

**CISSP in a nutshell**

**written by**

**Christine Kretschmann**

**March 2007**

## Operation Security

Operations Control	Personnel	Reacting to Failures	Threads
<p><u>Administrative Controls</u> Policies, Procedures, Guidelines, Baselines. Mechanisms who enforces things</p> <p><u>Technical Controls</u> <u>Logical level, to control access. (IDS, FW)</u></p> <p><u>Physical Control</u> <u>CCTV, fences, biometric devices Sub controls € (AC, TC, PC)</u> preventive controls : fences, locks detective controls : audit corrective controls : IDS, IPS recovery controls : RAID deterrent controls : Fired policy directive controls : administrative policy</p> <p><b><u>Personnel Operations:</u></b></p> <p><u>Operators:</u> Monitoring, Controlling, Jobs, IPL, mounting of volumes</p> <p><u>Network administrators:</u> Maintenance &amp; control of networks all devices &amp; system administrator</p> <p><u>Security administrator:</u> implementing user clearance level, setting initial password &amp; security profiles, configuring sensitivity levels, implementing security mechanisms, review of auditlogs.</p>	<p><b><u>Personnel procedures</u></b> Hiring procedures for new staff separation of duties job rotation, least privileges mandatory vacation Termination process</p> <p><b><u>Audit &amp; Monitoring</u></b> accountability</p> <p><u>Audit tools:</u> event viewer, snort, etherreal clipping level IDS (pattern &amp; behavioural) key stroking facility protection</p> <p><b><u>Configuration Management</u></b> complete change process =&gt; goal stability</p> <p><b><u>Media Control:</u></b> <b>Data Management</b> creation, protection, IO-controls removal: sanitation, overwriting, degaussing and destruction !residual data = data remanence</p> <p><b><u>Contingency Management:</u></b> developing plans &amp; procedures after an incident to effect operational systems =&gt; BCP</p>	<p><b><u>Trusted Recovery</u></b></p> <p><b><u>Fail-safe:</u></b> automatic termination &amp; protection of programs. <b><u>Fail-soft:</u></b> termination of non essential processes <b><u>Fail-secure:</u></b> preserver always a secure state <b><u>Fail-over:</u></b> backup system is activated</p> <p>Fax simile Security: encoder, fax server</p> <p><b><u>Software Backups:</u></b> network availability</p> <p>RAID ( Redundant array of inexpensive disks) 0: stripping 1: mirroring 2: hamming code parity 3: byte-level parity 4: block level parity 5: interleave parity 6: double parity 10: striping &amp; mirroring</p> <p>Failure resistant disk system =&gt; data loss through disk failure Failure tolerant disk system =&gt; component Disaster tolerant disk system =&gt; independent zones</p> <p><b><u>Backup:</u></b> HSM: hierarchical storage SAN: storage area network Backup Test Tape rotation Kinds of backups: =&gt; full, differential, incremental</p>	<p><b><u>Hack attacks:</u></b> insiders, outsiders, script kiddies, cooperate spies, government, ethical hacks.</p> <p>(D)OS Phreakers: telephone, pbx</p> <p><b><u>Good:</u></b> penetration</p> <p><b><u>Operational responsibilities:</u></b> unusual or unexplained occurrences deviations of standards unscheduled IPL /boots =&gt; incident</p>

## Security models and architecture

Computer components	Operation system security mechanisms	Security models
<p><b><u>System components</u></b></p> <p>CPU ∈ { RISC,CISC} process = application instruction in memory thread subinstruction of process Problem state = user mode Interrupts splits up CPU time</p> <p><b><u>Kinds of computer systems</u></b></p> <p><b><u>Multithreading:</u></b> process ≥ one thread <b><u>Multitasking:</u></b> process &gt; one process <b><u>Multiprocessing:</u></b> &gt; 1 CPU <b><u>Multiprogramming:</u></b> interleave &gt; 2 programms interleaved</p> <p><b><u>Storage &amp; Memory types</u></b></p> <p>Volatile storage = temporary storage Non volatile storage: ROM, EPROM Secondary storage: CD-ROMs, Sticks, AD Cache storage Virtual storage ∈ ( Main memory &amp; secondary storage) Memory Manager keeps track (page faults, page frames)</p> <p><b><u>Data Access Storage</u></b> sequential access: tapes direct access storage: memory &amp; disks</p> <p><b><u>Process Instructions</u></b> CPU ∈ machine language : 0s &amp; 1s assembly language compiler &amp; interpreter</p> <p><b><u>Operating States</u></b> Multilevel security OS : Dedicated ∈ (single,classified) Compartmented ∈ (read only parts)</p>	<p><b><u>Process isolation:</u></b> Security domain. Encapsulation objects,multiplexing of shared resources, naming distinction, virtual memory mapping, Software&amp; Hardware isolation.</p> <p><b><u>Protection Rings:</u></b> 0: Operating system kernel 1: OS security 2: OS utilities 3: application establish level of trust</p> <p><b><u>Virtual machine:</u></b> - specified security domain - mediate with host OS VMWARE, Java Sandbox</p> <p><b><u>Trusted Computing Base (TCB)</u></b> - combination of all security mechanism -TCB components provide CIA</p> <p><b><u>Reference Monitor &amp; Security kernel</u></b> - A reference monitor is an abstract machine that ensure that only authorized subjects could access objects. Mediates all access attempts. - The security kernel enforces rules of the reference monitor ∈ {HW,SW &amp; Firmware} ∈ TCB</p> <p>Trusted Path = protection of critical operation</p> <p><b><u>System validation</u></b> <b><u>Certification:</u></b> process of validation =&gt;system configure &amp;operate as expected.</p>	<p><b><u>Security Models</u></b></p> <p><b><u>Integrity models:</u></b> <b><u>Biba 77':</u></b> Simple integrity property : no read down Star * property : no write up</p> <p><b><u>Clark Wilson 87':</u></b> access through application, well-formed transactions, divide operations in subparts. Meets all 3 integrity goals: 1.) Prevent unauthorized users from making modifications 2.) Maintain internal &amp; external consistency 3.) Prevent authorized users from making improper modifications.</p> <p><b><u>Confidentiality models:</u></b></p> <p><b><u>Bell-La-Padula (state machine/information flow model) 70':</u></b> 1) Simple security rule: no read up 2) * security rule: no write down</p> <p><b><u>Take-Grant-Model:</u></b> take.grant, create and revoke operations</p> <p><b><u>Chinese Wall/Brewer and Nash Model:</u></b> prevent conflicts of interest {OS} problems</p> <p><b><u>Other models:</u></b> - Non-interference-model - Information flow model - Graham Denning model (based on protection rules) - Harrison-Ruzzo-Ullmann</p> <p><b><u>Open &amp; closed systems</u></b> open: allow input /interface</p>

