COMP432: Computer Security

Introduction to Computer Security

- **Information security is more general whereas cybersecurity is a part of information security.**
- Cryptology is information hiding
- Hashing is the process of transforming any given key or a string of characters into another value.
- Environment includes devices communicating over network
- **Data vs. Information?**
    - **Data: raw material**
    - **Information: group of data**
- Different users will contain different permissions within an application or website
    - Admins are provided with the most permissions
    - Users would be provided with the less permissions than admins
- Everyone looks to see if they can hide their assets (information)
- There are gaps or weak points in which you can compromise the system
    - The possibility of being hacked was greater back then than now due to the consistent maintaining occurring now
    - There was not internet of things, or even devices that communicated with each other via the internet
- Cybersecurity only came to exist after digital crimes and you can investigate digital crimes where the practice is called digital forensic.
    - Digital crimes increased the more people became dependent on digital devices.
    - Internet of vehicles (IoV) is another important reason we should find solutions to potential digital crimes.
- Block chain’s purpose is to store the data integrity because each data connected from the chain are all related to the data that comes before and after it. It is used to record transaction.

- Security is about protection of assets
- **Prevention-Detection-Reaction**
  - **Prevention**: to try and prevent a hacker the hacker can't recognize or hack into your information
    - Examples: VPN, using anonymous to be able to hide your identity, or firewall, biometric face authentication, two-factor authentication, multiple-factor authentication.
      - Firewall depends on white and black list meaning some transactions are allowed to be assessed and others aren't, if there's something new that isn't recognized by firewall then it enters which is a problem.
    - Take measures that prevent your assets from being damages or stolen
  - **Detection**: to try and detect the hacker but it doesn't take any action
    - Take measures so that you can detect when how and by whom asset has been damaged
  - **Reaction**: reaction towards the hacker hacking
    - Take measures so that you can recover your assets
- **CiA: Confidentially, Integrity, Availability**
- You store sensitive data in encrypted format that is stored in the cloud for better privacy
  - To decrypt the data, it's possible to work on it without fully decrypting it
- **IDS (Intrusion Detection System)** is connected on the system like any other systems and there was traffic, it could potentially go down because the **IDS** will send an alert, but by then the other systems would have already taken a hit
  - You can still reset so it doesn't lose too much information.
- **IPS (Intrusion Prevention System)** is the same but it also takes action by blocking all the connection.
- **Trojan virus** is a type of malware that downloads onto a computer disguised as a legitimate program.

- **Two types of virus attacks**
  - **Passive**
    - **Just reads the data**
  - **Active**
    - **Modifies the data**
    - To fight these viruses, we use **hashing**
      - **One-way encryption** is a type of encryption used to secure and protect passwords and other sensitive data
        - **It encrypts the data by changing a plain text to a unique digest that is irreversible.**
- There is no single consistent terminology for security
- **Basic security concepts**
  - **Confidentiality**: prevent unauthorized disclosure of information
    - Ensuring that only authorized users can assess certain information that is authorized to them
    - Ensuring security and privacy
  - **Integrity**: prevent unauthorized modification of information
    - Ensuring that the data is received to the person that is meant to receive it and can confirm the integrity of the data being received
    - There could be a potential Main in the middle attack (MITM Attack)
      - The MITM attack is where a perpetrator gets in the middle of the communication to eavesdrop or impersonate (they could possibly alter the communication between the two parties).
  - **Availability**: prevent unauthorized withholding of information or resources
    - I want to confirm **the system is usable and available whenever the user wants**
  - **Authenticity**: “know whom you are talking to”
    - Do you have **privilege** or not to be accessing these documents?

Triple As

Authentication
Authorization
Accountability

        - **To confirm each user is in fact the user they say they are**, so Samantha Bamboo is in fact Samantha Bamboo
    - **Accountability** (non-repudiation): prove that an entity was involved in some event
        - **Cannot deny having performed a transaction**
    - **Authorization**

- **Internet Shopping Example**
    - **Prevention**
        - Encrypt your order and card number, enforce merchants to do some extra checks, don't send card number via internet
    - **Detection**
        - An unauthorized transaction appears on your credit card statement
    - **Reaction**

- **Carving is recovering a file from raw data where we only have 10% of the original file but can confirm it's the same as the one we are trying to recover.**

- **Confidentiality**
    - **Either data is hidden or behavior within the system is hidden** so no unauthorized person accesses it
    - Prevent unauthorized disclosure of information (prevent unauthorized reading)
    - **Secrecy**: protection of data belongs to an organization
        - **Follow standards and rules that are cemented within the company or person meaning**:
            - ***All files are encrypted***
            - ***All data is hidden***
    - **Confidentiality vs. Secrecy:**
        - **If I want to hide the file, then its <u>Confidentiality</u>**
        - **If I want to hide the content of file or part of the file then its <u>Secrecy</u>**
    - Historically, security and secrecy were closed related; security and confidentiality are sometimes used as synonyms
    - Do we want to hide the content of a document or its existence?
        - Traffic analysis in network security
            - Sometimes **confidentiality means <u>hiding the network</u> itself** from outside sources
        - Anonymity, unlinkability

- **Privacy**
    - **Privacy: protection of personal data**
        - **Trying to put a level of protection for user's data**
    - **"Put the user in control of their personal data and to information about their activities"**
    - Taken now more seriously by companies that want to be trusted by their customers
    - Also: The right to be the left alone (e.g., not to be bothered by spam)

- **OECD Privacy Guidelines** are the outline principles for the **protection of privacy and personal data**. The principles include:
    - **Collection Limitation Principle**
        - **Limit the amount of data that is collected to ensure privacy**
        - Limiting the collection of personal data to what is necessary for specified purposes.
    - **Data Quality Principle**
        - **Data must be accurate and relevant that it is being used**
        - Ensuring that personal data collected is accurate, relevant, and up to date
    - **Purpose specification principle**
        - **I cannot use the data unless I have a justifiable reason**
        - Specifying the purposes for which personal data is collected and processed, and obtaining consent from individuals for such purposes
    - **Use limitation principle**
        - **I have access control on the data that is being used**
        - Restricting the use of personal data to the purposes for which it was collected, and preventing unauthorized access or disclosure
    - **Security safeguards principle**
        - Implementing appropriate security measures to protect personal data against unauthorized access, disclosure, alteration, or destruction

Hashing vs. Encryption
Hashing is a one-way encryption
Encryption is two-way with encrypting and decrypting

- Integrity
    - States that even if he was able to see the data and it wasn’t secured, the data would still not be able to be modified
        - Integrity has no problem with passive attacks, however there is a problem when there is an active attack that modifies the data
    - Prevent unauthorized modification of information (prevent unauthorized writing)
    - Data integrity the state that exists when computerized data is the same as that in the source document and has not been exposed to accidental or malicious alteration or destruction (integrity synonymous for external consistency)
        - Data integrity is wanting to confirm if the data that you received is the same as the data that is in the source
    - Detection (and correction) of intentional and accidental modification of transmitted data
    - No user of the system, even if authorized, may be permitted to modify data items in such a way that assets or accounting records of the company are lost or corrupted
    - In the most general sense: make sure that everything is as it is supposed to be
        - (This is highly desirable but cannot be guaranteed by mechanisms internal to the computer system)
    - Integrity in a prerequisite for many other security services, operating systems security has a lot to do with integrity

- **Collagen-free where you give two inputs and they can’t give the same output**
    - **For example: if there was a message X and another message Y, then the outputs cannot both be output R.**

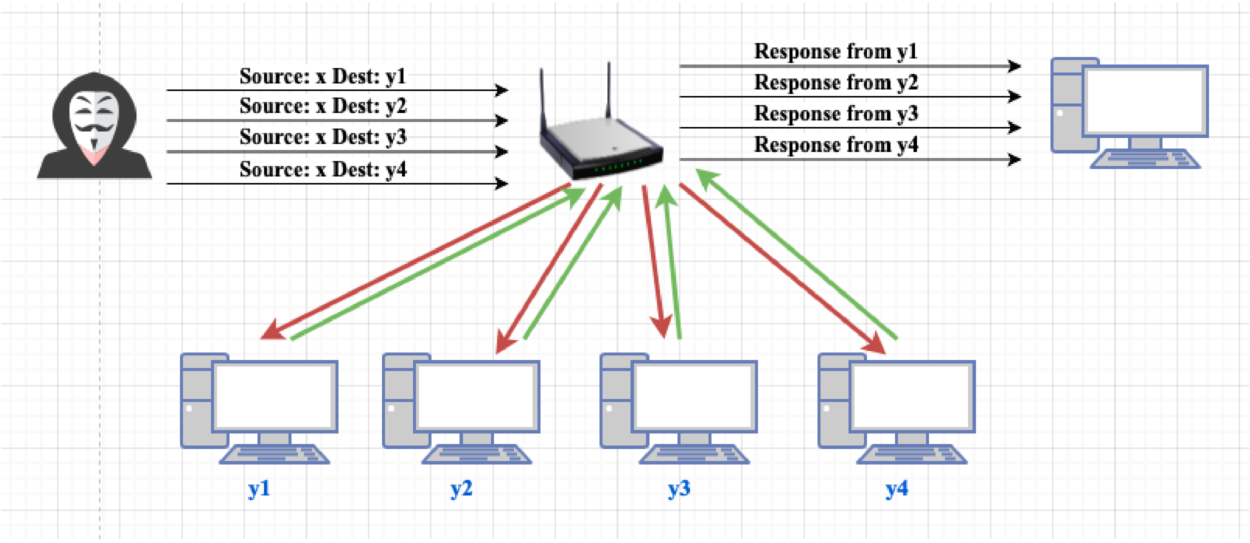
    - **OS Data Integrity**
        - **System Integrity: the overall integrity of the operating system itself is crucial. Operating systems should be resistant to unauthorized changes that could compromise their stability, security, or functionality. Protesting system integrity involves measures such as secure boot processes, file system protections, and kernel integrity checks, based on using techniques such as files integrity checks**
        - **What are two ways to confirm data integrity?**
            - **Signature data vs encrypted data?**
                - **Signature data: is data that is clear but is a signature with clear value (but cannot be defined because the signature data if modified would be recognized)**
                - **Encrypted data: is data that is not a clear text and a cypher text**
                    - **What’s a type of attack that can continue attempting the trial-and-error to get the data?**
                        - **brute force attack**

