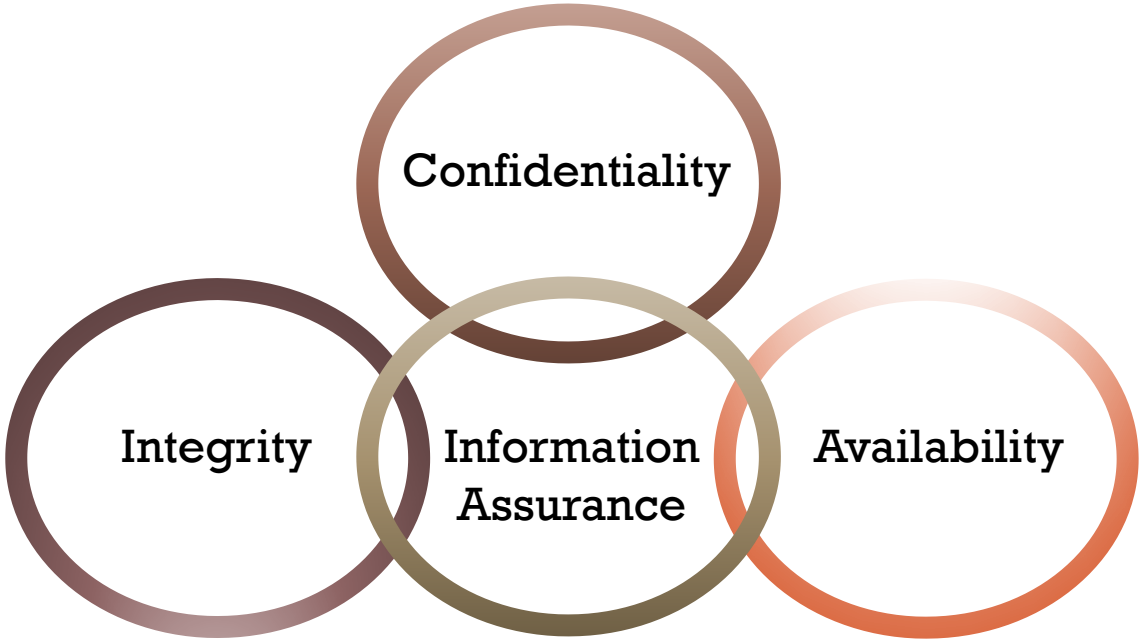
1.1 ELEMENTS OF INFORMATION SECURITY

- Information Security Overview
- Security Controls
- Access Control

WHAT IS INFORMATION SECURITY?

- The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction
- The goal is to provide confidentiality, integrity, and availability of systems and data

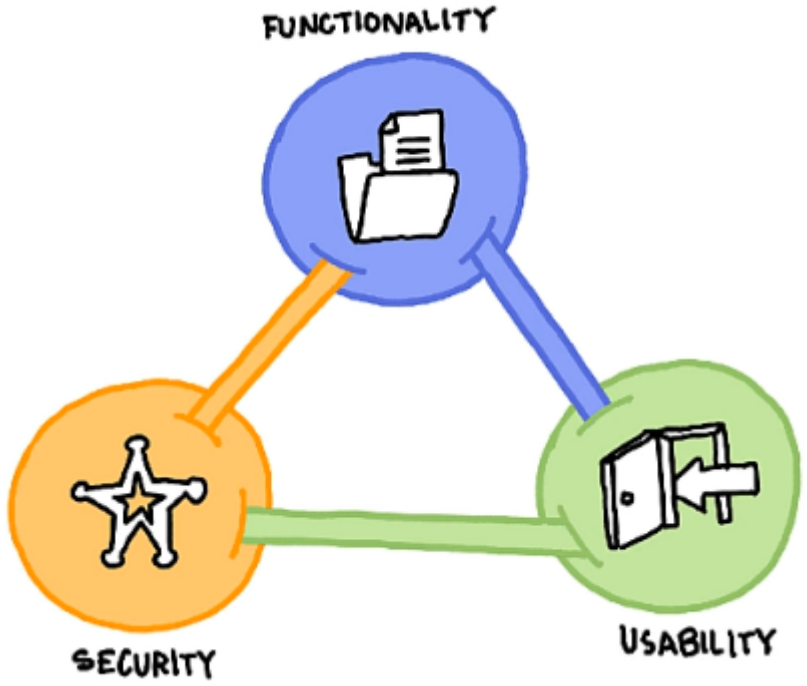


CIA TRIAD

- **Confidentiality**
  - Only allow authorized parties to access the data or system
- **Integrity**
  - Protect the data from unauthorized modification or deletion
- **Availability**
  - Ensure that data and systems that you are protecting can still be accessed and used as needed