## Computer components

## Operation system security mechanisms

## Security models

Accreditation: formal approval of certification

closed: no interfaces

### **Documents & Guidelines:**

Rainbow Series:

Orange book Trusted computer evaluation criteria  
standalone systems, measurement of *confidentiality*

4 categories:

A: verified protection: highest security division

B: mandatory security: protection TCB

C: discretionary security

D: minimal protection

subcategories:

A1: formal approval of certification

B1: labeled security protection

B2: structured protection

B3: security domains

C1: discretionary protection

C2: Controlled access protection

Red book Trusted Network Interpretation

*Integrity & confidentiality*

80' ITSEC Information Technology Security Evaluation

10 functionality classes & 7 assurance classes

to TOE=Target of Evaluation

97' Common Criteria ISO 15408

TCB entities 10 EAL {Evaluation Assurance Levels}

ST=Security Target

BS7799 ISO27001

Security Framework € {Security policy, organization, Asset control & classification, environmental & physical security, employee security, computer & network management, BCP, access control, system development & maintenance, compliance

## Law, Investigation and Ethics

Computer Crimes	International property laws	Parameters of investigations
<p><u>Crimes:</u> software privacy,terrorism, pornography</p> <p><u>Common attacks:</u> keystroke logging, wire tapping, spoofing(DNS,IP,ARP), Hijacking advance spoofing attacks</p> <p><u>Manipulation attacks:</u> shopping cart attacks salami attacks data diddling</p> <p><u>Social engineering:</u> dumpster diving</p> <p><u>Ethics:</u> <u>ISC^2 Code of Ethics</u> – protect society,commonwealth &amp; infrastructure – act honourably,honestly,justly, responsible &amp; legally – provide diligent service&amp; component service – advance &amp; protect profession</p> <p><u>Computer Ethics Institute</u> <a href="http://www.cosrc.org">www.cosrc.org</a> : 10 commandments</p> <p><u>Internet Activities Board</u> RFC 1087 January 87' characterize unethical &amp; unacceptable behaviour</p>	<p><u>UNCRITRAL:</u> Untied Nations Commission International Trade Law WTO World Trade Organization</p> <p>- <u>trade secret</u> - <u>copyright:</u> legal device - <u>trademark:</u> symbol - <u>patent:</u> ownership on design</p> <p><u>Privacy Laws:</u> EU98'€{data is sued only for the purpose it was collected, report over stored data,correction, transmission.} - Computer Fraud and Abuse Act 86' - Federal Sentencing Guideline 91' - Economic Espionage Act 96'* - US Child Pornography Prevention Act 96' - US health Insurance Portability and Accountability Act - US Patriot Act 2001 - Employee Monitoring</p> <p><u>Types of Laws</u></p> <p>- <u>Civil Law (0 tort):</u> against individual &amp; company - <u>Criminal Law:</u> violations of rules (government) - <u>Administrative Law:</u> government imposed standars - <u>Common Law:</u> based on rule of reasonable doubt - <u>Customary Law:</u> - <u>Muslim Law:</u></p>	<p><u>Computer Crime Investigation</u></p> <ol style="list-style-type: none"> <li>1) Plan &amp; prepare by means of procedures</li> <li>2) Secure &amp; isolate</li> <li>3) Record</li> <li>4) Interview suspects &amp; witnesses</li> <li>5) Systematically search</li> <li>6) Collect and seize</li> <li>7) Package &amp; transport evidence</li> <li>8) Submit evidence</li> </ol> <p><u>Incident Response Procedures</u> Information security, legal,HR,PR,physical security,network &amp; system administration,internal auditor.</p> <p><u>Forensics</u> well defined methodology 1) <u>Acquire:</u> bit level copy 2) <u>Authenticate:</u> data unchanged 3) <u>Analyse:</u> document</p> <p><u>Handling Evidence</u> - chain of custody - trace evidence: remnance - drive wiping: overwriting</p> <p><u>Evidence Types</u> relevant,legally permissible,reliable,identifiable,property preserved &amp; documented - Best evidence: e.g. Original documents - Secondary: copy or oral description - Hearsay: second-hand {computer record} - Direct: gathered 5 witnesses senses</p> <p><u>Enticement &amp; entrapment</u>  Enticement: luring activity Entrapment: illegally induce trick</p>