- **Availability**
    - **Any system that is accessible and can be used by the user at any time is considered available.**
    - **Botnet can keep sending servers which is considered flooding the server**
        - **In any server, you have to receive every request**
    - **Attacker will take advantage of the ICMP to attack**
    - **The router looks for the best path using Dijkstra and if the router doesn't find the best path then it would affect the availability. If this happened then it would be a ICMP attack**

- **Spoofing**
    - **Where an attacker disguises themselves as a trusted source.**
        - **For example:**
            - **An attacker sending an email to the user about credit card renewal. The email tells the user to click on link to renew their credit card**
    - **The spoofing is not passive or active, its mostly just concentrating on seeing if the system is available**

- **How can we do spoofing is another way?**
    - **ICMP fragmentation attack: it's part of the data and they come in fragments so you have to wait until all the fragments are complete, which is a process known as defragmenting**

- **Smurfing**
    - **Where an attacker will send ICMP echo requests to a broadcast address using the victim/target's address**
        - **For example:**
            - **The hacker in the figure below has an address of 4.4.4.4 and the target/victim has an address of 4.4.4.5. The hacker decides to use the target's address which now means the hacker's address shows as 4.4.4.5 (spoofing). The hacker will then ping (ICMP echo request message) hosts within the network. The hosts will then respond to the ping messages (ICMP echo reply message), and the target/victim will receive a huge number of IP packets. The memory of the target will then be overflowed and overworked which will result in the target's system being unavailable, causing a denial-of-service attack.**



- **Purpose is to make the target system or network resource unavailable for intended users**
- **Smurfing happens in the Network Layer**

Which type of attack takes more requests ?

- **Smurf**

There are two types of data management operations

- **One to many**
  - **Fragmentation occurs when a file or data is divided into smaller parts scattered across a storage medium which leads to inefficiencies in accessing or managing that data**
- **Many to one**
  - **Defragmentation occurs when reorganizing fragmented data on a storage medium to improve efficiency and performance. The scattered parts of a file or data are rearranged on a storage medium.**

- **Accountability**
  - **To ensure the people involved take responsibility**
  - **Accountability is useful for Digital Forensic because all data, log files, and information is stored and recorded. Upon opening up recorded documents, it would be recognized who had agreed on what, their IP address, who transmitted what, etc.**
  - **In single computers, you'll have everything recorded**
  - **In multiple computers within the system, the way it's done is it will ensure anything sent will be recognized by who sent it and whoever it was sent will be recorded, and whoever modified it will be recorded as well.**
    - **How do we know who did what?**
      - **Using Watermark and digital signature**

- How is the digital signature done?
  - Using hashing, if the file was modified in anyway, the Dijkstra and the data. The data that was previous to the modification would be 12345 and after modification would be 123450 meaning it was modified.

Types of Encryptions:

- **Asymmetric encryption uses pairs of related keys. Each key pair consists of a public key and its private key.**
  - **Example: RSA, Diffie-Hellman**
  - **Nadeen, hind, and Mustafa, where each person has a public and private key. If Nadeen wants to send a document to Mustafa, then she would need his public key to encrypt the document with his public key. When Mustafa receives his document, he will decrypt it using his private key.**
- **Symmetric encryption**
- **Consensus encryption**

- **Reliability and safety**
  - **The system will do all the functions and without committing mistakes or any failures by accident or not**

- **Dependability**
  - **The system must be resilience, reliable, safety, and secure**
  - **The system has to be comfortable for the user, but sometimes this could affect the security**

- **Aspects of Security**
  - **Distributed systems**
    - **Multiple computers with encryption**
  - **Communications**

    - **Integrity**
    - **Hashing**
  - **Computer security**
    - **IDS**
    - **Firewalls**
    - **log files**
    - **access control**
    - **authentication**
    - **privileges**
    - **authorization**
  - **Application Security**
  - **Security management**
    - **How to implement the security principles with the resources we have with us like the data and privileges**
- **The fundamental dilemma of computer security**
  - **To balance accessibility and usability with security.**

- **Principles of Computer Security**
  - **The dimensions of computer security:**
    - **Application Software**
      - **How can I ensure security in the software?**
        - **There should be a security in every part of the life cycle of software, the security will be added to the software as a layer.**
          - **For example, the password would have restrictions, encryption,**
          - **TLS: transport layer security is where the session between users will be secured to ensure safety of private information**
            - **Diffie-Hellman Algorithm**
    - **Resource (Object)**
      - **Resources are where you’re interacting with logic data or data that is transmitted**

            - Ensuring the resources are encrypted and not easily modified
        - Hardware
            - Digital forensics will try to find hard evidence, hard disk drive, flash memory, or computer where they have the ability to place it in a safe area where it won’t be modified.
            - Hardware could be a part of resources, memory, etc. that you work with in computer security
        - User (subject)
            - Privilege escalation is a network attack where the user can get privileges beyond their necessary privileges.
            - There’s access control and rules to follow for each user like the manager having manager privileges, customer having customer privileges.

- Where to focus security controls?
    - The focus will be on the integrity of data, operations, and users
- Where to place security controls?
    - Applications
    - Services
        - Web services
    - Operating System
    - OS Kernel
        - Enter process communication on the level of the kernel, where there will be encryption
    - Hardware

If the system depends on layers, then its more secure.

- **The Man-Machine Scale**
    - **If I was closer to the man, then the system would be more complex**
        - **Complexity depends on the access control and the decision-making**
    - **If I was closer to the machine, then the system would be simpler**
    - **The outer ring would be more specified, the more we enter the ring (inner rings), the more generic and simpler it becomes**

- **Defense in Depth**
    - **There are multiple layers of defense to ensure that the system is properly secured.**
    - **The layers of defense's concept come from the Onion model where the idea is to provide redundancy and toughness in security measured**

- **Layers**
    - **Hardware layers**
        - **Has sensors, movement detection, access control, etc.**
    - **Kernel Layers**
        - **Critical control system where its responsible for the managements of the system resources and communication between these sources**
    - **Operating System layer**
        - **Permissions**
        - **Encryptions**
        - **Anti-viruses, IDS (Intrusion Detection System), IPS (Intrusion Prevention System)**
        - **Firewall filters incoming connections that enter the system in where you can identify if the data is legitimate or malicious. The database would have**

the dataset (whitelist) that is approved to enter the system.

- **The incoming traffic would be filtered through the firewall where it will have a signature that is either allowed to enter, which means its legitimate, or not allowed to enter (From the blacklist) meaning its malicious**
- **Firewall is static**
- **TDCGAN**
  - **Using deep learning where we keep training the system on different attacks ensuring it can protect itself and stay secure through each attack**
    - **When a hacker decides to attack, the system would be able to easily protect itself due to the continuous attacks that it learned**

- **Service Layer**
  - **IDS and IPS also work in this layer**
  - **servers, sessions, and services work in this**
- **Application Layer**
  - **Authentication and Authorization because we’re interacting with the user**

- **How is the data and information are related to the security?**
  - **Data is in the low level and the information is in the high level, where they’re both related to each other.**
  - **Data security where the data is in the database**
  - **If the data is being moved modified etc. it would be in the information security**
  - **Data interacts with two types of databases: sql and nosql**
  - **To secure the data, I need encryption**
- **Diffie-Hellman algorithm is used on TLS, using the Diffie-Hellman key exchange.**

- **Complexity or Assurance?**
    - **Complexity makes the system more secure but will affect the usability of the system**
    - **Assurance makes the system more reliable and transparent for users but the overly complex assurance processes could potentially become sources of vulnerabilities.**
- **Centralized or Decentralized Control?**
        - **The domain should have controls enforced to ensure security**

- **Blocking Access to the Layer Below**
    - **Blocking the user from attempting to go from layer to layer to get more permissions**