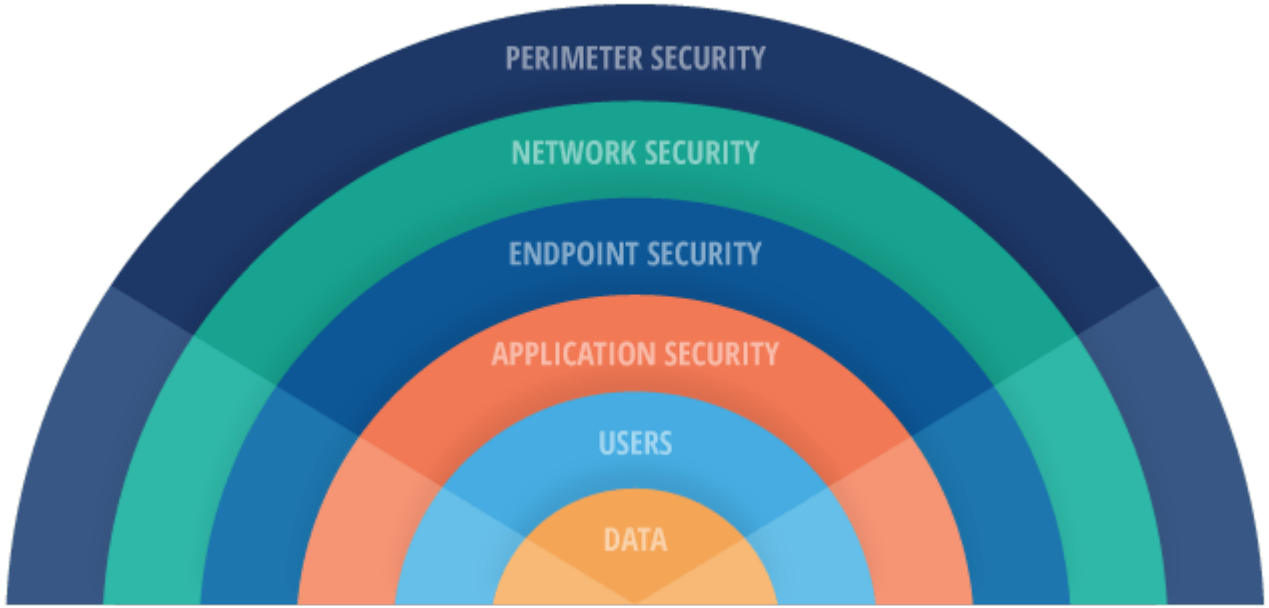
SECURITY, FUNCTIONALITY, USABILITY

- These attributes are interlocked
- Security is at odds with nearly every other organizational process
- Increasing security usually requires decreasing functionality and usability
- You need to find an acceptable balance between these three



DEFENSE IN DEPTH

- Multiple layers of security controls
- Provides redundancy in the event of a control failure



THREE TYPES OF ACTIVE DEFENSE

- Annoyance
  - Involves tracking a hacker and leading them to a fake server
  - Waste their time
  - Make them easy to detect
- Attribution
  - Identify the attacker
  - Use tools to trace the source of an attack back to a specific location, or even an individual
- Attack
  - This is most controversial--and risky
  - You "hack back"
    - Access an alleged hacker's computer
    - Delete data or take revenge
    - Both steps are considered illegal

ESSENTIAL TERMINOLOGY

Term	Definition
Hack value	Perceived value or worth of a target as seen by the attacker
Vulnerability	A weakness or flaw in a system
Threat	Anything that can potentially violate the security of a system or organization
Exploit	An actual mechanism for taking advantage of a vulnerability
Payload	The part of an exploit that actually damages the system or steals the information
Zero-day attack	An attack that occurs before a vendor is aware of a flaw or is able to provide a patch for that flaw
Daisy Chaining / Pivoting	Using a successful attack to immediately launch another attack.
Doxing	Publishing personally identifiable information (PII) about an individual usually with a malicious intent

ESSENTIAL TERMINOLOGY (CONT'D)

Term	Definition
Non-repudiation	The inability to deny that you did something Usually accomplished through requiring authentication and digital signatures on documents
Control	Any policy, process, or technology set in place to reduce risk
Mitigation	Any action or control used to minimize damage in the event of a negative event
Accountability	Ensure that responsible parties are held liable for actions they have taken
Authenticity	The proven fact that something is legitimate or real
Enterprise Information Security Architecture (EISA)	The process of instituting a complete information security solution that protects every aspect of an enterprise organization

SECURITY CONTROL TYPES

Control Type	Description	Example
Physical	Tangible mechanisms designed to deter unauthorized access to rooms, equipment, document, and other items	Guards, lights, cameras, motion detectors, walls/fences, bollards, mantraps, turnstiles, locks, alarms, disposal tools such as document and hard drive shredders
Administrative	Procedures and policies that inform people on how the business is to be run and how day to day operations are to be conducted. Can be enforced through management policing, physical and technical means.	Training awareness, policies, procedures, guidelines, software bug bounties, engaging an security audit team
Technical	Any measures taken to reduce risk via technological means	IDS/IPS, firewall, anti-virus software, encryption, authentication protocols, access control lists

SECURITY CONTROL TYPES (CONT'D)

Control Type	Description	Examples
Preventive	• Makes it difficult or impossible for a bad actor to carry out the threat • Designed to keep errors or irregularities from occurring in the first place • Most security controls are preventive	Fences, gates, locks, authentication, logical access controls, encryption, segregation of duties, employee screening and training
Detective	Designed to detect errors, irregularities and intrusions that have already occurred Assure their prompt correction	Audits, intrusion detection, cameras, motion sensors, anti-virus, mandatory vacations, job rotation
Deterrent	Discourages the bad actor from attempting to carry out a threat	Warning signs, lights, high fences, guards, dogs, logon banners

