CISSP 2016 Reference Sheet

CIA triad

Confidentiality only intended can see
Integrity complete/accurate/~~changed~~
Availability available when needed
Non-repudiation 2 parties are ok

OSI

Please Do Not Trust Sales Ppl Anymore

1. **Physical** (802.*, DSL, Bluetooth)
2. **Data** (PPP,SLIP,ATM)
3. **Network** (ipv4/6,icmp,ipsec)
4. **Transport** (TCP/UDP)
5. **Session** (PPTP,SOCKS)
6. **Presentation** (ASCII,JPG)
7. **Application** (HTTP,FTP,SMTP)

Common Ports

21 FTP, 22 SSH, 23 Telnet, 25 SMTP, 53 DNS, 80 HTTP, 110 POP3, 123 NTP, 443 HTTPS, 1433 MSSQL

TCP

Stateful, SYN → SYN/ACK → ACK
Application, Transport, Internet, Link

Secure communicating

SSL → TLS is standard (HTTPS)
Tunneling: PPTP,L2F,L2TP,IPSec
VLAN (separate networks)

Intrusion detection (IDS)

IDS=Intrusion Detection System, **IPS**=Prevention (stops), **HIDS**=Host IDS, **NIDS**=Network IDS (invisible, mirror port)
Knowledge IDS = data base, behavior

Business Continuity Planning

1. Scope & Planning
   a. Organization analysis
   b. BCP team (all depts., tech, legal,mgmt)
   c. Resource assessment
   d. Legal analysis
2. BIA Business Impact Assess: qualitative(good/bad)/quantitative $
   a. Priorities (AV/MDT/RTO)
   b. Risk identification
   c. Likelihood assessment (ARO)
   d. Impact assessmnt (EF,SLE,ALE)
   e. Resource Prioritization
3. Continuity Planning, Approval & implementation
   a. Strategy development (MDT)
   b. Provisions and Processes (Procedures for people, building, sites, infra)
   c. Plan approval (Top level mgmt.)
   d. Plan implementation
   e. Training & Education

People safety

Always comes first
Least Privilege, Separation of Duties, Monitoring, Mandatory vacations, Job rotation
Off boarding / termination procedure is important, stop accounts

AAA

Identification (username), Authentication (password), Authorization(user ok?), Auditing(log),Accounting(review)

RISK Calculations

AV=Asset Value,**EF**=Exposure Factor
SLE=Single Loss Expectancy,
ARO=Annualized Rate of Occurrence,
ALE=Ann Loss Expectancy
ACS=Ann Cost Safeguards
SLE=AV x EF
ALE=SLE x ARO
Calculate 2 situations, then:
Benefit =ALE_{new}-ALE_{old}-ACS
Total risk = threats x vulnerabilities x AV
Residual risk = left after accepting risk
Total – residual = control gap
Risk management framework: categorize, select, implement, assess, authorize, monitor

Data roles

Owner (responsible classify, label, protect), **System owner** (system ok), **Business/Mission owner** (value for organization), **Data processor** (3rd party), **Administrator** (grant access after owner tells them to), **User**, **Custodian** (day to day protecting and storing)

Information Flow Models

Bell-Lapadula,@DoD, Confidentiality

- Simple prop: ~~read up~~, read down
- Star prop: ~~write down,~~ write up

Biba, nonmilitary, Integrity

- Simple prop:~~read down~~, read up
- Star prop: ~~write up~~, write down

Systems Security Eval Models

Rainbow Series ->Orange = TCSEC -> Labels A=best, D=worst protection

Encryption

- Plaintext → Key → Cypher text
- Hashing = one way = Integrity = md5,sha,..
- Encryption = Confidentiality = ssl, tls, pgp(mail), S/MIME (mail)
- PKI = server certificates

Transpos=shuffle, substitution=replace rules

Symmetric

Same password to encrypt and decrypt.
#keys=(n*(n-1))/2
Fast, not scalable, C

Asymmetric

Public (known to world) + private key (secret).
Slower, scalable, CIA

Attacks

Military, Business, Financial, Terror, Grudge (against old boss),Thrill (fun)
XSS =Cross Side Scripting, requests between sites, **SQL injection** = bad data input, change/ read more data than allowed CI, **MiTM** = Man in the Middle, eavesdrop C , **DoS** = make unavailable A , **DDoS** = lots of 'attackers' A, **Eavesdrop** listen in C, **Impersonating/Masquerading, Replay, Social engineering**

Access control

Subject → Object

DAC	not centralized,per server
MAC	security levels and labels
RoBAC	roles (centralized)
RuBAC	firewall

Preventive (stop), Detective (see), Corrective (remove virus,reboot), Deterrent (policy), Recovery (corrective++,backup), Directive (policies), Compensation (extra lock), Administrative (processes), Logical/technical (systems), Physical (fence)

Identity, tokens, bio

Synchronous token = clock
Asynchronous token = counter
Something you Know, Have, Are
Type1=false negative, good not enter
Type2=false positive, bad can enter

Testing

Static=not running,Dynamic= running,Fuzz=garbage, Interface test

Incident

Event that has negative effect on CIA of data.
Detection & Identification →Response &Reporting → Recovery & Remediation
Scanning/Complomise/MalCode/DoS

Change management

Change mgmt. goal = keep CIA good
Change mgmt. benefit = rollback

Kerberos

Key Distribution Center KDC, Ticket Granting server TGS, Ticket granting ticket TGT, Ticket

Laws

Criminal=federal/state, Civil=between 2 parties, Administrative = government day to day
Copyright(books),Trademark(name/slogan/logo),Patent(creations), Trade secret(internal)
PII = Personal Ident Info, PHI = Protected health info

Relax, take breaks!

V 1.0 Karlo Luiten