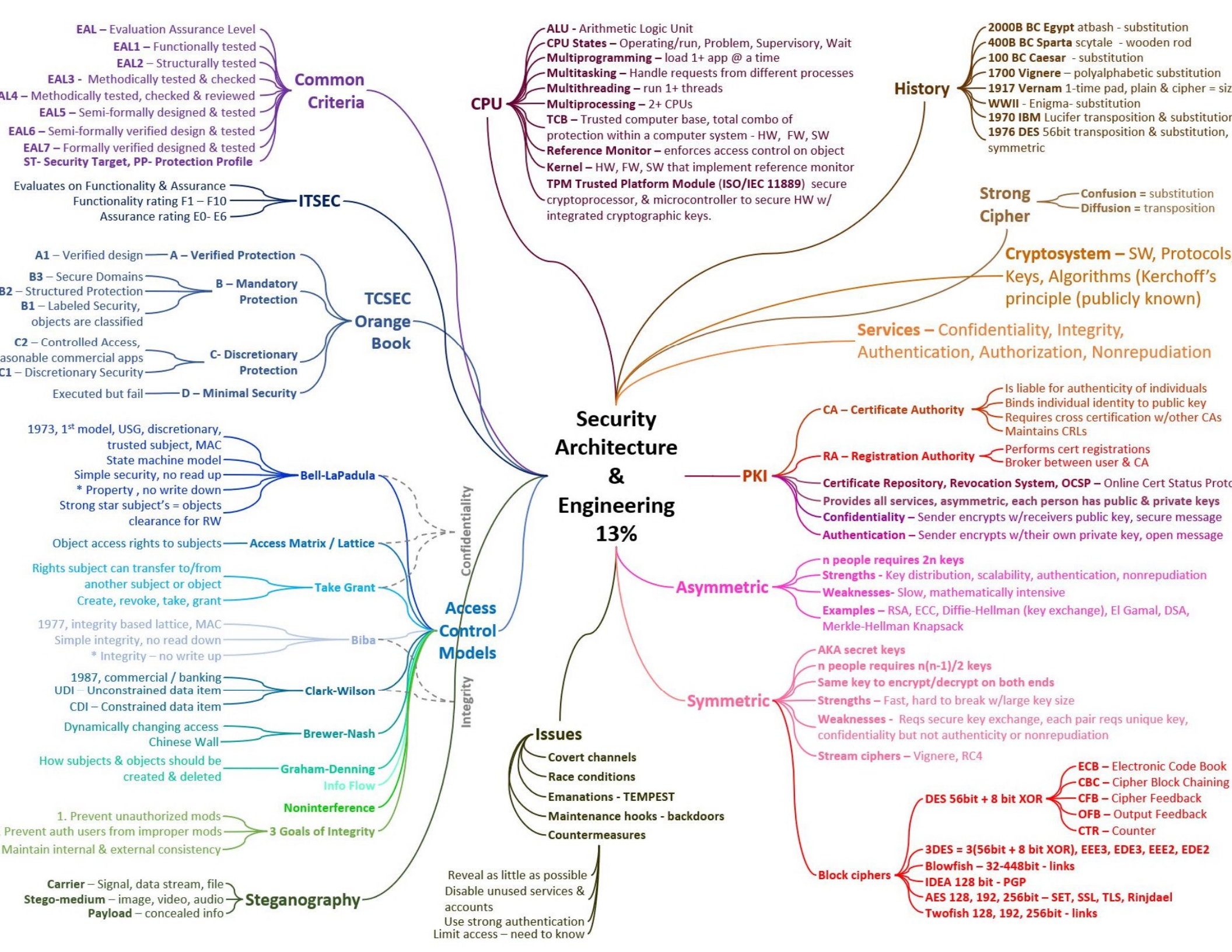
Security Architecture & Engineering 13%
Common Criteria
EAL – Evaluation Assurance Level
EAL1 – Functionally tested
EAL2 – Structurally tested
EAL3 - Methodically tested & checked
AL4 – Methodically tested, checked & reviewed
EAL5 – Semi-formally designed & tested
EAL6 – Semi-formally verified design & tested
EAL7 – Formally verified designed & tested
ST- Security Target, PP- Protection Profile
ITSEC
Evaluates on Functionality & Assurance
Functionality rating F1 – F10
Assurance rating E0- E6
TCSEC Orange Book
A1 – Verified design
A – Verified Protection
B3 – Secure Domains
B2 – Structured Protection
B1 – Labeled Security, objects are classified
B – Mandatory Protection
C2 – Controlled Access, asonable commercial apps
C1 – Discretionary Security
C- Discretionary Protection
Executed but fail
D – Minimal Security
Access Control Models
Confidentiality
Integrity
1973, 1st model, USG, discretionary, trusted subject, MAC
State machine model
Simple security, no read up
* Property , no write down
Strong star subject's = objects clearance for RW
Bell-LaPadula
Object access rights to subjects
Access Matrix / Lattice
Rights subject can transfer to/from another subject or object
Create, revoke, take, grant
Take Grant
1977, integrity based lattice, MAC
Simple integrity, no read down
* Integrity – no write up
Biba
1987, commercial / banking
UDI – Unconstrained data item
CDI – Constrained data item
Clark-Wilson
Dynamically changing access Chinese Wall
Brewer-Nash
How subjects & objects should be created & deleted
Graham-Denning
Info Flow
Noninterference
1. Prevent unauthorized mods
Prevent auth users from improper mods
Maintain internal & external consistency
3 Goals of Integrity
Steganography
Carrier – Signal, data stream, file
Stego-medium – image, video, audio
Payload – concealed info
CPU
ALU - Arithmetic Logic Unit
CPU States – Operating/run, Problem, Supervisory, Wait
Multiprogramming – load 1+ app @ a time
Multitasking – Handle requests from different processes
Multithreading – run 1+ threads
Multiprocessing – 2+ CPUs
TCB – Trusted computer base, total combo of protection within a computer system - HW, FW, SW
Reference Monitor – enforces access control on object
Kernel – HW, FW, SW that implement reference monitor