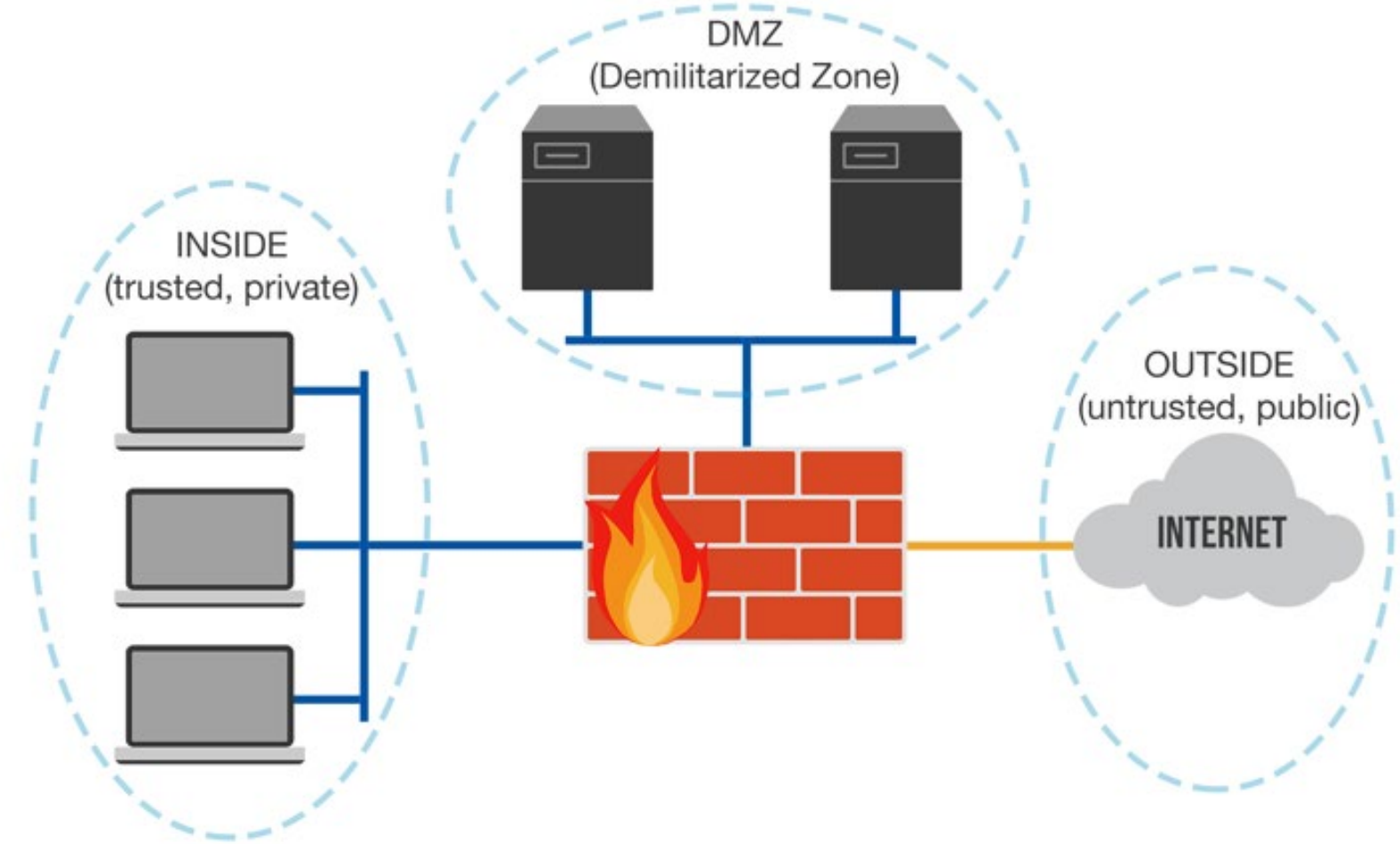
SECURITY CONTROL TYPES (CONT'D)

Control Type	Description	Examples
Mitigating/ Recovery	Minimize the impact of a security incident	System isolation, repair, restore operations, fire suppression
Corrective/ Compensating	• Alternative fixes to cover any gaps in the other control types • Provides equivalent or comparable protection • Might have to sacrifice conveniences to achieve the desired result	• A medical instrument uses an older operating system that still has unpatched vulnerabilities that could expose it to remote code execution. • If the device does not need to be connected to the network to provide its primary clinical functions, the compensating control could be to disconnect it from the network.

NETWORK SECURITY ZONING

- Network Security Zoning allows an organization to manage different levels of network security
  - Defines security levels for specific areas of the company network
- Used to define clear security boundaries between different parts of the network
- Examples:
  - Internet Zone
    - Uncontrolled zone; outside the organization
  - Internet DMZ Zone
    - Controlled zone; defense between internal network and Internet
  - Production Zone
    - Restricted zone; access is strictly controlled
  - Intranet Zone
    - Controlled zone; no extreme restrictions
  - Management Zone
    - Secured zone; with strict policies