Security Management

- **In general, Security Management means managing, maintaining, applying, achieving privacy, integrity, confidentiality, and so on.**
- **Rules to avoid attacks and keep the system secured.**
- **Attack**
    - **Managing at its core is to stop attacks**
    - **Attacks are exploiting some vulnerabilities and weak points**
        - **Vulnerabilities: algorithms, policies, humans (users with less awareness), and so on.**
            - **To Fix users with less awareness is to train them into not opening each attachment, link, or video.**
    - **An attack can be recognized as a cyber-attack (vulnerabilities), cyber intrusion (both of which are malicious attempts)**
        - **Cyber-attack: malwares and viruses which is warm attacks**
        - **Cyber intrusion: the attacks that have been successful and have caused distrust within users who use the system that has been attacked.**
        - **Digital attacks exploit vulnerabilities**
        - **What are scenarios that could cause attacks?**
            - **Social Engineering: based on the user's friendships and relationships, the hacker could figure out their passwords and track their interests. Additionally, there could be fake websites (like a fake Facebook website), where the hacker would get your information from you adding your information to the fake Facebook website.**
                - **This is solved using two-step authentication**

- Example of Social Engineering: fishing attacks
- If the URL was the same as the original website link how to spot it?
  - Checking for “\” or “?” in the end of URL
- What is the motivation and classification?
  - Organized crime, terrorists, governments, competition, hacktivists, or/and for fun.
  - There are levels of attackers: from beginners/script kiddies to the elite/highly skilled

- Security Policy
  - Security and security policy in general should have awareness
    - What is necessary from the user to ensure security?
  - Security policy is the set of rules that determines the organization intentions, principles and guidelines to protect the resources
    - Organizational Level is where we can ensure secured assets via laws rules and practices that the organization uses
    - Technical level is where the system is secured via the computer system and technology such as access controls, firewalls, security protocols, etc.

- Measuring Security
  - I want to calculate and measure the security
    - Measure and see how many bugs and vulnerabilities, which is known as quantitative
  - We want to count the number of users rather than the type users because one of them could easily be compromised and are a vulnerability to the system
    - One of the users could cause problems with the privileges, authentication, and so on

  - Strongest attacks are within the system rather than out of it.
- We can’t necessarily trust the users because we don’t exactly know who they are. To continuously confirm them we use dynamic authentication or continuous authentication
- We want to calculate the number of attacks in total and the number of attacks that have in fact succeeded
- The number of attacks that have in fact succeeded is quantitative
- Measuring security is a complex task where we measure the security of a system to see if it’s in fact secure or not. There are two types of security measures
  - Qualitative Security Measures focuses on characteristics and description such as security policies, procedures, guidelines, and standards
    - To measure the security of the system in ensure privacy and integrity.
  - Quantitative Security Measures focuses on the numerical or measurable data that calculates the effectiveness, efficiency, the amount of security incidents, time to detect the response time for the incoming attack, and the cost of the security investments
    - Incident detection is used to find the number of incidents that occurred.
      - We are able to find the numerical value and measure based on the incidents so we can response and deal with these incidents.
      - Nowadays, AI-based protection is a solution that depends on deep learning that deals with attacks like unknown attack and incoming unknown requests

that isn’t specifically dedicated easily in black and white lists.

- What are vulnerabilities in the system?
  - Default Configuration is a weak point and
  - Mean time between the failure and redundant failures.
    - Like the system going down once, every week, then every month. It’s a redundant failure.
- Ways
  - Number of bugs (quantitative)
    - What type of bugs (Qualitative)
  - Software security
    - Product Surface such as vulnerabilities with the connections such as network connections, users with weak passwords and bad awareness, and so on.
      - What does number of interfaces mean (Product Surface)?
        - Anything THAT deals with the system, amongst them is GI
          - Increased interfaces would affect the security
          - Anything increasing will affect the security.
    - Number of accounts with weak accounts is quantitative.
    - Qualitative measures are the security policies, how good the measurement.

        - **Dangerous instructions Coding and implementation for the software has caused an SSS attack**

- **Important Concepts**
    - **Product surface (GI interface and number of interfaces)**
        - **Each interface represents a potential entry point that could be exploited.**
    - **Dangerous instructions refer to coding practices or software behaviors that could potentially be exploited**
        - **The software could be flooded because the code that was written could potentially increase the ability to exploit the system**
        - **Deployment is an important concept to ensure security**
        - **SQL injection attack occurs when you process before checking and validating any data that is entered**
            - **Such as user registering and their data being removed**
        - **Employing outdated functions that can easily be exploited affects security level**
        - **Insecure libraries and APIs affects security level**
        - **Ignoring error handling messages can lead to program states exploited by attackers affects security level**

  - Privilege escalation attack, which aim to get unauthorized higher-level of privilege.
- What causes a user to ignore error handling that could potentially cause attacks?
  - User awareness

- Standard
  - ISO 27002
    - Security policy
    - Organization of information Security
    - Asset management
    - Human resources security
      - Training awareness for the employees and what level should each employee have.
    - Physical and environmental security
    - Communication and operation
      - Integrity check

- Risk Analysis
  - Divided into two: qualitative and quantitative
    - Risk = Assets X Threats X Vulnerabilities
      - Assets will definitely affect the threats
        - The bigger the company (the more clients they have), the greater the risk
        - Data such as customer information, bank ids, etc. are all assets
          - All of these values are for the process of measuring and calculation of the probability of threat.
      - Threats: the potential attack that could be done on the assets
      - Vulnerabilities: weak points

- Assets
    - Hardware, software, data and information, reputation, and money+ customer + competition
- Vulnerabilities
    - One of the vulnerabilities in software is the Access point because you could compromise it by configuring it and attack it to intercept network traffic, launch man ITMA, or infect devices with malware.
    - Accounts with privileges where the password hasn’t been changed
    - Programs with unnecessary privileges
        - Giving users authorization to stuff that isn’t needed for them
    - Weak
        - Not upgrading the users role when necessary
    - Weak firewall configurations
        - If the firewall isn’t efficient at filtering, it could make connections with malicious intents or let in a lot of unauthorized traffic into the user’s device
        - You need to look at security to ensure that the firewall isn’t outdated and could still filter properly.
    - How much is critical
    - Scanners or risk analysis tool
- Threats
    - Purpose is to exploit the vulnerabilities to damage the assets
- Attack tree
    - Guess password
        - Manually: looking at your birthdate, your dogs, marriage date, etc.
        - Automatically: looking at the common passwords that people in general would use.

    - Some companies will ask users to insert a certain number of digits for their password where the password will have for each digit from 0 to 9 for numbers and 0 to 26, which will mean the possibility of guessing your password right would be from 6^{36}
    - There are online and offline systems
        - Online system is difficult in the sense that you have to flood it and send multiple requests to potentially hack and attack it
        - Offline system is much easier since the device is in front of you and it's easy to hack into it

- **Risk and Risk mitigation**
    - **Risk quantitative**
        - **Value of assets**
            - **Example: the Code 200k dollar, data 300k dollar, and so on.**
        - **Critically of vulnerability**
            - **how weak this vulnerability is sensitive and critical, such as the data**
                - **It wouldn't necessary be bad if the system went down for a bit, but it's a problem if the client's information or information about the company was revealed**
                - **Data breach 30% critical as a vulnerability**
                - **DOS attack 45% critical as a vulnerability**

        - **Likelihood of threat**
            - **What's the possibility of the weak point being exploited and attacked**
        - **Example:**
            - **The data breach is 300k of the entire assets value 650k so how critical it is, is 40%**

            - **Risk, the value of lost in assets-> 300k x 0.4 x 0.2 = 24000$**
    - **Countermeasures**
        - **Risk analysis depends on the time to deal with the risk**
            - **Baseline protection approach**
        - **Risk analysis could be a measurement**

Authentication

- To confirm that the user is in fact the user (Samantha Van is in fact Samantha Van)
    - One to one
    - We can confirm using email or password.
    - The actions being committed by the user should be registered, so that the user
    - How can the user get into the system?
        - IAAA (I triple A), identification and then authentication, authorization, accountability.
        - What's the difference between identification and authentication?
            - Identification is the act of identifying a particular user (establish the identity), often through a username. Authentication is the proof of the user's identity (verifying the claimed identity), which is the commonly managed by entering a password.
                - Email is the identity and the password with the email is authentication.
                - Relationship of identification
                    - One identification and you can enter many systems, applications, and websites.
                - Relationship with identification and authentication
                    - One identification with one password
- Identifier and Identification
    - The identifier is useless without the identification
- Authentication
    - Mechanism used to verify the identity of users so they could correctly access the system network or resource.
    - Prevents unauthorized access to the system

    - **Authentication is the first line of defense and security for the system**
- **Authentication: Parties Involved**
    - **There are 3 parties**
        - **The user: is the individual who wants to access the system**
        - **The verifier: the system, service, or entity that is responsible for verifying and confirming the user's identify**
        - **The attacker: an unauthorized individual or entity that uses fake information or stolen information to access the system, service, or resource with malicious intent.**
    - **Authentication: 3 Authentication Factors**
        - **Know: something only you would know and remember such as your password, pass phrases, pass**
            - **What do we mean by password management?**
                - **Where do I want to store the password and how do I want it to be stored (strong password and making sure other sites**
            - **What does apple password manager or google password manager?**
                - **It saves the passwords for the different websites that the user**
                - **If you want to store your password, then your specific account would control and store your password**
                - **The account would control by warning you that your passwords from one site is the same as the other site.**
                - **Tracking and evaluation are how strong it is and if it's a good password, and that there are no similarities between this**

password and another password from a different browser.

