**Confidentiality –** information is only available to those authorized. **Integrity** – information cannot be modified or damaged by others. **Availability** – information is always accessible. **Authentication and non-Repudiation**.

**Cryptography:**

**Stream** – key goes into a pseudo random or random sequence generation. This key is then used with an operation like XOR to change the plaintext bit stream into the ciphertext stream one bit at a time. High speed of transformation low error propagation however low diffusion and susceptible to malicious insertion and modification. **Block** – with a k bit key and n bit blocks each n bits are encrypted until the length of the plaintext is encrypted. High diffusion and immunity to insertion of symbols however slow and lots of error propagation.

**ECB**- Message sent in individual blocks encrypted independently, relatively weak and identical ciphertexts are sent if the plaintext/keys are the same across all sessions. ECB is weak and not recommended unless transmitting single values. Can be used for example to send an encrypted IV value for CBC.

**CBC** - Removes independence between message blocks, you must establish an IV (initialization vector), each ciphertext relies on the previous block ciphertext (after the initial IV). Error propagation problems can occur. CBC does not have identical cipher for same block. Used for large plaintext encryption

**CFB** - Uses cipher block from previous step in the next block cipher. CFB is a useful stream cipher (in a scenario when data is arriving in bytes/bits). Similar to CBC where the cipher requires previous blocks to function correctly CBC preforms XOR before encryption CFB after.

**OFB** - Message is treated as a stream of bits, similar to CFB where the output is used to generate next sequential blocks. OFB is useful for noisy channels, vulnerable to stream message modifications though. Similar to ECB, OFB will generate the exact same output for identical plaintext/keys so you need to be wary of this.

**CTR** - Newest block encryption method compared to the others, used in high speed network transfers. Uses the counter value instead of the feedback value, requires different keys and counter values for each plaintext block that is encrypted.

Need to generate O(N^2) keys for N users. So public and private was derived where you only need to share one key to communicate with people.

**Symmetric –** Shared secret key, Classified or open algorithm, required key distribution, **Pros;** Fast and easy to use, **Cons;**No authenticity and shared secret key. **Asymmetric** – Public and private key pair, open algorithm, not required key distribution, **Pros;** authentication and private key is kept secret, **Cons;** Need to manage public keys and is slow.

**DH** – DH and DSA applications in DNS SSH HTTPS, IPSec. Pick a random number A and B and g (g < p) then encrypt with C = P^E mod N decrypt With P = C^D mod N. Users exchange a secret key over an untrusted network. Then both parties compute K from p and g which are publicly available numbers where P is at least 512 bits. Attacker only has G^a g^b and pg. To compute G^AB this is discrete logarithm which is computationally hard. Susceptible to MITM attack where someone intercepts the G^a mod p and sends both receivers back their K1 and K2 thus acting as each other’s requested receiver. Need to use authentication to prevent MITM for example assuming bobs public key is known to alice, send bobs signature back to Alice and Alice’s signature back to bob to prevent identity misuse attacks. RSA can be used for message encryption and can provide authentication and allows anyone to communicate with the user. DH only exchanges shared key typically for symmetric ciphers and you must already identify who you want to communicate with.

**Blockchain –** A distributed ledger tech to connect different untrusted parties over the internet and store data securely from tampering. Uses chained hash blocks for authenticity. Different untrusted people agree on the state of the system. Decentralized. When a transaction occurs everyone in the network records it. Each block records a list of transactions and the next block is chained from the previous one. **Merkle tree** – allows you to summarize all the transactions with a digital fingerprint. Quickly and simply verify transactions, each branch can be downloaded for verification. **Blockchain** – sequence of hash chained records that are immutable and stored in distribution. Proof of work is a consensus algorithm used to confirm transactions and add new blocks to the chain where miners compete against each other to complete transactions on the network and guess a hash.

**Social Engineering -**is the persuasion and manipulation of human entities to disclose sensitive information**.** Phishing is a massed distribution of a spoofed emails pretending to come from well known organisations**.** Pharming redirects a website’s traffic to another website using DNS tampering. Can be mitigated by establishing frameworks and trust establishment.Offensive (or ‘Bad’) USBs are USBs that serve to tamper and affect a target machine

**Properties of Phishing Emails** Spelling mistakes are prominent**.** Isn’t personalized**.** Requests for you to download an attachment**.** Links to sites not related to the sender**.** Links to a dodgy site, check domain name and TLD**.** Sent from a different email to sender’s usual

**Malware -** Viruses are a malicious program that spreads through the network by infecting various files. Infected files will execute malicious program first and then run as normal. Will also replicate by replacing other executables with themselves.Infected files will execute the malicious program without the user knowing first, and then run the normal program. Worms focus on spreading through the network and exploits various network vulnerabilities to spread itself. Worm can be prevented by patching applications and OS from vulnerabilities and education on prevention.Malvertising is malware spread through advertising**.** Ransomware is malware that encrypts a system and forces a user to pay for it to be decrypted steps are **Distribution, Installation, Communication, File Search, Encryption, Ransom Demand.** Convince user to download, determine system configuration connect to server transmit encryption details, encryption is run silently encrypts important files removes any backups.

