Security Fundamentals Based on Security+

Hello!

I am Green Timothy

Cybersecurity Expert,
Penetration Tester &
Trainer.

CompTIA Sec+ ,ISC2

You can find me at:

Linkedin:
https://www.linkedin.com/in/green-timothy-91526319a/

Part 3 .
Architecture and Design

Architecture Frameworks and Secure Network Architectures

Standards:

Standard is a document approved by a recognized body – there can be multiple standards for one product.

Standards after widespread adoption may become regulations

Guidelines:

provide recommendations or good practices.

Framework:

Generally includes more components than a guide and is used as a basis for the implementation and management of security controls

Regulatory Requirements

- Regulatory requirements are created by governmental agencies and are mandated by law
- The Health Insurance Portability and Accountability Act (HIPAA)
- The Payment Card Industry Data Security Standard (PCI DSS)

- Noncompliance can result in fines or a negative impact on stock value and investor relations

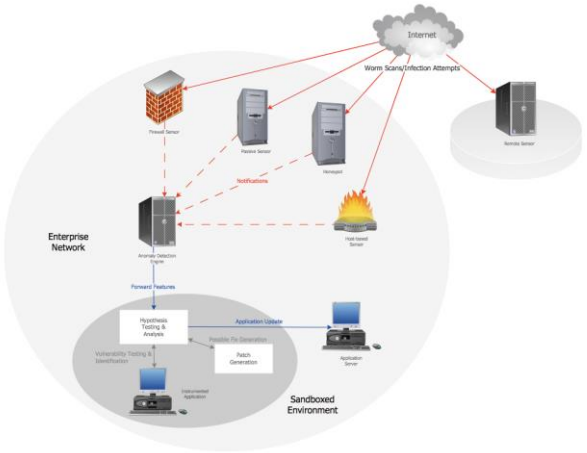
Non-regulatory Requirements

Developed by agencies that provide technology, metrics, and standards development for the betterment of the science and technology industry.

- No rule of law
- May be strongly suggested
- A regulation may be in the works
- Get used to the impending change
- Creates value for yourself and/or others
- You don’t need a law if it’s the right thing to do

Architecture Frameworks and Secure Network Architectures

- The security architecture of an organization should be based on some type of security framework.
- When an organization is multinational or does business in another country, the organization could be subject to additional restrictions, based on regulatory compliance in that country.



DEFENSE-IN-DEPTH/LAYERED SECURITY

Physical controls

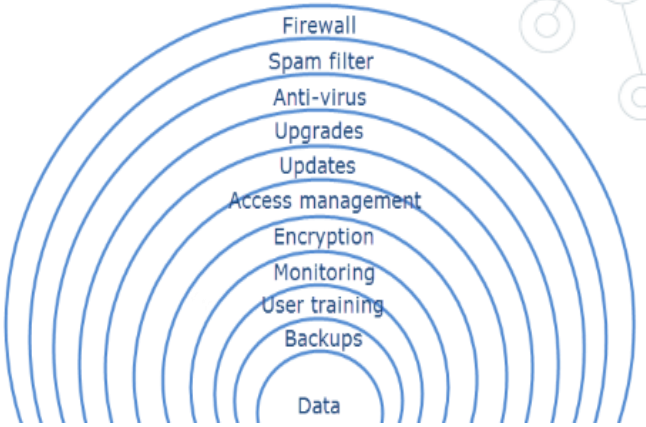
- Keep people away from the technology
- Door locks, fences, rack locks, cameras

Technical controls

- Firewalls, disk encryption

Administrative controls

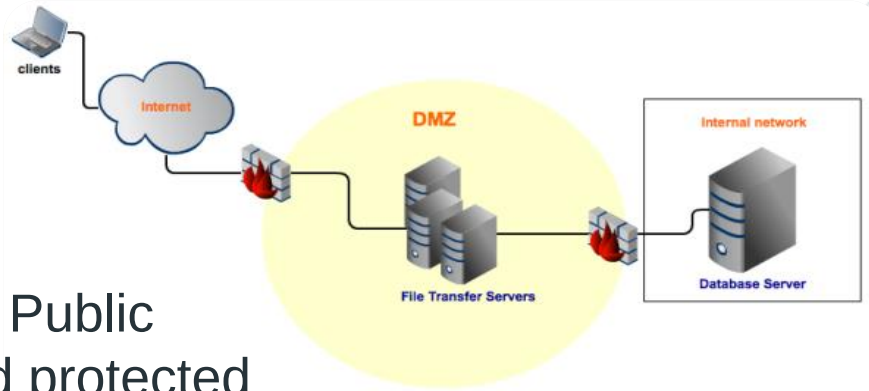
- Policies and procedures
- Backup media handling