- This improves security.

- How do passwords get stored?
    - Hashing: in one way so that the password becomes cypher text but the cypher text is not decrypted.
- How would the password manager know similarities between two passwords?
    - The password manager adds a key that is random but unique. The unique and random number is saved and hashed alongside the password. So, the password and unique key/ID is appended and then hashed and then stored. The manager would then be able to compare the new password with the hashed passwords.
- When signing up, you answer a few questions like your favorite teacher’s name or your dog’s name
- Advantages
    - Cheap: it needs a low-cost technology and doesn’t require any advanced or high-tech tools
    - Easy to implement: it’s easy to connect the API with any application or website
    - Portable
    - Widely Available
- Disadvantages
    - Snigging attacks
    - Easy to guess, share
    - Cost of handling forgotten passwords
    - Hard to remember
    - Dependent on the user

- Have: something you hold and it must be physical like tokens (contact or contactless) or cards
    - Example: A card reader that opens the main door to a building, for all the residents in a building so only the residents can access the building.
    - Advantages
        - Hard to abuse, easy to use: it doesn’t require much training to use it and doesn’t easily break or get destroyed.
        - Fastest and quickest way to verify a user
    - Disadvantages
        - Costs a lot because there’s a card reader and the card. The card reader is an expensive tech device.
        - Can easily be lost or stolen
        - It’s difficult to replace
    - The have authentication is usually used with password or pin code.
- Are: something related to the user specifically such as their behavior or physiological (a person’s physical features)
    - Behavioral is dynamic because users tend to change
        - Signature
    - Physiological is static because users tend to have the same features
        - Fingerprint
        - Biometric
            - IDF soldiers would usually use the face ID biometric on Palestinian citizens to confirm their identity.
        - Retina
        - Iris

- **Why is Iris the strongest kind of is: authentication?**
  - **Because there is are certain and specific measurements done to confirm its uniqueness.**
- **Face**
- **DNA**

- **Behavioral**
  - **Voice**
    - **Change of a person’s voice over time**
  - **Signature**
  - **Key**
  - **Gait as Biometric Authentication**
    - **All people could be identified via their walking**
      - **Whether the person limps or not, how their back moves as they walk, how the one leg looks to the other leg, etc.**

- **Advantages**
  - **Easy to use**
  - **Portable**
- **Disadvantages**
  - **Expensive**
  - **Replay attacks**
    - **The cyber-attack where the attacker intercepts or compromises the data (previously recorded) by snipping or retransmitting it.**
    - **Privacy issues**

- **Violated privacy such as the heart rate, retina, and other biometric**
  - **Sometimes you need to interact with the finger print, or show your face towards the face identifier, however after corona they realized how unhygienic it was, so they stopped it.**
- **Authentication: other factors**
  - **Somewhere you are**
    - **Finding user’s location from GPS satellite**
  - **Something you think**
- **Multi Factor Authentication**
  - **One authentication is not necessary enough; therefore, we use multiple authentications to confirm security. MFA can improve security by:**
    - **Reduce risk of unauthorized access which stops the attacker or unauthorized user from accessing the system**
    - **Mitigation of credential theft**
    - **Enhanced security against automated attack**
    - **Increased authentication**
- **Biometric Technologies are automated methods**
  - **You’ll use the physiological or behavior characteristics just to confirm if the person I’m interacting with is in fact a human being.**
- **How can we distinguish between living capture**
  - **Facial expression recognition**
    - **facial features moving and signs of life in their features**
  - **Eye movement**

- Everyone’s eye twitches, which could be a way to identify if the user is human and whether they are living
- Response to actions
  - The systems will provide challenge response mechanisms to the user in a way to figure out if they’re human.
    - Like how the mouse moves to the button to verify. The mouse would move at random if the user was human, rather than a straight line.
- Multi-model biometric
  - This is the best biometric technology
  - Example:
    - I want to enter my email and the email informs me to authenticate myself from the other device I logged into.
    - To log into your phone, you need your password or face (or finger print), the more biometric technologies, the more secure it is.

- Positive/Negative
  - Positive:
    - preventing multiple users from having the same identity
      - Many to one
    - tries to find a positive match between an actual user’s login information and their registration information
  - Negative:
    - preventing one user from using multiple different identities
      - One to many
    - Tries to detect attempts of malicious intent such as attack the system or impersonating as another user

- **Positive Recognition**
    - **Uniqueness of Biometric traits**
        - **Knowing that the biometric traits are unique and using that to create technology to identity users**
    - **Enrollment process**
        - **When a user registers, their biometric features are captured (such as face id or fingerprint) and is then secured and stored for that specific user.**
    - **Matching process:**
        - **The user's stored data would make a positive match with the data that the user inputted when logging in (returning back to the system). This positive recognition is considered accurate and precise.**
- **Negative Recognition**
    - **Prevent a single user from using a different identity, or stealing someone else's identity.**
    - **Identity Verification**
        - **Ensuring that the user's biometric features do not match any prohibited or unauthorized identities in the database,**
            - **Negative recognition in identity verification aims to catch people trying to fake their identity or used multiple ones.**

- **One to many is negative recognition**
    - **Single user has access to different systems and has stolen identity or faked his identity to get into unauthorized individuals**
- **Many to one is positive recognition**
    - **Many users interact with the same system.**

- **Scenarios**
    - **Enrollment**

- A university wouldn't enable you to enter the university unless you had some form of identity. Such as a student ID with your face on it, to confirm you are a student.

- Access control
  - Employees have a facial recognition or finger print as proof they're employees
- Authentication Attempt
  - Authorized employees
    - The system matches the employee's face with the employee's face that is stored on the database (for the facial recognition).
  - Positive recognition
  - Unauthorized individual
    - When the malicious intent user tries to gain access by using a mask or photo with an employee's face
  - Negative recognition
  - No match detected

- Behavioral does change overtime
- Physiological does not change
  - Anatomy
    - Captures the body (example: ear) as a picture.
  - Measurements
    - Measures the body's pivot points (ex: ear).
    - It's possible to see two people who look the same, however it's difficult for them to have the same measurements based on their pivot points (such as a

face’s nose measurements, eyebrows, eyes, jawline and so on).

- **Thermograms of each person is different (their body heat looks different on each person)**

- **What is Distance based authentication?**
  - **I can identity a user from a distance**
    - **There’s no need for a user to get close to a device (which is now considered unhygienic since covid).**
  - **Capturing the biometric features from a distance.**
    - **Capturing their face which would be physiological**
    - **Capturing their walk which would be behavioral.**

- **Odor being used to identity a person**
  - **Each human being has their own odor which could be used to identify them**
  - **The problems with it are the sensors being expensive and not as mainstream, and identifying a person via odor contains a lot of errors.**
- **Retinal Scan**
  - **The retinal scan is capable of identifying even twins apart from each other.**
  - **It’s not user friendly because a user must get close to the device and its annoying and uncomfortable**
    - **Didn’t we say it’s either be secure or be comfortable? So, for the retinal scan, its secure but the problem is that its uncomfortable.**

- **Characteristics**
  - **Universality**
    - **Is this biometric as general and common?**
    - **FER (the percentage of the failure to enroll)**

    - Failure to Enroll Rate
    - Example:
      - When 5 out of 100 fail to enroll, then it would be considered a number of those who failed to sign in.
      - When user signs up with a password and username and the system does not enable them to sign up.
  - The enrollment process should be easy to use for users but capable of capturing the correct information.
  - FER = (number of failed enrollments / total number of enrollments attempts) x 100%
    - Failure enrollment rate is related with enrolling the user into the system.
  - Everyone can sign in and enroll onto this system. HOWEVER, the sign ins should be logical and correct.
  - Universality: The number of users that are capable of enrolling into the system with the correct information.
- FER: Commons factors that lead to a higher FER?
  - Biometric quality: the individual characteristics cannot properly be identified either due to the environment around the machine identifying them or the users have a physical problem that doesn't identify them
  - Sensor quality: biometric sensors used for capturing a user can impact the enrollment process
  - User experience: the enrollment process should be user friendly.
    - My system should not have any bugs in the sense that it can identify anyone from any race, gender, face, etc.