NETWORK ZONES EXAMPLE



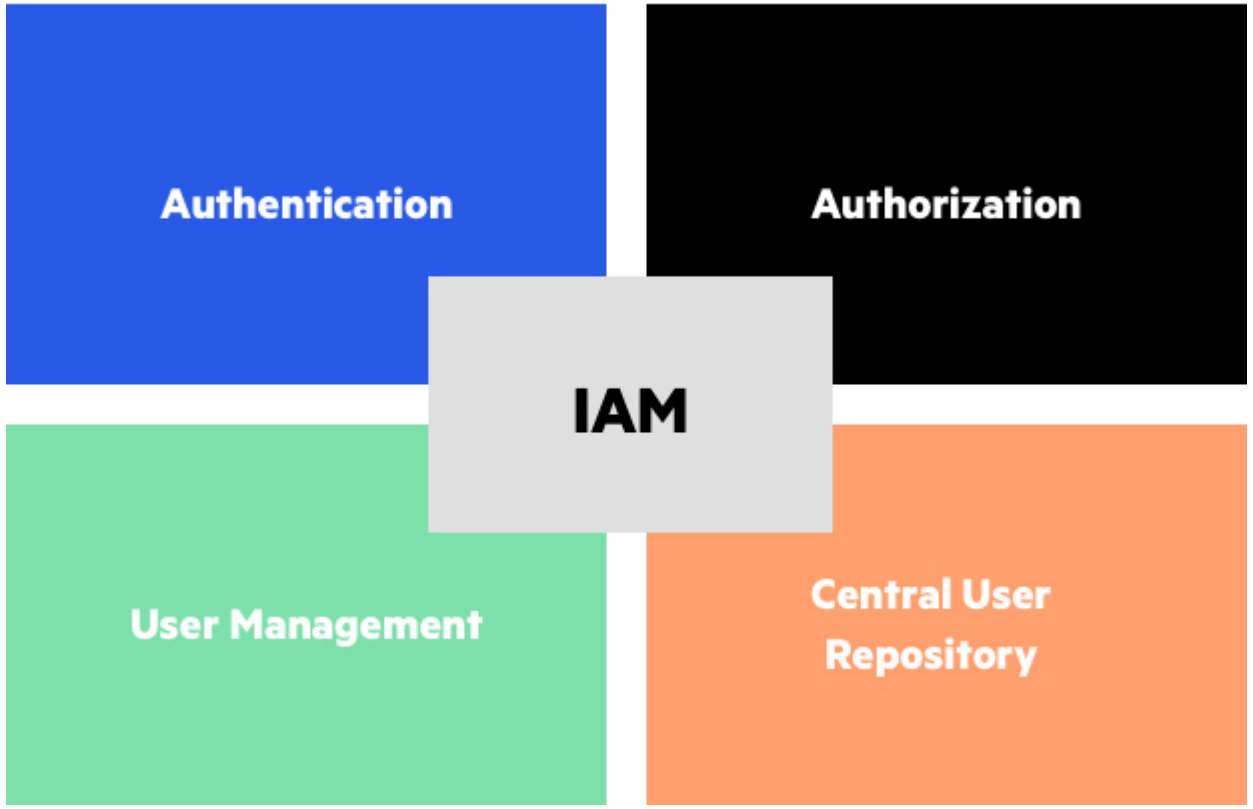
IDENTITY AND ACCESS MANAGEMENT

WHO

can

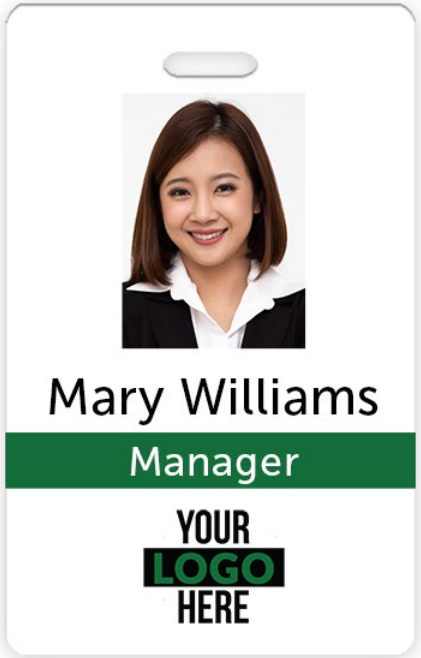
ACCESS

WHAT



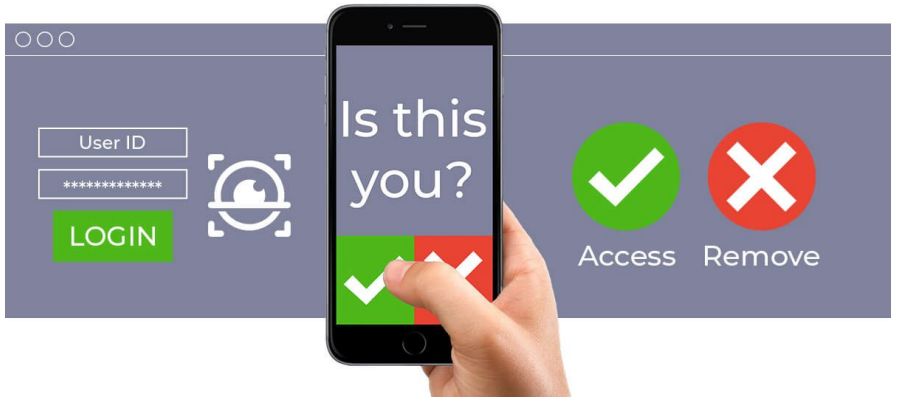
IDENTIFICATION

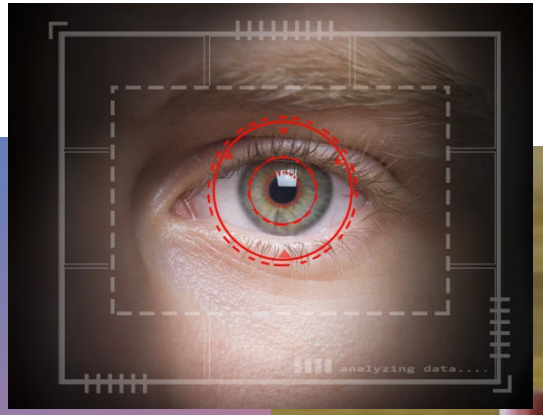
- The action or process of identifying someone
- Can include:
  - Your name, picture, username, ID number, employee number, SSN etc.
- Can also apply to non-human entities such as devices, applications, services
  - Anything that needs to make use of system or network resources