Vendor Diversity

Having multiple suppliers creates vendor diversity, which reduces the risk from any single supplier

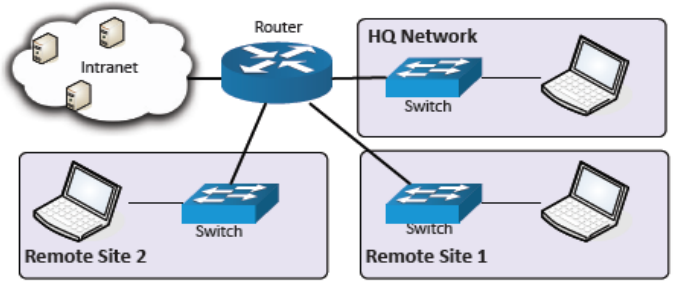
DMZ (Demilitarized zone)



DMZs act as a buffer zone between Public areas of a network (the Internet) and protected areas (sensitive company data stores)

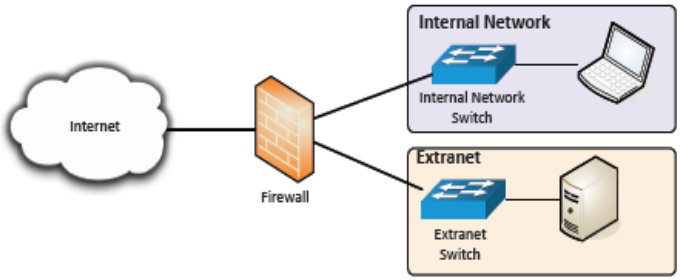
Intranet

- A private network only available internally
- Company announcements, important documents, other company business.



Extranet

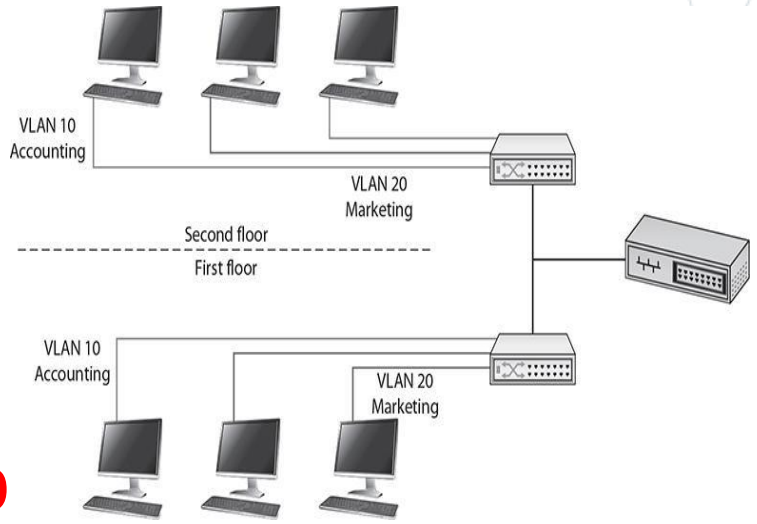
- A private network that allows a business to share information with customers, suppliers, partners, and other trusted groups
- Usually requires additional authentication



Physical Segmentation

Physical segregation requires creating two or more physical networks, each with its own servers, switches, and routers

- Devices are physically separate
- Must be connected to provide communication



Logical VLAN segmentatio

Allows computers connected to different physical networks to act and communicate as if they were on the same physical network

Time for Testing ourselves and answering some questions!