## Physical Security

Environment	Perimeter	Server Placement
<p><b><u>Physical Risk</u></b></p> <p>- <u>Natural Disasters</u>: hurricanes, typhoons, tropical cyclones, tidal waves/tsunamis, floods, earthquakes, tornado's, fire</p> <p>- <u>Man-made-threats</u>: terrorism, vandalism, theft, destruction, criminal activities</p> <p>- <u>Emergency situations</u>: communication loss, utility loss, equipment failure</p> <p><b><u>Requirements for new site locations</u></b></p> <p>- Accessibility</p> <p>- climatology &amp; natural disasters</p> <p>- local considerations</p> <p>- utilities</p> <p>- visibility</p> <p><b><u>Location &amp; Construction</u></b></p> <p><u>Doors, walls, Windows and ceilings</u>:</p> <p><b>Doors</b>: fail safe locks (disengaged lock on case of emergency) no more than 2 doors, solid core doors</p> <p><b>Ceilings</b>: waterproofed, adequate fire rating Electrical &amp; HVAC</p> <p><b>Windows</b>: shatter proofed, opaque, translucent</p>	<p>Fire escapes: practice fire drills fire detection: smoke detectors, sprinklers</p> <p><b><u>Perimeter controls</u></b></p> <p>- fences, gates and bollards</p> <p>- layers defence = defence in depth</p> <p>- Fence 8 feet high with topping of barbed wire (3 layers)</p> <p>- CCTV cameras</p> <p>- Mantraps: prevent piggybacking or tail gating</p> <p>- Card keys:     <i>dumb</i> = badges with photo     <i>smart cards</i> {active electronic, electronic circuit, magnetic stripe, optical coded, photo card}</p> <p>-RFID (Radio Frequency Identification Tags) could be active or passive or both (semi passive)</p> <p>-Lighting: 8 feet high 2-foot candle light</p> <p>-Guards and dogs</p> <p>- Locks {Pre-set key locks, mobile security locks, programmable cipher locks, hostage alarm, delay alarms, master key locks}</p> <p>-Biometric access controls {finger scan, palm scan, hand geometry, iris scan, facial scan}</p>	<p><b><u>IDS</u></b></p> <p>- Photoelectric</p> <p>- motion detectors</p> <p>- pressure sensitive</p> <p><b><u>Environmental controls</u></b> control of temperature, electrostatic, humidity</p> <p><b><u>Electrical Power</u></b> Blackout, burnout, sag, fault, spike, surge, noise, transient, inrush</p> <p>- power conditioners, surge protectors</p> <p><b><u>UPS Uninterruptible power supply</u></b> <u>Online</u>: short term outages <u>Standby</u>: relies on generators longer power outages</p> <p><b><u>Fire Prevention, detection &amp; suppression</u></b> <u>Fire suppression</u></p> <p>- <u>Class A</u>: paper or wood =&gt; water &amp; soda acid - <u>Class B</u>: gasoline or oil =&gt; CO2, halon, soda acid - <u>Class C</u>: electronic or computer =&gt; CO2, halon - <u>Class D</u>: combustible metals =&gt; dry powder</p> <p>!! Halon types 1211 extinguishes or 1201 fixed system !! Replacement of Halon: FM-200, CEA-410, NAF-S-II, FE-13, Argon, Argonite</p> <p><b><u>Water sprinklers</u></b></p> <p>- <u>Dry pipe</u>: no standing water, delay of watering</p> <p>- <u>Wet pipe</u>: full of water, fusible link</p> <p>- <u>Preaction</u>: initially dry, 2 trigger activate water</p> <p>- <u>Deluge</u>: when trigger water comes out</p>

## Security Management Practices

Fundamentals	Standards	Data classification
<p><b><u>Risk assessment:</u></b>                      -overall goal to ensure CIA                      - process of identifying &amp; prioritizing                      - worst bottom up security, best it comes from senior management</p> <p><b><u>Risk management:</u></b>                      Threat,exposer,vulnerability,countermeasure/safeguards, risk, residual risk                      - determined threats                      - {thread,vulnerability,controls}                      =&gt; thread agent is needed for an attack</p> <p><b><u>Risk management team:</u></b>                      all employee in each department                      e.g. {IT security,IT &amp; operations management,system &amp; network administration,internal audit,physical security,business process &amp; information owners,HR,legal,physical safety}</p> <p><b><u>Identifying threads:</u></b>                      - human factors could be internal (employees) or external (virus)                      - natural threads                      threads =&gt; thread agent =&gt;vulnerability</p> <p><b><u>Quantitative Risk Assessment:</u></b>                      1) Estimate potential loss                          Single loss expectancy (SLE)                          SLE= Assset value x exposure factor                      2) Annual rate of occurrence (ARO)                          “Means how often a thread happen”                      3) Annual loss expectancy                          ALE= SLE x ARO</p>	<p><b><u>Qualitative Risk Assessment:</u></b>                      CIA as categories {low,medium,high}                      - Delphi Technique                      - FRAP {Facilitated Risk Assessment Process}                      - IAM (NSA) Information Assurance Methology</p> <p><b><u>Handling Risk</u></b>                      - risk reduction                      - risk transference                      - risk acceptance                      - risk rejection/ avoidance</p> <p><b><u>Policies,Procedures, Standards, Baseline &amp; Guideline</u></b>  <u>Security Policy:</u> high level (meet advisories,informative and regulatory needs)  <u>Advisory Policy:</u> inform about consequences  <u>Informative Policy:</u> inform &amp; enlighten  <u>Regulatory Policy:</u> complies with law</p> <p><b><u>Standards: tactical document</u></b>                      Baseline: minimal level of security                      Guidelines: recommendation or suggestions                      Procedures: “how its done”                      Those 3 issues enforces the security policy</p> <p>Implementation have to come from the top</p> <p>Blueprints – architectural BS 7799                      TCSEC (Trusted Computer Security Evaluation Criteria)                      ITSEC (Information Technology Security Evaluation Criteria)                      =&gt; Common Criteria (ISO 15408)</p>	<p><b><u>Military:</u></b>                      unclassified,sensitive,confidential,secret,top secret</p> <p><b><u>Public/Private:</u></b>                      public,sensitive,private and confidential</p> <p><b><u>Roles &amp; Responsibilities</u></b>                      data owner , data custodian , user, security auditor</p> <p><b><u>Security Controls</u></b>                      Administrative: policies                      Technical: logical mechanism                      Physical: hardware</p> <p><b><u>Training &amp; Education</u></b>                      Triangle of Awareness, Training and education</p> <p><b><u>Security Awareness</u></b>                      Senior Management, data custodians,users</p> <p><b><u>Auditing</u></b>                      sound policies in policies</p> <p>MSR Minimal Security Requirement</p>