- **Distinctiveness**
    - **The system should know that this data is related to the actual person.**
    - **Ensuring there is no collision between the users' data**
        - **Example: Hind data belongs to Hind**
    - **When the data doesn't match to the correct person its called FMR (False Match Rate)**
        - **Example: if Ahmad were to log in and he ends up logging into Yazan's account, then that's FMR.**
        - **If a user stays away from the system too long, then there could be a potential FMR.**
            - **Example: if Mohammad travelled for 2 years and came back, he could have different biometric features.**
    - **What is the replay attack?**
        - **Network attack where an attacker captures a valid network transmission and then retransmits it later**
        - **Example: Watching the traffic and waiting for Yazan to log into his account, in which the hacker will take his data and log into Yazan's account.**
    - **Can there be a false rejection rate (FRR)?**
        - **Yes.**
    - **FAR (False acceptance rate)**
        - **A user could not login and they are an actual legitimate user.**

  - **Permanence**
    - **False Non-Match Rate (FNMR)**
      - **The data didn't match correctly**
        - **Example: You're a legitimate user, the user says you're not a legitimate user. This is because the system was not able to properly match the data.**

FMR/ FAR: malicious user enters the system and gets accepted
FNMR/FRR: the user is a legitimate user and gets rejected.

  - **FER is more on the problem with the human's biometric features who is trying to enter the system.**
    - **FER is statistical.**

  - **FCR is more on the problem with the device or the environment.**
    - **FCR is biometrical.**

- **FRR being high means that the system is sensitive**
- **FAR being high means that the system is not sensitive**
  - **FRR and FAR are inverse relationships.**

What is more dangerous, FMR or FNMR?

FMR, because it usually tends to come from malicious intent since the malicious user could then gain privileges and authorization levels through passive and active attacks.

- Collectability
    - Biometric property should be easy to collect and capture such as scanners cameras and sensors
    - Can the data be collected? Is the process of collecting data easy and has the ability to be collected? Can the process of capturing be measured? The data should be able to be quantified.
- Performance
    - The system should have a good speed and accuracy. The accuracy should be able to match the data with the user properly and correctly.
    - The system should have a balance that is accurate, speed, and friendly
    - FCR (Failure to capture rate): the system can't even capture the user at all.
    - FNMR (Failure non match rate): the system can't even register a legitimate user into the system
        - FER: The user cannot even be enrolled onto the system at all. During sign up
            - Ex: Input password and it does not let you in
        - FCR: the system cannot verify them and cannot capture the user's biometric features
            - Ex: Face ID does not work

- Acceptability
    - User experience: The user is the core of the system. Is the biometric system easy? User-friendly?
    - Privacy and security: Is the system trusted and secure?
        - How can I confirm I got a good security?

        - When I get a low FMR, FRR, FCR, FER.
      - Encrypted data
      - Biometric data is securely stored
    - Accuracy and reliability
      - FAR and FRR are low
    - Transparency and Control
      - is the data’s reason for being collected stored and used clear to the users?
      - Users should be aware where their data is stored, collected, and used.

  - Circumvention
    - Refers to overcoming attempts made to deceive the biometric system to gain authorized access
    - Purpose is to try and secure the system to ensure it can deal with
    - Why is the Circumvention related to the FMR?
      - The FMR value would measure the system’s circumvention.
      - Low FMR, High Circumvention
      - High FMR, Low Circumvention
- Applications
  - Overt vs. Convert
    - Overt: The awareness of the user and knows that the biometric features are being measured
      - Example: when the user knows to use their face for face id, fingerprint for fingerprint id, etc.
    - Convert: the user is not aware and the process of the biometric features are being measured without his knowledge.
      - Example: distance factor authentication that captures a user’s biometric features

- **Habituated vs. non-Habituated**
  - **Habituated: the system is used daily**
    - **The system's Accuracy should be high, Complexity should be low, and it should be user-friendly by being easy to use and fast.**
  - **Non-habituated: the system is not used daily**

- **Attended vs. Unattended**
  - **Attended**
    - **The system is being continuously watched alongside the user who uses it**
  - **Non-attended**
    - **The system is not observed**

- **Standard vs. Non-standard**
  - **Standard in a static environment using known biometric authentication systems.**
    - **Finding solutions for stable environments to ensure Low FMR, robust, and stable**
  - **Non-standard in a dynamic environment**
    - **Finding solutions for the environments that have changes like noises, faces, environments.**

- **Public vs. Private**
  - **Public**
    - **Anybody uses the system**
  - **Private**
    - **Specific system for a private organization and their employees**

- **Open vs. Closed**
    - **Open**
        - **Able to interact with other systems in order to share information**
        - **Example: twitter being used on google, shopping on a website that is on google.**
        - **Advantages**
            - **Those outside the organization can access the system (Example: Customer)**
            - **The organization can make use of other services**
                - **Like twitter using google or amazon using apple pay and other SDKs and APIs.**
                -
            - **Less time crafting from scratch, so saves time and cost.**
    - **Closed**
        - **Its locally and could only be worked on within the system**
        - **Keep all information contained and do not communicate with other systems**
        - **One to one.**
        - **Advantages**
            - **Hackers can’t access the system from the outside**
            - **Organization has full control**

    - **What is third-party involvement?**
        - **I’m forced to send the data that I collected to a third party for the sake of verification**

- **Biometrical Systems**
    - **Enrollment**
        - **The user will first enroll into the system, which is an extremely important part**
        - **User interface**
            - **What’s the quality checker?**
                - **Confirms if the data that is being captured is correct and accurate and can be dependent on in the future. Quality checker is not necessary during verification. However, it is necessary during enrollment and sign up to confirm that the user’s template during sign up and log in have a close distance metric.**
        - **Data acquisition**
            - **The user inputs data**
        - **Feature Extraction**
            - **The system takes the user’s feature (like a fingerprint)**
        - **Mathematical Transformation**
            -
        - **Template Construction**
            - **The user’s profile/template is built**
        - **Store templet in the database**
            - **The user’s template is stored in the database**
    - **Verification**
        - **User interface**
        - **The user should enter the data for him specifically**
        - **Taking the data (like a fingerprint) from the user**
    - **Mathematical Transformation**
    - **Template Construction**

- There are now two templates for the user (template of user login and templet for the user's sign in)
- Distance measure is where there will be a matching between the user's information that they logged in and what they signed up
    - The distance measure is the measure of how close the two temples will match each other
    - The distance between the two templates could be close, but the digest does not have to be close.

What is hashing most used for?
Signature. Generates a digest which is dependent on the content of the file. The asymmetric function is considered a signature.

What is a Dictionary attack?

There's a list of all the common passwords. Rather than trying a billion passwords, hackers will try the list of common passwords on the system until they can enter the system.

- **Digest has made it difficult on even dictionary attacks.**

What is a rainbow table attack?

Rainbow table is a set of hash values used to crack password databases that have their information not stored as plaintext.

Algorithms/Problem/Effect	What are they?
Blowfish Algorithm	a symmetric key block cipher, where it scrambles data and can only unscramble data using a special key.
Salting Algorithm	An algorithm where random strings of characters are added to the user's password, then scrambled using a hashing algorithm and stored.

	Ex: “secret” being the random string of characters (Salt) and “hind110” being the password. Salting algorithm would be combining them like “secrethind110” and scrambling them like “sehi1n1d0ret”
Birthday Problem	The problem states how in a room of 23 people, there are at least 2 people with the same birthday.
Heuristic Algorithm	A problem-solving algorithm that uses methods to find solutions quickly. It's important in computer security because it provides an immediate solution to a threat detection.
Avalanche Effect (in hashing)	An effect where even the smallest changes in something would make a big difference. Ex: If I have a message, place it into a hash function (to scramble), it would provide me with a hash code. Then, if I go on to change even the slightest thing in the message, place it into the hash function, it will give a completely different hash code than the previous hash code.
Dictionary attack (Passwords Attack)	manually hashing each password

rainbow table attack (Passwords Attack)	**There is a Hashing that's known as resource consumption because it uses a lot of time.**
DevSecOps attack	**Targets the integration of security in the software development lifecycle, which exploits vulnerabilities within the system.**
Ping-update attack	**A type of cyber-attack where an attacker exploits the behavior of ping (ICMP Echo Request) messages to disrupt or degrade the performance of a target system or network** **Ex: Spoofing**
Zero-day attacks	**new attacks where there's no signature or vulnerabilities in the blacklist or whitelist**

Equal Error Rate (EER)

- **EER is where FMR and FNMR are equal**

FMR/ FAR: Allowing the user into the system because the system assumed the user was a legitimate user

Distance Metrics -1

- **Threshold is the cut point.**
  - **The threshold determines if the FMR and FMNR are high or low**
- **What do we want to measure the distance of?**

    - The user's template of sign up and the user's template of log in.
- The best way to measure the distance is between the inter person and intra person
    - Inter person distance must be large
        - The distance between two people
    - Intra person distance must be small
        - The distance between yourself
        - The template of the user who signed up on month 4 should have a close distance to the same user logging in again on month 6.
- If the inter person has a small distance and intra person has a large distance, would the FMR high and FNMR is low?
    - Yes, because the distance between two people should be large so the FMR would be low.
    - The distance between a user and themselves should be small, therefore the intra person should have a small distance. Since the intra person has a large distance, then it would cause a high FNMR.

- The distance must be less than the threshold for the user to be accepted into the system.
    - The distance should also be zero or close to zero for intra person.
- If the distance is more than the threshold, then the system would reject them from the system.
- Threshold is the point or value that determines whether a user is rejected or accepted.

