Security engineering

Jaan Priisalu
ITC8050

Topics

- Measures
- Crypto algorithms and systems
- Identity and access management
- Processes and standards
- Hardening principles
- Certification and accreditation

http://www.cl.cam.ac.uk/~rja14/book.html

http://cacr.uwaterloo.ca/hac/

Security properties

Availability

Integrity

Confidentiality

Security measures

Types

- Physical
- Information technology
- Organisation

Roles

- Preventive
- Detective
- Corrective

Risk management

Risk=Threat*Vulnerability*Asset

- Foundation is inventory
- Limits of reasonable estimations
- Probability is not a trivial concept
- Risk treatment
- Attack trees (or scenarios partial orders)
- Security proof models

Cryptoalgorithms

- Random
- Hash
- Sym encrypt
- Asy encrypt

Cryptosystems

Primitives

- digital signature
- timestamp

Protocols - caution!

- ephemeric key exchange
- zero knowledge authentication
- e-elections
- digital cash

https://www.cryptool.org/en/, cipher suits

Blockchain

Partial order of Merkle tree record blocks

- Timestamp
- Immutable distributed database
- Abstract machine
- Ledger
- Money is one application

Access

1. Identification - claim
2. Authentication - proof
3. Authorization - decision

Authentication

- Physical - token
- Knowledge - i.e. password
- Biometric - body

FRR, FAR and recovery

Authorisation

- Access control lists
- Grouping ressources
- Assigning roles
- Mandatory access control

Capability based - SSO, Kerberos, attribute certificates,

IT Architecture

- ITIL - incident, problem, change, release
- TOGAF
- ITSM & ISO/IEC 20000
- COBIT
- ISO OSI

Business alignment, continuity, maturity

Security policies

Confidentiality -

- Bell-LaPadula
- Chinese Firewall

Integrity

- Biba

Black- vs whitelisting

Principles

- Know yourself and know your enemy
- KISS
- Divide and conquer
- Segmentation
- Attack surface
- Encapsulation
- Layered defence
- Virtualisation
- Tunneling

Security standards

- Common Criteria for purchases, prot. profiles
- Processes ISO/IEC JTC1/SC27 27000
- Assets - IT-Grundschütz — Iske
- Capital - Basel II/III
- KRI/KPI

NIST-CSFW

Licensing

Certification

- Measures security properties
- Compares to requirements profile

Accreditation

- Business decision to authorise usage
- Compares to mission and threat profile