Part 3 .
Architecture and Design

Hardware Security and OS

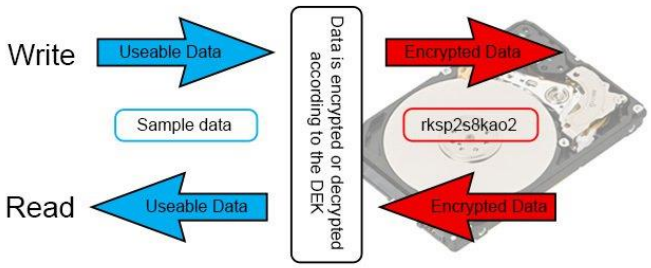
Full disk encryption (FDE)

- Encrypt an entire drive
- Protects all of your data As well as the operating system
- Bitlocker, Truecrypt, Veracrypt

Self-Encrypting Drives (SED)

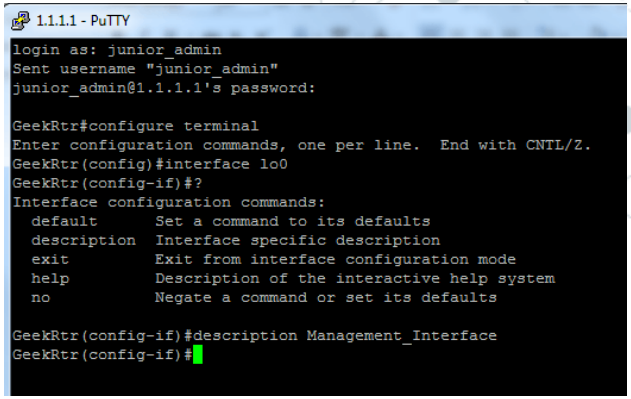
a type of hard drive that automatically and continuously encrypts the data on the drive without any user interaction

s



Network OS

- OS that works on routers and switches to supports servers, workstations, and other network-connected devices
- Ex: Cisco IOS



Appliance

- Usually a minimal pre-configured OS, often unseen by the user

Kiosk

- OS is tightly locked down for public device

Patch Management

- Patch management involves downloading, testing, and installing multiple patches to multiple computer systems

Hotfix

- A small software update designed to address a specific problem
- Produced and released rather quickly

Patch

- Larger update that can address several or many problems
- Patches are usually developed over a longer period of time

Service pack

- A collection of patches and hotfixes rolled into a single pack

Time for Testing ourselves and answering some questions!

Virtualization

The act of creating a virtual version of something, including virtual computer hardware platforms, storage devices, and computer network resources.

- Each self-contained VM is completely independent.
- Ex: have OS operating at the same time on one server or workstation.

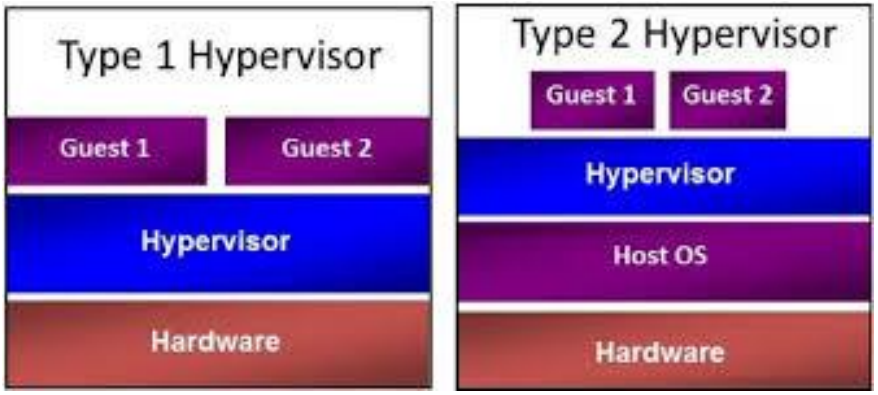
The Hypervisor

A software decouples the virtual machines from the host and dynamically allocates computing resources to each virtual machine as needed

Hypervisor Type 1

Run and install directly with hardware

- Ex: VMware ESXi or Hyper-V)
- Faster than type 2

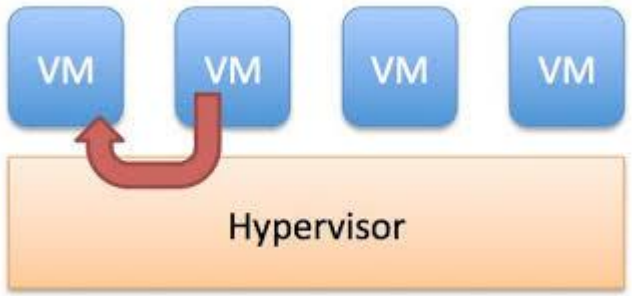


Hypervisor Type 2

- Run on top of Windows, Linux, etc.
- (Ex: VirtualBox or VMware Player)

VM escape protection

Break out of the VM and interact with the host operating system or hardware.

