

"Computer Security"

⇒ Network Security ⇒

→ Network, Data & System को Unauthorised Access, Misuse, Modification, destruction & disruption से protect करता।

↓
ट्रिव्युव्हान / Availability

→ ये ensure करता है -

- * C - Confidentiality → Data केवल Authorised users तक ही पहुँचे। } Network Security
- * I - Integrity → Data विभिन्न permission के Modify नहीं हो सकता है। } के 3 Goals/Tried
- * A - Availability → Network Services हमेशा Available हो।

*Client Server Network Security =>

- Client Server architecture में एक Central Server होता है और Multiple clients connect होते हैं, जो server से Services / Security Access करते हैं।
- इस Architecture में Security extremely important होती है, because -
 - A. Server में central Data store होता है।
 - B. Multiple clients एक ही server से connect होते हैं।
 - C. Network communication बहुत sensitive होता है।
 - D. Attacker किसी एक machine से Compromise करके पुरा Network Hack कर सकता है।

* Client Server Architecture में Security Requirements :-

A. Authentication :-

→ Verify करना कि कोई client जिसकी identity claim कर रहा है, वह वही हमारा नहीं।
Ex = Password, OTP, Biometric, certificates etc.

B. Authorization :-

→ किसी client की क्षमा access मिलता चाहिए प्रारंभिक क्षमा रहीं।
Ex = Files Read/Write permissions.

C. Encryption :-

→ Data को scramble करके secure बनाना ताकि Attacker Data को intercept करके भी Read & understand नहीं कर सके।
Ex = HTTPS, SSL, TSL, VPN etc.

D. Auditing & logging ⇒

- Server पर सारी activities record करना।
- Unauthorised access detect करने में help मिलती है।

E. Firewall & IDS/IPS ⇒

- Firewall unauthorised clients / traffic को block करता है।
- IDS (Intrusion Detection System) = Firewall से More Secure.
- IPS (Intrusion Prevention System) = Intrusion को भी Block कर देता है।



F. Data Backup & Recovery ⇒

- Server Data का Regular Backup.
- Ransomware या crash के case में Data Recovery किया जा सकता है।

* Client Server Architecture के Major Security Threats :-

1. Malware Attacks :-

- Malicious Software
- ऐसे software जो Data & System को Damage करे, Data की पुरानी और unauthorised access की permission देते हैं।
- Types :-
 - A. Virus → ऐसे program जो खुद की copy करते हैं और किसी भी program को infect करते हैं।
 - B. Worm → Network से विभिन्न user की permission के सबसे fast spread & damage करता है।
 - C. Trojan horse → legal app जैसा लिखता है, परन्तु Malicious code को रखता है और self Replicate करता है।
 - D. Ransomware → Data को encrypt करके Ransom / किरणी demand की जाती है। नहीं करता है।
- Impact = Data loss, Data corrupt, System slow/ crash, Privacy loss, Business shutdown etc.

2. Phishing Attack :-

- ग़ायली प्रक़ार्ता।
- इसमें Attacker fake communication (Message, whatsapp, website, Email) Send करता है, जिसमें -
 - A. Bank / Trusted services का नाम use में लिया जाता है।
 - B. Users को Link पर click करने, OTP Fill करने वा Password लिखने को force किया जाता है।
 - C. कभी-2 Malware download करवा देता है।
- इसे सबसे ज्ञानादार dangerous फ़ालिए जाना जाता है, क्योंकि user अपनी details रखुद भी के देता है।

3. DOS/DDOS

- Denial of Services / Distributed Denial of Services
- इन होने में attackers, Server पर excessive traffic फ्रेजकर overload कर देते हैं।
- DoS = Single System से flood
- DDOS = Botnet (infected Systems का Network) से Coordinated Attack.
- Result =
 - A. Website slow या completely down.
 - B. Businesses का बड़ा financial loss.
 - C. Genuine users access नहीं कर पाते हैं।

4. MITM (Man In The Middle) Attack =>

- इसमें Attacker Client & Server को बीच Silently घुस जाता है।
- यह Attack unsecured public wi-fi में होता है।
- इसमें attacker -
 - A. Message intercept करता है।
 - B. Data modify कर सकता है।
 - C. Business logins, Session cookies, Emails steal कर सकता है।
- सबसे Common type = Fake wifi Hotspot (Evil Twin)

5. SQL Injection Attack

- SQL Injection रख देता है, जब Website user input को properly validate नहीं करती है।
- Attacker malicious SQL command inject कर देता है, जो -
 - A. Database read कर सकती है।
 - B. Tables Delete/update कर सकती है।
 - C. Admin account create कर देता है।
- Impact = Sensitive data leak, Complete Database compromise, Business shut down.