**Virus Types - Oligomorphic** – using multiple decryptors. **Polymorphic** – mutates certain part of itself. **Metamorphic** – rewrites all (or most) of itself. Antiviruses that scan email attachments Incorporate sandboxing, AI, data mining and machine learning Firewalls.

**Spyware -** is malware that allows the monitor and captured by a third party**. Keyloggers** take note of all keypresses a user inputs**.** Protection can include automatic form fillers, antivirus ect**.** Unsolicited software is commercial software installed unbeknownst to the user**. Scumware** is malicious code that entered the system without the user’s consent or permission**.** Trojans allow for the remote control of a user’s machine

**Rootkits -** Rootkits are used to obtain the root privilege**. Firmware** – hides in firmware**. Kernel-mode** – hides from kernel list of active processes**. User-mode** – runs along with other applications

**Botnet -** are a collection of applications that run automated tasks over the Internet in order to DDoS and spam. Botnet infects users, then the bot on the infected PC establishes communication with the command server and then the bots are used to send out spam or carry out DDos.

**Zero-day -** attacks take advantage of software vulnerabilities for which there are no available fixes. Detection techniques include; Statistical based using historical data to build attack profiles, Behavioral based which analyses the exploits interaction with users and Hybrid based which blends the two.

**Network Attacks**

**Sniffing**

Sniffing is a passive, undetectable attack that captures network traffic between two communicating nodes

**Spoofing -** is a form of ‘lying’, to claim that you are someone (or something) else, such as a different IP, DNS, or MAC address. Reset the existing connection, then the attacker guesses the sequence number, once this number is guessed they can join into the stream of packets and insert any data they want. IP spoofing happens after this, once we have reset the connection we can alter the source address in the packet allowing us to bypass firewall or IDS for internal attacks.

**Remote Access/Shell -** Remote shells are shells that are controllable remotely from the network**. Reverse shells** – server hacking client**. Forward shells** – client hacking server

**Denial of Service -** attacks are actions that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space**.** Distributed Denial of Service attacks are when several clients carry out a DoS attack.Two kinds **Volume attack** which relies on sending a large amount of traffic to the server to overload it and legitimate traffic cannot access the server. **Protocol attack** This attack relies on exploiting flaws in protocols to flood the network and use up resources to the point of exhaustion. Example SYN attack exploiting the nature of the SYN protocol by continuously sending SYN packets and receiving the ACK response from the server however these are discarded and repeatedly send SYN packets until the server is overloaded and legitimate traffic is bricked. **Reflection attack** – relies on using legitimate servers which send intended legitimate responses from the attacker but the attacker will pass these onto the victim server overloading it. **Amplification attack** – Servers which send amplified responses back similar to reflection the attacker will send a large amount of requests to these servers and passes these amplified packets onto the victim server. **Prevention** **and preemption**, Detection and filtering, Trace-back and identification and reaction. Most useful Detection and filtering: This is usually the most effective method of DoS prevention. It’s not that easy to prevent an attack from occurring as there are a large amount of protocols in use that can’t be stopped and as newer ones are found, paired with the simplicity of DoS attacks nowadays. It’s simply easier to detect and filter (mitigate) the attack, there’s new measures in place when large amounts of traffic is incoming such as scaling server sizes upwards to cater for these (scalability available in cloud computing or installs like Docker and Kubernetes), deep machine learning algorithms that can detect fake traffic etc.

**Buffer Overflow -** An anomaly where a program while writing data to a buffer, overruns the buffers boundary and overwrites adjacent memory locations. Often changing its return value. C/C++ offers no bounds checking for certain functions you can therefore write into locations that wasn’t allowed originally. The writing of extra memory into adjacent locations can allow attackers to inject malicious code. Prevention, use different code, non executable stacks data execution prevention, randomizing memory areas in stack, adding canary in code where if a canary is modified the program is terminated.

**Web Based Attacks**

**SQL Injection** - is an attack that manipulates SQL statements and queries in order to exploit an application that communicates with a database

**Types of SQLi - In-band** – error-based or union-based, visible to the attacker allowing them to make modified SQL queries and see the results**. Inferential** – Boolean-based blind or time-based Blind SQLi attacks as there is no output, instead they rely on time based execution or true or false in the HTTP response**. Out-of-band** – enabled feature-based requires unconventional feature eg set up a canary in order to see results of the execution

**SQLi Techniques-** Escaping with ; running false query on left and correct on right. Shell injection of Open Database Connectivity apps. Account creation. Blind injection

**Prevention -** Client-side character checking (not allowing user to pass apostrophes hyphens for comments. Prepared Statements disabling multi command calls. Don’t allow access to the database as an unprivileged user. Limit the user to only queries required (prepared statements). Don’t include any database passwords in code

**Cross-site Scripting (XSS) -** is the act of sending foreign scripts from a server to a client for the client to execute exploiting the fact that web browsers can execute commands. Servers send malicious script codes to the client, client executes the malicious script on its browser. **Stored** – more damaging, when malicious script is injected directly into the website that is being accessed. **Reflected** – less common and less harmful, its when a form on a website is not escaped allowing the user to essentially enter custom data that could be potentially malicious in nature. This is not so much of a problem for a user but if an attacker can somehow convince their target to enter this data or send them a link where it is pre written it could be dangerous.

**Defense Mech** – **SSL/TLS**

**IPSec**