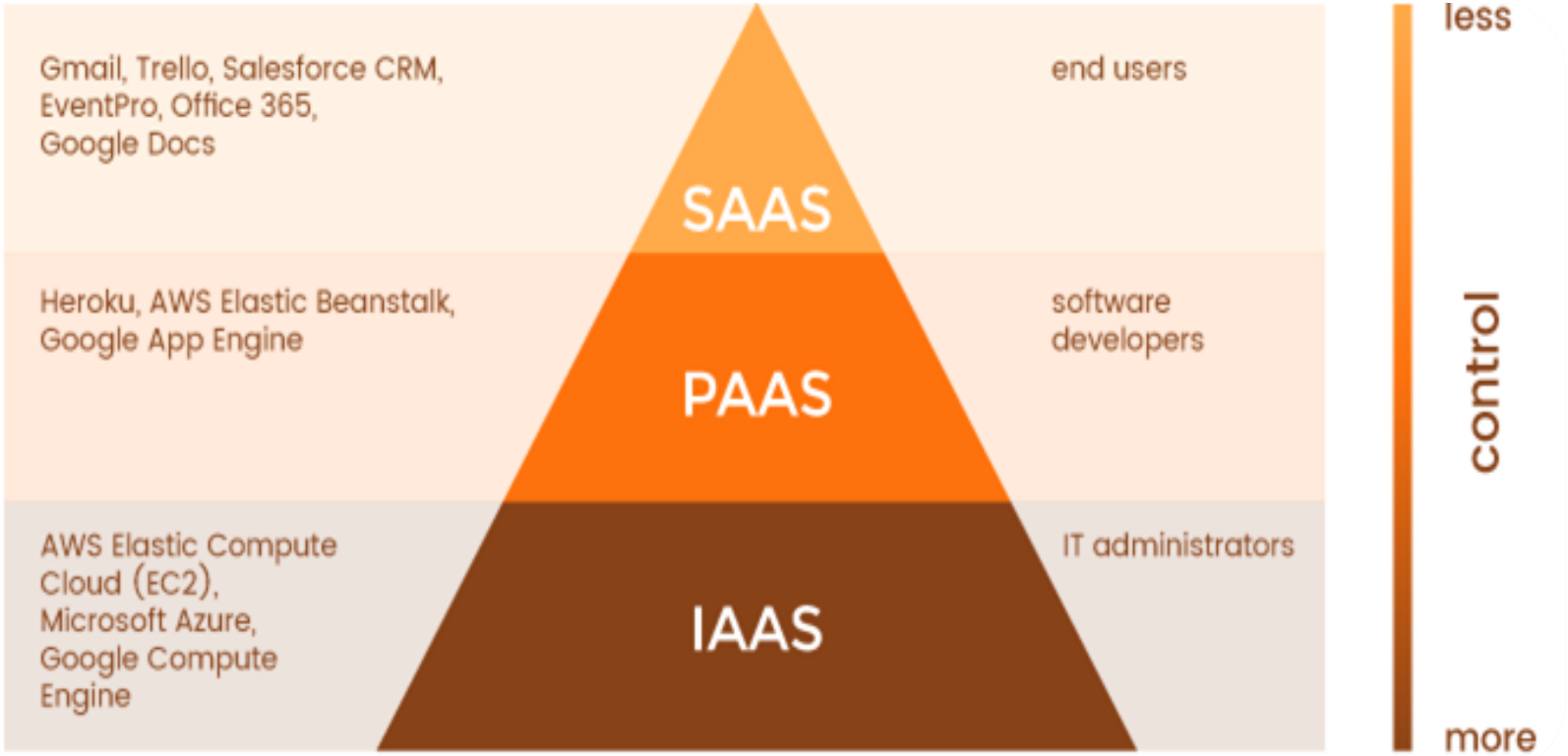


VM sprawl avoidance

- Click a button and you've built a server
- Can get out of hand very quickly
- Formal process and detailed documentation
- You should have information on every virtual object