## Access Control Systems & Methodology

Fundamentals	Methods	Models
<p><b><u>Threads against access control:</u></b>            Password attacks:            dictionary crack , brute-force {rainbow table}</p> <p>D(DOS)={ping of death,smurf,synflood,trinoo}  <u>Emanation Security</u>            radiation emanate            TEMPEST, noise &amp; control zones are used against</p> <p><b><u>Access Control Types</u></b>            Administrative control: password policies            Technical control: encryption, AV controls            Physical controls: fences, CCTV</p> <p><b><u>Identification, Authentication &amp; Authorization</u></b>            Identification: public piece of information (user name)            Authentication: private piece of information (pin, passphrase)            Authorization: rights of access</p> <p><b><u>IDS (Intrusion Detection Systems)</u></b>            NIDS= Network based intrusion detection system            HIDS= Host based intrusion detection systems            signature based = typical pattern € { model or state based}            behaviour based = learn from network traffic</p> <p>sensor,central monitoring system, report analysis database            &amp; storage components, response</p> <p><b><u>Penetration Testing</u></b>            1) Discovery,enumeration,vulnerability mapping,exploitation</p> <p>Application security testing,DOS testing, war dialing, wireless            network testing, social engineering testing, honeypots</p>	<p><b><u>Authentication:</u></b>            username/password,tokens, smart cards,certificates, magnetic            stripe cards, biometrics</p> <p>Typ 1: something you know =&gt; password            Typ 2: something you have =&gt; tokens, smart cards            Typ 3: something you are =&gt; biometrics</p> <p><b><u>Passwords:</u></b>            Password policy: no personal information, 7-14 character, expire at            least every 30 days, no common words, mix upper and lower case letters            and characters</p> <p>Login attempts should be limited = clipping level</p> <p><u>Cognitive Passwords:</u> sequence of passwords</p> <p><u>Token device:</u> synchronous(SecurID) or asynchronus ( challenge            response)</p> <p>Biometrics € { finger scan, hand geometry, palm scan,retina            pattern, iris recognition, key dynamics}</p> <p>Typ I = false rejection rate            Typ II = false acceptance rate            Typ I= Typ II =&gt; crossover error rate</p> <p><u>Awareness</u>=&gt; employee buy in, age gender or            occupation,physical status</p> <p><u>Strong authentication</u>            combine of methods PIN and passwords</p> <p><b><u>Single-Sign-ON</u></b></p> <p><u>Keberos</u> = {Authentication Service,TGT,TGS}            keberos client = principal            - time sensitive,tokens can be cracked,keberos server single</p>	<p><b><u>Centralized Access Control {RADIUS,TACAS;DIAMETER}</u></b></p> <p><u>RADIUS</u> {Remote Authentication &amp; Dial-in User Server}            udp based RFC 2058/59            3 services = authentication,authorization &amp; accounting            encrypt passwords</p> <p><u>TACAS</u> {Terminal Access Controller Access Control Systems}            TACAS+=CISCO= encrypts all negotiation data</p> <p><u>DIAMETER</u>            capability of authentications (IPSEC)</p> <p><b><u>Decentralized Access Control Administration</u></b>            peer-to-peer relationship            =&gt; hybrid administration</p> <p><b><u>Data Access Controls</u></b></p> <p><u>DAC Discretionary Access Control</u>            - access control to owner discretionary            File &amp; data ownership/access rights &amp; permissions</p> <p><u>MAC Mandatory Access Control</u>            based on predetermined list of access privileges. Access is            determined by system</p> <p>subject = user, system, program or file            object = provide data or information</p> <p><u>RBAC Role Based Access Control</u>            assign rights based on their roles</p>

Fundamentals	Methods	Models
	<p>point of failure</p> <p><u>Sesame</u> use symmetric and asymmetric crypto technique for key exchange PAC</p> <p><u>Thin Clients</u> Client holds no data, server has all data. Once login =&gt;no re authentication</p> <p><u>LDAP</u></p>	<p><u>Others Type of Access Controls</u> Content dependent access controls Lattice based access controlled Rule based access control</p>

## Telecommunication & Network Security

Fundamentals	Methods	WAN components
<p><b><u>Threads:</u></b>  <u>DOS attacks</u> : {ping of death, smurf,teardrop,land, synflood}</p> <p><u>Disclosure attacks</u>: sniffing,arp poisoning, dns spoofing,pharming attack,phishing, war dialing, war driving,spyware,virus,worms</p> <p><u>Destruction attacks</u>: database attacks,cellphone attacks, data diddling, identity theft,password cracking, privilege escalation, salami attack, software privacy, session hijacking,spamming</p> <p><b><u>LAN &amp; Components</u></b>            LAN Local Area Network            WAN Wide Area Network            MAN Metropolitan Area Network</p> <p>most common protocol (85%) Ethernet protocol 75'            IEEE 802.3 (LLC or SNAP) =&gt;Etherframe {64 byte &gt; 1518}            18byte for control =&gt; 46-1500 byte long</p> <p><b><u>Network topologies</u></b>  <u>Bus topology</u>: single cable =&gt; lowspeeds  <u>Star topology</u>: attach on hub, widely use  <u>Ring topology</u>: token ring &amp; FDDI</p> <p><b><u>LAN cabling</u></b>  <u>coaxial cable</u>: copper core,outer jacket, resistant EMS            50-75 Ohm, 10 Base-2(185m), 10 Base 5 (500m)  <u>twisted pair cable</u>:            shielded twisted pair = STP less attenuation than UTP            unshield twisted pair = UTP  <u>Fiber</u>:glass, no EMS,dispersion =&gt; backbone</p>	<p><b><u>Signals</u></b>            Analog signals = carrier signal            Digital signals = square wave signal as carrier = easier to extract</p> <p>Asynchronous communication use start and stop bit            Synchronous communication</p> <p><b><u>Transmission methods</u></b>            unicast: one-to-one transmission            multicast one-to many (radio)            broadcast one-to-all</p> <p><b><u>Cable issues</u></b>            attenuation =&gt; loss of signal strength            cross talk spill over to another wire</p> <p><b><u>Fire rating</u></b>            plenum-rated cables for ceilings            nonplenum: normal use</p> <p><b><u>Broadband &amp; base band</u></b>            broadband: cable into channels {T1,T3.ISDN,ATM,DSL}            base use full cable</p> <p><b><u>Remote access methods &amp; technology</u></b>            NAS network access server (authentication &amp; authorization)            best practice; put all dial ups modems in one place            review yearly,VPN,predetermined, disable if not used            direct (RADIUS) or Internet</p> <p><b><u>Wireless technology</u></b>  <u>WIFI</u>:802.11a 5.15-5.35 to 5.725-7.825 Ghz 54 Mbps            802.11b 2.4-2.28 GHz 11 Mbps            802.11g 2.4 GHz 54 Mps            WAP Wireless access point            WEP Wireless exchange privacy 40 bit RC4</p>	<p><b><u>WAN</u></b>            - packet switching =SVC,PVC            - circuit switching</p> <p><b><u>Packet switching</u></b>            X.25, Frame Relay,ATM,VOIP</p> <p><b><u>Circuit switching</u></b>            plain old telephone services=POTS,ISDN,T-Carriers(T1-T3),DM, cable modem</p> <p><b><u>Network models &amp; standards</u></b>            Physical,Data,network,transport,session,presentation,application =&gt; OSI 8' =&gt; ISO 7498</p> <p><b><u>TCP/IP 82'</u></b>            4 layers:            - network (OSI 1-2)            - internet (OSI 3)            - host-to-host (OSI 4-5)            - application (OSI 6-7)</p> <p>class A: 1.0.0.0-126.255.255.255            class B: 128.0.0.0-191.255.255.255            class C: 192.0.0.0-223.255.255.255            class D: 224.0.0.0-239.255.255.255            class E: 240.0.0.0-254.255.255.255</p> <p>ICMP Internet Control Message Protocol € Internet layer            threads: smurf sourcerouting redirect</p> <p>ARP Address resolution protocol            unauthenticated MAC &lt;=&gt; IP =&gt; Spoofing</p>

