security protocols.

- To be studied under…..
  - Data Control
  - Encrypt Everything
  - Regulatory and Standards Compliance

DATA CONTROL

- The main practical problem is that, factors that have nothing to do with your business can compromise your operations and your data.
- Some of the events are:
  - 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 CONTROL (CONTD..)

- 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.

ENCRYPT EVERYTHING

- In the cloud, your data is stored somewhere; you just don't know exactly where. However, you know some basic parameters:
  - Your data lies within a virtual machine guest operating system, and you control the mechanisms for access to that data.
  - Network traffic exchanging data between instances is not visible to other virtual hosts.
  - For most cloud storage services, access to data is private by default. Many, including Amazon S3, nevertheless allow you to make that data public.

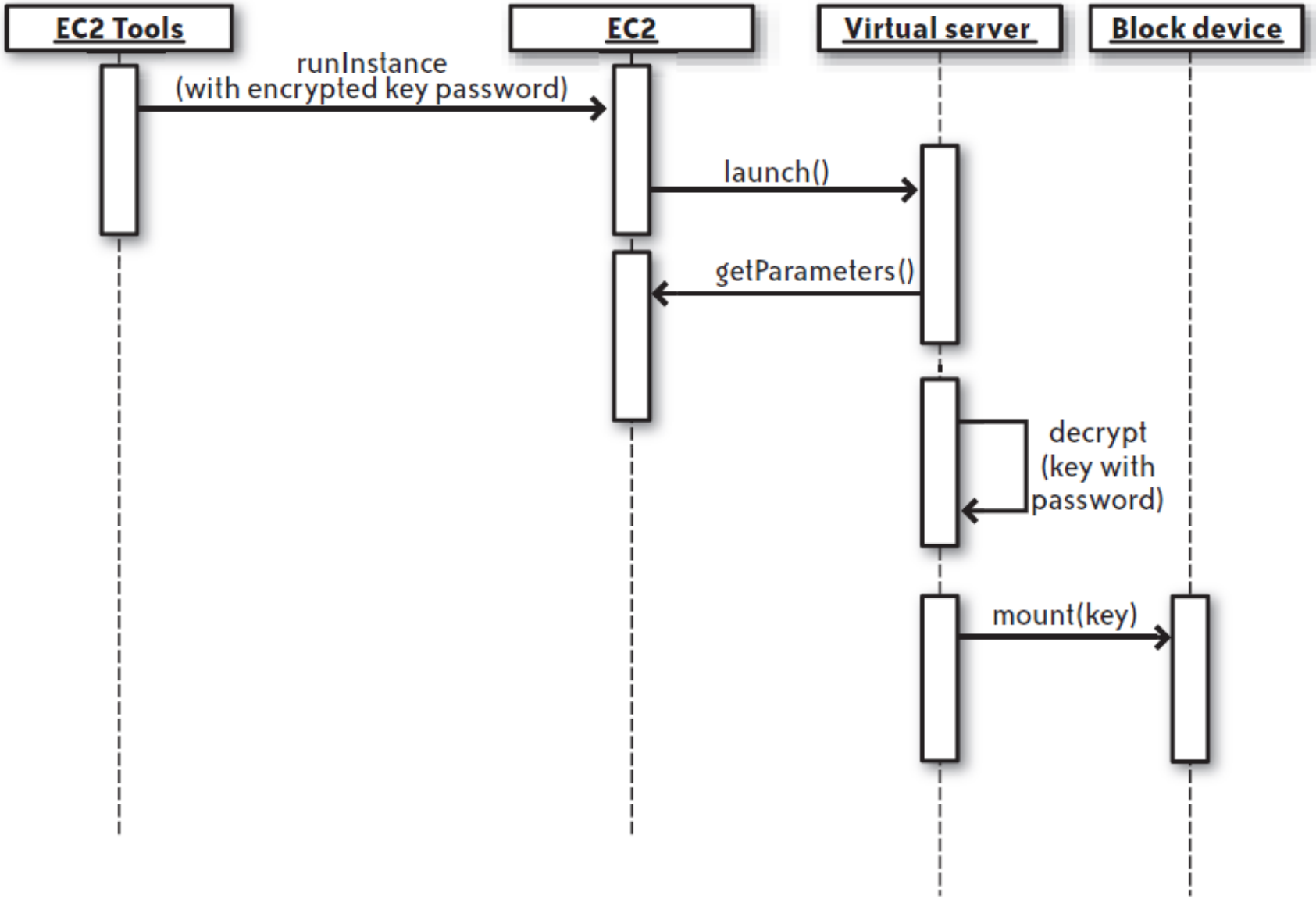


FIGURE 5-1. The process of starting a virtual server with encrypted filesystems

REGULATORY AND STANDARDS COMPLIANCE

From a security perspective, you'll encounter three kinds of issues in standards and regulations:

"How" issues

These result from a standard such as PCI or regulations such as HIPAA or SOX, which govern how an application of a specific type should operate in order to protect certain concerns specific to its problem domain. For example, HIPAA defines how you should handle personally identifying health care data.

"Where" issues

These result from a directive such as Directive 95/46/EC that governs where you can store certain information. One key impact of this particular directive is that the private data on EU citizens may not be stored in the United States (or any other country that does not treat private data in the same way as the EU).

"What" issues

These result from standards prescribing very specific components to your infrastructure. For example, PCI prescribes the use of antivirus software on all servers processing credit card data.

NETWORK SECURITY

Amazon's cloud has no perimeter. Instead, EC2 provides security groups that define firewall-like traffic rules governing what traffic can reach virtual servers in that group due to reasons such as:

- Two servers in two different Amazon EC2 availability zones can operate in the same security group.
- A server may belong to more than one security group.
- Servers in the same security group may not be able to talk to each other at all.
- Servers in the same network segment may not share any IP characteristics—they may even be in different class address spaces.
- No server in EC2 can see the network traffic bound for other servers (this is not necessarily true for other cloud systems). If you try placing your virtual Linux server in promiscuous mode, the only network traffic you will see is traffic originating from or destined for your server.

FIREWALL RULES(CONTD..)