CLOUD Computing

Cloud computing is a service that delivers shared computing resources (software and/or data) on demand via the



Software as a Service (SaaS):

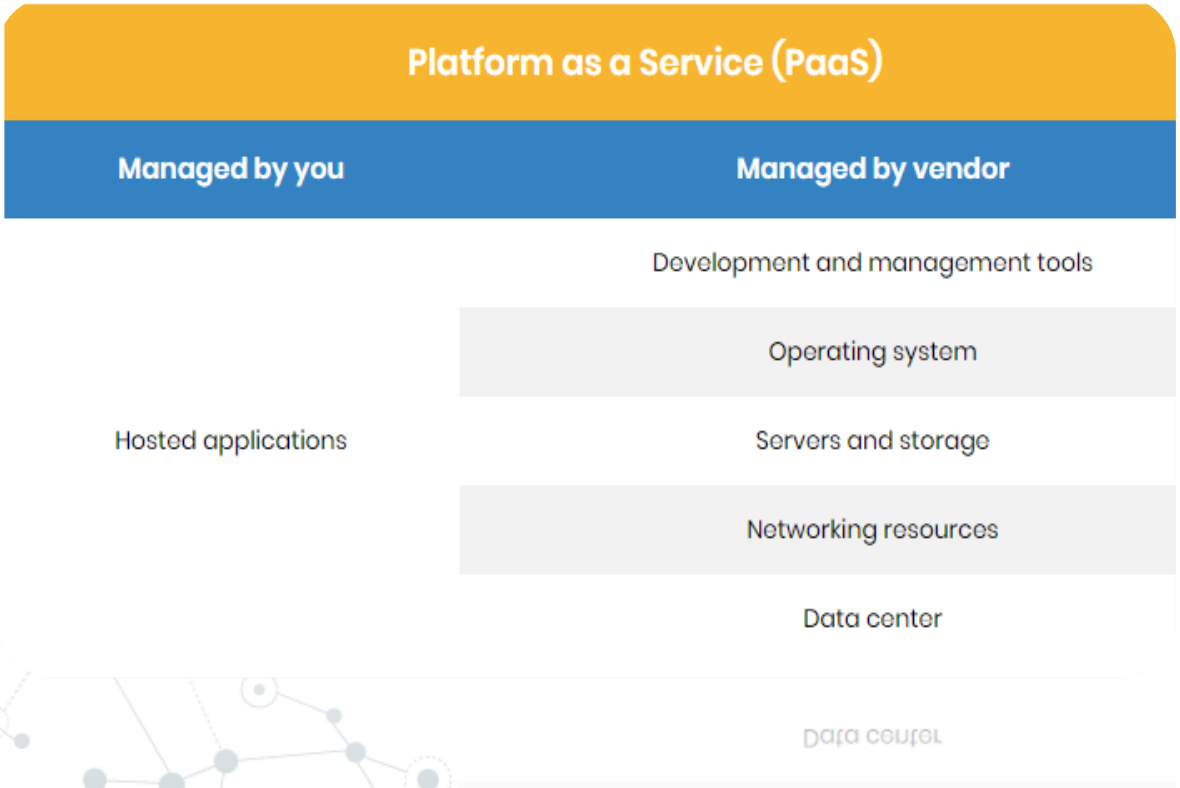
Offering software to end users over the Internet. Rather than installing software on client machines.

- EX: Office 365, Google Docs
-

Software as a Service (SaaS)	
Managed by you	**Managed by vendor**
	Hosted applications
	Development and management tools
	Operating system
	Servers and storage
	Networking resources
	Data center
	Data control

Platform as a Service (PaaS):

User can compute and storage, text editing, version management, compiling and testing services from anywhere via a web browser.