6. Brute force Attack

- इस फ्रॉर्स के attack में Attacker, Password को guess करने के लिए हर संभव प्रयास करता है और possible combination try करता है।
- Weak passwords जल्दी break हो जाते हैं।
- Automated tools का use कर 1000 times per second password crack करने की try की जाती है।
- इससे बचने के लिए strong password, 2FA (Two factor Authentication), MFA (Multi Factor Authentication), Account lockout का use किया जा सकता है।

7. Insider Attack ↗

→ Insiders की जोग होते हैं, जिनके पास Already authorised access होता है।
Like = Employees, Contractors, Family members etc

→ Types =

A. Malicious Insider ⇒ जानबुझकर Data को steal / Modify करता है।

B. Negligent Insider ⇒ Accidentally data को leak कर देता है।
using USB, emails, phishing

C. Compromised Insider ⇒ Employees का account hijack हो जाते हो महसूस dangerous
threat होता है, क्योंकि उन्हें पहले दी access granted होता है।

8. Spoofing Attack :-

- Attacker अपनी identity fake करता है।
- ये Attacks mostly Trust bypass करने के लिए किए जाते हैं।
विश्वास के साथ विश्वास घात

3 Types :-

- A. IP Spoofing = Fake IP Address से Request भेजना।
- B. MAC Spoofing = Fake MAC Address से Network में entry ली जाती है।
- C. Email Spoofing : Fake Sender Name use करना।

9. Eavesdropping / Packet Sniffing =>

→ Network में गोजे जाने वाले packets को Capture करके Attacker -

- A. Password
- B. Form Data
- C. Cookies
- D. Session Data / Tokens
- E. Source & Destination IP

को sniff / steal कर सकता है।

→ Mostly unsecured HTTP Networks में होता है।

10. Session Hijacking →

- इसमें Attacker user के Active session का Token steal कर लेता है।
- माटे session cookies के द्वारा दोता ही भी Attacker निया password के login से दक्षता है।
- Common Scenarios =
 - A. Public Wi-fi
 - B. Poor Session Management
 - C. Unencrypted websites

* Firewall →

- Network security device/ software जो incoming & outgoing traffic को Monitor & Control करता है।
- प्रद सecurity rules based होता है।
- प्रद Network को outsider attackers से protect करता है।
- Main Tasks ⇒
 - A. Unauthorised access को Block करना।
 - B. Untrusted traffic को Block करना।
 - C. Network packets inspect करना।
 - D. Internal network को external threats से protect करना।
- 4 प्रकार ⇒
 - A. Packet filter Firewall
 - B. Statefull Inspection Firewall
 - C. Proxy Firewall
 - D. Next Gen Firewall

A. Packet Filter Firewall ⇒

- IP Address, Port Number & Protocol check करता है।
- Fast & Basic protection.

B. Stateful inspection Firewall ⇒

- Previous connections को माप रखते हुए New connections को Check करता है।
- More Secure.

C. Proxy Firewall ⇒

- Works as middleman between Client & Server.
- Traffic को forward करने से पहली ही Filtered कर देता है।

D. Next Gen Firewall (NGFW) ⇒

- Deep packet inspection.
- Application layer filtering.
- IDS/IPS integrated & Malware detection.

* firewall की Limitations →

- Attackers किसी नये तरीके से Attack करे, तो firewall detect नहीं कर पाता है।
- Insider Threats को नहीं शोक सकता है।
- Only Entry | Exit points ही filter कर सकता है।

* Firewall v/s IDS v/s IPS =

Feature	Firewall	IDS	IPS
1. Full form	-	Intrusion Detection System	Intrusion Prevention System
2. Core Concept	Network Traffic को Control (Allow/Block) करता।	Suspicious activities को detect करता।	Suspicious activities को detect + Block करता।
3. Placement in network	Network के edges Main Gateway पर।	SPAN/Mirror port की Side में।	Inline/Traffic के बीच में।
4. Traffic handling	Traffic को filter/route करता।	Traffic को केवल read करता।	Traffic को Inspect + Modify/ block करता।
5. Real Time Response	Medium (Basic Allow/Deny)	No real time action	Real Time attack prevention
6. Block Capability	Yes, Basic rules के हिताब से	No	Yes, advance level पर