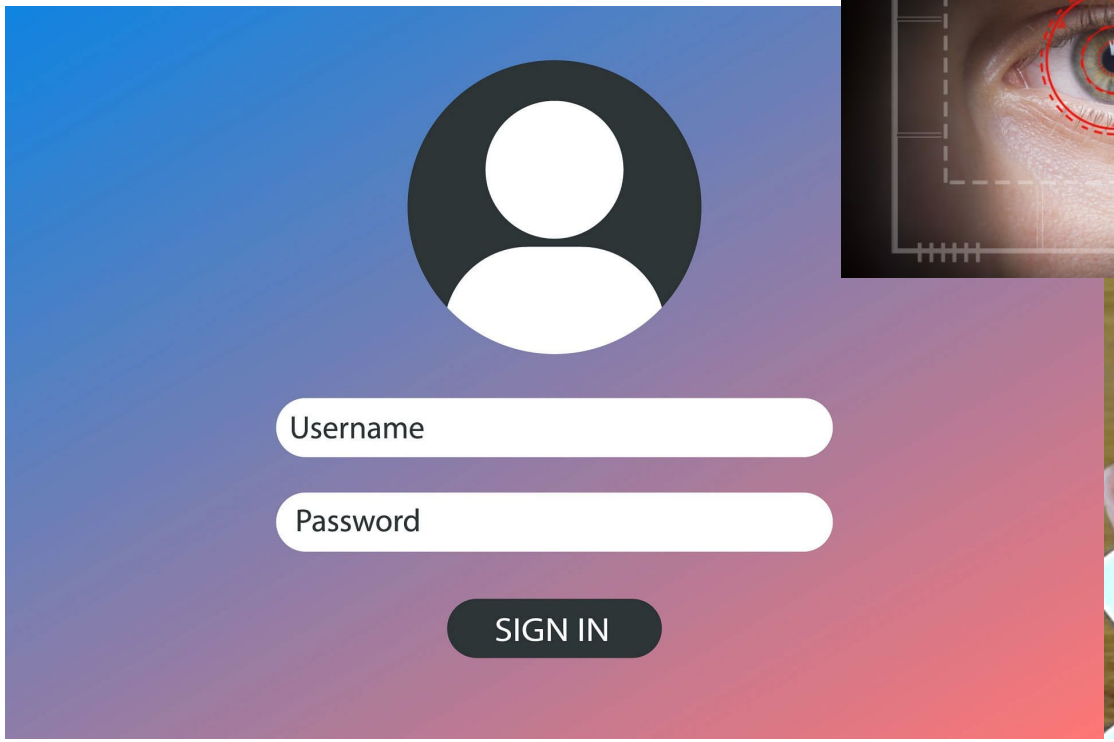


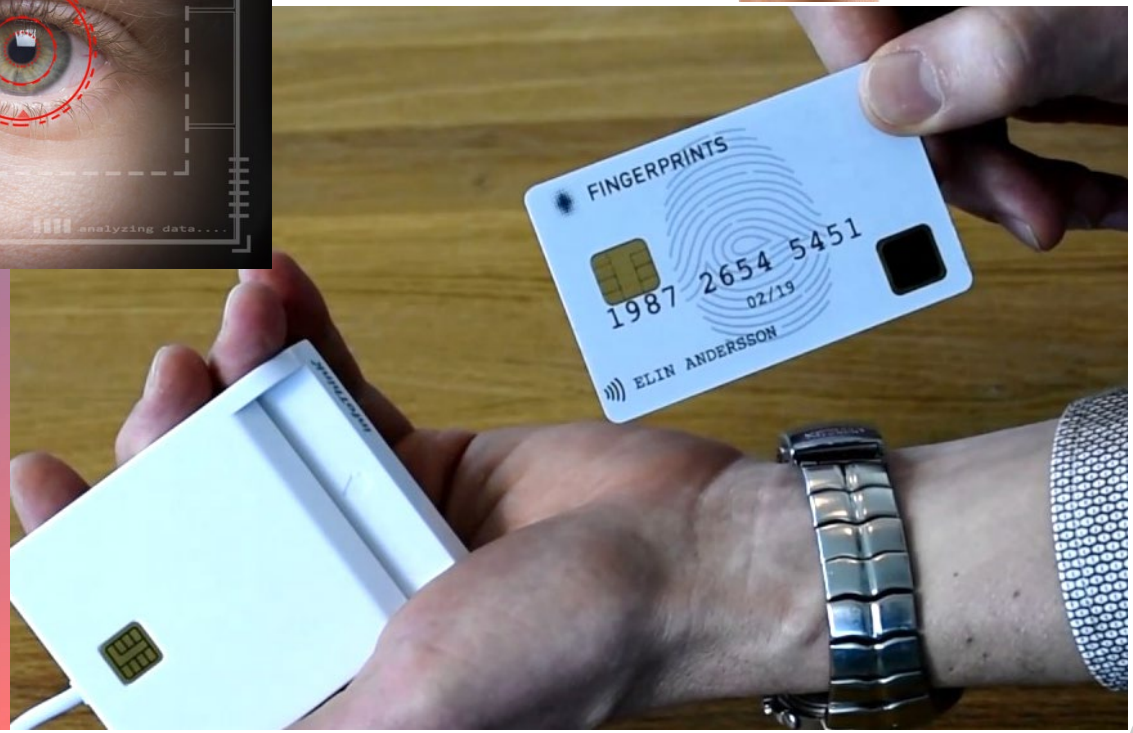
AUTHENTICATION

Prove it's you









AUTHENTICATION FACTORS

- Something you know
  - (PIN, password)
- Something you have
  - (smart card, certificate, authenticating app on a phone)
- Something you are
  - (fingerprint, iris scan, facial recognition)
- Something you do
  - (signature dynamics, typing dynamics)
- Somewhere you are
  - (geolocation)

Multi-factor authentication uses two or more factors
Not from the same category

AUTHORIZATION

- What you are allowed to access/do
- Applied after successful authentication
- Permissions:
  - Applied to resources
- Rights / Privileges:
  - Assigned at the system level
- Authorization strategies:
  - Least privilege
    - Give the user the minimal level of access or permissions – just enough to do their job
  - Separation of Duties
    - AKA Segregation of duties
    - Prevent the conflict of interest
    - Reduce the risk of unauthorized access and fraudulent activity