Infrastructure as a Service (IaaS):

a cloud service that provides basic computing infrastructure: servers, storage, and networking resources. In other words, IaaS is a virtual data center

Ex: Amazon Web Services, Microsoft Azure

Infrastructure as a Service (IaaS)	
Managed by you	**Managed by vendor**
Hosted applications	Servers and storage
Development and management tools	Networking resources
Operating system	Data center

Time for Testing ourselves and answering some questions!

Resiliency and Automation Strategies

Resilient systems are those that can return to normal operating conditions after a disruption.

Automated Action using scripts

Scripts are small computer programs that allow automated courses of action

- Should be approved before use in the production environment.
- The best friend of administrators, analysts, investigators.

Continuous Monitoring

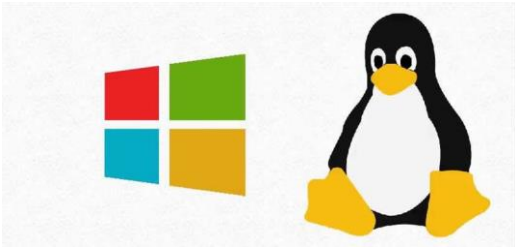
- As most enterprises have a large number of systems
- They use Automated dashboards and alerts that allow them to focus on the parts of the system that need attention rather than sifting through terabytes of data
- Giving you the opportunity to react to that changing situation

Configuration Validation

- When you place a system into service, you should validate its configuration against security standards
- When other things are added to or taken away from the system, Is the configuration still valid

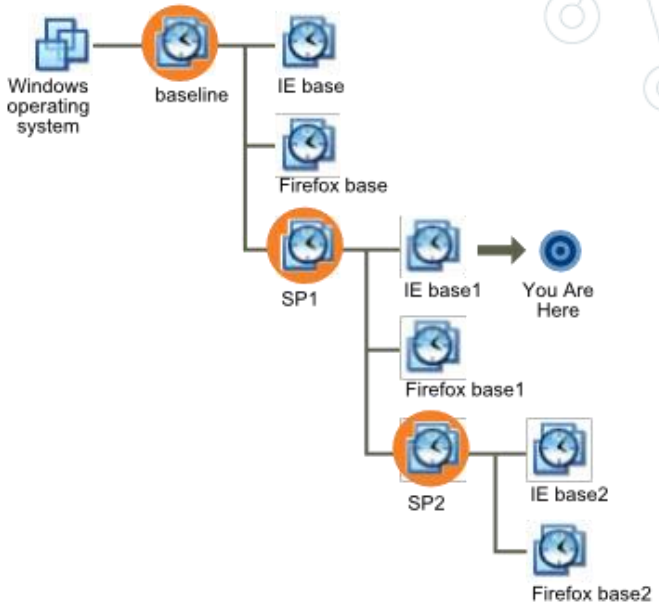
Master Image

- Instead of building the server, desktop each time, create a customized image
- Build the perfect deployment
- Save it as a master image



NON-PERSISTENCE

Non-persistence is when a change to a system is not permanent. Making a system non-persistent can be a useful tool when you wish to prevent certain types of malware attacks.

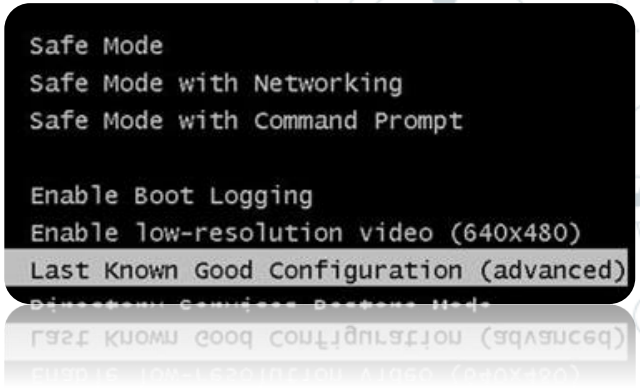


Snapshot

- A snapshot captures the entire state of the virtual machine at the time you take the snapshot.
- Snapshots are useful when you need to revert the known state

Rollback to Known Configuration

if you make an incorrect configuration change in Windows and the system won't boot properly. Reboot, press F8, select select "The Last Known Good Configuration option"