7. Working Theory	Rules, Ports, IP Filter	Signature + Anomaly analysis Detailed inspection (DOS, Malware, exploit pattern)	Signature + Anomaly analysis + In-line blocking Detailed detection + inspection + immediate stop
8. Attack handling	Basic attacks (Ports + Unauthorised access)	Low impact (only Alert होता है।) Deep inspection (Stateful + Content)	High (जलत Alert Traffic को भी block कर सकता है।) IDS जैसी Deep inspection + Active control
9. False Alert or Action	Yes, Statefull firewall traffic को track करता है।	L2 - L7 inspection Monitoring teams	L2 - L7 inspection + action Highly sensitive networks
10. Statefull inspection	L3 / L4 Small to large business	CCTV	Security Guard
11. Protocols	Gatekeeper		
12. Useful for			
13. Summary			

* Virus →

- मह एक Malicious (harmful) Program होता है, जो files & systems को damage, crash या corrupt कर देता है।
- मह Self-replicating होता है मार एक system से दुसरे में spread होता है।

* Types of Computer Virus →

1. Boot Sector Virus →

- Boot Sector को Infect करता है।
↓
System Start होने वाला Part.
- प्रदृश्य Virus, Computer start होने से Activate हो जाता है।
- System को Boot होने से रोकता है।

2. File Infector Virus →

- Program files (.exe, .com) को Infect करता है।
- File open होने से Activate हो जाता है।
- System slow & files को corrupt कर देता है।

3. Macro Virus =

- MS Word, Excel जैसे documents के Macro में hide होता है।
- Document open करते ही spread हो जाता है।
- Open files को corrupt कर देता है।

4. Polymorphic Virus =

- हर बार अपनी Shape / Structure को change करता रहता है, इसलिए Antivirus के लिए detect करना गुश्किल होता है।
- Highly dangerous & advanced virus types.

5. Metamorphic Virus ⇒

- प्रत्येक Replication में भवना Complete Code की change कर देता है, इसलिए इसे Detect करना बहुत Tough है।
- Complex & powerful Virus.

6. Resident Virus ⇒

- System RAM में load हो जाता है और Background में चलना रहता है।
- File Access द्वारा ही Attack कर देता है।
- System को slow & unstable कर देता है।

7. Non-Resident Virus

- RAM में permanently नहीं रहता है।
- एक specific file को infect करता है, फिर दुसरी दुःखी ढुँता है।
- Speed slow होता है but damage करता है।

8. MultiPartite Virus ⇒

- Boot Sector + Program files दोनों को infect करता है।
- Dual action के माध्यम से detect & remove करना मुश्किल।
- System को badly damage कर सकता है।

9. Overwrite Virus

- Infected file के data को overwrite करके destroy कर देता है।
- File open ही नहीं ढोती है।
- System को उमादा infect नहीं करता है।

10. Spacefiller / Cavity Virus

- Files में empty space find कर उसमें अपना code insert कर देता है।
- File size change नहीं करता है, इसलिए detect करना मुश्किल।

11. Web Scripting Virus →

- Browser scripts (JavaScript / VB Script) को exploit कर देता है।
- Fake websites, Pop-ups & Ads के through spread होता है।
- Browsing data steal कर लेता है।

* Data & Message Security =>

- Data की unauthorised access से बचाना & integrity maintain करना।
- Confidentiality ⇒ Data को केवल Authorised लोग ही देख सकते हैं, इसके लिए Encryption का use किया जाता है।
- Integrity ⇒ Data Transfer के दौरान उसमें कोई Modifications नहीं होना चाहिए।
- Authentication ⇒ Verify करना कि Sender & Receiver सही हैं या नहीं।
- Non-Repudiation ⇒ इस ensure करना कि जो Actions किए गए हैं, उनके लिए Sender & Receiver deny नहीं करें, क्योंकि इन Actions का Record होता है।

* Methods to achieve Security :-

A - Encryption :-

→ Data को encode करके send करता, ताकि Attacker उस data को read नहीं कर सके।

B - Hashing :-

→ Data को एक unique hash (जैखे - Fingerprint, Face) generate करके भेजता, ताकि Data की Integrity verify की जा सके।