Fundamentals	Methods	WAN components
<p><b>Network Equipment</b></p> <p><u>Hubs</u>: everyone can communicate with each other</p> <p><u>Repeater (physical layer)</u> : amplifies signal &amp; extends networks</p> <p><u>Bridge(data layer)</u>: forward frames &amp; filters based on MAC</p> <p><u>Router(Network layer)</u>: separates &amp; connect LAN, filter based on IP port numbers &amp; protocol types</p> <p><u>Brouter(data &amp; network layer)</u>: route packets &amp; forward frames</p> <p><u>Switch(data &amp; network layer)</u>: private virtual link, VLAN, reduces traffic, impedes network sniffing</p> <p><u>Gateway(application layer)</u>: connect different networks perform protocol and format transaction</p> <p><b>Protocols</b></p> <p><u>Hub &amp; Repeaters</u>: MAC based</p> <p><u>Switches</u>: observing source &amp; destination MAC, store-and-forward, cut-through, fragment free, VLAN</p> <p><u>Routers</u>:</p> <p>ACLs determine proper interface</p> <p><u>Distance vector protocols</u>: Bellmann Ford algorithm, RIP Routing information protocol, every 30 sec new table</p> <p><u>Link-state-protocol</u>: Disjkstra alogorithm, best path with metric OSPF Open shortest Path first BGP Border Gateway protocol used on internet TCP</p> <p><b>NAT Network address translation</b></p> <p>- overwhelm IP shortage RFC 1918 10.0.0.0/172.16.0.0/192.168.0</p> <p>Static NAT: one-to one mapping Dynamic NAT pool-of addresses Port address translation PAT: DSL</p>	<p>TKIP Temporal Key Integrity Protocol 256 bit</p> <p><b>Bluetooth belong to PAN (Personal area networks)</b> class 1: less equal than 100m 100mW 2,45Ghz class2: less equal than 20m 2,5mW class3: less equal than 10m 1mW</p> <p><b>Access methods &amp; remote connectivity</b></p> <p><u>PPP Point-to-Point Protocol 94'</u> dial-up connections, replacement for slip, carry only ZP, no detection <u>authentication</u>:</p> <p><u>PAP Password authentication protocol</u> password in clear text 2 way handshake</p> <p><u>CHAP Challenge Handshake authentication Protocol</u> 3-way handshake, MD5 encrypt challenge PW, MS-CHAP storea password encrypted</p> <p><u>EAP extensible authentication protocol</u> digital certificates, token cards, md5 used 802.12i WIFI WPA protocol</p> <p><b>VPN</b></p> <p>PTP/L2TP(Layer 2 Tunnelling protocol)/IPSEC 2 types of tunnels: LAN-to-LAN or Client-to-LAN</p> <p><u>IPSEC "IPV6 include IPSEC"</u></p> <p><u>AH Authentication header</u> protects against modifications</p> <p><u>ESP Encapsulation security payload</u> protects privacy and modification</p> <p><u>IKE Internet key exchange</u> exchange keys</p> <p><u>Transport mode</u>: host-to-host protects pay load</p> <p><u>Tunnel mode</u>: act as gateway protects payload and data</p> <p><b>Message Privacy</b></p> <p>PGP S/MINE Secure Multipurpose Internet Extensions = Mail X505 PEM Privacy Enhanced Mail older Standard</p>	<p><u>Host-to-host layer</u> TCP &amp; UDP protocol TCP: - 3-step setup (syn, sync, ack, ack, data transmission) - 4-step shutdown (fin ack, ack, fin ack, ack)</p> <p>UDP: none handshaking process =&gt; spoofing</p> <p><u>Application layer</u> application support: ftp, telnet, smtp, dns, http, snmp Voice-over IP</p> <p><b>Firewalls</b></p> <p><u>Packet Filtering</u>: pro: scalable high performance, application independent contra: no look into packets, low security, no state connection control</p> <p><u>Proxy Firewall</u> - between trusted and untrusted network - talks directly to outside, one IP address application level proxy FW: 1 per application circuit level proxy: wide variety protocols, header information is evaluated (SOCKS)</p> <p><u>Stateful firewalls</u> each connection has a state table decide allow or not allow tracking connectionless protocol UDP</p> <p><b>Firewall architecture</b></p> <p>- dual home FW out-FW-in DMZ: buffer zone between network Bastion host: locked down € DMZ Screened host: FW protected by a screening packet filter Screened subnet: outer screening router =&gt; FW =&gt; inner screening router =&gt; DMZ and layers of protection</p>

