The International CISSP Summary
Swedish edition

Den internationella CISSP sammanfattningen

Skriven av
John Wallhoff (CISA, CISSP)

Översatt av
John Wallhoff (CISA, CISSP)

1 Introduktion

Förversionen av ***The International CISSP Summary*** skrevs som ett projekt i samband med förberedelser inför CISSP certifieringen, vilken publicerades under namnet "CISSP Summary 2002" på CISSP Open Study Group, www.cccure.org 2002. Detta har resulterat i förfrågningar från hela världen, från personer som varit tacksamman för dokumentet, har haft kommentarer på olika ämnen eller som enbart behövde en version som gick att skriva ut.

En dag fick jag en förfrågan om sammanfattningen kunde översättas till Japanska. Eftersom CISSP examinationen inte är tillgänglig på något annat språk än Engelska, såg jag detta som en utmärkt ide för att stödja tillväxten och införandet av CISSP certifieringen. Jag kom även att tänka på andra språk som det skulle vara intressant att ha översättningen gjord för.

Målet med detta projekt är att få "The International CISSP Summary" översatt till så många språk som möjligt, men fortfarande behålla designen och strukturen på samma sätt. Det är inte skrivet för att ersätta CISSP seminarier och böcker som är tillgängliga, istället är det en checklista över alla de olika ämnen som omfattas av de 10 CBK domänerna.

Summering omfattar alla tio Common Body of Knowledge Domains (CBK) som krävs för CISSP examinationen. Jag har också lagt till en sida för relaterade länkar och referenser som kan vara användbara. Sidan är långt från komplett och det finns mycket mer att finna.

Min rekommendation till den som planerar en examination är att upprätta en egen studieplan. Några av er har kanske redan varit inblandade i alla domäner tidigare, men jag gissar att flertalet av er kommer att finna några domäner enklare och andra svårare. Jag förberedde mig under 2 ½ månad på min lediga tid (sent på kvällen när barnen gått och lagt sig), hela tiden osäker på om jag läst för mycket eller för lite. Jag klarade min examen, men fortfarande vet jag inte om jag läst för mycket eller för lite.

Sist men inte minst för dina förberedelser. En gång i tiden berättade en lärare på universitet för min klass "fyra inne – fem ute". Det var inte hur många timmar som du skulle använda för din examen. Om du sov fyra timmar varje natt, skulle du troligtvis klara det. Om du sov fem timmar, var det troligt att du misslyckades. Till din tröst sov jag mer än fem timmar varje natt och jag klarade det. Så för alla er som förbereder er för examen, kvalitet i tid är mycket bättre än kvantitet.

Lycka till för alla er som fortfarande är övertygade om att klara examen.

November 2002

John Wallhoff

2 Index

3 CBK#1 Åtkomstkontroll system & metoder

3.1 Säkerhetsprinciper

Konfidentialitet:
Försäkaran om att information inte har avslöjats för ej godkända individer, program eller processer.
Integritet:
Information måste vara riktig, komplett och skyddad från icke godkänd förändring.
Tillgänglighet:
Information, system och resurser behöver vara tillgängliga för användare på ett lämpligt sätt för att produktiviteten inte påverkas.

3.2 Identifiering

Beskriver metoder för att försäkra att ett subjekt (användare, program eller process) är den enhet som den gör anspråk på att vara. Identifiering kan verifieras genom att använda sig av referenser.

3.2.1 Biometri

Verifierar en individs identitet genom ett unikt personligt kännetecken, vilket är är en av de mest effektiva och korrekta metoder för att verifiera identitet.

Tre centrala prestandamått -
- FRR / Felaktigt avvisande tal[1] eller Typ I fel – Procentsatsen för giltiga subjekt som avvisas felaktigt.
- FAR / Felaktigt accepterande tal[2] eller Type II fel – Procentsatsen för subjekt som felaktigt accepteras.
- CER / Korsvis feltal [3]– Procentsatsen där felaktigt avvisande tal är lika med felaktigt accepterande tal.

Andra faktorer som måste beaktas -
- Registreringstid – Tiden det det tar för att initialt "registrera" i ett system genom att presentera ett exempel av biometriskt karaktärsdrag för utvärdering.
- Genomströmningstal- Talet som anger hur många individer som kan bearbetas och identifieras eller autensieras av ett system.
- Acceptans – Övervägande om privatliv, intrångs- och psykologiskt- och fysiskt-välbefinnande när systemet används.

Typer av biometrisystem -
Fingeravtryck: Skapas av åsar och grenar som visar sig av slitningariåsar och andra detaljerade karaktärsdrag som kallas för "minutiae".
Scanning av handflata: Handflatan har veck, åsar och skåror som är unika för en specifik person.
Hand geometri: Formen av en persons hand (längd och vidd av hand och fingrar) mäter handens geometri.
Retina scan: Avläsning av blodkärls mönster i retina längst bak i ögongloblen.
Iris scan: Avläsning av de färgade delarna av ögat som omgärdar pupillen.

[1] False Rejection Rate
[2] False Acceptance Rate
[3] Crossover Error Rate

Signatur dynamik: Elektriska signaler avseende hastighet och tid som kan fångas när en person skriver en signatur.
Tangentbordsdynamik: Fångar elektriska signaler när en person skriver en speciell fras
Röstavtryck:Urskiljer olika skillnader i människors talljud och mönster.
Ansikts scanning: Tar attribut och karatärsdrag som benstrukturer, näsåsen, ögonavstånd, pannstorlek och form på haka i beräkning.
Hand topologi: Ser på storleken och bredden för en individs hand och fingrar.

3.3 Autentiering

Subjektet krävs att visa en andra del av referens uppsättning.
Passerkoder:
Är en skyddad sträng av tecken som används för att autensiera en individ.
Klippningsnivå – Ett tillåtet antal felaktiga inloggningsförsök som måste inträffa innan en användare blir utelåst.
Passerkods testare – Test av användarvalda lösenord.
Passerkods generatorer – Generatorer som skapar användares lösenord.
Passerkods åldrande – Utgångsdatumet för passerkoder.
Begränsat antal inloggningsförsök – Tröskel inställd för att endast tillåta ett bestämt antal misslyckade inloggningsförsök.
Kunskapsmässiga passerkoder:
Fakta eller uppfattningsbaserad information som används för att verifiera en individs identitet.
Engångs lösenord / dynamiska lösenord:
Efter att passerkoden har använts, är den inte längre giltigt.
Token enheter:
Är en passerkodsgenerator och tillsammans med autensieringstjänsten den behöver vara synkroniserad med eller använda samma utmaning-svars[4] schema för att kunna autensiera en användare.
Synkrona token enheter – Synkroniserar med autensieringstjänsten genom att använda tid eller en händels som kärnkomponent i autensieringsprocessen.
Tidsbaserade synkrona token enheter – Enheten och autensierings tjänsten måste hålla exakt samma tid inom sin interna klocka.
Händelse synkronisering – Användaren måste initiera inloggningssekvensen på datorn och trycka på en knapp på token enheten.
Asynkrona token enheter – Använder utmaning-svars schema för att kommunisera med autensieringstjänsten.
Kryptografiska nycklar:
Bevisa en identitet genom att presentera en privat nyckel eller en digital signatur.
Passerfraser:
Är en sekvens av tecken som är längre än en passerkod. Användaren skriver denna fras i en applikation och applikationen översätter värdet till en virtuell passerkod.
Minneskort:
Ett kort som sparar information, men som inte bearbetar information.
Smarta kort:
Ett kort som har förmågan att bearbeta information eftersom det har en mikroprocessor och integrerad krets införlivad i själva kortet.
Ett smart kort förser en två faktors autensieringsmetod, eftersom användaren måste registrera en användaridentitet och PIN kod för att låsa upp den smarta enheten.

[4] challenge-response

3.4 Auktorisation

Ger åtkomst för ett subjekt till ett objekt efter att subjektet har blivit riktigt identifierat och autensierat.
Behov-att-veta[5]:
Användare behöver endast ha nödvändiga rättigheter och tillstånd som de behöver för att kunna fullgöra förpliktelser med deras arbete inom företaget.

3.5 Enkel påloggning[6]

Förmåga som tillåter en användare att registrera referenser en gång och kunna få tillgång till alla resurser i primära och sekundära domäner.
Skript:
Batchfiler och skript som innehåller varje användares ID, passerkod och påloggnings kommando som är nödvändiga för varje enskild platform.
Eftersom skript innehåller referenser, måste de lagras i en skyddad area och överföringen av skript måste hanteras försiktigt.
Kerberos:
Använder symetrisk nyckelkryptering och ger säkerhet ände-till-ände, vilket innebär att information överförs mellan en användare och tjänsten är skyddade utan utan något behov av mellanliggande komponenter.
Huvud komponenter -
- KDC / Key Distribution Center:
Lagrar alla användares och tjänsters kryptografiska nycklar. Erbjuder autensieringstjänster, såväl som nyckeldistributions funktionalitet. KDS utrustar säkerhetstjänster till enheter som kan refereras som uppdragsgivare, vilka kan vara användare, applikationer eller tjänster.
En biljett skapas av KDC och ges till en uppdragsgivare, när uppdragsgivaren behöver autensiera en annan uppdragsgivare.
En KDC utrustar säkerhetsjänster för en uppsättning komponenter och uppdragsgivare. Detta kallas värld/rike i Kerberos.
- AS / Authentication Service:
Är den del av KDC som autensierar en uppdragsgivare.
- TGS / Ticket Granting:
Är den del av KDC som skapar biljetter och överlämnar dem till uppdragsgivaren.
Svagheter -
KDC är en enskild punkt för fel[7]
AS måste kunna hantera en stor mängd förfrågningar.
Hemliga nycklar sparas temporärt på användares arbetsstationer.
Sessionsnycklar avkrypteras och ligger på användarens arbetsstationer.
Är sårbar för lösenordgissning.
Nätverkstrafiken är inte skyddad.
När en användare ändrar sitt lösenord, förändras den hemliga nyckeln och KDS måste uppdateras.
SESAME:
Använder publik nyckelkryptering för att distribuera hemliga nycklar.
Använder en biljett för auktorisation, vilken kallas för Priviligerat Attribut Certifikat[8]
Är sårbar för lösenordsgissning.
Tunna klienter:

[5] *Need-to-know*
[6] Single Sign-on
[7] single point of failure
[8] Privilege Attribute Certificate

Dumma terminaler som autensierar sig mot en server.

3.6 Åtkomstkontroll modeller

Är ett ramverk som dikterar hur subjekt ges åtkomst till objekt.
DAC / Discretionary Access Control:
Gör det möjligt för ägaren till en resurs att specificera vilket subjekt som kan få åtkomst till specifika resurser.
Åtkomst är begränsat med utgångspunkt från den auktorisation som beviljas till användare.
Det vanligaste införandet av DAC är genom ACL listor.
MAC / Mandatory Access Control:
Användare får ett säkerhetsgodkännande och data är klassificerad.
Klassificeringen sparas i säkerhetsmärket för resursen.
När systemet tar ett beslut om uppfyllande av en förfrågan att ges åtkomst till ett objekt, utgår det från godkännandet av subjektet och klassificeringen av objektet.
Modellen används i miljöer där informationsklassificering och konfidentialitet är absolut viktigast.
Känslighetsmärken:
När MAC används måste varje subjekt och objekt ha ett känslighetsmärke. Det innehåller klassificering och olika kategorier. Klassificeringen indikerar den känslighetsnivå och kategorierna indikerar vilka objekt som tar till sig av klassficeringen.
RBAC / Rollbaserad åtkomstkontroll[9]:
Kallas även för "nondiscretionary access control".
Använder en centraliserad adminstrationsuppsättning av kontroller för att bestämma hur subjekt och objekt påverkar varandra.
Tillåter åtkomst till resurser baserade på den roll som användaren har i företaget.
RBAC modeller kan använda -
- Rollbaserad åtkomst[10]: Bestäms av rollen användaren har inom företaget.
- Uppgiftsbaserad åtkomst[11]: Bestäms av uppgiften som tilldelats till en användare.
- Gallerbaserad åtkomst[12]: Bestäms av det känslighetsmärke som tilldelats till rollen.