FMR and FNMR Roles

- **FMR is the measure of malicious users over the total number of malicious user's trials that have been accepted**
- **FNMR is the measure of genuine users who have been rejected over the total amount of genuine users**

Passwords

Password: Kinds of Passwords

Password is the first line of defense that protects a user from being hacked.

- **Password**
  - **A string of characters that could be letters, digits, or/and special characters.**
- **Pin-code**
  - **A string of numbers usually used on the ATM machine or mobile phone**
- **Pass Phrase**
  - **Sentence such as "what was your first dog's name" to try and verify the user.**
- **Associative and Cognitive Passwords**
- **Pass face, pass image**

Password: Password Space – S

PWD Space= content ^ No digits

_ _ _ _ || 4 digits contains just binary numbers {0, 1}

From 0000 ⟶ 1111

If there was a brute force attack, the hacker would be able to figure the password out because it's obvious that its binary numbers from 0 until 16.

Password Space: 2*2*2*2 = 16 = 2^4

The space is the number of tries or iterations to get the correct password in the worst-case scenarios.

Examples:

Question 1:

_ _ _ _ _ || 5 digits contains just binary numbers {0, 1}

From 00000 ⟶ 11111
Password Space: 2*2*2*2*2 = 32 = 2^5

Question 2:

_ _ _ _ _ _ || 6 digits contains just decimal numbers

From 0…9 0…9 0…9 0…9 0…9 0…9
Password Space: 1000000 = 10^6

Greater PWD Space, means a greater security.

Question 3:
_ _ _ _ || 4 digits contains just decimal numbers

From 0…9 0…9 0…9 0…9
Password Space: 10000 = 10^4

Question 4:
Password numbers, letters
Numbers = 10
Letters = 26

Space at each digit = 10+26 = 36
Password 6 digits ⟶ Password Space = 36^6

The password space is affected by the digits and the content of the password.

Question 5:

Password numbers, letters (upper case and lower case)
Numbers = 10
Letters = 26

Space at each digit = 10+26+26= 62
Password 6 digits ⟶ Password Space = 62^6

Question 6:

Password numbers, letters (upper case and lower case), and symbols
Numbers = 10
Letters = 26
Symbols: 32

Space at each digit = 10+26+26+32= 94
Password 6 digits ⟶ Password Space = 94^6

Password: The Art of Counting

- **What's the possibility that a single dice (with 6 faces) will fall on 4?**
  - **1/6**
  - **The total (1/Pi) = 1/ (1/6+1/6+1/6+1/6+1/6+1/6)= 6/6 = 1**

- **What's the possibility that two dices (with 6 faces each) will fall on {4, 1}?**
    - **1/36**
    - **The total (1/Pi) = 1/ (1/36+1/36+1/36…+1/36)= 36/36= 1**

Password: Combinatorics -1

- **No restrictions: references how the user can input any numbers, letters, symbols, etc.**
    - **If the password only allows numbers, or only allows letters, or only allows numbers, upper-case letters, symbols then that's a restriction**

- **High Restriction:**
    - **If the user cannot input a redundancy like "MMMMM", which is good because it increases the security since it becomes more difficult to guess.**
    - **Randomness increase, stronger password.**

Password: Combinatorics -2

- **R1 (Restriction 1) ⟶ At least one number (Uppercase + Lowercase + Special) = 26+26+32 = 84**
- **Space = All – Wrong**
    - **Wrong = All – right = $94^6 - 10^6 = 84^6$**
    - **Space = $94^6 - 84^6$**

- **R1 (Restriction 1) ⟶ At least one upper case letter**
- **Space = All – Wrong**
    - **Wrong = All – right = $94^6 - 26^6 = 68^6$**
    - **Space = $94^6 - 68^6$**
- **R1 (Restriction 1) ⟶ Password must contain 6 different characters (94)**
  _ _ _ _ _ _ || Mohamd
- **Space = 94 + 93 + 92 + 91 + 90 + 89 = 549**

Password: Combinatorics – 4

- **R1 (Restriction 1) ⟶ At least one upper case and one lower case (94)**
- **All = WrongOne – WrongTwo + WrongBoth = $94^6 - 68^6 - 68^6 + 42^6$**

Greater restriction causes greater Randomness and variance

Password: Combinatorics – 5

- **R1 (Restriction 1) ⟶ Exactly one number, 6 digits.**
- **Space = $84^5 * (10 * 6)$**
  - **Why 10*6? Because we are only allowed to put in one slot, and there are 6 slots.**
  - **Why 84? Because we stated exactly one number so we removed 0…9 on one slot.**
  - **Why multiply 84^5 and $(10 * 6)$? The same way we would usually multiply the slots together.**

Password: Combinatorics – 6

- **R1 (Restriction 1) ⟶ Exactly one number and one upper case**
  - **Space = $58^4 * (10 * 6) * (26 * 5)$**

Password: Combinatorics – 7 and 8

Combination Formula:

$$\frac{n!}{m! * (n-m)!}$$

- **R1 (Restriction 1) ⟶ Exactly 2 Numbers**
  - **$\frac{n!}{m!*(n-m)!} = \frac{6!}{2!*(6-2)!} = \frac{6*5*4!}{2!*4!} = \frac{6*5}{2} = 15$**
  - **Space = $15*10^2 * 84^5$**
    - **The reason, we didn't do $84^5 * (10 * 6) * (10* 5)$ is because $(6*5) * 10^2$ would give redundancy like (1, 1), (2, 1). To remove redundancy, we removed the 15 redundant numbers. Now the numbers are (1, 1), (2, 2), and so on. 15 or 30 q the slots where we put the numbers.**
- **R1 (Restriction 1) ⟶ Exactly one number, two upper case. 5 digits.**
  - **$\frac{5*4}{2} * 26^2 = 10 * 26^2$**

Password: Probabilities

- **What is the probability that a random password of 6 characters has no number in it?**
  - **Space = $\frac{84^6}{94^6}$**
- **What is the probability that a random password of 6 characters has no upper case in it?**
-

Password: Statistics – Introduction

- **X ⟶ 1, 2, 3, 4, 5**
  - **Mean = 1 + 2+ 3+ 4+ 5/ (5) = 3**
  - **The variance is low**
- **Y ⟶ 72, 6, 3**
  - **Mean = 72 + 6 + 3 / (3) = 27**
  - **The 27 does not represent the Y values**
  - **The variance is high**

Variance is the measure of how far the average is from the data sample

To test whether the password is strong or not, use the variance to test it.

Password: Statistics – Covariance (What is Covariance?)

- **0 Correlation: there is no relation, there is no covariance**
- **Positive covariance: direct relationship both increase or decrease**
- **Negative covariance: inverse relationship one decrease one increase**
- **Correlation is from -1 to 1, and covariance is from infinite to infinite.**

Entropy

- **Entropy is the measure of how much randomness we have in the password.**
- **Increase of entropy will increase the strength of the password.**

Password: Good Properties

- **Hard to guess:**
  - **Ex: it doesn't matter what a person knows about the user, whether it's his birthday, favorite food, etc., if the password is hard to guess, the person wouldn't be able to guess the user's favorite password.**

- Easy to remember
  - in order not to consistently reset your password, you must ensure its easy to remember

- Private
  - don't give your password to anyone, not friends nor family.

- Secret
  - only the owner should have access to the password

Network Security

- Computer security is branched out into computer networks and so on.
  - This is also related to how computer networks and cybersecurity are closely related and dependent on each other
- How is Blockchain encrypted?
  - How is the data between the blockchains

Terminology and Classical Cryptology

- What is cryptology?
  - Main purpose: to hide information
  - Cryptography (encryption): Change plain text to ciphertext to make the text/message secure.
  - Cryptanalysis: trying to break the ciphertext
- Terminology -2

-
    - The key used in the encryption process was able to get the ciphertext, and that same key was used in the decryption to change from ciphertext to plain text
- The process of encryption and decryption
    - Encryption process
        - Ek(Plaintext) = CipherText ⟶ C
            - Encrypting the plain text using the key will get ciphertext
    - Decryption process
        - Dk(CipherText) = PlainText ⟶ P
            - decrypting the ciphertext using the key will get plain text.
    - The key must be a secret

- The core part in encryption is the key

- Ciphertext-only attack/ Frequency-based attack:
    - Attacker has a dictionary or dataset in order to continuously try and find the plain text
    - Example:
        - Substitution ⟶ Plaintext: Mohammad ⟶Ciphertext: Adallah
            - Changing the plaintext via shifting
            - Caesar Cipher shifts number of bits
                - Mohammad⟶ 3bits ⟶ Ciphertext(PRK) (from mohammad using the alphabet)
                - ABCDEFGHIJKLMNOPQRSTUVWXYZ
        - Permutation ⟶ Plaintext: Mohammad ⟶Ciphertext: hamamed
            - Shuffling the word mohammad

    - Why did we put 26 for (mod 26)?

        - For example, if we took X, then it would be 24+ 3, but that would be 27. To stay in the table, we do mod 26. Therefore, we would end up making a circular table.