    - Identify and mitigate control failures such as security breaches, information theft and circumvention of security controls

ACCOUNTING

- Trace an action to an entity
- Prove who or what performed an action
- Log the action for:
  - Compliance
  - Auditing
  - Later reference

MANDATORY ACCESS CONTROL (MAC)

- Every object is assigned a **sensitivity** label:
  - Unclassified, Confidential, Sensitive But Unclassified, Secret, Top Secret
- Subject receives a **clearance** level
  - Subject undergoes extensive investigation to determine if they are granted clearance
    - Public Trust
    - Secret
    - Top Secret
- Neither can be arbitrarily changed
- Subjects can access objects at or below their clearance level
- Top Secret access can also be compartmentalized
  - Based on need-to-know

MAC EXAMPLE

General Public

Public Trust

Secret Clearance

Top Secret Clearance

TS

Secret

SBU

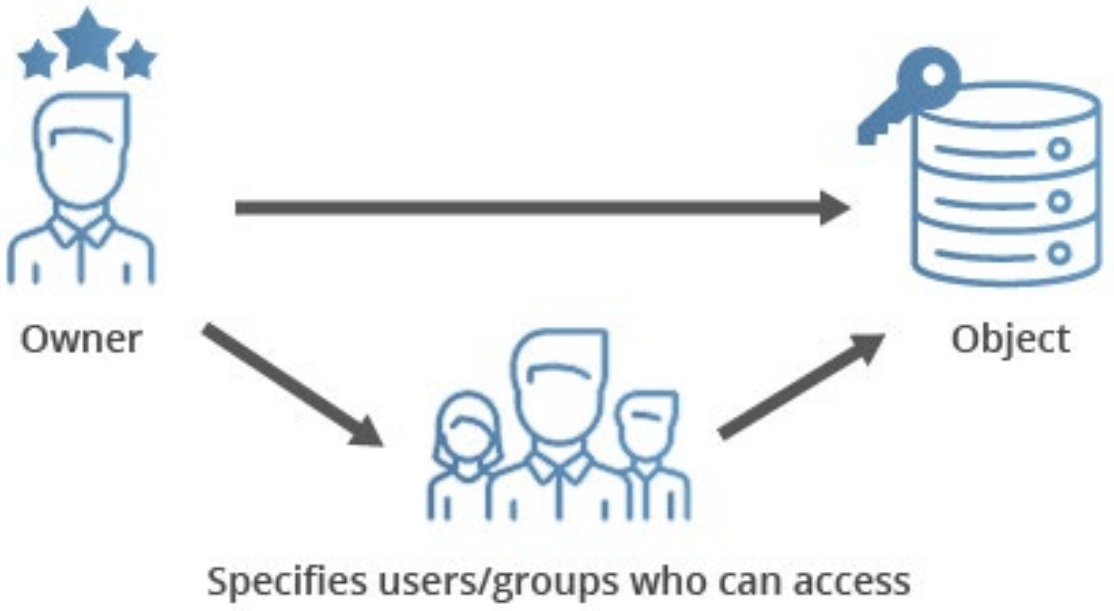
Confidential

Unclassified

Resource Sensitivity Label

DISCRETIONARY ACCESS CONTROL (DAC)