3.7 Åtkomstkontroll tekniker och teknologier

Tekniker och teknologier tillgängliga för att stödja olika åtkomst kontroll modeller.
Rollbaserad åtkomstkontroll:
Utgår från den uppgift och ansvar som individer behöver för att utföra och fullgöra skyldigheter i deras position i företaget.
RBAC kan användas med -
- DAC, administratörer kan utveckla roller och ägare kan besluta om dessa roller kan ha tillgång till deras resurser.
- MAC, roller kan utvecklas och känslighets märken tilldelade till dessa roller indikerar deras känslighetsnivå.

Regelbaserad åtkomstkontroll[13]:
Utgår från specifika regler som indikerar vad som kan och inte kan hända med ett objekt.
En en typ av MAC eftersom administratören fastställer regler och användare kan inte förändra dessa kontroller.
Begränsade gränssnitt:

[9] *Role-based access control*
[10] Role-based access
[11] Task-based access
[12] Lattice-based access
[13] *Rule-Based Access Control*

Begränsade användares åtkomstförmåga genom att inte tillåta dem att begära vissa funktioner, information eller ha tillgång till specifika system resurser.
Tre typer av begränsade gränssnitt -

- Menyer och skal: Användare ges möjlighet till de kommando som de kan utföra.
- Databasvyer: Är mekanismer som används för att begränsa användar åtkomst till data som ryms i databaser.
- Fysisk begränsade gränssnitt: Kan införas genom att endast förse vissa nycklar på en nyckelplatta eller berörings knappar på en skärm.

Åtkomstkontroll matris:
Är en tabell av subjekt och objekt som indikerar vilka aktiviteter individuella subjekt kan utföra på individuella objekt.
Är vanligtvis ett attribut av DAC modeller och åtkomsträttigheter kan tilldelas direkt till subjektet (förmåga) eller till objektet (ACL listor).

Förmågetabeller:
Specificerar åtkomsträttigheter ett särskilt subjekt kan äga tillhörande specifika objekt.
Subjektet är bundet till förmågetabellen.
Används i Kerberos.
Åtkomstkontrollistor:
Är listor av subjekt som är autoriserade att få åtkomst till ett specifikt objekt och de definierar vilken nivå av autorisation som beviljas.
Auktorisation kan vara specifierad till en individ, roll eller grupp.
Innehållsberoende åtkomstkontroll:
Åtkomst till objekt bestäms av innehållet i objektet.

3.8 Åtkomstkontroll administration

Centraliserad:
En enhet (avdelning eller individ) är ansvarig för att bevilja alla användare till resurser.
Ger en konsistens och enhetlig metod för att kontrollera användares åtkomsträttigheter.
Exempel på centraliserad åtkomstkontroll tekniker:
- Radius / Remote Authentication Dial-in User Service:
Är ett autensieringsprotokoll som autensierar och auktoriserar användare, vanligtvis uppringda användare.
- TACACS / Terminal Access Controller Access Control System:
Är ett klient/server protokoll som ger samma funktionalitet som Radius.
Tre generationer -

* TACACS – Kombinerar autensiering och auktorisation
* XTACACS – Separerar autensiering, auktorisation och redovisningsprocesser
* TACACS+ - Separerar autensiering, auktorisation och redovisningsprocesser, med utökad två-faktor användar autensiering.

Decentraliserad och distribuerad åtkomst administration:
Ger kontroll över åtkomst till människor närmare resurserna.
Ger inte enhetlighet och rättvisa över organisationer.
Exempel på decentraliserade tekniker för åtkomstkontroll administration:
Säkerhetsdomän -
Kan beskrivas som ett rike av förtroende.
Alla subjekt och objekt delar gemensamma säkerhetspolicy, procedurer och regler och de är styrda av samma ledningssystem.
Varje säkerhetsdomän är olika beroende av olika policy och ledningen förvaltar det.

Kan införas i hierarkiska strukturer och relationer.
Används inom operativsystem och applikationer för att säkerställa att fientliga aktiviteter inte av olyckshändelse förstör viktiga systemfiler och processer.
Skydd av säkerhetsnivåer görs genom segmentering av minnesutrymme och adresser.
En säkerhetsdomän kan också beskrivas som resurser som är tillgängliga för en användare.
Hybrid:
Är en kombination av centraliserad och decentraliserad åtkomstkontroll administraions metod.

3.9 Åtkomstkontroll metoder

3.9.1 Administrativa kontroller

Policy och rutiner -
Är plan på hög nivå som definierar ledningens målsättning angående hur säkerhet bör utföras inom en organisation, vilka aktiviteter är acceptabla och vilken risknivå som företaget är beredd att acceptera. Ledningen skall besluta om DAC, MAC eller RBAC åtkomstmetoder bör användas och om det borde administreras genom centralisering eller decentralisering.

Personliga kontroller -
Indikerar hur anställda förväntas att interagera med säkerhetsmekanismer samt icke efterlevnadsärende avseende dessa förväntningar.
- Uppdelning av arbetsuppgifter: En enskild individ kan inte utföra en kritisk uppgift ensam som kan bevisas vara bestämmande för företaget.
- Kollision: Mer än en person behövs för att utföra ett bedrägeri och denna prestation behöver utföras i samförstånd med varandra.
- Roterande arbetsuppgifter: Människor vet hur de skall fullgöra sina skyldigheter för mer än en tjänst.

Övervaknings struktur -
Varje anställd har en överordnad att rapportera till och den överordnade är i sin tur ansvarig för den anställdes handlingar.
Säkerhetsmedvetenhets utbildning -
Människor är vanligtvis den svagaste länken och orsakar de flesta säkerhetsluckorna och blottställningar.
Tester -
Alla säkerhetskontroller och mekanismer behöver testas på periodisk nivå för att försäkra att de ordentligt stödjer säkerhetspolicyn, mål och syfte som definierats för dem.

3.9.2 Fysiska kontroller

Nätverks separation -
Kan utföras genom fysiska eller logiska medel.
Omgivningssäkerhet -
Mekanismer som förser fysisk åtkomstkontroll genom att ge skydd för individer, lokaler och komponenter inom lokalerna.
Dator kontroll -
Fysiska kontroller installerade och konfigurerade.
Arbetsområdes seperation -
Kontroller som används för att stödja åtkomstkontroll och den övergripande säkerhetspolicyn för företaget.

Data säkerhetskopia[14] -
Garanterar åtkomst till information vid händelse av en olycka eller avbrott i nätverk eller ett system.
Kablar -
Alla kablar behöver vägledas genom hela lokalen på ett sätt som inte är i människors väg eller som skulle kunna utsättas för någon fara för att bli klippta, brända, veckade eller avlyssnade.

3.9.3 Logiska kontroller

System åtkomst -
En teknisk kontroll som kan tvinga fram åtkomstkontroll mål.
Nätverksarkitektur -
Kan konstrueras och tvingas genom flera logiska kontroller för att förse separation och skydd av en miljö. Kan segregeras fysiskt och logiskt.
Nätverksåtkomst -
Åtkomst till olika nätverkssegment bör vara grovkornig[15] i sin natur. Router och switchar kan användas för att försäkra att endast vissa typer av trafik släpps igenom till varje segment.
Kryptering och protokoll -
Arbetar som tekniska kontroller för att skydda information medan den passerar genom ett nätverk eller ligger på datorer.
Kontroll zon -
I en specifik area som omger och skyddar nätverksenheter som lämnar ifrån sig elektriska signaler.
Tekniska kontroller som separerar aktiviteter inom ett nätverk, på en nätverksenhet eller på en specifik dator.

3.10 Åtkomstkontroll typer

(P – Fysiska[16] / A – Administrativa[17] / T – Tekniska[18])

Förebyggande: Kontroller som används för att upptäcka och undvika att oönskade händelser inträffar.
P - Fönster, lås, namnbrickor, säkerhetsvakter, biometri system, rävsax[19] dörrar, belysning, intern TV[20], larm.
A – Säkerhetspolicy, bevakning och övervakning, uppdelning av arbetsuppgifter, arbetsrotation, informationsklassificering, personalrutiner, tester, säkerhetsmedvetenhets utbildning.
T – Åtkomstkontroll listor[21], kryptering, IDS, antivirus programvara, brandväggar, smarta kort, återuppringnings system.

[14] Backup
[15] granular
[16] Physical
[17] Administrative
[18] Technical
[19] Mantrap
[20] CCTV
[21] ACLs

Upptäckande: Kontroller som används för att identifiera oönskade händelser som har inträffat.
P – Säkerhetsvakt, biometri system, rörelse detektorer, intern TV, larm, säkerhetskopior.
A – Bevakning och övervakning, arbetsrotation, personalrutiner, utredningar, säkerhetsmedvetenhets utbildning.
T - Revisionsloggar, IDS, antivirus programvara, brandväggar.

Korrigerande: Kontroller som används för att korrigera oönskade händelser som har inträffat.
P - Staket, lås, namnbrickor, säkerhetsvakt, biometri system, rävsax dörrar, belysning, intern TV, larm.
A – Säkerhetspolicy.
T - IDS, antivirusprogramvara.

Avskräckande: Kontroller som används för att avskräcka säkerhetsöverträdelser.
P - Säkerhetskopior.
A – Bevakning och övervakning, uppdelning av arbetsuppgifter, personal rutiner.
T - Kryptering, IDS, brandvägg.

Återställande: Kontroller som används för att återställa resurser och förmågor
P - Staket, lås, säkerhetsvakt, rävsax dörrar, belysning, larm.
A -
T - Antivirus programvara.

Kompenserande: Kontroller som används för att förse alternativ till andra kontroller.
P -
A – Bevakning och övervakning, personal rutiner.
T -

Granskning av revisions information:
Revisions reducering – Reducerar mängden av information inom en revisionslog.
Varians-detektions verktyg – Övervakar trender för dator och resursanvändande och upptäcker variationer.
Attack signaturs upptäckande verktyg – Applikationen har en databas av information som har lärt sig att upptäcka specifika attacker.

Tangentbords övervakning:
Granskning och samling av tangenttryckningar som skrivs av en användare under en pågående session.

3.11 Åtkomstkontroll bevakning

IDS / Intrångs detektering:
Nätverks-baserad – Bevakar ett nätverk eller ett segment av nätverket.
Värd-baserade: Bevakar ett specifikt system.
Kunskaps-baserade / signatur-baserade – Modeller över hur attacker utförs och utvecklas.
Beteendemässigt-baserade / statistiska – Observerar och upptäcker avvikelser från förväntat beteende hos användare och system.
TIM / Tidsbaserade framkallade maskiner[22] – utför upptäckande av onormala händelser i realtid.

[22] Time-based induction machine

Honungsställe[23] – Ett falskt system som inte är låst och som har öppna portar och tjänster tillgängliga inom nätverket.
Nätverks sniffers – Är en sorts avlyssning som ansluts till nätverket i syfte att avlyssna nätverkstrafik.

3.12 Hot mot åtkomstkontroll

Attacker med ordlistor[24]:
Program som möjliggör för en attackerare att identifiera användarreferenser. Programet förses med listor av vanligt använda ord och kombinationer av tecken och programmet använder dessa värden i inloggningsfältet.
Attack med rå kraft[25]:
En attack som kontinuerligt testar olika indata för att uppnå ett fördefinierat mål. Används också i krigsringnings[26] försök.
Lura vid inloggning[27]*:*
Ett program som presenterar en flask inloggningsskärm, för att få tag på användarreferenser.