TPM Trusted Platform Module (ISO/IEC 11889) secure cryptoprocessor, & microcontroller to secure HW w/ integrated cryptographic keys.
History
2000B BC Egypt atbash - substitution
400B BC Sparta scytale - wooden rod
100 BC Caesar - substitution
1700 Vignere – polyalphabetic substitution
1917 Vernam 1-time pad, plain & cipher = siz
WWII - Enigma- substitution
1970 IBM Lucifer transposition & substitution
1976 DES 56bit transposition & substitution, symmetric
Strong Cipher
Confusion = substitution
Diffusion = transposition
Cryptosystem – SW, Protocols, Keys, Algorithms (Kerchoff's principle (publicly known)
Services – Confidentiality, Integrity, Authentication, Authorization, Nonrepudiation
PKI
CA – Certificate Authority
Is liable for authenticity of individuals
Binds individual identity to public key
Requires cross certification w/other CAs
Maintains CRLs
RA – Registration Authority
Performs cert registrations
Broker between user & CA
Certificate Repository, Revocation System, OCSP – Online Cert Status Proto
Provides all services, asymmetric, each person has public & private keys
Confidentiality – Sender encrypts w/receivers public key, secure message
Authentication – Sender encrypts w/their own private key, open message
Asymmetric
n people requires 2n keys
Strengths - Key distribution, scalability, authentication, nonrepudiation
Weaknesses- Slow, mathematically intensive
Examples – RSA, ECC, Diffie-Hellman (key exchange), El Gamal, DSA, Merkle-Hellman Knapsack
Symmetric
AKA secret keys
n people requires n(n-1)/2 keys
Same key to encrypt/decrypt on both ends
Strengths – Fast, hard to break w/large key size
Weaknesses - Reqs secure key exchange, each pair reqs unique key, confidentiality but not authenticity or nonrepudiation
Stream ciphers – Vignere, RC4
Block ciphers
DES 56bit + 8 bit XOR
ECB – Electronic Code Book
CBC – Cipher Block Chaining
CFB – Cipher Feedback
OFB – Output Feedback
CTR – Counter
3DES = 3(56bit + 8 bit XOR), EEE3, EDE3, EEE2, EDE2
Blowfish – 32-448bit - links
IDEA 128 bit - PGP
AES 128, 192, 256bit – SET, SSL, TLS, Rinjdael
Twofish 128, 192, 256bit - links
Issues
Covert channels
Race conditions
Emanations - TEMPEST
Maintenance hooks - backdoors
Countermeasures
Reveal as little as possible
Disable unused services & accounts
Use strong authentication
Limit access – need to know