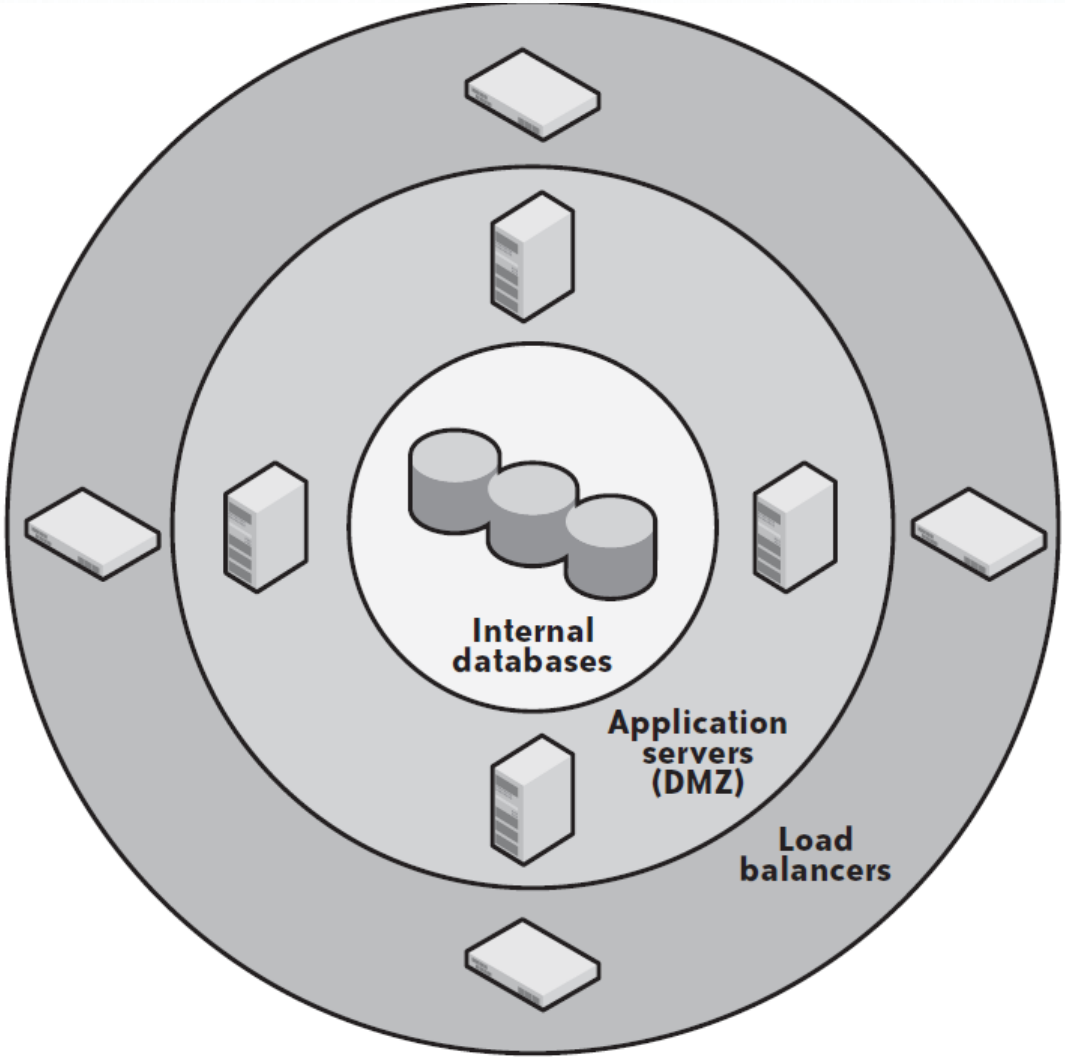


FIGURE 5-2. Firewalls are the primary tool in perimeter security

FIREWALL RULES

- Typically, a firewall protects the perimeter of one or more network segments.
- A main firewall protects the outermost perimeter, allowing 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.
- 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.
- The perimeter architecture's chief advantage is that a poorly structured firewall rule on the inner perimeter does not accidentally expose the internal network to the Internet unless the DMZ is already compromised.

FIREWALL RULES(CONTD..)

- You can set up security groups to help you mimic traditional perimeter security.
- For example, you can create the following:
  - A border security group that listens to all traffic on ports 80 and 443
  - A DMZ security group that listens to traffic from the border group on ports 80 and 443
  - An internal security group that listens to traffic on port 3306 from the DMZ security group

FIREWALL RULES(CONTD..)

Two other advantages of this security architecture are the following:

- Because you control your firewall rules remotely, an intruder does not have a single target to attack, as he does with a physical firewall.
- You don’t have the opportunity to accidentally destroy your network rules and thus permanently remove everyone’s access to a given network segment.

FIREWALL RULES(CONTD..)

A few best practices for your network security include:

- 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

The purpose of a network intrusion detection system

Network intrusion detection exists **to alert you** of attacks before they happen and, in some cases, foil attacks as they happen.

NIDS (CONTD..)