[23] Honeypot
[24] *Dictionary attack*
[25] *Brute Force Attack*
[26] wardialing
[27] *Spoofing at Login*

4 CBK#2 Telekommunikation & nätverks säkerhet

4.1 Öppen system förbindelse modell

Protokoll – En standard uppsättning av regler för att bestämma hur system skall kommunicera över nätverket.

OSI modell	**TCP/IP**
Applikation	Applikation
Presentation	
Session	
Transport	Värd-till-värd[28]
Nätverk	Internet
Datalänk	Nätverks åtkomst[29]
Fysisk	

Varje lager lägger till sin egen information till datapaketet.

4.1.1 7. Applikations lagret[30]

Bearbetar och formaterar ordentligt data och skickar det vidare ner till nästa lager.
Protokoll som används - SMTP, HTTP, LPD, FTP, WWW, Telnet, TFTP.

4.1.2 6. Presentations lagret[31]

Förser ett allmänt medel för att representera data i en struktur som kan bearbetas ordentligt av slutsystemet.
Formatterar grafik till TIFF, GIF eller JPEG.
Hanterar datakomprimering och kryptering.

4.1.3 5. Sessions lagret[32]

Etablerar en anslutning mellan två datorer, upprätthåller denna medan data överförs och kontrollerar nerstängning av anslutningen.
Protokoll som används - SSL, NFS, SQL, RPC

4.1.4 4. Transport lagret[33]

Förser med början-till-slut transport tjänst och etablerar den logiska anslutningen mellan två kommunicerande datorer.
Protokoll som används - TCP, UDP, SPX
Information skickas ner från olika enheter i ett högre lager till transport lagret, vilket måste sätta ihop informationen till en ström.

[28] Host-to-host
[29] Network Access
[30] Application layer
[31] Presentation layer
[32] Session layer
[33] Transport layer

4.1.5 3. Nätverks lagret[34]

Infogar information i paketens huvud så att det ordentligt kan transporteras.
Protokoll som används - IP, ICMP, RIP, OSPF, BGP, IGMP.
Protokoll som arbetar i detta lager ger inte någon försäkran om leverans av paketen.

4.1.6 2. Datalänk lagret[35]

Operativsystemet formaterar dataramen[36] för ordentlig överföring över nätverk (Token Ring, Ethernet, ATM or FDDI).
Protokoll som används - SLIP, PPP, RARP, L2F, L2TP, FDDI, ISDN.
Varje nätverksteknik har definierat elektronisk signal och bit mönster.

4.1.7 1. Fysiska lagret[37]

Konverterar bitar till volt för överföring.
Standard gränssnitt - HSSI, X.21, EIA/TIA-232, EIA/TIA-449.
Sessions lagret möjliggör kommunikation mellan två datorer i tre olika former:
- Simplex: Kommunikation genomförs i en riktning.
- Half-duplex: Kommunikation genomförs i båda riktningarna, men endast ett system åt gången kan skicka information.
- Full-duplex: Kommunikation genomförs i båda riktningar och båda system kan skicka information samtidigt.

4.2 TCP/IP - Transmission control protocol/Internet protocol

IP:
Dess huvuduppgift är att stöjda Internet adressesering och vidarebefordring paket och rutt
Det är ett anslutningslöst protokoll som kuverterar data som det får från transport lagret.
TCP:
Är ett tillförlitligt och anslutnings-orienterat protokoll, som försäkrar att paket levereras till destinations datorn.
Om ett paket förloras under överföring, har TCP förmågan att sända det på nytt.
Förser tillförlitlighet och försäkrar att paketet är levererat.
Det finns mer överflöde i TCP paketet.
Data – Ström -> Segment -> Datagram -> Ram[38]
UDP:
Är ett bästa forsök och anslutningslöst orienterat protokoll.
Har inte paket sekvensering, flöde och stockningskontroll och destinationen bekräftar inte varje paket det tar emot.
Det finns mindre överflöde i UDP paketet.
Data - Meddelande -> Packet -> Datagram -> Ram
TCP Handskakning:
1. Värd skickar ett SYN paket.
2. Mottagaren svarar med ett SYN/ACK paket.
3. Värd skickar ett ACK paket.
IPv4 – Använder 32 bitar för sin adress.
IPv6 - Uses 128 bitar för sin adress.

[34] Network layer
[35] Data Link layer
[36] frame
[37] Physical layer
[38] Frame

4.3 LAN media åtkomst tekniker

Ethernet:
Karaktärsdrag: Dela media / Använder utsändning[39] och kollisions[40] domäner / Använder bärarkänslig åtkomst med kollisions detektering (CSMA/CD) åtkomst metod / Stödjer full-duplex på "twisted-pair" implementationer / Kan använda koaxial eller "twisted-pair" media / Definierar av standard 802.3.
10base2 implementation: "ThinNet", använder koaxial kabel, maxlängd 185 meter, ger 10 Mbps.
10base5 implementation: Thicknet, använder koaxial kabel, maxlängd 500 meter, ger 10 Mbps.
10base-T implementation: Använder twisted-pair kabel, ger 10 Mbps, vanligtvis implementerad i stjärntopology.
Fast Ethernet implementation: Använder twisted-pair kabel, ger100 Mbps.
Token ring:
Använder token-sändnings teknologi med stjärn konfigurerad topolgi.
Varje dator är ansluten till en central hub, MAU - Multistation Access Unit.
Överför data med 16 Mbps hastighet.
Aktiv övervakning – Tar bort ramar[41] om kontinuerligt cirkulerar i nätverket.
Lysning[42] – om en dator upptäcker ett problem med nätverket, skickas en lysnings ram. Den skapar en feldomän där datorer och enheter försöker att återkonfigurerar vissa inställningar för att försöka arbeta sig runt det upptäckta felet.
FDDI—Fiber Distributed Data Interface:
Är ett hög hastighets token-sändande media åtkomst topologi.
Överför data med 100 Mbps.
Erbjuder feltolerans genom en motcirkulerande fiberring.
Möjliggör flera token att vara närvarande i ringen samtidigt.

4.4 Kablage

4.4.1 Koaxial kabel

Är mer motståndskraftig mot EMI, elektromagnetisk störning, erbjuder en större bandbredd och längre kablelängd jämfört med twisted pair.
Kan för över med en basbandsmetod, där kablarna endast bär en kanal.
Kan föra över med en bredbandsmetod, där kablarna bär flera kanaler.

4.4.2 Twisted pair

Är billigare och enklare att arbeta med än coaxial kabel.
STP Avskärmad twisted pair – Har ett yttre folie avskärmning vilket ökar skyddet mot störning från radio vågor.
UTP Oavskärmad twisted pair – Olika kategorier av kablar som har olika karaktärsdrag.

4.4.3 Fiberoptik kablage

Eftersom glas används, har det högre överföringshastighet som kan färdas över längre sträckor och är inte påverkad av försvagning och EMI jämfört med kablage som använder koppar. Det utstrålar inte signaler som UTP kablage och är väldigt svårt att avlyssna.
Är dyrt.

[39] broadcast
[40] collision
[41] frames
[42] beconing

4.4.4 Problem med kablage

Störning – Den mottagande anslutningen tar inte emot data i den form som den ursprungligen sändes med.
Kan orsakas av motorer, datorer, kopiatorer, florucerande ljus och mikrovågsugnar.
Försvagning – Förlusten av signal styrka allt eftersom det transporteras eller orsakas av kabel avbrott eller kabel krångel.
Överhörning – När elektriska signaler från en tråd spiller över till en annan tråd. UTP är mycket mer sårbart för detta än STP och koaxial kabel.

Plenum utrymme – Nätverks kablage som placeras i ett utrymme för att motsvara specifika brandklasser för att försäkra att det inte kommer att orsaka eller framkalla skadliga kemikalier i händelse av brand.
Komprimerade rör – Inkapsling av kablar för att om ett försök till att få åtkomst till kablarna, kommer trycket på rören att förändras och ett larm kommer höras eller ett meddelande kommer att sändas till administratören.

4.5 Typer av överföring

Analog överföring av signaler – Modulering av signaler, elektriska vågor.
Digital överföring av signaler – Representerar biniära siffror som elektronisk puls.

Asynkron kommunikation – Två enheter är inte synkroniserade på något sätt. Avsändaren kan skicka data när som helst och mottagaren måste alltid vara beredd. Kan vara en terminal, terminalserver eller modem.
Synkron kommunikation – Inträffar mellan två enheter som synkronsierade, vanligtvis genom en klock mekanisam. Överför data som en ström av bitar.

Basband – Använder hela kablen för sin överföring.
Bredband – Delar vanligtvis in kablen i kanaler för att olika typer av data kan överföras samtidigt.

Unicast metod – Ett paket måste gå till ett särskilt system.
Multicast metod – Ett paket behöver gå till en specific grupp av system.
Broadcast metod – Ett paket går till alla datorer på subnätet.

4.6 Nätverks topologi

4.6.1 Ring Topologi

Har en serie av enheter anslutna genom överföringslänkar som inte är riktningsstyrda, vilka formerar en ring. Varje nod är beroende av att den föregående noden och om ett system upphör att fungera, kan alla andra system upphöra att fungera.

4.6.2 Bus Topologi

En enkel kabel som stödjer hela nätverket. Varje nod beslutar om att acceptera, bearbeta eller ignorera paketet. Kablen där alla noder ansluts är potentiell enskild punkt för fel avseende avbrott.
Linjär buss – Har en enda kabel med noder anslutna till sig.
Trädtopologi – Har grenar från den enskilda kablar och varje gren kan innehålla många noder.

4.6.3 Stjärn Topologi

Alla noder ansluts till en central hub eller switch. Varje nod har en dedikerad länk till den centrala hubben.

4.6.4 Nätverks Topologi

Alla system och resurser är anslutna till varandra på ett sätt som inte följer enhetligheten som beskrivs i tidigare topologier.

4.7 LAN Media Åtkomst Teknologier

MTU – Är en parameter som indikerar hur mycket data som en ram kan bära på ett specifikt nätverk.
Token sändning:
Är en 24-bitars kontroll ram som används för att kontrollera vilka datorer som kommunicerar och med vilka intervall. Toknet ger en dator rättighet att kommunicera. Orsakar inte kollisioner eftersom endast en dator kan kommunicera samtidigt.
CSMA Carrier sense multiple access:
CSMA/CD, kollisions detektering – Övervakar överförings aktiviteter eller bärar aktiviteter i kablen för att fastställa när det bästa tillfället att föra över data kommer. Datorer lyssnar efter frånvaron av bärartoner på kabeln, vilket indikerar att ingen annan för över data samtidigt.
Strid – Noden måste konkurrera om samma delade medium.
Kollision – Inträffar när två eller flera ramar kolliderar.
Tillbakagångs[43] algoritm – Alla stationer kommer att utföra en slumpmässig kollisions tidtagning för att tvinga fram en fördröjning innan de försöker föra över data.
CSMA/CA, kollisions undvikande – Är en åtkomstmetod där varje dator signalerar dess avsikt att föra över data innan den verkligen gör det.
Kollisions domäner:
Är en grupp av datorer som innehåller och konkurrerar om samma delade kommunikations medium.
Röstning:
Några system är konfigurerade för att vara primära stationer och andra är sekundära stationer. Vid fördefinierade intervaller, kommer den primära stationen att fråga den sekundära stationen om den har någonting att föra över.

