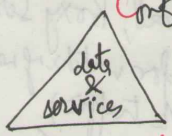
Computer Security

Basic principles & terms

- Security & functionality → (vice-versa) = reciprocal
- CIA Triad
- Authentication & Authorization
- Security clearance & need to know (sensitivity levels for data/system protection)
- Accountability & Auditing (ability to trace an action to a specific user/responsibility by auditing)
- Least Privilege & Separation of duties

CIA Triad



Availability (by backup, clusters, redundant / protection against malicious access)

Attack vectors (from technological / human) → social Engineering

Defense concepts → (defense in depth) → measures (control) → admin/mgmt. → policies, procedures, training, security clearances,

vulnerabilities, threats, and exposure (weaknesses/gaps used to exploit system, threat is potential problem by human/natural, intentional/accidental, measured in terms of exposure)

Basic risk concepts (quantitative & qualitative) (transfer risk, business risk)

Annual LE = SLE x ARO

Annualized Rate of Occurrence = (how many times in a year you would lose the asset)

Single loss Expectancy = (how much money you would lose if you lost the asset)

* Attack vectors (attempts to destroy/expose/alter/disable computer systems, or to gain unauthorized access to/make unauthorized use of an asset)

(DOS) → Denial of Service

attempt to deny the use of computer system/data from their users

* Network security for (defense in depth)
- attack via unprotected host
- " through firewall/..
- " spoofed (faked) source IP
- " ports/protocols
- " malformed/unusual packets
- "

C:/ netstat -an

* Network security devices :-
Hub, switch, router, Firewall, Proxy server,
intrusion detection devices (SW/Hardware for watching network traffic),
sniffer (SW/Hardware that 'sniffs' network traffic),
Wireless Access Point (to connect all to a large wired network),
VPN devices (hardware/computer/..),
Remote Access Servers (Dial-in/VPN servers),
Authentication devices, &

* Internet & email security -
- internet threats (hackers, spyware, virus, social engineering, ...)
phishing