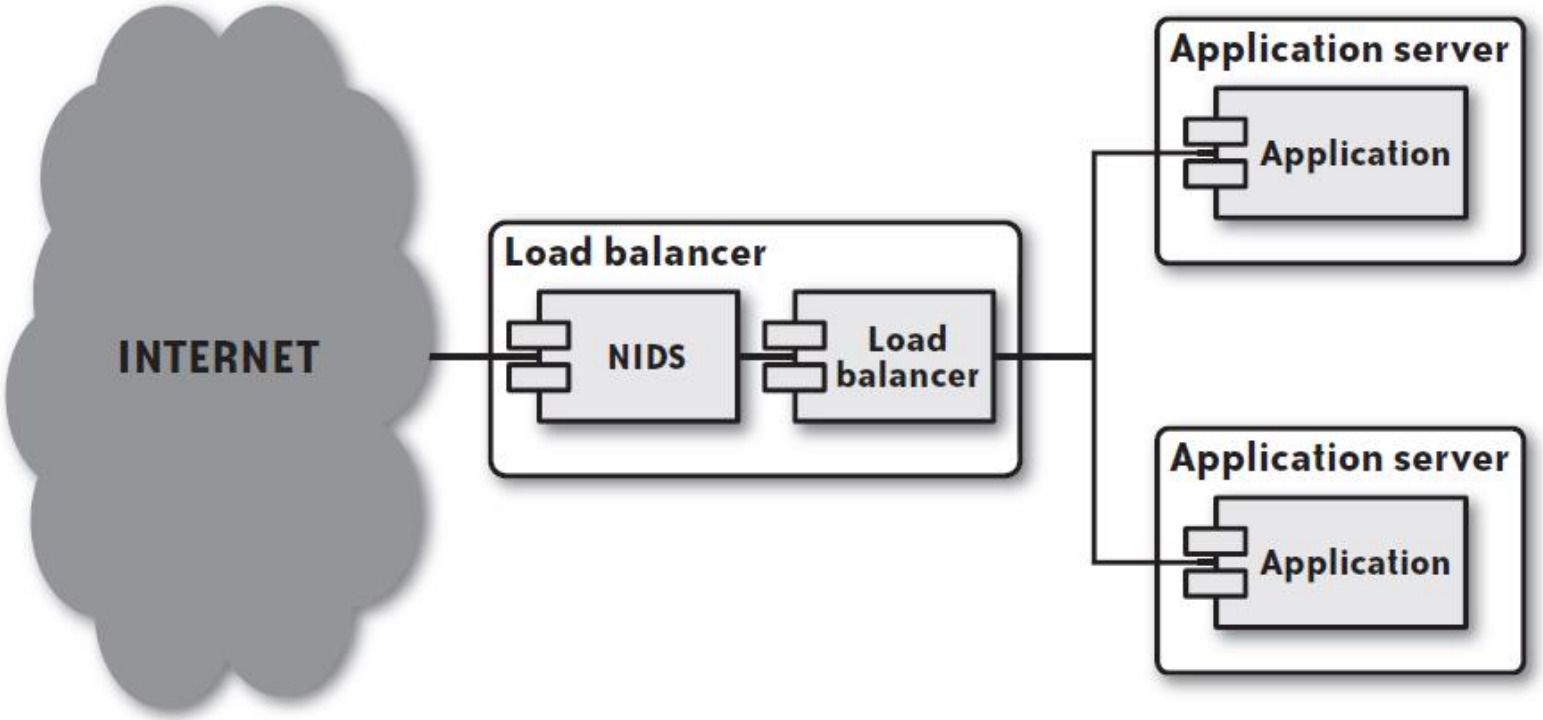


FIGURE 5-4. A network intrusion detection system listening on a load balancer

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.

Given the assumption that your services are vulnerable, your most significant tool in preventing attackers from exploiting a vulnerability once it becomes known is the rapid rollout of security patches.

Three steps of rollout patch:

1. Patch your AMI with the new security fixes.
2. Test the results.
3. Relaunch your virtual servers.

SYSTEM HARDENING

Machine hardening is pre-processing of the machine imaging phase.

A hardened system should meet the following criteria:

- 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, such as a chroot jail.

HOST INTRUSION DETECTION

- A network intrusion detection system monitors network traffic for suspicious activity, a host intrusion detection system (HIDS) such as OSSEC monitors the state of your server for anything unusual.
- OSSEC has two configuration profiles:
    - Standalone, in which each server scans itself and sends you alerts.
    - Centralized, in which you create a centralized HIDS server to which each of the other servers sends reports.