4.8 Protokoll

ARP – Känner till IP adressen och sänder ut en förfrågan för att finna den matchande hårdvaruadressen, MAC adressen.
RARP – Känner till hårdvaruadressen och sänder ut en förfrågan för att finna IP adressen.
Maskerad attack – En inkräktare förändrar ett systems ARP tabell så att den innehåller felaktig information, ARP tabells förgiftning.
DHCP – En dator är beroende av att en server tilldelar den rätt IP adress.
BOOTP – Kan ta emot disklösa datorers IP adresser från en server.
ICMP – Levererar meddelande, rapporterar fel, svarar på vissa frågor, rapporterar transportvägs information och används för att testa anslutningsförmåga och testar problem i IP nätverk.

[43] Back-off

4.9 Nätverks enheter

Enhet	OSI lager	Funktionalitet
Repeater	Fysisk	Förstärker signaler och utökar nätverket
Bridge	Data länk	För paket vidare med filter baserat på MAC adressen; För meddelande om trafik vidare, men ingen kollisionstrafik.
Router	Nätverk	Delar och ansluter LAN genom att skapar Internet nätverk. Router filtrerar baserat på IP adressen.
Brouter	Datalänk och nätverk	En hybrid enhet som kombinerar funktionaliteten hos en bridge och en router. En brouter kan brygga multipla protokoll och kan transportera paktet för några av dessa protokoll.
Switch	Data länk, mer intelligenta switcher i nätverkslagret	Levererar en privat virtuell lank mellan kommunikationsenheter, tillåter VLAN, minskar trafik och hidrar nätverkssniffning.
Gateway	Applikation, även om olika typer av gateways kan arbeta i andra lager.	Ansluter olika typer av nätverk, genomför protokoll och format översättning.

Kommentarer på bryggor:
Tre typer av bryggor:
- Lokal brygga: Ansluter två eller flera LAN segment inom ett lokalt område.
- Fjärrstyrningsbrygga: Kan ansluta två eller flera LAN segment över ett “wide area network” genom att använda telekommunikation.
- Översättningsbrygga: Om två LAN har anslutits och olika typer av trafiktyper och använder olika standarder och protokoll.
”Broadcast” storm – Eftersom bryggor för all trafik vidare, skickas även alla ”broadcast” paket.
STA Spanning Tree Algorithm – Försäkrar att ramar inte cirkulerar för evigt i nätverket, förser med redundanta vägar i händelse av att en brygga upphör att fungera, tilldelar prioritetsvärde till dessa olika bryggor samt beräknar kostnaden för vägar.
Käll routing[44] – Paketet som innehåller den vidartransporterade informationen för att de skall hitta sin väg till destinationen av sig själv, utan att bryggor och routers dikterar vägen.

VLAN Virtuella LAN:
Möjliggör administratörer att logiskt dela upp och gruppera användare utifrån resurskrav, säkerhets eller affärsmässiga behov istället för den standard fysiska platsen för användare.
PBX Private Branch Exchange:
Är en telefonswitch som är placerad i ett företags egendom.

4.10 Brandväggar

Begränsar åtkomst från ett nätverk till ett annat, internt eller externt.
DMZ - Demilitariserad Zon:
Ett nätverks segement som finns mellan det skyddade och oskyddade nätverket.

[44] Source routing

4.10.1 Paketfiltrering

En metod som kontrollerar vilken data som kan flöda till och från ett nätverk.
Genomförs genom att använda ACL listor, vilka är utvecklade och används för en enhet.
Baseras på nätverkslagrets information, vilket betyder att enheten inte kan titta långt in i själva paketet.
Är inte applikationsberoende.
Håller inte reda på statusen för en anslutning.
Tillhandahåller hög prestanda.
Används i första generationens brandväggar.

4.10.2 Tillståndsmässig paketfiltrering[45]

Ett paket kommer till routern och routern går igenom sin ACL lista för att se om paketet skall accepteras eller avvisas. Denna kräver att brandväggen upprätthåller en tillståndstabell, vilken är ett statusställningsblad över vem som sa vad till vem.
Tar beslut om vilka paket som är tillåtna och otillåtna.
Arbetar på nätverkslagret.

4.10.3 Proxy brandväggar

Står mellan ett betrott och ett obetrott nätverk och upprättar den verkliga anslutningen, åt båda håll, på vägnar av källan.
Tar en kopia av varje accepterat paket innan det överförs och återpaketerar paket för att dölja dess verkliga ursprung.
Arbetar på applikations lagret.

4.10.4 Dual-homed brandvägg

Har två gränssnitt, ett mot det externa nätverket och ett annat mot det interna nätverket.
Har två NIC och har stängt av vidarebefordring av paket.
Används ofta när ett företag använder proxy brandväggar.

4.10.5 Applikationsnivå proxies

Undersöker hela paket och gör åtkomstbeslut baserat på det verkliga innehållet i paketet.
Förstår olika tjänster och protokoll och de kommando som används inom dem.
Det måste finnas en applikationsnivå proxy för varje tjänst.
Arbetar på applikationsnivå.

4.10.6 Omkrets nivå baserad[46] proxy

Skapar en omkrets mellan klient datorn och servern.
Den känner källan och destinationsadressen och tar åtkomstbeslut utifrån denna information.
Kan hantera en mängd olika protokoll och tjänster.
Arbetar på nätverkslagret.

4.10.7 SOCKS

Är ett exempel på en omkrets-nivå baserad proxy gateway som förser en säker kanal mellan två TCP/IP datorer.
Erbjuder inte detaljerade protokoll specifika kontroller.

[45] Stateful Packet Filtering
[46] Circuit-level

4.11 Brandväggs arkitektur

4.11.1 Bastion Värd[47]

Är maskinen som kommer att ge åtkomst av vilken som och alla enheter som försöker få åtkomst eller lämna nätverket.
Kan stödja paket filtrering, proxy och hybrid brandväggs applikationer.

4.11.2 Kontrollerande Värd[48]

Är en bastion värd som kommunicerar direkt med en gränsrouter och det interna nätverket.

4.11.3 Kontrollerade subnät[49]

Den kontrollerande värden, som skyddar brandväggen, är inklämd mellan två routrar. Det externa tillämpar paket filtrering och det interna filtrerar också trafiken.

4.11.4 Borden avseende brandväggar

Standardaktivitet för alla brandväggar bör obetingat förneka alla paket som utrycklingen inte är tillåtna.

4.11.5 Maskering/skojare[50]

Inkräktaren förändrar huvudet i ett paket så att det får samma källadress som värden inom nätverket som han eller hon vill angripa.

4.11.6 Honungsställe[51]

Är den dator som befinner sig i DMZ med avsikt att lura angripare till sig istället för de verkliga produktions datorerna.

4.12 Nätverks tjänster

NOS – Nätverksoperativsystem[52]:
Är designat för att kontrollera åtkomst till nätverksresurser och erbjuda de nödvändiga tjänster för att göra det möjligt för en dator att interagera med det omslutande nätverket.
DNS – Domännamns tjänster[53]:
Är en metod för skilja på värdnamn.
Nätverk är uppdelade i zoner.
Den DNS server som håller filer för en av dessa zoner är sagd att vara den auktoriserande namnservern för en särskild zon.
Det rekommenderas att det finns en primär och en sekundär DNS server för varje zon.
Katalogtjänster[54]:
Har en hierarkisk katalogtjänst över användare, datorer, skrivare, resurser och attribut för var och en.

[47] Bastion Host
[48] Screened Host
[49] Screened Subnet
[50] Masquerading / spoofing
[51] Honeypot
[52] *Networking operations system*
[53] *Domain Name service*
[54] *Directory Services*

4.13 Intranät och extranät

4.13.1 Intranät

När ett företag använder Internet eller web baserad teknologi inom sitt eget nätverk.

4.13.2 Extranät

Möjliggör två eller fler företag att dela samma information och resurser.

4.13.3 NAT Nätverksadress översättning[55]

Är en "gateway" mellan ett nätverk och Internet eller ett annat nätverk, som utför transparent routing och adressöversättning.

4.14 MAN – Storstadsområdes nätverk[56]

Vanligtvis en ryggrad[57] som ansluter företag till WAN, Internet eller andra företag.
En majoritet är SONET / Synchronous Optical Network eller FDDI ringar.

4.15 WAN – Vidspritt Nätverk[58]

Används när kommunikation behöver transporteras över stora geografiska områden.
Dedikerade länkar:
Kallas också för leasade linor eller punkt-till-punkt länk.
T-bärare:
Dedikerade linor som kan bära röst och datainformation över trasiga linor.
S/WAN – Säkra WAN:
Baseras på VPN som skapas med IPSec.

4.16 WAN Teknologier

4.16.1 CSU/DSU – Kanaltjänst enhet / Datatjänst enhet[59]

Krävs när digital utrustning kommer att användas för att ansluta ett LAN nätverk med ett WAN nätverk.
DSU konverterar digitala signaler för att överföras över telefonbolagets digitala linjer.
CSU är enheten som ansluter nätverket direkt till telefonbolagets linjer.
Ger ett digitalt gränssnitt för DET – Data terminal utrustning[60]
Förser ett gränssnitt till DCE – Data omkrets avslutande utrustnings enhet[61].

4.16.2 Switching

Omkrets switching – Skapar en virtuell anslutning som agerar som en dedikerad länk mellan två system.
Paket switching – Paket kan färdas längs med många olika rutter till samma destination.

[55] Network Address Translation
[56] Metropolitan Area Network
[57] backbone
[58] Wide Area Network
[59] Channel Service Unit / Data Service Unit
[60] Data Terminal Equipment
[61] Data Circuit-Terminating Equipment device

4.16.3 Ram transmission[62]

Är ett WAN protokoll som arbetar på data länk lagret.
Använder sig av paketswitchnings teknologi.
CIR / Tilldelat Informationsvärde[63] – Företag som betalar mer är försäkrade om att en större bandbredd alltid kommer att vara tillgänglig för dem.
Två huvudtyper av utrustning används:
- DTE / Data Terminal Utrustning[64] – Kundägd.
- DCE / Data Krets-Avslutande Utrustning[65] – Ägs av tjänsteleverantören eller telefonbolaget.

4.16.4 Virtuella kretsar[66]

PVC / Permanenta Virtuella Kretsar[67] – Fungerar som en privat lina för en kund med en avtalad bandbredd tillgänglig.
SVC / switched virtual circuits – Kräver steg liknande en uppringnings och anslutnings rutin.
X.25:
Är ett äldre WAN protokoll som definierar hur enheter och nätverk etablerar och bibehåller anslutningar.
Är en switchnings teknologi.
Data delas in i 128 byte och kapslas in i High-level Data Link Control, HDLC ramar. Dessa ramar adresseras därefter och skickas vidare genom bärarswitchar.

4.16.5 ATM – Asynkront Överförings Läge[68]

Är en switchnings teknologi.
Använder sig av cellswitchnings teknologi. Detta innebär att data segmenteras i bestämda celler, 53 byte, istället för paket med variabel storlek.
Är en höghastighets nätverks teknologi som används för LAN, WAN och tjänsteleverantörers anslutningar.
Skapar virtuella omkretsar, vilka agerar som dedikerade vägar mellan källa och destination. Dessa virtuella omkretsar kan garantera bandbredd och Kvalitet-på-service.

4.16.6 SMDS – Switchat Mulitmegabit Datatjänst[69]

Är ett höghastighetspaket switchande teknologi som används för att möjliggöra för kunder att utöka deras LAN över MAN och WAN.
Är anslutningsoberoende och kan förse med bandbredd vid efterfrågan.

4.16.7 SDLC – Synkron Data Länk Kontroll[70]

Baseras på nätverk som använder dedikerade, leasade linor med permanenta fysiska anslutningar.
Erbjuder val av media som åtkomst teknologi, vilken är en mekanism som möjliggör sekundära stationer att kommunicera över nätverket.