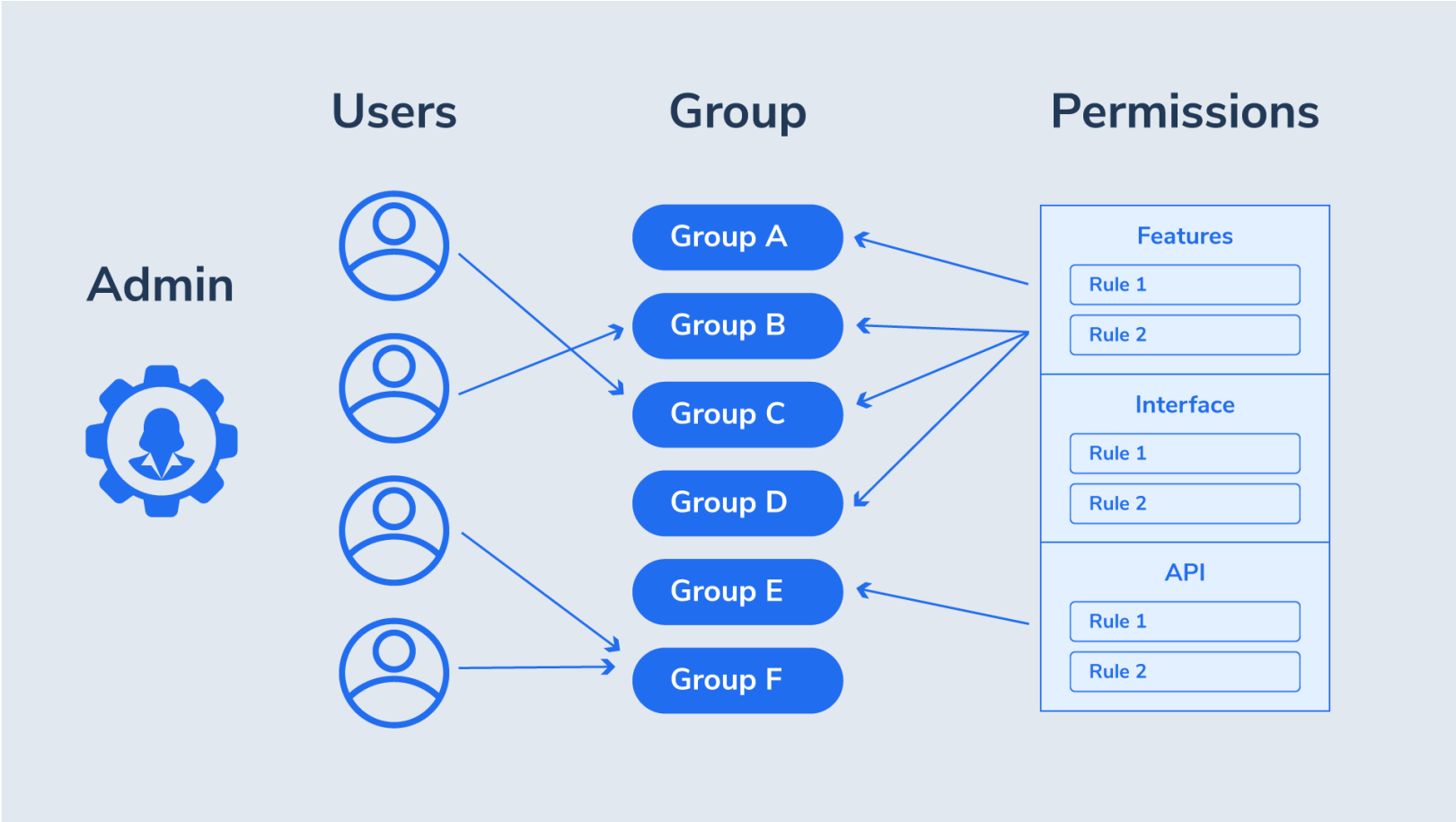
- Used in most operating systems
- Owner of the data defines access at their discretion
- Flexible but weak
- Examples of permissions
  - Read
  - Write
  - Execute
  - Delete
  - List
  - Take ownership



ROLE-BASED ACCESS CONTROL (RBAC)

- Access to resources is defined by your role/job function in the organization
- Permissions are granted to the role, not individual users
- Users can be added to or removed from a role
- In Windows, groups are used to represent roles

RBAC EXAMPLE



RULE-BASED ACCESS CONTROL (RULEBAC)

- Access is granted or denied based on whether or not a rule is met
- Firewalls and packet-filtering routers use RuleBAC to permit or deny network packets

Requirement	Permission	Protocol	Source	Destination	Port
1	ALLOW	IP	ANY	192.168.1.25	80
2	ALLOW	IP	ANY	192.168.1.25	443
3	ALLOW	UDP	ANY	192.168.1.10	53
4	DENY	TCP	ANY	ANY	53
5	DENY	IP	ANY	ANY	53
6	DENY		ANY	ANY	

1.4 HACKING

- Concepts
- Terminology

WHAT IS HACKING?

- Exploiting system vulnerabilities and compromising security to gain unauthorized access to system resources
- Modifying system or application features to achieve a goal
- Used to steal and redistribute intellectual property leading to business loss

TRADITIONAL HACKING MODEL

Reconnaissance	OSINT Footprinting Scanning/Fingerprinting
Penetration	Active hacking Delivering malware Social engineering Physical intrusion
Control	Planting backdoors Instructing zombies Covering tracks

WHO IS A HACKER?

