## Element of security: Application security

Including dev, add, test security features

Type: Authentification, Authorization, Encryption, Logging, App security testing

## CIA triad

Confidentiality: the one who is not authorized should not have access to data. **Way to steal:** capture data. Should send through vpn tunnel or encryption

Integrity: only authorized people can modify. **Check:** use hash, like MD5 and SHA

Availability: always ready. **Should** maintain, avoid bottle neck, check upgrade, backup plan

## TCP 3 handshakes

SYN: synchronize sequence number is sent to server, want to connect

ACK-SYN: server acknowledge, send back the syn number to start with

ACK: acknowledge the message, send back the ACK to server and establish connection

## DNS

Easy way for user to remember address to find specific website.

Consist of subdomain.to-pdomain

Manage by domain registries

URL = domain name+protocol+specific location

Type domain name => browser ask DNS => look up => give IP address

## Firewall

Hardware/Software-base network security device

Monitor incoming, outgoing traffic and can accept, deny, drop

Base on defined rule

## VPN

Create tunel

Connect to VPN services--connect to vpn server-all data transfer through that server

## Port

Well-known port

Registered port

Dynamic port

## Malware

Worm; spread quick, infect file and file-sharing. Cause data loss, data leak, malware installation, detected by fw and antivirus

Spyware: spy, no other

Ransomware: gain access to sensitive data end encrypt, require vip card

Trojan: need host (unlike worm) to spread, pretend to be a cutie program, gain access to system, detected by antivirus

Adware

Rootkit: gain admin access, need specialized tools, not just av

## Encryption-Decryptio

| Sym | Asym |
| --- | --- |
| DES, Double DES, Triple DES | RSA |
| Advanced ES | |
| Blowfish: use 18 key of 32-bit, quick and effective | |



Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com