---

[62] Frame relay
[63] Committed Information Rate
[64] Data Terminal Equipment
[65] Data Cricuit-Terminating Equipment
[66] Virtual Circuits
[67] Permanent virtual circuit
[68] Asynchronous Transfer Mode
[69] Switched Mulitmegabit Data Service
[70] Synchronous Data Link Control

4.16.8 HDLC – Hög-nivå Data Länk Kontroll[71]

Är ett bit-orienterat länknivå protokoll som används för överföring över synkrona linor.
Arbetar med primära stationer som kontaktar sekundära stationer för att etablera dataöverföring.

4.16.9 HSSI – Hög-hastighets Seriellt Gränssnitt[72]

Används för att ansluta mulitplexor's och router's till hög hastighets kommunikationstjänster som ATM och frame relay.

4.16.10Multitjänst Åtkomst[73]

Kombinerar olika typer av kommunikations kategorier över en överförförings lina.
Jittering – När någon som använder VoIP för telefonsamtal får fördröjningar i konversationen.

4.16.11H.323

Är en del av ITU-T rekommendationer som täcker ett vidsträckt antal mulitmedia kommunikations tjänster.

4.17 Fjärr åtkomst[74]

4.17.1 Dial-up och RAS

RAS / Fjärråtkomst tjänste server[75]– Genomför autenciering genom att jämföra den presenterade referensen med databasen av de referenser som underhålls.
Wardialing – Är en process som används av många inkräktare för att identifiera fjärranslutnings modem.

4.17.2 ISDN – Integrerat Service Digitalt Nätverk

Delar telefonlinan i olika kanaler och för över data i digital form i motsats till den gamla analoga implementationen.
Tre metoder -
- BRI / Basic Rate Interface - 2 B kanaler och 1 D kanal.
- PRI / Primary Rate Interface - 23 B kanaler och 1 D kanal.
- BISDN / Broadband – Hanterar olika typer av tjänster samtidigt.

D kanalen erbjuder en snabbare uppringning och process för att upprätta en anslutning.

4.17.3 DSL - Digital Abonnemangs Linje

Är en bredbandsteknologi.
Tjänst kan vara symestrisk -> Hastighet motströms <> nerströmst.
Ansluten hela tiden.

4.17.4 Kabel modem

Erbjuder höghastighetsåtkomst.
Ansluten hela tiden.

[71] High-level Data Link Control
[72] High-Speed Serial Interface
[73] Multiservice Access
[74] Remote Access
[75] Remote Access Service server

4.18 VPN – Virtuella Privata Nätverk

Är en säker privat anslutning genom publika nätverk.

4.18.1 PPTP – Punkt-till-punkt tunnel protokoll[76]

Är en inkapslingsmetod som baseras på PPP.
Arbetar med data länk lagret och det möjliggör en enskild punkt-till-punkt anslutning.
Krypterar och kapslar in PPP paket.
När förhandling utförs, PPP kan inte kryptera denna information eftersom krypteringen befinner sig i processen att anropas.
Kan endast fungera ovanpå IP nätverk.

4.18.2 L2TP - Lager 2 Tunnel Protokoll

Kan köras ovanpå och tunnla igenom nätverk som använder andra protokoll.
Är inte ett krypterings protokoll.
Stödjer TACACS+ och RADIUS.

4.18.3 L2F – Lager 2 Vidarbefordring

Erbjuder ömsesidig autenciering.
Ingen kryptering.

4.18.4 IPSec

Hanterar flerfaldiga anslutningar samtidigt.
Erbjuder säker autenciering och kryptering.
Stödjer endast IP nätverk.
Fokuserar på lan-till-lan kommunikation hellre än ett uppringnings protokoll.
Arbetar på nätverkslagret och erbjuder säkerhet ovanpå IP.
Kan arbeta i tunnel läge, vilket betyder att nyttolasten och huvudet är krypterat eller transport läge, vilket innebär att endast nyttolasten är krypterad.

4.18.5 PPP – Punkt-till-punkt

Används för att kapsla in meddelanden och för över dem genom ett IP nätverk.

4.18.6 PAP - Lösenords Autensieringsprotokoll

Erbjuder identifiering och autenciering av användaren som försöker få åtkomst till nätverket från ett fjärrsystem.

4.18.7 CHAP – Utmaningshandskaknings Autensierings Protokoll

Är et autencieringsprotokoll som använder utmaning/svar[77] mekanism för att autensiera istället för att skicka ett användarnamn och lösenord.

4.18.8 EAP – Utökat Autensieringsprotokoll

Erbjuder ett ramverk för att möjliggöra många sorters autencieringstekniker för att användas vid PPP anslutningar.

[76] Point-to-point tunnelling protocol
[77] challenge/response

4.19 Nätverk och resurstillgänglighet

4.19.1 Enskild punkt för avbrott[78]

Om en enhet går isönder, påverkas ett segment eller hela nätverket negativt.

4.19.2 RAID – Redunant uppsättning av billiga diskar

En teknologi som används för redundans och prestandaförbättringar som kombinerar flera fysiska diskar och aggregerar dessa till logiska uppställningar.

4.19.3 Klustring

En grupp servrar som syns logiskt som en server för användare och som hanteras som ett system.

[78] Single point of failure

5 CBK#3 Styrning av säkerhet i praktiken

5.1 Fundamentala principer för säkerhet

5.1.1 *Säkerhetsmål*

Konfidentialitet:
Erbjuder förmågan att försäkra att den nödvändiga säkerhetsnivån är införd.
Integritet:
Vidmakthålls när försäkran om riktighet och tillförlitlighet i information och system erbjuds och ej auktoriserad förändring av data har förhindrats.
Tillgänglighet:
Förhindrar störingar i tjänster avseende produktivitet.

5.1.2 Definitioner

Sårbarhet:
Är en mjukvara, hårdvara eller rutinmässig svaghet som kan erbjuda inkräktaren en öppen dörr som han söker efter för att komma in i en dator eller ett nätverk och få ej auktoriserad åtkomst till resurser inom miljön.
Hot:
Är en möjlig fara för information och system.
Risk:
Är sannolikheten för att en hotagent drar fördel av en sårbarhet.
Utsättning:
Är ett exempel på att bli utsatt för förlust från en hot agent.
Motåtgärder / skyddsåtgärder
Lindrar en möjlig risk.
Uppifrån-ner angreppsätt:
Initieringen, stödet och riktning kommer från högsta ledning och arbetar sig genom mellan nivån och sen ner till enskilda medarbetare.
Nerifrån-upp angreppsätt:
Säkerhetsprogram utvecklat av IT utan att få ordentlig ledningsstöd och riktning.
Operativa mål:
Dagliga mål.
Taktiska mål:
Mellan-långa mål.
Strategiska mål:
Långsiktiga mål.
Risk hantering[79]:
Är procesen för att identifiera, bedöma och minska risken till en acceptabel nivå och införa rätt mekanismer för att upprätthålla denna risknivå.

[79] *Risk Management*

5.2 Risk Analys

Är en metod för att identifiera risker och bedömma den möjliga skada som kan orsakas för att rättfärdiga säkerhetsmässiga skyddsåtgärder.
Tre huvudmål:
- identifiera risker.
- kvantifiera påverkan av möjliga hot.
- erbjuda en ekonomisk balans mellan påverkan av risken och kostnaden för motåtgärder.

Risker har en förlustpotential: Företaget skulle förlora något om en hotagent verkligen utnyttjar en sårbarhet.
Försenad förlust: Har en negativ påverkan på ett företag efter att en risk initialt har exploaterats.

5.2.1 Kvantitativt angreppssätt

Försöker ange verkliga tal för skyddsåtgärdernas kostnader och omfattning av skadan som kan inträffa.
Erbjuder konkreta sannoliketsprocenttal när sannolikhet av hot och risker skall bedömas.
Ren kvantitativ riskanalys är inte möjlig att göra eftersom metoden försöker kvantifiera kvalitativa punkter.

Steg i en riskanalys -
- Tilldela information och tillgångar ett värde.
- Uppskatta den möjliga förlusten per risk.
- Genomför en hotanalys .
- Härled den övergripande förlustpotentialen per risk.
- Välj hjälpande åtgärder för att motverka varje risk.
- Minska, tilldela eller acceptera risken.

Beräkning av risk -
EF, Utsatthetsfaktor[80] = Procent av tillgång som förlorats orsakad av identifierat hot.
SLE, Enskild förväntad förlust[81] = Värde på tillgång * Utsatthetsfaktor.
ARO, Årlig andel av händelser[82] = Uppskattad frekvens att ett hot kommer att inträffa inom ett år.
ALE, Årlig förväntad förlust[83] = Enskild förväntad förlust * Årlig andel av händelser.

5.2.2 Kvalitativt angreppssätt

Genomgång av olika scenario av risk möjligheter och rankning av allvarlighetsgraden för hoten och känsligheten för tillgångar.
Rutiner för att genomföra ett scenario:
- Ett scenario skrivs för att adressera varje stort hot.
- Scenariot granskas av affärenhetschefer för att verifiera rimlighet.
- Riskanalysteamet rekommenderar och utvärderar olika skyddsåtgärder för varje hot.
- Riskanalysteamet arbetar genom varje avslutat scenario genom att använda hot, tillgång och skyddsåtgärd.
- Teamet förbereder deras upptäckter och lämnar dessa till ledningen.

[80] Exposure faktor
[81] Single Loss Expectancy
[82] Annual rate of occurence
[83] Annualized Loss Expectancy

5.2.3 Delphi Teknik

Är en gruppbeslutsmetod och används för att försäkra att varje medlem i gruppen ger ett ärligt svar av vad han eller hon anser om resultatet för en särskild risk.

5.2.4 Beräkning av motåtgärder och risk

Varje skyddsåtgärd för företaget = (Årlig förväntad förlust (ALE) innan varje införd skyddsåtgärd) – (Årlig förväntatad förlust (ALE) efter införda skyddsåtgärder) – (årlig kostnad för skyddsåtgärder).
Total risk = hot * sårbarhet * tillgångens värde.
Återstående risk = (hot * sårbarhet * tillgångens värde) * kontroll gap.
Total risk = hot * sårbarhet * tillgångens värde.

5.2.5 Hantering av risker

Överföra risker -> Köp en försäkring.
Reducera risker -> Inför motåtgärder.
Avvisa risker -> Förneka dess risker och ignorera det.
Acceptera risken -> Företaget förstår vilken risknivå som de påverkas av och kostnaden för den skada som är möjlig och som de har beslutat att leva med.

5.3 Säkerhetsprogram

Kategorier av policy:
- Reglerande
- Vägledande
- Informativa

5.3.1 Säkerhetspolicy

Är ett generellt uttalande framtaget av högsta ledningen för att diktera vilken typ av roll som säkerhet spelar inom organisationen.
Skrivs i vidsträckta och övergripande termer för att täcka många olika områden på ett generellt sätt.
- Organisatoriska säkerhetspolicy: Ger omfattning och riktning för alla ytterligare aktiviteter inom organisationen.
- Ärendespecifika policy: Adresserar specifika säkerhetsärenden som ledningen anser att de kräver mer detaljerade förklaringar och uppmärksamhet för att vara säker på att omfattande struktur byggs och att alla anställda förstår hur de skall efterleva dessa säkerhetsärenden.
- Systemspecifika policy: Presenterar ledningens beslut som är närmre de verkliga datorerna, nätverk, applikationerna och datan.

5.3.2 Standarder[84]

Specificerar hur hårdvaru- och mjukvaruprodukter skall användas. De erbjuder ett medel för att vara säker att specifika teknologier, applikationer och parametrar och rutiner kan utföra på ett enhetlig sätt genom hela organisationen.
Dessa regler är vanligtvis tvingande inom ett företag och de behöver genomdrivas.

5.3.3 Baskrav[85]

Ger en miniminivå av säkerhet nödvändig genom hela organisationen.