## Application and System development security

Threads	Methods	Language
<p><b>Malicious Code</b>  <u>Viruses and Worm:</u>  Master boot record infection,file infection,macro infection  <u>Worms:</u> no interaction  <u>Virus:</u> need interaction</p> <p><u>Buffer overflow:</u> gain privilege through limit buffers  DOS: smurf,fraggle,teardrop,ping of drop,land,syn attack  DDOS: trinoo,shafi,tribal flood network,TFN”K,stacheldraht</p> <p><u>Malformed Input (SQL injection)</u>  client side validation,cross-site-scripting, direct os commands, path traversal, unicode encoding,url encoding</p> <p>Spyware  Backdoors and Trapdoors: Back office sub7,netbus,beast  <u>Action against</u> change detection  <u>Failure states</u>  fail safe: termination of services or disabling of the system  fail soft: terminate no critical process</p> <p><b>Software</b>  1) Project initiation  2) Functional requirements  3) System design  4) develop and document</p> <p><b>System development Life Cycle</b>  NIST 800-14  1) project initiation  2) development/ acquisition  3) Implementation  4) Operation/Maintance  5) Disposal (run down of application)</p>	<p><u>Certification:</u> technical evaluation and analysis of the security features</p> <p><u>Accreditation:</u> formal process of management approval</p> <p><b>Software development Methods</b>  <u>Waterfall model:</u> developers go back only one step, not for large projects  <u>Spiral model:</u> start design goal,ends with client review, each step risk management =longer 88'  <u>Joint Application Development JAD 77':</u> users workshop environment  <u>Rapid Application Development RAD:</u> poor design =&gt; Delphi and Visual Basic  <u>Computer-Aided Software Engineering CASE</u>  tools and automation,systematic analysis, design and development,prototyping.</p> <p>OLTP Online transaction processing</p> <p><b>Change Management</b>  1) Define Change Management process  2) RFC  3) Plan and document  4) Implement and monitor  5) Evaluate and report  6) Modify if necessary</p> <p><b>Programming Language</b>  <u>Gen 1:</u> machine language  Gen 2: assembly  Gen 3: High level language (PASCAL)  Gen 4: Very high level language ( SQL)  Gen 5: natural language Prolog,LISP</p>	<p><b>Object Orientation Programming</b>  modular form,class,objects, inheritance  encapsulation/polymorphism/polyinistiation</p> <p><u>Corba Common Object request Broker Architecture</u>  middleware, mediate between different programmms ORB  Object Request Broker</p> <p><b>Database management</b>  - hierarchical database management system  -network database MS: lattice struture  -relational database MS: tables, linked key,SQL  -object-oriented database MS:modeling and creation of data as object  !! Interference == deduce information !!</p> <p>DB interface:  OLE,DCOM,ActiveX,JDBC,ADO,ODBC,XML</p> <p><u>Transaction processing</u>  ACID test:  Atomicity,consistency,isolation,durability</p> <p><u>Database terms</u>  aggregation,attribute,field,foreign  key,granularity,relation,tuple,schema,primary key,view</p> <p><u>Database housing</u>  analyse different databases ==&gt; trend analysis</p> <p><u>Data Mining:</u>  process analysing data ==&gt; metadata</p> <p><u>Knowledge Management</u>  databases, document management, business process and IT systems  classification approach, probabilistic, statical</p>

## Business Continuity Planning

Fundamentals	Strategies	BCP
<p><b><u>Type of disasters:</u></b>  <u>natural:</u> earthquake, fire, floods  <u>system/technical:</u> outages, malicious codes, worms, hackers  <u>supply systems:</u> electrical power systems, Equipment outages, utility, problems or water shortages  <u>Human-made/political:</u> disgruntled employees, riots, vandalism, theft =&gt; interruption in operations  <u>Minor:</u> several hours less equal than 1 day  <u>Intermediate:</u> disrupted for a day or longer need secondary side  <u>Major:</u> entire facility destroyed =&gt; new building</p> <p><b><u>Business Continuity Management</u></b>                      - holistic management process identifies potential impacts</p> <p><b><u>Business Continuity Plan (BCP)</u></b>                      goal: minimize outage                      1) project management and initiation                      2) business impact analysis BIA                      3) Recovery strategy                      4) Plan design &amp; development                      5) testing, maintenance, awareness and training</p> <p><b><u>1 Project Management and Initiation</u></b>                      scope of the project, appointment of a project, planner, determination of who will be on the team. Finalize the project plan, determine the data collection method</p> <p><b><u>2 Business Impact Analysis BIA</u></b>                      - select individuals to review                      - methods for gathering information                      - customized questionnaires                      - analyse compiled data                      - determine time critical business process and functions                      - determine max. tolerable downtimes                      - prioritize based on MTD (Maximum tolerable downtime)                      - Document the findings and report your recommendations to management</p>	<p><b><u>Measurement</u></b>                      - allowable business interruption : MTD                      - financial &amp; operational considerations = cost(outages), SLA                      - regulatory requirements: violation of laws, legal penalty                      - organizational reputation</p> <p><b><u>Recovery Strategy</u></b>                      operation can be interrupted in several ways                      - data interruptions =&gt; backups, offsite storage, remote journaling                      - operational interruptions =&gt; loss of equipment, hot sites, RAID, redundant equipment, BPS(Backup Power System)                      - facility &amp; supply interruptions =&gt; fire, loss of inventory                      - business interruptions =&gt; loss of personnel, strike, office space</p> <p><b><u>Best recovery strategy</u></b>                      1. Document all costs for all possible alternative                      2. Obtain cost estimates for any outside service                      3. develop written agreements with vendors for such services                      4. evaluate resumption strategies                      5. documents findings and report management</p> <p><b><u>Plan design &amp; Development</u></b>                      guide for implementation  <u>Objective:</u>                      1. identify critical functions &amp; priorities for restoration                      2. identify support systems needed by critical functions                      3. estimate potential disasters &amp; calculate min. resources                      4. select recovery strategies =&gt; vital personnel, systems                      5. Determine who will manage restoration and testing                      6. calculate cost</p> <p><b><u>Testing, Maintenance, Awareness &amp; Training</u></b>                      5 types of BCP testing                      1. <u>Checklist:</u> copies of plan to each department                      2. <u>Tabletop:</u> engineering &amp; mgt team &amp; business unit managers are walked through the plan.                      3. <u>Walkthrough:</u> actual simulation, test proceeds to point of recovery =&gt; test if anyone is aware of BCP                      4. <u>functional:</u> starts operation at alternative side                      5. <u>full interruption:</u> complete test</p>	<p><b><u>BCP process responsibilities</u></b>  <u>Senior management:</u> project initiation, ultimate responsibilities, overall approval &amp; support  <u>Mid management or business unit manager:</u> identification &amp; prioritization  <u>BCP committee &amp; team members:</u> planning, day-to-day management, implementation &amp; testing  <u>Functional business units:</u> plan, implementation, co-operation &amp; testing</p> <p><b><u>Awareness &amp; Training</u></b>                      design &amp; develop training programs =&gt; save life  <b><u>Disaster Recovery Plan (DRP)</u></b>                      get damaged organization back to business</p> <p><u>Salvage:</u> restoring functionality, damage assessment/salvage operation/repair/restoration  <u>Recovery:</u> get alternate site running</p> <p><b><u>Alternative sites &amp; hardware backup</u></b>                      - <u>reciprocal agreement:</u> 2 organizations, hard to enforce                      - <u>cold site:</u> rooms &amp; rudimentary equipment                      - <u>warm site:</u> cold site + data equipment &amp; cables                      - <u>hot site:</u> ready to go =&gt; expensive</p> <p>Multiple data centres (twin cores)                      Service bureaus: offsite needs to a service bureaus  <u>Other alternative</u>                      - database shadowing: use 2 redundant disk                      - electronic vaulting: copy of backup                      - remote journaling: information process parallel</p> <p><b><u>Software backup</u></b>                      - full backup                      - incremental backup: backup only those files which has been modified, need all tapes                      - differential: backup all files changed since last full backup</p> <p><b><u>Tape rotation strategies</u></b>                      test backup tapes                      simple: one tape a day                      grandfather-son: 4 tapes for weekly backup, 1 tape for month                      tower of hanoi: 5 tapes A-E</p>