- Known-plaintext Attack
- Chosen-plaintext
    - Chooses letters and tries to get the plaintext from the cipher
        - Example: AAA -> PPP, would give the attacker a better chance of figuring out the hacker
- Adaptive Chosen-Plaintext Attack

Transposition Cipher - 1

P -> Message from Mary Stuart kill the Queen
Key -> 491753286

1	2	3	4	5	6	7	8	9
M	e	s	s	a	g	e	f	r
o	m	M	a	r	y	S	t	u
a	r	t	k	i	l	l	t	h
e	Q	u	e	e	n	X	Y	Z

Key	4	9	1	7	5	3	2	8	6
C	sake	ruhz	Moae	esLx	arie	smtu	emrQ	ftty	qyLN

You can make Factorial of (9) of cipher texts with a key from 123456789.

Modern Ciphers

Perfect Secrecy

Claude Shannon stated to reach perfect secrecy is to use one time padding: is to work using stream cipher that is working with bit-by-bit encryption. Each bit or character should not be repeated and be different, where every bit or character

- In other words, Shannon thought of two concepts:
  - Diffusion
    - Achieved through different sub rounds in which permutation operations are used (such as P10, P8, and P4)
    - diffusion is where the ciphertext and plaintext should not be one to one.
  - Confusion
    - Achieved in block cipher through the generation of sub keys, in which substitution operations are applied. (S-boxes)

- The plaintext being changed should affect the cipher text by a lot.
  Example: block cipher

- The difference between block cipher and stream cipher
  - One bit in plaintext will cause a difference in cipher text.
    - Stream cipher will take MBC and if only M is changed then everything else is encrypted the same.
      - Ex: MBC is ERA, altering M results in ABC which will be FRA
    - Block cipher will alter the entire cipher text
      - Ex: MBC is ERA, altering M results in ABC which will be QWP

- **Any change in block cipher is going to change all the cipher text.**
- **Any changes in stream cipher will only change the bit changed for the cipher text.**
    - **Stream cipher uses more keys than block cipher**

Problem with the stream cipher is that it requires many keys. Why does it require many keys, and why is it a problem?

- **24 different encryptions. The key needs management, meaning that many keys will be difficult to manage. Store, manage, and use the key. Increase of keys will cause an increase in traffic.**

What do we do with a symmetric algorithm's key when we want to give it to another person to ensure security?

- **Distribute the key via the 20 packages, others use steganography, others use tunnel/socket**
- **Others used key exchange algorithms. They were able to create a shared key between a sender and receiver, where only the sender and receiver can access this key.**
    - **AES is the most powerful symmetric where the keys were much longer such as 128 lengths of key, 256, 224, 512 are all lengths of keys that caused AES to be as powerful as it is.**

- **Problem with an asymmetric encryption or public key encryption is that it has overhead. Now, there's no need to make an encryption key.**

- **What's the principle for achieving the goals for symmetric?**

    - **The sender and receiver have a shared key where only they can modify the data, therefore meaning it has integrity.**

When we used public key for encryption and private key for decryption, what security services we used?

- **Confidentiality. because when we encrypted, only the person whose file was modified and encrypted was able to look at the information of the file.**
- **To accomplish integrity, the file was encrypted via the private key and the file was then decrypted using the public key.**
    - **Data integrity: the security increased**

Feistel Cipher EXAMPLE

Encryption

Given

Plain Text: HI

K1: 11101010

K2: 10001001

Step 1:

A	B	C	D	E	F	G	H	I
65	66	67	68	69	70	71	72	73

L0 = H = 72 ⟶ 01001000
R0 = I = 73 ⟶ 01001001

L1 = R0 = 01001001
R1 = L0 XOR (R0 OR K1)

R0 OR K1

R0	0	1	0	0	1	0	0	1
K1	1	1	1	0	1	0	1	0

OR	**1**	**1**	**1**	**0**	**1**	**0**	**1**	**1**

R1 = L0 XOR 11001001

L0	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**0**
OR	**1**	**1**	**1**	**0**	**1**	**0**	**1**	**1**
R1	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**1**

Step 2:
L2 = R1 = 10100011
R2 = L1 XOR (R1 OR K2)

R1 OR K2

R1	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**1**
K2	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**
OR	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**1**

R2 = L1 XOR 10101011

01001001

L1	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**1**
OR	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**1**
R2	**1**	**1**	**1**	**0**	**0**	**0**	**1**	**0**

R2 = 11100010, L2 = 10100011

Cipher text: R2 L2
Cipher text: 11100010 10100011

Decryption

Given

Cipher text: 11100010 10100011

K1: 11101010

K2: 10001001

Step 1

L0 = 11100010

R0 = 10100011

L1 = R0 = 10100011

R1 = L0 XOR (R0 OR K2)

R0	1	0	1	0	0	0	1	1
K2	1	0	0	0	1	0	0	1
OR	1	0	1	0	1	0	1	1

R1 = L0 XOR 10101011

L0	1	1	1	0	0	0	1	0
OR	1	0	1	0	1	0	1	1
XOR	0	1	0	0	1	0	0	1

R1 = 01001001

Step 2:

L2 = R1 = 01001001

R2 = L1 XOR (R1 OR K1)

R1	0	1	0	0	1	0	0	1
K1	1	1	1	0	1	0	1	0
OR	1	1	1	0	1	0	1	1

R2 = L1 XOR 11101011

L1	1	0	1	0	0	0	1	1
OR	1	1	1	0	1	0	1	1
XOR	0	1	0	0	1	0	0	0

R2 = 01001000,   L2=01001001

Plaintext = 01001000 01001001

= 72 73

= HI

Key generation: P10 rearranges the content, like if you have 10 bits then it takes the 10 bits and outputs 10 shuffled bits in 5 and 5.

SDES	DES
8 bit	64 bits
2 rounds	rounds -> 16R

- **SDES is the simplified version of DES, where SDES has more rounds**

Simple DES Example

Given

Key = 1100011110

Plaintext = 00101000

P10									
3	5	2	7	4	10	1	9	8	6
1	2	3	4	5	6	7	8	9	10

P8							
6	3	7	4	8	5	10	9
1	2	3	4	5	6	7	8

P4			
2	4	3	1
1	2	3	4

Expansion Operation EP							
4	1	2	3	2	3	4	1
1	2	3	4	5	6	7	8

IP							
2	6	3	1	4	8	5	7
1	2	3	4	5	6	7	8

S0	0	1	2	3	
	1	0	3	2	0
	3	2	1	0	1
	0	2	1	3	2
	3	1	3	2	3

S1	0	1	2	3	
	0	1	2	3	0
	2	0	1	3	1
	3	0	1	0	2
	2	1	0	3	3

Step 1: Key Generation

Key	1	1	0	0	0	1	1	1	1	0
Numbering	1	2	3	4	5	6	7	8	9	10
P10	3	5	2	7	4	10	1	9	8	6
P10(Key)	0	0	1	1	0	0	1	1	1	1

P10(Key) = 0011001111

P10(Key)	0	0	1	1	0		0	1	1	1	1

Shift Left Once for Each Five bits

P10(Key)	0	1	1	0	0		1	1	1	1	0

becomes
LS-1(Key) = 01100 11110

Key	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**1**	**1**	**0**
Numbering	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
P8	**6**	**3**	**7**	**4**	**8**	**5**	**10**	**9**		
P8(Key)	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**1**		

P8(Key) = 11101001
K1=11101001

LS-1(Key) = 01100 11110
Shift Left Twice for Each Five bits

P10(Key)	**1**	**1**	**0**	**0**	**0**		**1**	**1**	**1**	**0**	**1**
LS-2(Key)	**1**	**0**	**0**	**0**	**1**		**1**	**1**	**0**	**1**	**1**

LS-2(Key) = 10001 11011

Key	**1**	**0**	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**1**
Numbering	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
P8	**6**	**3**	**7**	**4**	**8**	**5**	**10**	**9**		
P8(Key)	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**1**		

P8(Key) = 10100110
K2 = 10100111
K1=11101001

Step 2: Plaintext Encryption First Round

Plaintext	0	0	1	0	1	0	0	0
Numbering	1	2	3	4	5	6	7	8
IP	2	6	3	1	4	8	5	7
IP(Plaintext)	0	0	1	0	0	0	1	0

This will lead to IP(Plaintext) = 0010 0010

L = 0010 R = 0010

f_K1 = (L (XOR) (R (XOR) K1), R)

K1=11101001

R = 0010

- we can't expand left side, so we have to compress it
- We can't expand left side, so we expand the right side