[84] Standards
[85] Baselines

5.3.4 Rågivande[86]

Är rekommenderade åtgärder och operativa guider till användare, IT medarbetare, operativa medarbetare och andra när en specifik standard inte går att använda.

5.3.5 Rutiner[87]

Är steg-för-steg aktiviteter för att uppnå en specifik uppgift.
Rutiner anses som den lägsta nivån i policykedjan.

5.4 Data klassificering

Det primära syftet med data klassificering är att indikera nivån för konfidentialitet, integritet och tillgänglighet som krävs för varje typ av information.
Det hjälper till för att försäkra att data skyddas på det mest kostnadseffektiva sättet.

Vanliga klassificeringsnivåer (från lägsta till högsta nivå):
Kommerciell verksamhet->
- Konfidentiell
- Privat
- Känslig
- Publik

Militär->
- Topphemlig
- Hemlig
- Konfidentiell
- Känslig men ej klassificerad
- Ej klassificerad

5.5 Nivåer avseende ansvar

5.5.1 Högsta ledningen

Ytterst ansvarig för säkerhet inom organisationen och skyddet av dess tillgångar.

5.5.2 Säkerhets specialister

Funktionellt ansvariga för säkerhet och utför känsliga lednings direktiv.

5.5.3 Dataägare

Är vanligtvis en medlem i högsta ledningen och är ytterst ansvarig för skyddet och användandet av data.
Bestämmer klassificeringen av den data han eller hon är ansvarig för och förändrar klassificeringen när behov uppstår.
Delegerar ansvaret för det dagliga underhållet av data, vilket är ansvaret för data förmyndaren[88].

5.5.4 Data förmyndare

Har givits ansvaret för underhåll och skydd av data.

[86] Guidelines
[87] Procedures
[88] data custodian

5.5.5 Användare

Vilken individ som helst som rutinmässigt använder data för arbetsrelaterade uppgifter. Måste ha den nödvändiga åtkomstnivån till data för att utföra sina skyldigheter som tillhör positionen och är ansvarig för att följa operativa säkerhetsrutiner för säkerställa datat's Konfidetialitet, Integritet och Tillgänglighet för andra.

5.5.6 Struktur och genomförande

Uppdelning av uppgifter:
Försäkrar att en individ inte kan fullfölja en riskfylld uppgift själv.
Maskopi:
Mer än en person måste arbeta tillsammans för att orsaka någon typ av destruktion eller bedrägeri och detta minskar sannolikheten drastiskt.
Icke avslöjande avtal:
För att skydda företaget om och när en anställd lämnar företaget av en eller annan orsak.
Job rotation:
Ingen enskild person bör stanna på en position för en lång tidsperiod eftersom det kan sluta i att för mycket kontroll inom versksamhetssegmentet ges till denna enskilda individ.

5.6 Säkerhetsmedvetenhet

Typer av utbildning:
- Säkerhetsrelaterad arbetsutbildning för operatörer.
- Medvetenhetsutbildning för särskilda avdelningar eller personalgrupper med säkerhetskänsliga positioner.
- Teknisk säkerhetsutbildning för personal som stödjer IT och systemadministratörer.
- Avancerad informations säkerhetsutbildning för säkerhets utövare och IT revisorer.
- Säkerhetsutbildning för högre chefer, funktionschefer och affärsområdesansvariga.

6 CBK#4 Säkerhet för applikationer & Systemutveckling

6.1 Databassystem och databas administration

Typer av databaser:
- Hierarkisk
- Mesh
- Objekts orienterad
- Relations

DBMS / Databas administrations system[89] -
En samling av program som används för att hantera stora samlingar av strukturerad data med ad-hoc frågemöjligheter för många olika typer av användare.
Databas:
En samling av data lagrad på ett meningsfullt sätt som möliggör flera användare och applikationer att få tillgång till, visa och förändra data efter behov.
Databas termer/jargon -
- Post: Samling av relaterade datadelar.
- Fil: Samling av poster av samma typ.
- Databas: Samling av filer med korsreferens.
- DBMS: Administrerar och kontrollerar databasen.
- Bas relation: En tabell lagrad i en databas.
- Tuple: En rad i en databas.
- Attribut: En kolumn i en databas.
- Primär nyckel: Kolumner som gör varje rad unik.
- Vy: Virtuell relation definierad av databasen som kontrollerar subjektet att se viss data.
- Främmande nyckel: Attribut från en tabell som är primär nickel i en annan tabell.
- Cell: Korsning mellan en rad och en kolumn.
- Schema: Innehåller data som beskriver en databas.
- Datauppslagsbok[90]: Central förvaring av data element och deras relation.
- Kardinalitet: Antalet rader i en relation.
- Grad: Antalet kolumner i relationen.
- Domän: Är en samling av tillåtna värden som ett attribut kan anta.

6.1.1 Databas modeller

Relationsdatamodell -
Använder attribut, kolumner, och tuple, rader, för behålla och organisera information.
En primär nyckel är ett fält som länkar all data inom en post till ett motsvarande värde.

Hierarkisk datamodell -
Kombinerar poster och fält som är relaterade i en logisk trädstruktur.
Kan ha ett barn, många barn, inga barn.
Är användbara för att kartlägga en-till-många relationer.

Distribuerad datamodell -
Har data lagrad i mer än en databas, men är logisk sammanknuten.

[89] Database Management System
[90] Data dictionary

Möjliggör olika databaser att hanteras av olika administratörer, även om en person eller grupp måste hantera hela den logiska databasen.
Relationsdatabas komponenter:
DDL / Data Definitions Språk[91] -
Definierar strukturen och schema för databasen.
- Struktur: tabell storlek, nyckelplacering, vyer och relationer mellan dataelement.
- Schema: Typen av data som kommer att lagras och manipuleras och deras egenskaper.

DML / Data Modifikations Språk[92] -
Alla kommandon som som gör det möjlig för en användar att se, manipulera och använda databasen.
QL / Fråge språk [93] -
Gör det möjligt för användare att göra förfrågningar i databasen.
Rapportgenerator -
Skapar utstkrifter av data på en användardefinierat sätt.

6.1.2 Data uppslagbok[94]

Är en central förvaring av data element och deras relationer.
Är en samling av data element, schema objekt och referens nycklar.
Schema objekt – Kan innehålla tabeller, vyer, index, procedurer, funktioner och triggers.

6.1.3 Nycklar

Primär nyckel -
Är en unik identifierare i tabellen som otvetydigt pekar på en individuell tuple eller rad i tabellen.
Är en delsamling av kandiderande nycklar inom tabellen.
Främmande nyckel -
Ett attribut i en relation som har värden som matchar den primära nyckeln i en annan relation.

6.1.4 Integritet

Sammanträffande[95] problem -
Försäkra sig om att olika subjekt tar emot den senast uppdaterade informationen.
Semantisk integritet -
Försäkra sig om strukturella och semantiska regler genomdrivs. Dessa regler gäller data typer, logiska värden, unika restriktioner och operationer som avsevärt påverkar strukturen i databasen.
Referens integritet -
Mekanism som försäkrar att ingen post kan innehålla en referens till en primär nyckel i en icke existerande post eller NULL värde.
Enhets integritet -
Om ett attribut är NULL.
Rulla tillbaka [96]-
Är ett uttalande som avslutar en pågående transaktion och avbryter alla andra förändringar i databasen.

[91] Data Definition Language
[92] Data Manipulation Language
[93] Query Language
[94] Data dictionary
[95] Concurrency
[96] Rollback

Överlämna [97] -
Avslutar en transaktion och utför alla förändringar som precis har blivit utförda av användaren.
Kontrollpunkt[98] -
Används för att försäkra sig att om ett systemfel uppstår och om ett fel upptäcks, kan användare alltid återvända till en punkt innan systemet kraschade.

6.1.5 Databas säkerhets frågor

Aggregering -
När en användare inte har godkännande eller tillåtelse till viss specifik information, men hon har tillåtelse till komponenter av denna information. Hon kan då lista ut resten och få tillgång till restriktiv information.
Slutsats -
Inträffar när ett subjekt härleder information som är begränsad från data han har tillgång till. Detta inträffar när data i en lägre säkerhetsnivå indirekt avporträtterar data på en högre nivå.
Innehållsberoende åtkomstkontroll -
Tittar på innehållet i en fil när den tar beslut om åtkomstkontroll. Denna typ av åtkomstkontroll ökar bearbetningsbelastning, men den ger bättre finkornig[99] kontroll.
Cell undertryckning -
Är en teknik som används för att gömma eller inte visa specifika celler som innehåller information som skull kunna användas i en slutledningsattack.
Partitionering -
Involverar uppdelning av databasen i olika delar, vilka gör det mycket svårare för en icke auktoriserad individ att finna sammankopllade delar av data som kan sättas samman och annan information härledas och bli avslöljad.
Störning och förvirrning –
Är en teknik som infogar påhittad information i hopp om att den dirigerar en attackerar i fel riktining och förvirrar ärendet tillräckligt mycket för att den verkliga attacken inte skall bli framgångsrik.
Databas vyer -
Tillåter en grupp eller en specifik användare att se viss information, medan andra grupper är begränsade från att se allt.
Flera instanser[100] -
Möjliggör en relation för att innehålla multipla rader med samma primära nyckel med varje instans avskiljd av en säkerhetsnivå.
OLTP / Realtids transaktions bearbetning[101] -
Förser mekanism som ser efter problem och hanterar dem ändamålsenligt när de inträffar.
- Två-fas överlämnande service: Kommer att försäkra sig om att en transaktion inte är fullständing förrän alla databaser tar emot och reflekterar en förändring.

Datalager -
Kombinerar data från flera databaser in i en stor databas med syfte att uppnå större omfattaning på informationsuthämtning och data analys.
Data mining -
Är processen av att förmedla data som finns i datalagret till mer användbar information.

[97] Commit
[98] Checkpoint
[99] Granular
[100] Polyinstantiation
[101] On Line Transaction Processing

- Metadata: Data som skapas av data mining verktyg för att finna associationer och samband.

OODB / Objekts orienterad databas[102] -
Har som karaktärsdrag att vara enkelt att återanvända kod och analyser, minskat underhåll och en klar omvandling från analys av problem till design och införande.
Dess största nackdel är en skarp inlärningskurva och höga prestandakrav på hårdvara och mjukvara som är nödvändiga för utveckling och drift.
Objekt-relations databas -
Kombinerar attributen i en objekt-orienterade och relations teknologier.

6.2 Systemlivscykel faser / mjukvarulivscykel utvecklingsprocess

6.2.1 System Livscykel Faser

- Projekt initiering:
  - Presentation av projektdefinition
  - Förslag och inledande studie
- Funktionell design analys och planering
  - Krav avslöjas och definieras
  - Systemmiljö specifikation fastställs
- System design specifikation
  - Funktionell designgranskning
  - Funktionalitet bryts ner
  - Detaljerad planering sätts på plats
  - Kod design
- Mjukvaruutveckling
  - Utveckling och programmering av mjukvara
- Installation / implementation
  - Produkt installation
  - Test and granskning
- Drift/underhåll
  - Produktförändringar, fixar och mindre förändringar
- Avyttring / revision och ersättning
  - Förändring av produkt med revisioner eller ersättning av allt.