C. Digital signature :-

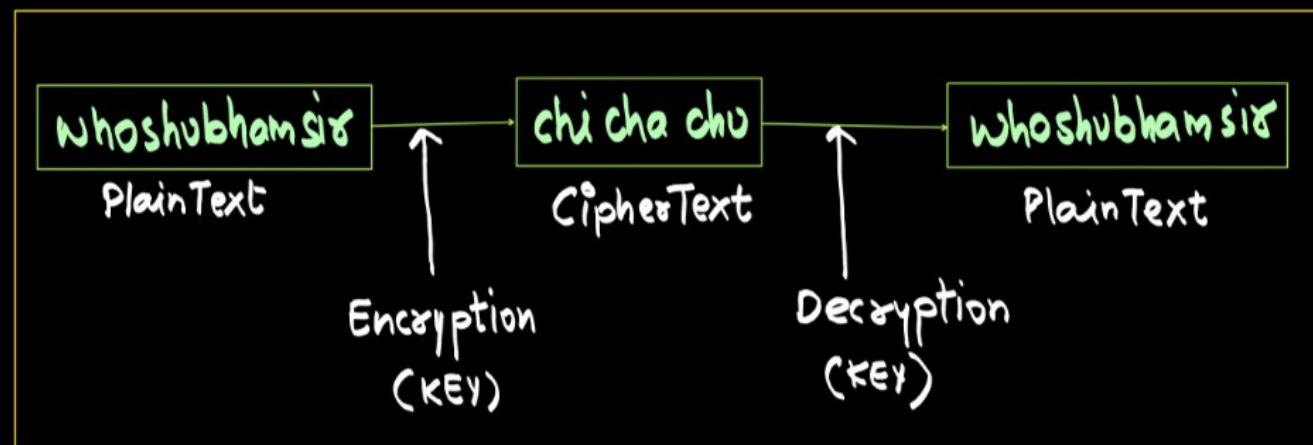
→ Data के साथ Sender का signature attach करता जिसमें Receiver verify कर सके, कि message सही है।

* Cryptography →

- Data को Encrypt / Secure करने की Technique ताकि Unauthorised users उके Access नहीं कर सकें।
- Main Goal - Confidentiality , Integrity & Authentication को ensure करना ।

* Key Terminologies →

1. PlainText / ClearText
2. CipherText / Encrypted Text
3. Encryption
4. Decryption
5. Key



1. Plain Text ⇒

- Original data जो user देता है।
- इसे ही Encrypt किया जाता है।
- CleanText / ClearText / Normal Text

2. CipherText ⇒

- Data जो Encrypted होता है & unauthorised users के लिए unreadable होता है।
- Normal Text को CipherText में Convert करने की Technique = Encryption
- Encrypted Text / Unreadable Text

3. Encryption ⇒ Normal Text को CipherText में Convert करने की Method.

4. Decryption ⇒ CipherText को Normal Text में convert करने की Method.

5. Key ⇒ Secret value जो data को Secure करती है।

* Algorithms of Cryptography ⇒

1. Block Cipher
2. Stream Cipher

1. Block Cipher ⇒

→ यह Algorithm एक बार में fix size of data के block को encrypt करती है। जैसे = AES, DES.

2. Stream Cipher ⇒

→ यह Algorithm continuous stream of data को encrypt करता है। जैसे - RCT.

* AES ⇒

- Advanced Encryption Standard
- Symmetric
- Encryption & Decryption के लिए Same key का use.
- Fast & Secure Algorithm जिसमें Data को blocks में बोड़कर encrypt किया जाता है
- Use = File encryption, Wi-fi Security, VPN, Disk encryption.

* RSA ⇒

- Rivest Shamir Adleman Algorithm
- Asymmetric
- Public & Private both keys used.
 - ↓
 - Data Encrypt ↓ Data Decrypt
- Large prime number based.
- Use = Secured data Transfer, Digital certificates, SSL/TLS

★ DES =

- Data Encryption Standard
- Symmetric
- Encryption & Decryption के लिए same key used.
- Old algorithm जो 56 Bits की key का use करता था।
- Outdated & weak.
- Old banking system में use.

★ ECC =

- Elliptic Curve Cryptography
- Asymmetric
- Public & private both keys used.
- कम Key Size से ज्यादा security.
- More efficient & faster than RSA.
- Use = Mobile devices, IOT & SSL/TSL

* 3DES *

- improvement of DES.
- इसमें DES को 3 Times apply किया जाता है, जिससे प्रति DES से ज्यादा strong है।
- Outdated.

* Blowfish *

- Symmetric key algorithm
- Key size variable
- AES & DES से ज्यादा Flexible

★ Symmetric Key Cryptography :-

- इस Algorithm में Sender & Receiver data को encrypt & decrypt करने के लिए same key का use करते हैं।
- Ex = AES,
DES,
Blowfish etc.
- इस Algorithm में single key use होने के कारण बहुत Fast होती है।
- इसमें यदि Key leak हो जाए तो पुरी Security compromise हो सकती है।
- Multiple users के लिए different Keys manage करना मुश्किल हो जाता है, इसलिए इसमें Scalability problem होती है।