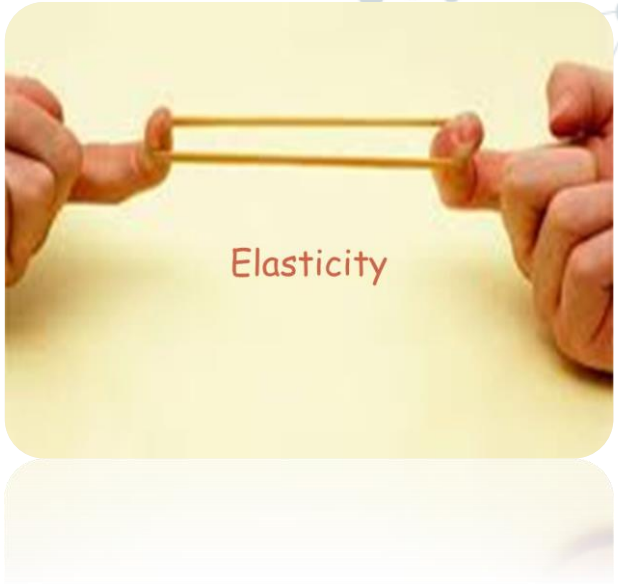


Live Boot Media

- Run the operating system from removable media

ELASTICITY

Elasticity is the ability of a system to dynamically increase the workload capacity using additional, added-on-demand hardware resources to scale out



- Elasticity - Provide resources when demand requires it
- Scale down when things are slow
- Only paying for the actual resources you use.
- In a server farm that you own, you pay for the equipment even when it is not in use.

Time for Testing ourselves and answering some questions!

Part 4 .
Identity and Access Management

Identity and Access Management Concepts

Identification

the process of ascribing a computer ID to a specific user, computer, network device, or computer process.

- Usually your username

Authentication

Authentication is the process of verifying an identity previously established in a computer system.

- Password and other authentication factors

Authorization

the process of permitting or denying access to a specific resource

- What access do you have?

Accounting

The process of ascribing resource usage by account for the purpose of tracking resource utilization

- Resources used: Login time, data sent and received, logout time.

Multi-factor authentication

- Something you are
  Fingerprint, iris, voiceprint
- Something you have
  Smart card, Phone
- Something you know
  Password, PIN.
- Somewhere you are
  Must be in some location
- Something you do
  Handwriting analysis

Biometric acceptance rates

False acceptance rate (FAR)

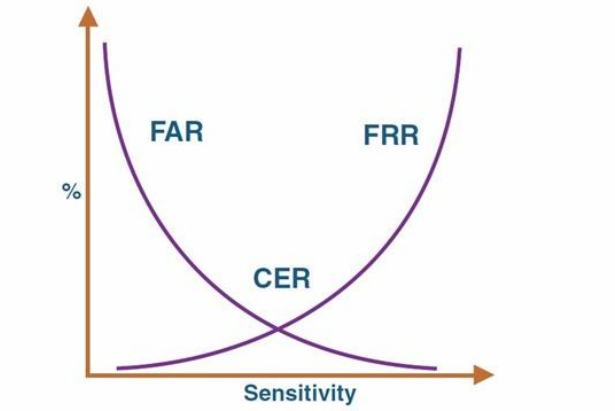
- Likelihood that an unauthorized user will be accepted

False rejection rate (FRR)

- Likelihood that an authorized user will be rejected

Crossover error rate (CER)