6.2.2 Vattenfalls modellen

- Systemkrav
- Mjukvarukrav
- Analys
- Program design
- Kodning
- Test
- Drift & underhåll

[102] Object-Oriented Data Bases

6.2.3 Modifierad Vattenfalls modell med införlivad V&V

- System lämplighet -> validering
- Mjukvaru planer & krav -> validering
- Produkt design -> verifiering
- Detaljerad design -> verifiering
- Kodning -> unit test
- Integration av produkt -> verifiering
- Implementation -> system test
- Drift & underhåll -> återvalidering

6.2.4 Säkerhets ställningstagande

- Säkerhet bör beaktas i varje fas av systemutvecklingen. Säkerhet bör inte beaktas i slutet av utvecklingen eftersom det innebär tillkommande kostnader, tid, anstängningar och bristande funktionalitet.
- Uppdelning av arbetsuppgifter bör praktiseras i roller, miljö och funktionalitet som har att göra med utvecklingen av produkten.

- En programmerare borde inte ha direkt tillgång till kod i produktionsmiljön.
- Certifiering har att göra med testning och bedömning av säkerhetsmekanismer i ett system.
- Ackreditering har att med ledningens formella acceptans av systemet och dess säkerhetsnivå.
- Förändringar måste bli auktoriserade, testade och dokumenterade. Förändringar får inte påverka systemets säkerhetsnivå och dess förmåga att genomdriva säkerhetspolicyn.

6.2.5 Förändringskontroll subfaser

- Beställningskontroll
- Förändringskontroll
- Frisläppningskontroll

6.2.6 Förändringskontroll faser

- Gör en formell begäran om förändring.
- Analysera begäran.
  - Utveckla införande strategin.
  - Beräkna kostnader för införandet.
  - Granska säkerhetspåverkan.
- Dokumentera förändringsbegäran.
- Lägg fram förändringsbegäran för godkännande.
- Utveckla förändringen.
  - Omkoda segement i produkten och lägg till eller dra ifrån funktionalitet.
  - Länka dessa förändringar i koden till den formella förändringsbegäran.
  - Lägg fram mjukvara för test och kvalitetsgodkännande.
  - Repetera tills kvaliteten är tillräcklig.
  - Gör versionsförändringar.

6.2.7 Konfigurationsstyrning

- Konfigurations identifiering.
- Konfigurations kontroll.
- Konfigurations status redogörelse.
- Konfigurations granskning.

6.2.8 CMM / Mjukvaru mognadsmodell

- Nivå 1: Initiering – Kompetent personal och hjältar, processer är informella och ad hoc.
- Nivå 2: Repeterande - Projekt styrningsprocesser; projekt styrning utövas och är formellt etablerat.
- Nivå 3: Definierad – Utvecklingsprocesser och organisatorisk support, tekniskt utförande är integrerat med ledningsutförande som är formellt etablerat.
- Nivå 4: Styrd - Produkt och process förbättringar, produkt och processer är kvantitativt kontrollerade.
- Nivå 5: Optimerad – Kontinuerliga processförbättringar; processförbättringar är formellt etablerade.

6.3 Applikationsutvecklings metoder

6.3.1 Typer av språk

Maskin språk: Är i en form som datorn och processorn kan förstå och arbeta med direkt.
Assembler språk: Kan inte förstås direkt av systemet och måste bearbetas, med maskinkod som resultat.
Hög-nivå språk: Kan inte förstås direkt av systemet utan måste bearbetats, med maskinkod som resultat.

6.3.2 Program

Tolkande program: Har instruktioner som läses och översätts av ett program med en instruktion åt gången.
Kompilerade program: Är skrivna i ett hög-nivå språk och omvandlas till maskinläsbart format av ett kompileringsprogram.

6.3.3 OOP / Objekt-Orienterad Programmering

Arbetar med klasser och objekt med dessa klasser.
När en klass är definierad, kan atributen återanvändas för varje ny medlem eller instans av klassen som skapas.
Objekten inkapslar attributvärden, vilket innebär att denna information är paketerad under ett namn och kan återanvändas som en enhet av ett annat objekt.
Ett objekt kan ha en delad del - Gränssnittet möjliggör det att interagera med andra komponenter.
Ett objekt kan ha en privat del - Hur det verkligen arbetar och utför den efterfrågade uppgifter
Meddelande går igenom gränssnittet för att specifiera den eftefrågade uppgiften eller metoden som skall utföras.
Informationsdöljning – Det finns inget behov för andra komponenter att veta hur varje objekt fungerar internt.
Abstraktion – Är förmågan att undertrycka irrelevanta detaljer för att de viktiga, ärvda egenskaperna kan utvärderas och granskas.

6.3.4 Faser i objektorientering

OORA / Objekt orienteriad krav analys[103] -
Definierar klasser av objekt och deras interaktion.
OOA / Objekt orienterad analys[104] -
I termer av objektorienterade koncept, förståelse och att göra modeller av ett speciellt problem inom en problemdomän.
DA / Domän Analys[105] -
Söker att identifiera klasserna och objekten som är vanliga för alla applikationer inom en given domän.
OOD / Objekt orienterad design[106] -
Objekt är den grundläggande enheten för moduläritet, objekt är instanser av en klass.
OOP / Objekt orienterad programmering [107]-
Framhålla användning av objekt och metoder istället för typer av tranformationer som andra program närmar sig.

6.3.5 Specialiteter för OOP

Enkapsulering – Gömmer intern data och bearbetningar.
Polymorfism – Gör kopior av objekt och gör förändringar för dessa kopior.
Polyinstaniation – Multiple distinkt skillnad mellan data inom objekt för att motarbeta lägre nivåsubjekt från att läras sig av information i en högre säkerhetsnivå.
Arv – Delar egenskaper och attribut.
Multipelt arv – Är situationen där en klass ärver de beteendemässiga karatärsdragen från mer än förälders klass.
Delegation – Vidarbefordran av en förfrågan från ett objekt till ett annat objekt eller ombud. Denna vidarebefordran är nödvändig av det faktum att objektet som tar emot förfrågan inte har någon motod för att hantera förfrågan.

6.3.6 Data modellering

Strukturerat analysangreppssätt:
Ser på alla objekt och subjekt för en applikation och kartlägger relationerna, kommunikationsvägarna och arvsegenskaperna.
Data modellering:
Betraktar data oberoende av vägen som data bearbetas och komponenterna som bearbetar data.

6.3.7 Data Strukturer

Data struktur:
Är en representation av logiska relationer mellan element av data.
Sammanhängande[108]:
En sammanhängande modul kan utföra en enskild uppgift med liten eller ingen hjälp från andra moduler.
- Lågt sammanhängande: Virrig, gör flera uppgifter.
- Hög sammanhängande: Fokuserar på en uppgift.

[103] Object-Oriented Requirements Analysis
[104] Object-Oriented Analysis
[105] Domain Analysis
[106] Object-Oriented Design
[107] Object-Oriented Programming
[108] Cohesive

Den bästa programmeringen använder de mest sammahängande moduler som är möjliga, men eftersom olika moduler behöver föra över data och kommunicera, kan de vanligtvis inte vara fullständigt sammanhängande.
Koppling[109] :
Är ett mätvärde på anslutningar mellan moduler i en applikation.
- Låg koppling: Främjar moduloberoende.
- Hög koppling: Är beroende av andra moduler.

Ju lägre koppling, desto bättre är mjukvarudesignen, eftersom det främjar moduloberoende. Ju mer oberoende en komponent är, desto mindre komplex är applikationen och det är enklare att modifiera och söka fel.

6.3.8 OMA / Objektstyrningsarkitektur[110]

ORB / Objektförfråge förmedlare[111]:
Hanterar all kommunikation mellan komponenter och möjliggör dem att interagera i en hetrogen och distribuerad miljö.
CORBA / Vanlig arkitektur för objektförfråge förmedlare[112]:
Förser interoperabilitet mellan den vidsträckta uppställning av olika mjukvaror, plattformar och hårdvara i miljön.
Möjliggör för applikationer att kommunicera med varandra oberoende var applikationen finns och vem som har utvecklat den. Att införa detta kompatibla utbytet, en användare utvecklar en liten mängd av initial kod och ett gränssnitts definitionsspråk, IDL[113], fil.
COM / Vanlig objektmodell[114]:
Stöder utbytet av objekt mellan program.
DCOM / Distribuerad vanlig objektmodell[115]:
Definierar standarden för att dela objekt i en nätverks miljö.
Använder en global unik identifierare, GUID, för att unikt identifiera användare, resurser och komponenter inom en miljö.
ODBC / Öppen Databas Förbindelse[116]:
Förser en standard SQL dialekt som kan användas för att få tillgång till många typer av relationsdatabaser.
DDE / Dynamiskt Data Utbyte[117]:
Möjliggör olika applikationer att dela data genom att förse en IPC:
Är en kommunikations mekanism som möjliggör direkt konversation mellan två applikationer.
DCE / Distribuerad Datorbearbetnings miljö[118]:
Är en samling av styrningstjänster med ett kommunikationslager baserat på RPC.
Är ett lager mjukvara som finns på toppen av nätverkslagret och förser tjänster till applikationer ovanför det.
Använder universal unik indentifierare, UUID, för att unikt identifiera användare, resurser och komponenter inom en miljö.

[109] Coupling
[110] Object Management Architecture
[111] Object Request Brokers
[112] Common Object Request Broker Architecture
[113] Interface Definition Language
[114] Common Object Model
[115] Distributed Common Object Model
[116] Open Database Connectivity
[117] Dynamic Data Exchange
[118] Distributed Computing Environment

RPC funktionen samlar argument och kommandon från det sändande programmet och förbereder dem för överföring över nätverket.
DFS / Distrbuerad Fil tjänster[119] förser ett enskilt integrerat filsystem som alla DCE användare kan använda för att dela filer.

6.3.9 Expert system / kunskapsbaserade system

Använder artificiell intelligens / emulerad mänsklig kunskap för att lösa problem.
Är ett datorprogram som innehåller en kunskapsbas och en samling algoritmer och regler att dra slutsatser om ny fakta från kunskap och inkommande data.
- Regelbaserad programming: Är en vanlig väg att utveckla expert system.
- Mönster matchning: Baseras på om-sen logiska enheter.
- Slutsats maskiner: En mekansim som automatiskt matchar fakta mot mönster och fastställer vilken regel som är tillämpbar.

6.3.10 Artificiella Nerv nätverk

Är en elektronisk modell som baseras på nervstrukturen i hjärnan.
Försöker att återskapa de grundläggande funktionerna i nerverna och deras omlopp för att lösa problem på ett nytt sätt.

6.3.11 Java

Är plattforms oberoende eftersom den skapar mellanliggande kod, bytekod, vilken inte är processor specifik. Den Java Viruella Maskinen konverterar sen bytekoden till maskinkod.
Java applettar använder ett säkerhetsschema som använder en sandbox för att begränsa applettens tillgång till vissa specifika områden inom användarens system och skyddar dem från främmande eller dåligt skrivna appletter.

6.3.12 ActiveX

Microsoft teknologi som används för att skriva kontroller som Internet användare kan ladda för att öka deras funktionalitet och Internet erfarenhet.
Utövar säkerhet genom att informera användaren varifrån programmet kommer ifrån.
Använder autensieringskods[120] teknologi som förlitar sig på digitala certifikat och förlitande certfikat utgivare.

6.3.13 Främmande kod

Virus, maskar, trojanska hästar, logiska bomber, …
Kan upptäckas genom
- Ökad filstorlek.
- Många oväntade diskar har givits åtkomst.
- Förändringar i uppdateringar och förändringar i tidssämplar.

6.3.14 Virus

Är ett program som söker efter andra program och infekterar dem genom att inbädda sig en kopia av sig själv.
När det infekterade programmet exekveras, exekveras det inbäddade viruset vilket fortplantar infektionen.
- Boot sektor virus: Flyttar data inom boot sektorn eller skriver över sektorn med ny information.