Expand R

R	0	0	1	0				
Numbering	1	2	3	4				
EP	4	1	2	3	2	3	4	1
EP(R)	0	0	0	1	0	1	0	0

EP(R) = 00010100

R	0	0	0	1	0	1	0	0
K1	1	1	1	0	1	0	0	1
XOR	1	1	1	1	1	1	0	1

XOR	1	1	1	1		1	1	0	1

S0(Row) = 11= 3
S0(Column) = 11 = 3

S1(Row) = 11 = 3
S1(Column) = 10 = 2

S0	0	1	2	3	
	1	0	3	2	0
	3	2	1	0	1
	0	2	1	3	2
	3	1	3	2	3

S1	0	1	2	3	
	0	1	2	3	0
	2	0	1	3	1
	3	0	1	0	2
	2	1	0	3	3

S0S1 = 22 = 1000

K1 = 1000

K1	1	0	0	0
P4	2	4	3	1
Numbering	1	2	3	4
P4(K1)	0	0	0	1

L	0	0	1	0
P4(K1)	0	0	0	1
XOR	0	0	1	1

f_K1 = 0011, 0010

Step 3: Plaintext Encryption Second Round

SW = 0010, 0011
L = 0010, R = 0011

f_K2 = (L (XOR) (R (XOR) K2), R)
K2=10100111
R = 0011

Expand R

R	0	0	1	1				
Numbering	1	2	3	4				
EP	4	1	2	3	2	3	4	1
EP(R)	1	0	0	1	0	1	1	0

EP(R) = 10010110

R	1	0	0	1	0	1	1	0
K2	1	0	1	0	0	1	1	1
XOR	0	0	1	1	0	0	0	1

XOR	0	0	1	1		0	0	0	1

S0(Row) = 01 = 1
S0(Column) = 01 = 1

S1(Row) = 01 = 1
S1(Column) = 00 = 0

S0	0	1	2	3	
	1	0	3	2	0
	3	2	1	0	1
	0	2	1	3	2
	3	1	3	2	3

S1	0	1	2	3	
	0	1	2	3	0
	2	0	1	3	1
	3	0	1	0	2
	2	1	0	3	3

S0S1 = 22 = 1010
K2 = 1010

Numbering	1	2	3	4
K2	1	0	1	0
P4	2	4	3	1
P4(K2)	0	0	1	1

L	0	0	1	0
K2	0	0	1	1
XOR	0	0	0	1

f_K2 = 0001, 0011

Final Step: IP inverse

IP	2	6	3	1	4	8	5	7
Numbering	1	2	3	4	5	6	7	8
IP^{-1}	4	1	3	5	7	2	8	6

Numbering	1	2	3	4	5	6	7	8
f_K2	0	0	0	1	0	0	1	1
IP^{-1}	4	1	3	5	7	2	8	6
IP^{-1}(f_K2)	1	0	0	0	1	0	1	0

⟶Ciphertext is 10001010

Ciphertext
Step 1: Ciphertext Decryption First Round

Ciphertext	1	0	0	0	1	0	1	0
Numbering	1	2	3	4	5	6	7	8
IP	2	6	3	1	4	8	5	7
IP(Ciphertext)	0	0	0	1	0	0	1	1

IP(Ciphertext) = 00010011
L = 0001, R = 0011

f_K2 = (L (XOR) (R (XOR) K2), R)
K2 = 10100111
R = 0011

Expand R

R	0	0	1	1				
Numbering	1	2	3	4				
EP	4	1	2	3	2	3	4	1
EP(R)	1	0	0	1	0	1	1	0

EP(R) = 10010110

R	1	0	0	1	0	1	1	0
K2	1	0	1	0	0	1	1	1
XOR	0	0	1	1	0	0	0	1

XOR	0	0	1	1		0	0	0	1

S0(Row) = 01 = 1
S0(Column) = 01 = 1

S1(Row) = 01 = 1
S1(Column) = 00 = 0

S0	0	1	2	3	
	1	0	3	2	0
	3	2	1	0	1
	0	2	1	3	2
	3	1	3	2	3

S1	0	1	2	3	
	0	1	2	3	0
	2	0	1	3	1
	3	0	1	0	2
	2	1	0	3	3

S0S1 = 22 = 1010
K2 = 1010

Numbering	1	2	3	4
K2	1	0	1	0
P4	2	4	3	1
P4(K2)	0	0	1	1

L	0	0	0	1
K2	0	0	1	1
XOR	0	0	1	0

f_K2 = 0010, 0011

SW(f_K2) = 0011 0010
L = 0011, R = 0010

Step 2: Ciphertext Decryption Second Round

f_K1 = (L (XOR) (R (XOR) K1), R)
Expand R

R	0	0	1	0				
Numbering	1	2	3	4				
EP	4	1	2	3	2	3	4	1
EP(R)	0	0	0	1	0	1	0	0

EP(R) = 00010100

R	0	0	0	1	0	1	0	0
K1	1	1	1	0	1	0	0	1
XOR	1	1	1	1	1	1	0	1

XOR	1	1	1	1		1	1	0	1

S0(Row) = 11 = 3
S0(Column) = 11 = 3

S1(Row) = 11 = 3
S1(Column) = 10 = 2

S0	0	1	2	3	
	1	0	3	2	0
	3	2	1	0	1
	0	2	1	3	2
	3	1	3	2	3

S1	0	1	2	3	
	0	1	2	3	0
	2	0	1	3	1
	3	0	1	0	2
	2	1	0	3	3

S0S1 = 20 = 1000
K1 = 1000

Numbering	1	2	3	4
K1	1	0	0	0
P4	2	4	3	1
P4(K1)	0	0	0	1

L	0	0	1	1
K1	0	0	0	1
XOR	0	0	1	0

f_K1 = 0010, 0010

Final Step: IP inverse

IP	2	6	3	1	4	8	5	7
Numbering	1	2	3	4	5	6	7	8
IP^{-1}	4	1	3	5	7	2	8	6

Numbering	1	2	3	4	5	6	7	8
f_K2	0	0	1	0	0	0	1	0
IP^{-1}	4	1	3	5	7	2	8	6
IP^{-1}(f_K2)	0	0	1	0	1	0	0	0

⟶Plaintext is 00101000

Firewalls and IDS Introduction

- **Hardware has a centralized security and high performance because hardware can handle traffic efficiency without affecting other parts and does not affect the security of other layers. One of the firewalls is hardware.**
  - **One firewall is for the device, one is for monitoring and configuration of the system.**
  - **Even if the system was down, the hardware security is always on because it's a separate layer than the other layers.**

- **Software as a solution is where there's a program that gets installed on the system, router, computer, server, etc.**
  - **it's a firewall and it has many advantages:**
    - **it is easy to use**
    - **very flexible**
    - **it can be altered and updated**
    - **cost effective**
    - **enable APIs and so on.**

  - **Disadvantages of software:**
    - **Limited protection means that only the device that we have installed software security on is going to be the only one protected.**
    - **software based security consumes power, processors, memory and so on.**

- **Should we use software-based or hardware-based security?**

    - **A simple application should be software-based solution because its less costly and flexible. Something large would be hybrid where it uses both software and hardware based security.**

- **Firewall should be placed on the gate where the cyber-attacks could be stopped before the attack the user's device.**
    - **The first layer of protection that protects the system from the attacks**
    - **Proxy is one of the types of firewalls.**
        - **Proxy could be balancing, or a firewall, and at the same time be a layer of defense.**
        - **The main feature of proxy is that it does filtering on the content.**
        - **Virtual private network (VPN) is a hidden network that can easily bypass proxy and firewall.**

- **Why is it called a firewall?**
    - **It was called a packet filtering firewall. It's called a firewall because it acts as a wall that slows down the fire (attacks).**

White and blacklist is one of the strategies where there's already predefined rules.

In firewalls, even if you attacked the external area, it would not affect the internal area due to the DMZ, dematerialized zone.

- **The local area has high trust level**
- **external area has low trust level**

- **The three zones are:**
    - **External (untrusted network)**

    - **DMZ (semi-trusted network)**
    - **Internal (trusted network)**

- **Packet filters**
    - **Packet filter can either allow or block packets dependent on the header.**

- **Why do we use proxy rather than just packet filtering?**
    - **It’s not logical for every packet to be filtered. Additionally, if the hacker changed their IP address, then the packet filter becomes invalid.**
    - **Packet filtering treats the packet like an isolated packet (isolated from the internet) which isn't a good idea.**

- **What does filtering depend on?**
    - **If filtering was done on IP, port number, protocols, and packet content.**
        - **There would be more filtering on the internal network than on accessing the external.**

- **Why do we use ports?**
    - **Ports allow computers to easily differentiate between different kinds of traffic.**

If the external to internal session was opened, then the firewall waits on the session.

- **Why is proxy much better in virus detection than packet filtering?**
    - **The virus is not static and the header in packet filtering would not be helpful in this aspect. Proxy specifies the rules where you can differentiate if something is blocked or allowed.**

- **What do we mean by cost?**
  - **Resources and money are high where the memory storage and CPU is taken up. And installing proxy on the device is costly (money wise).**

Permissive vs Restrictive

- **Permissive policies are a lightweight solution and less efficient solution. The problem is with forgetting a supposed to be blocked source, which is now able to interact with the internal area.**
- **Restrictive policies' problem is with forgetting to allow legitimate users to interact with internal area.**
  - **Permissive is false negative and restrictive is false positive.**

- **False positive: categorize the traffic as positive meaning its categorized as malicious or virus even though its legitimate**

- **False negative: categorize the traffic as negative meaning its categorized as legitimate even though its malicious**

1024 are well-known ports