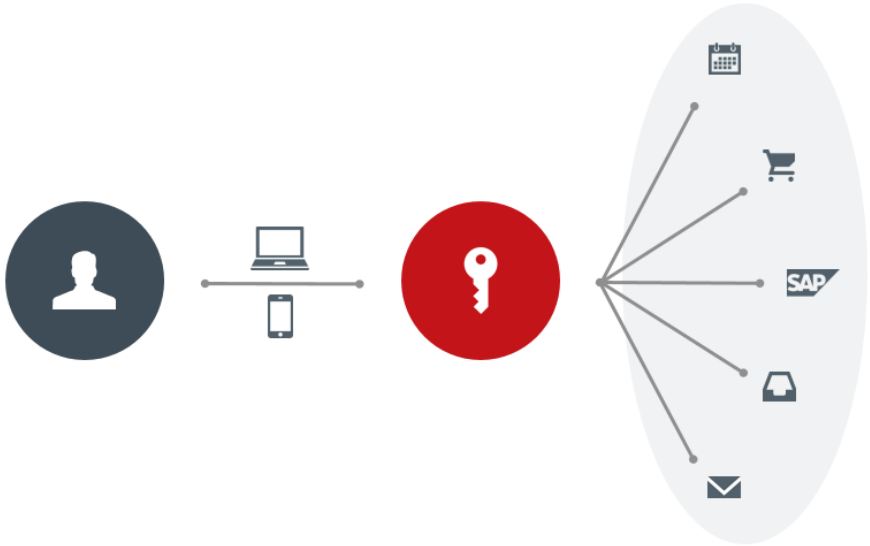
- The rate at which FAR and FRR are equal
- Used to quantitatively compare biometric systems



Single sign-on (SSO)

Single sign-on (SSO) is a form of authentication that involves the transferring of credentials between systems

- Authenticate one time
- Gain access to everything!
- Kerberos authentication and authorization
- 3rd-party options



Access control models

Mandatory Access Control or MAC:

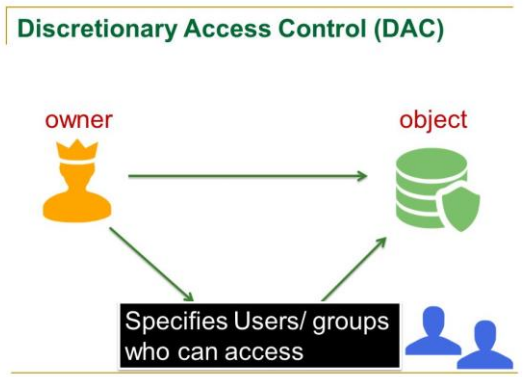
- Resources are classified using labels by owner
- Clearance labels are assigned to users who need to work with resources

For example, some data may have “top secret” or level 1 label. Other information may have a “secret” or level 2 level.
If we have clearance level 1, we can access all data.

If we have clearance level 2, we can access data labeled with “secret” , but we can’t access information labeled with “top-secret”.

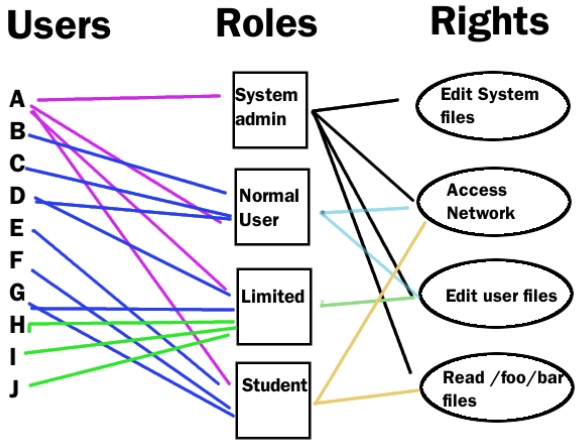
Discretionary Access Control (DAC)

- Used in most operating systems
- You create a spreadsheet as the owner, you control who has access
- You can modify access at any time
- Very flexible access control but very weak



Role Access Control (RBAC)

- Provides access control based on the position
- Instead of assigning John permissions as a security manager, the position of security manager already has permissions assigned to it



Rule Access Control (RBAC)

- Access is determined through rules by System administrators, not users
- Ex: network access is only available between 9-5
- Ex: Allow only from this this GPS location

ExamAlert

Remember that the exam might include alternative uses for the RBAC acronym, referring to rule-based access controls. In a rule-based access control solution, access rights can vary by account, time of day, the trusted OS, or other forms of conditional testing. Exam items that deal with conditional testing for access (for example, time-of-day controls) are examining rule-based access control. Items that involve assigning rights to groups for inheritance by group member accounts are focusing on role-based access control.

Least privilege

- Rights and permissions should be set to
- the bare minimum
- You only get exactly what's needed to complete your objective
- Applications should run with minimal privileges
- Limits the scope of malicious behavior

Time for Testing ourselves and answering some questions!

Time for Testing ourselves and answering some questions!