- Intelligent person with excellent computer and networking skills exploring a system or network
- Hobbyist testing vulnerabilities of systems and networks
- Consultant hired by an organization to improve network security
- Cyber criminal
- Anyone attempting to gain knowledge for legal or illegal purposes

HACKER CLASSES / TYPES

Hacker Class	Description
Black Hat	Performs malicious activities; cyber criminal
Grey Hat	Performs good or bad activities but do not have the permission of the organization they are hacking against
White Hat / Ethical Hacker	Uses their skills to improve security by exposing vulnerabilities before malicious hackers
Script Kiddie / Skiddie	Unskilled individual; uses malicious scripts or programs developed by others to attack systems and deface websites
State-Sponsored Hacker	Hired by a government to perform attacks on other governments or high-profile targets
Hacktivist	Hacks for a cause or political agenda
Suicide Hacker	Not afraid of going jail or facing any sort of punishment; they hack to get the job done
Cyber Terrorist	Motivated by religious/political beliefs to create fear or disruption

HACKER TYPE EXAMPLES

ADVANCED PERSISTENT THREAT (APT)

- APTs are external threats
- They seek to:
  - Quietly gain access to your system
  - Stay there undetected as long as possible
- They are usually sponsored by nation-states and well-funded
- They use multiple attack vectors (whatever they can) to gain access to sensitive data
- They are used for intelligence-gathering operations against government, military, and commercial networks
- There have recently been high-profile cases in the news of APTs exfiltrating and exposing corporate and government data

APT EXAMPLES

- APT 27 – LuckyMouse
  - Chinese group that focuses on Asian/Pacific nations/Middle Eastern states
  - Targets aerospace, education, and government sectors
  - Uses existing tools such as PsExec, Mimikatz, ProcDump and others
- APT 28 – Fancy Bear
  - Russian cyber espionage group sponsored by the Russian Government
  - Associated with the Russian military intelligence agency GRU
  - Targets NATO-aligned countries
  - Uses zero-day exploits, phishing and malware
- APT 35 – Charming Kitten
  - Iranian government cyber warfare group that uses phishing and social media
  - Developed a tool to steal data from well-known email providers such as Google, Yahoo, and Microsoft
  - Documented interference in US 2020 and 2022 elections
- APT 37 – Reaper
  - North Korean government hacking group
  - Mostly targets South Korean industries such as chemical, electronics, manufacturing, aerospace, automotive, and healthcare

APT 37 EXAMPLE

- Took advantage of the Oct. 29 Itaewon crowd-crush tragedy, which killed more than 150 people
- Used social engineering to trick South Koreans into downloading malicious files

INSIDER THREAT

- Trusted users who abuse/misuse the system
- Most insider threats are not intentionally malicious
  - Users cause accidental breaches
- Some insider threats are purposeful
  - Disgruntled employee
  - Corporate or government spy
  - Terminated employee or contractor whose access was not revoked upon termination

1.5 ETHICAL HACKING

- Understanding Ethical Hacking
- Ethical Hacker Skills
- Developing Technical Hacking Skills

WHAT IS ETHICAL HACKING?

- The use of hacking to improve security
- An attempt to identify vulnerabilities before they are exploited by a bad actor
- Ethical hackers use the same tools, steps, and techniques as other hackers
  - However the intent is to protect, not damage

WHY ETHICAL HACKING IS NECESSARY

- Keep ahead of unethical hackers
- Uncover and fix vulnerabilities before they are exploited by a bad actor
- Analyze and strengthen an organization's security posture
- The ethical hacker attempts to discover:
  - What an intruder can see
  - What an intruder can do
  - If any intrusions have already occurred
  - If systems are properly patched and protected
  - The amount of effort necessary to protect the system
  - If information security measures are in compliance with industry and legal standards

ETHICAL HACKING VS PENETRATION TEST

- Ethical hacking the primary mechanism of a penetration test
  - The ethical hacker is part of the penetration testing team
- In a penetration test, an organization engages a team of cybersecurity experts
  - Actively attempt to exploit systems, infrastructure, and people
- Not to be confused with vulnerability scan
  - A vulnerability scan is one small part of a penetration test
  - It identifies systems that *might* be vulnerable to hacking
  - It does not attempt to actually exploit the vulnerable system

TECHNICAL SKILLS OF AN ETHICAL HACKER

- In-depth knowledge of major operating environments, concepts, technologies and related hardware and software
- Should be a computer expert understanding technical domains
- Should be comfortable using the same tools and exploits that other hackers use
- Should have security knowledge and experience
- Should understand sophisticated attacks

NON-TECHNICAL SKILLS OF AN ETHICAL HACKER

- Ability to learn and adapt new technologies quickly
- Strong work ethic
- Commitment to the organization's security and policies
- Understanding of local, state, and federal laws and organizational compliance
- Ability to communicate concisely with the client
- Ability to explain that systems can never be fully secured
  - Security can always be improved
  - It is up to the organization to implement recommendations once vulnerabilities are discovered

ETHICAL HACKING PROCESS

- The client hires you to find vulnerabilities in their network
- A contract will clearly specify the rules of engagement:
  - The start time
  - Which systems will be tested
  - Which systems will not be tested
  - If the test will include processes and people
    - Social engineering