HOST INTRUSION DETECTION

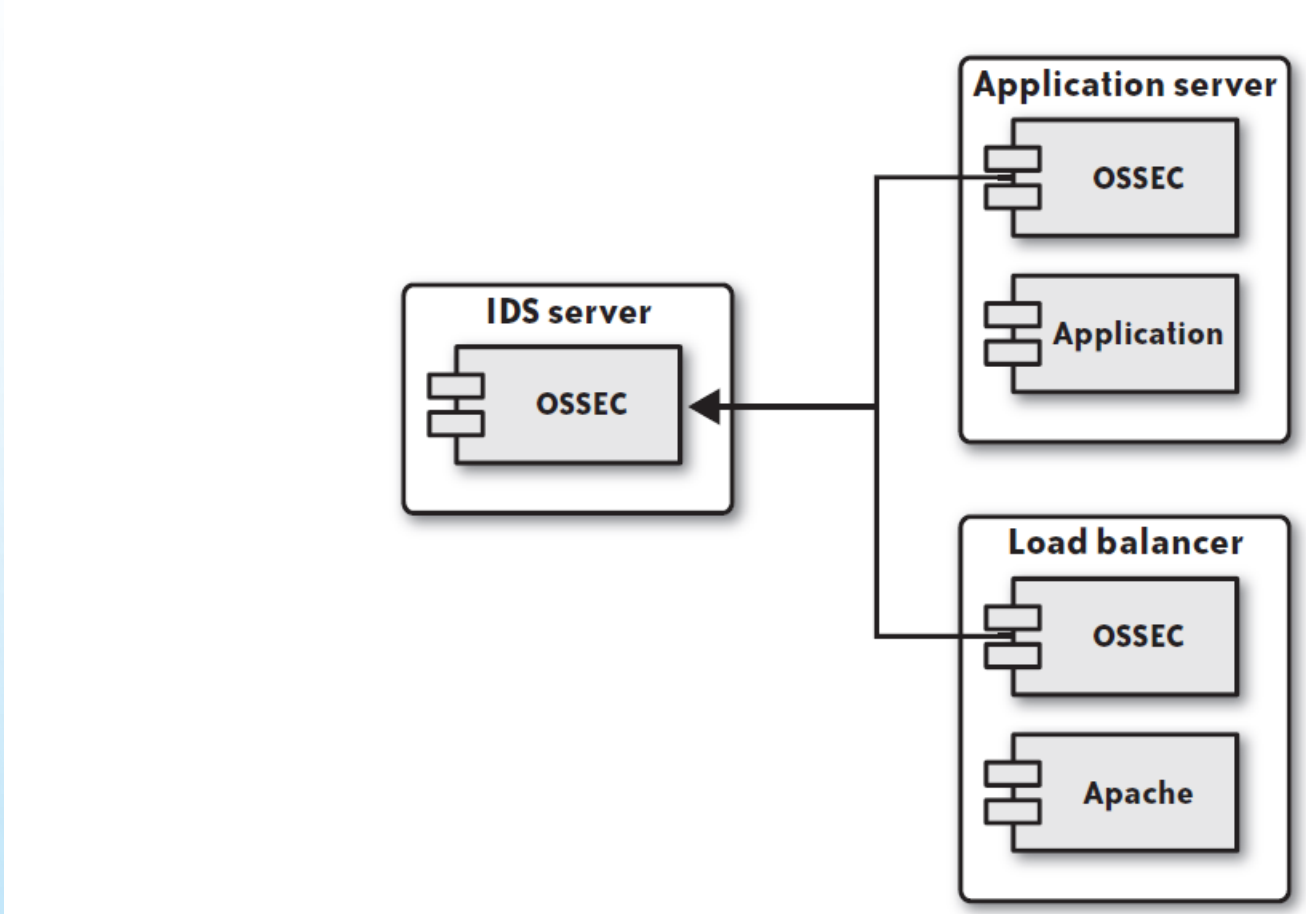


FIGURE 5-5. A HIDS infrastructure reporting to a centralized server

DATA SEGMENTATION

- In addition to assuming that the services on your servers have security exploits, you should further assume that eventually one of them will be compromised.
- Obviously, you never want any server to be compromised. The best infrastructure, however, is tolerant of—in fact, it 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.
- 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 non-existent.
- The segmentation of data based on differing levels of sensitivity is your first tool in minimizing the impact of a successful attack.

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 to providing access to virtual servers is the dynamic delivery of public SSH keys to target servers.
- In other words, if someone needs access to a server, you should provide her credentials to the server when it starts up or via an administrative interface instead of embedding that information in the machine image.

COMPROMISED RESPONSE

Responding to attack is a major step to be taken by digital forensic professionals. When you detect a compromise on a physical server, the standard operating procedure is a painful, manual process:

1. Remove intruder access to the system, typically by cutting the server off from the rest of the network.
2. Identify the attack vector. You don’t want to simply shut down and start over, because
3. the vulnerability in question could be on any number of servers. Furthermore, the intruder very likely left a rootkit or other software to permit a renewed intrusion after you remove the original problem that let him in. It is therefore critical to identify how the intruder compromised the system, if that compromise gave him the ability to compromise other systems, and if other systems have the same vulnerability.
4. Wipe the server clean and start over. This step includes patching the original vulnerability and rebuilding the system from the most recent uncompromised backup.
5. Launch the server back into service and repeat the process for any server that has the same attack vector.