## Cryptography Security Technology & Tools

Fundamentals	Ciphers	Assurance, Trust & Confidence Management
<p><b>Attacks:</b> Cryptanalysis: science of breaking ciphers or proof Cryptography: writing secrets, address integrity &amp; confidentiality</p> <p><b>Cryptanalytic attacks against ciphers:</b></p> <ol style="list-style-type: none"> <li><b>cipher text-only attack:</b> sample of ciphertext without plaintext</li> <li><b>know plaintext attack:</b> sample plaintext=sample ciphertext =&gt; recover key</li> <li><b>chosen-plain text attack:</b> sample quantity of plain text =sample ciphertext =&gt; recover key</li> <li><b>adaptive-chosen-plaintext attack:</b> choose plain text dynamically</li> <li><b>chosen ciphertext attack:</b> choose ciphertext = obtain plain text =&gt; recover key</li> <li><b>adaptive chosen ciphertext attack:</b> dynamically ciphertext</li> </ol> <p><b>Brute-force-attack:</b> exhaustive search attacks, separation of keys (eg DES)</p> <p><b>Symmetric Block Cipher Attack</b> (fixed block length pt &amp; ct) - differential Cryptanalysis: chosen pt attack - linear cryptanalysis: known pt attack (behaviour of block cipher, inspect sample of pt to ct) - Weak keys: similarity of keys - algebraic attack: multiple encryption don't result in better encryption</p> <p><b>Stream Cipher attack:</b> keystream XOR plain text = ciphertext. Depend on stream.</p> <p><b>Hash function attacks:</b> 1-way function should be collision free (birthday paradox) message authentication code (MAC) attacks: sophisticated birthday attack Main.in.the-middle: preventable for key exchange with hash functions</p> <p><b>Work factor:</b> amount of time to crack a crypt algorithm</p> <p><b>Block ciphers:</b> fixed-length block plain text are encrypted to fixed length ciphertext, symmetric algo.</p> <p><b>Stream ciphers:</b> keystream XOR plain text = ciphertext example: One-time pad result is used only once</p> <p><b>Hybrid systems:</b> combination of symmetric &amp; asymmetric algorithm</p> <p><b>Substitutions ciphers:</b> replace letter after certain scheme like caesar</p> <p><b>Transposition(Permutation):</b> put text in a grid &amp; transform text Weakness: linguistic patterns are visible =&gt; frequency analysis</p> <p><b>Poly alphabetic ciphers:</b> disguise frequency of letters. Use 3 or more ciphers alphabets (vignere)</p>	<p><b>Information Security &amp; Encryption</b> <b>Security objectives:</b> confidentiality, data integrity, authentication &amp; non-repudiation, availability, entity authentication, data origin, signature, access control, receipt, confirmation, authorization, ownership, certification, revocation, anonymity, validation</p> <p><b>Symmetric key cryptography</b> pro: speed, strength of algorithms, availability of algorithms contra: key management &amp; implementation <math>n*(n-1)/2</math> keys, key exchange, key distribution, scalability, limited security, offer CIA not non-repudiation</p> <p><b>DES</b> invented 77' NIST (National Institute of standards and technology) revise 97' AES Advance encryption standard</p> <p><b>DES simple</b> fixed block size 64 bit = 56 bit &amp; 8 bit for parity 16 rounds of substitution &amp; transposition</p> <p><b>DES Modes (stream ciphers)</b> <b>Cipher Feedback CFB:</b> output is feedback for next encryption level, need initialization vector <b>Output Feedback OFB:</b> final output is feedback for next encryption level.</p> <p><b>DES Modes (Block ciphers)</b> <b>Electronic Code Book ECB:</b> sequentially split text in 64 bit chunks &amp; decrypt it. <b>Cipher Block Chaining CBC:</b> IV(64 bit randomly), encrypt it with DES, XOR with the 64 bit chunks, encrypt output with DES Next IV=ciphertext(n-1)</p> <p><b>Double DES &amp; Triple DES</b> <b>Double DES:</b> 2 separate keys, size doubling to 112 bit. Man-in-the-middle-attack reduce 2 DES = DES <b>Triple DES 2-3 keys:</b> DES-EEE3: 3 DES encryption with 3 keys DES-EDE3: 3 DES operation with 3 keys DES-EEE2/EDE2: 163 use same key <b>Rijndael/AES:</b> key length is variable (128, 192, 256) /block size variable(128, 192, 256) /rounds(10-14)</p>	<p><b>Digital Signatures:</b> based on asymmetric algorithm and hashes, known as principle of irreversibility <b>Creation:</b> hash value (signed message &amp; private key) <b>Verification:</b> verify by private key &amp; compute a new hash of the message are both correct than signature valid</p> <p><b>Properties of digital signatures:</b> signer authentication, message authentication, affirmative act, efficiency (signature is from signer)</p> <p><b>Public key certificates &amp; certificate authorities</b> Trusted third party=CA (certificate authority) PKI (public key infrastructure) user referred to a CA (issue &amp; verify certificate) RA verify certificate directories where data is held (LDAP, X.500)</p> <p>CA, CR, CREVOC, ESCROW, Key update, Certificate management</p> <p>- <b>CR certification repository:</b> X.500.LDAP, Web srv, FTP, DNS, corporate DB -key backup &amp; recovery (escrow) -automatic key update (updating user certificates) -key history -cross certification -non-repudiation -time-stamping -client software</p> <p><b>PKI Core Services</b> Authentication, Integrity and Confidentiality <b>PKI enabled services</b> CA, CR, certificate revocation, key backup, key recovery, key update, key history, cross certification, clients software, authentication, integrity, confidentiality, secure time stamping, notarization, non-repudiation, secure data, archive, privilege/policy creation &amp; verification</p> <p><b>Core Service (CIA)</b> <b>Information Protection &amp; management services</b> -key management -key generation -distribution transferring the key -installation: get key in the storage of the process who needs them</p>

Fundamentals	Ciphers	Assurance, Trust & Confidence Management
<p><b><u>Secure TCP/IP Protocols</u></b>  <u>Application Layer:</u>  SSH,S-HTTP(individual),SET(Secure electronic transaction VISA)  <u>Transport &amp; Internet Layer:</u>  SSL(Framework fro communication, certificates,encrypted data),TLS(Transport Layer Security) encrypts communication between host &amp; client, TLS record protect &amp;TLS handshake</p> <p><b><u>IPSEC(Internet protocol security)</u></b>  ESP(encapsulated secure data)= confidentiality of data  AH(Authentication header): integrity &amp; authentication hash over message  ICV(Integrity check value)  SA(Security Authorization):Management for exchange of cryptographic information  IKE=Internet key exchange  exchange of key information(sym.keys)  consists ISAKMP(Internet Association &amp;key management protocol) algorithms &amp; key generation  OAKLEY carry out negotiations  Transport mode =Data encrypted &amp; tunnel mode = data and header encrypted</p> <p><b><u>Lower-layer cryptographic solution</u></b>  PAP (Password authentication protocol): user/password in clear text  CHAP(Challenge Handshake Authentication Protocol): client &amp; server know predefine password,verify user/password nothing in clear text  PPTP(point-to-point protocol): Port 1723,2 components transport &amp;encryption 40-bit or 128 bit</p> <p><b><u>Moving data</u></b>  end-to-encryption: encrypt message&amp; data packet header &amp; IP address are clear =&gt; speed +  Link encryption: encrypts all data, all intermediate devices must have additional software</p>	<p><b><u>IDEA(International Data Encryption algorithm)</u></b>  64 bit divided into 4 subblocks=input for first round. Result is xored with the result of other rounds</p> <p><b><u>RC5(Ron Rivest)</u></b>  50% quicker than DES/variabel block size(32,64,128)/key size (0-2040)/rounds(0-255)</p> <p><b><u>RC6</u></b>  inclusion integer multiplication &amp; 4 bit working register</p> <p><b><u>Asymmetric Cryptography</u></b>  70' diffie/Hellmann public/private key, based on trapdoor function,discrete logarithm,factor problem or elliptic curves (NP-hard)</p> <p><b><u>RSA(Rivest shamir Adelman)</u></b>  factoring 768/1024 provide Encryption &amp; signature</p> <p><b><u>ElGamal</u></b>  discrete logarithm 768/1024 provide Encryption &amp; signature</p> <p><b><u>DSA</u></b>  (FIPS 186 512 1024) signature</p> <p><b><u>Diffie-Hellmann</u></b>  768/1924 key exchange</p> <p><b><u>Merkle-Hellmann-Knapsack 78'</u></b>  selecting number of objects with given weigthts</p> <p><b><u>Chior-Rivest.Knapsack 84'</u></b>  don't use modular multiplication</p> <p><b><u>LUC</u></b>  NZ best feature EL Galmal,RSA &amp; Diffie</p> <p><b><u>Message Integrity Controls</u></b>  <u>MIC Message Integrity Code</u>  <u>MDC Modification Detection Code</u>  use hash functions produce message digest  hashes(SHA-1,HMAC,MD5.HMAC-MD5,HAMC-SHA-1)  <u>MAC Message Authentication Code</u>  message fingerprint use by a secret key</p>	<ul style="list-style-type: none"> <li>- Change: how long is key valid</li> <li>- Control: management use of key</li> <li>- Disposal :key should be disclosed</li> </ul> <p><b><u>Principles of key management</u></b></p> <ol style="list-style-type: none"> <li>1. key mgmt should be automated</li> <li>2. no key should ever appear in clear</li> <li>3. key should be randomly chosen from a big key space</li> <li>4. key encrypting keys must be separated from data Encryption keys</li> <li>5. key with long lifetime should be sparsely used</li> </ol> <p><b><u>Cryptographic Services</u></b>  <u>Secure Email:</u> digital signatures  <u>S/MIME:</u> Secure Multi-purpose Internet Mail Extension support X.509 and RSA  <u>PEM Privacy Enhanced Mail:</u> Provide authentication MD2/MD5 &amp; RSA  <u>MSP Message Security Protocol:</u> military answer to PEM provides authentication,integrity and non-repudiation.  <u>PGP Pretty Good Privacy:</u> Web of Trust no CA</p> <p><b><u>Laws</u></b>  <b><u>COCOM (Coordinating committee for multilateral export controls)</u></b>  prevents export of cryptography to dangerous countries,excluded from this regulation is mass market cryptography(public domain) First enact at 91 dissolved 94'  <b><u>Waasenaar Arrangement</u></b>  Enact 95' as follow up of COCOM. Control weapons &amp; dual use gods. Revise 98' with some relaxation(export sym. Crypt alg. Up to 56 bit, mass market crypt,DVD crypt &amp; license crypt)  <b><u>EU Controls</u></b>  - export under EU states is liberalized(general Intra community license)  - export to Australia,Poland, US (Community general export authorization)  - other countries (general national license)  <b><u>United State Controls</u></b>  no import restriction to US  - export regulation depend on the Waasenaar Arrangement  - revise 200 to EU  (any crypt key can be exported after a review/retail crypt o fro special user/opensource/subsidiaries</p>