[119] Distributed File Services
[120] authenticode

- Osynliga[121] virus: Gömmer förändringarna som har gjorts i filer eller boot poster.
- Polymorfiska virus: Producerar varierade men operationella kopior av sig själv.
- Multidels virus: Infekterar både boot sektorn på hårddisken och exekverbara filer.
- Själv-förvanskande virus: Försöker gömma sig för antivirus mjukvaror genom att förvanska sin egen kod. Allt eftersom viruset sprids, förändras sättet som det har blivit kodat.

6.3.15 Mask

De kan reproducera sig på egen hand utan att behöva någon värdapplikation och de är självinnehållna program.

6.3.16 Logisk bomb

Kommer att exekvera ett program, eller en sträng av kod, när en speciell händelse inträffar.

6.3.17 Trojanska hästar

Är ett program som döljer sig för andra program.

6.4 Attacker

6.4.1 DoS / Förnekande av tjänster[122]

En attack som förbrukar offrets bandbredd av resurser, som orsakar systemet att krascha eller upphöra att bearbeta andra paket.

6.4.2 Smurf

Kräver tre spelare: inkräktaren, offret och det förstärkande nätverket.
Inkräktaren lurar eller förändrar käll IP adressen i ett pakethuvud, för att få ett ICMP ECHO paket att se ut som om det hörde hemma i offrets systm. Detta ICMP ECHO meddelande sprids till det förstärkande nätverket, som kommer att svara på meddelandet med full styrka. Offrets system och offrets nätverk överväldigas.

6.4.3 "Fraggle"

Använder UDP som sitt vapen. Inkräktaren sprider ett förfalskat UDP paket till det förstärkande nätverket, som i sin tur svarar till offrets system.

6.4.4 SYN Flod

Kontinuerligt skickar offret SYN meddelande med förfalskade paket. Offret kommer att vidta de nödvändiga resurserna för att etablera denna kommunikation och kommer att skicka sitt SYN/ACK meddelande och väntar på ACK meddelandet i retur.

6.4.5 Tår[123]

En inkräktare skickar väldigt små paket som kommer att orsaka att systemet fryser eller startar om. Orsakas av det faktum att några system försäkrar sig om att paket inte är för långa, men kontrollerar inte om paket är för små.

[121] Stealth
[122] Denial of Service
[123] Teardrop

6.4.6 DDoS / Distribuerad förnekande av tjänster[124]

Är ett logiskt tillägg till DoS.
Inkräktaren skapar masterkontroller som i sin tur kan kontrollera slavar / zombie maskiner.

6.4.7 DNS DoS Attacker

En post i DNS servern ersätts av en ny post som pekar på falska IP adresser.
Cache förgiftning – Inkrätaren infogar data i cacheminnet på servern istället för att ersätta den verkliga posten.

[124] Distributed Denial of Service

7 CBK#5 Kryptografi

7.1 Definitioner

Algoritm: Den samling av matematiska regler som används vid kryptering och dekryptering.
Kryptografi: Vetenskap om hemligt skrivande som gör det möjligt för dig att lagra och transportera data i en form som är tillgänglig endast för de tilltänkta individerna.
Kryptosystem: Hårdvaru- och mjukvaruimplementation av kryptografi som omvandlar ett meddelande till chifferskrift och åter till vanlig text.
Krypto analys: Utövandet av att erhålla vanlig text från chiffertext utan en nyckel eller knäcka krypteringen.
Kryptologi: Studien av både kryptografi och kryptoanalys.
Chiffertext: Data i krypterad och oläsbart format.
Kryptera[125]: Handlingen för att omvandla data till ett oläsbart format.
Dekryptera[126]: Handlingen för att omvandla data till ett läsbart format.
Nyckel: Hemlig sekvens av bitar och instruktioner som styr handling för att kryptera och dekryptera.
Nyckelkluster: Tillfälle när två olika nycklar skapar samma chiffertext från samma vanliga text.
Nyckelutrymme: Möjliga värden som används för att konstruera nycklar.
Vanlig text: Data i läsbart format, refereras även som klartext.
Arbetsfaktor: Uppskattad tid, ansträngning och resurser som är nödvändiga för att knäcka ett kryptosystem.

7.2 Typer av chiffer

Substitutions chiffer: Ersätter bitar, tecken eller block av tecken med olika bitar, tecken eller block.
Transpositions chiffer: Förändring används, vilket innebär att bokstäver flyttas om. Nyckeln bestämmer positionerna som karaktärerna skall flyttas till.
Frekvens analys: Analys av frekventa mönster av bokstäver som används i meddelande och konversation.
Springande nyckelchiffer: Använder steg i den fysiska världen runt om oss, som böcker (sida, radnummer och ordräkning). Varje ord är beskrivet av en sekvens av nummer.
Fördöljande chiffer: Varje X antal av ord inom en text, är en del av det riktiga meddelandet.
Steganografi: Döljande av data i ett annat meddelande för att förekomsten av data är dold. Ett meddelande kan döljas i en wave-fil, i grafik eller i oanvända ytor på en hårddisk eller sektorer som är markerade som oanvändbara.
Clipper chip: Ett NSA skapat bevismanipulerat chip för kryptering av data. Använder SkipJack algoritmen. Varje Clipper Chip har ett unikt serienummer och en kopia av enhetnyckeln är lagrat i en databas under detta serienummer. Det sändande Clipper Chipet skapar och skickar ett ”Law Enforcement Access Field (LEAF)” värde som ingår i det överförda meddelandet. Baseras på en 80 bitars nyckel och en 16 bitars checksumma.
Nyckel “Escrow”: Enhetsnyckeln delas i två sektioner och lämnas över till två olika “escrow” agenter för lagring.
Rimligt kryptosystem: Delar den növändiga nyckel som är krävs för dekryptering, men denna metod tar utrymme i mjukvarukrypteringsprocessen genom användande av publik nyckel kryptografi, där nyckel “escrow” används i huvudsak när hårdvarukrypteringschip används.

[125] *Encipher*
[126] *Decipher*

7.3 Metoder för kryptering

7.3.1 Symetrisk kryptografi

Båda parter använder sig av samma nyckel för kryptering och dekryptering. Kan endast erbjuda konfidentialitet. Är snabba och svåra att knäcka.
Styrka – Mycket snabbare än asymetriska system / Svåra att knäcka om man använder sig av en stor nyckel.
Svaghet – Nyckeldistribution (kräver en säker mekanism för att leverera nyckeln ordentligt) / Skalbarhet (varje par av användare behöver ett unikt par nycklar) / Begränsad säkerhet (kan endast erbjuda konfidentialitet).
Utan-för-bandet metod: Nyckeln transporteras genom en annan kanal än meddelandet.

7.3.2 Asymmetriska algoritmer

Två olika asymetriska nycklar är matematiskt relaterade, publik och privat nyckel.
Styrka – Bättre nyckeldistribution än symetriska system / bättre skalbarhet än symetriska system / kryptering kan erbjuda konfidentialitet, autencering och oavvislighet.
Säkra meddelande format – Krypteras med mottagarens publika nyckel.
Öppna meddelandeformat – Krypteras med avsändarens privata nyckel.
Säkra och signeradeformat – Krypteras med avsändaren privata nyckel och krypteras sen med mottagarens publika nyckel.

7.4 Två typer av symetriska algoritmer

7.4.1 Ström chiffer

Behandlar meddelandet som en ström av bitar och bytes och gör matematiska funktioner för dem individuellt. Nyckelen är ett slumpmässigt värde infört i ström chiffret, vilket används för att säkerställa slumpmässigheten i nyckelströms data. Är mest tillämpliga för hårdvaru implementationer, eftersom de krypterar och dekrypterar en bit i taget. Är intensiva eftersom varje bit måste manipulieras, vilket fungerar bättre på silikon nivå.

Karaktärsdragen för en stark och effektiv chiffer algoritm – Långa perioder av icke repeterande mönster inom nyckelströms värden / statistikt oförutsägbara / nyckelströmmen är inte linjärt relaterad till nyckeln / statistikt icke snedfördelad nyckelström (lika många 0or som 1or).
Nyckelströms generator – Skapar en ström av bitar som är XOR-bearbetade med vanliga textbitar för att skapa chiffertext.

7.4.2 Block chiffer

Meddelande delas upp i block av bitar. Använder sig av spridning och förvirring i sina metoder.
Använder substituions boxar (S-boxar) i varje steg. Det är nyckeln som bestämmer vilka funktioner som tillämpas för den vanliga texten och i vilken ordning. Är mer lämpliga för mjukvaruimplementationer, eftersom de arbetar med block av data vilket ofta är bandbredden för databussen (64 bits). Block chiffer arbetar ibland i ett läge som emulera ett ström chiffer.
Förvirring – Olika okända nyckelvärden används.
Spridning – Sätter bitar in i den vanliga texten genom många olika funktioner så att de sprids genom algoritmen.
S-box – Innehåller en uppslagstabell som ger instruktioner hur bitar skall förändras eller flyttas runt. Nyckeln som används i dekrypteringsprocessen dikterar vilka S-boxar som används och vilken ordning.

7.5 Typer av symetriska system

7.5.1 Datakrypeterings standard [127]

Certfierad av NIST, baserad på IBM's 128 bitars algoritm Lucifer. Är en blockkrypto algoritm. 64 bitar in -> 64 bitar ut. 56 bitar utgör den riktiga nyckeln och 8 bitar används för paritet. Ett block med 64 bitar delas i halvor och varje tecken krypteras ett åt gången. Tecknen går igenom 16 runder av transponering och ersättningsfunktioner. Har fyra distinkta läge för att fungera:
ECB[128] / Elektronisk kodbok – Inhemskt krypteringsläge. Erbjuder receptet för substitutioner och förändringar som kommer att utföras för block av vanlig text. Data inom en fil behöver inte bli krypterat i en speciell ordning. Används för små mängder av data, som utmaning-svar, nyckelhanterings uppgifter. Används också för att kryptera PIN koder i ATM maskiner.
CBC[129] / Chiffer block länkning – Varje block av text, nyckeln och det värde som baseras på det tidigare blocket bearbetas i algoritmen och tillämpas på nästa block av text.
CFB[130] / Chiffer gensvars läge – Den tidigare genererade chiffertexten från det senast krypterade blocket av data förs in i algoritmen för att generera slumpvärde. Dessa slumpmässiga värden bearbetas med det nuvarande blocket av vanlig text för att skapa chiffertext. Detta läge används när kryptering av enskilda tecken krävs.
OFB [131] / Reslutat Gensvar - Fungerar som ett strömchiffer genom att skapa en ström av slumpmässiga binära bitar för att kombineras med den vanliga texten för att skapa chiffertext. Chiffertexten förs tillbaka till algoritmen för att skapa den av nästa indata för att kryptera nästa ström av bitar.
DEA – Data Krypterings Algoritm[132].
FIPS – Federal Informationsbearbetnings Standard[133].

7.5.2 Trippel-DES, 3DES

Använder 48 runder i sin beräkning. Kräver mycket prestanda och kan ta upp till tre gånger så lång tid som DES för att utföra kryptering och dekryptering.

7.5.3 Avancerad Krypterings standard[134]

NIST ersättning av standard för DES. Vinnare var Rijndael, vilket är ett blockchiffer med en variabel blocklängd och nyckellängd.
Använder en kretslopps omvandling som omfattar tre lager av distinkta och inverterade omvandlingar: Det icke linjära lagret / det linjära blandningslagret / lagret för att lägga till nycklar. Är anpassat för höghastighetschip utan utrymmes restriktioner / en kompakt stödprocessor på ett smart kort.
Internationell Data Krypterings Algoritm[135]:
Blockchiffer som arbetar på 64 bitars block av data. Nyckeln är 128 bitar lång. Det 64 bitars datablocket delas i 16 mindre block och varje har åtta runder av matematiska funktioner som utförs på det. Det används i PGP krypterings mjukvara.
Blowfish:

[127] Data Encryption Standard (DES)
[128] Electronic Code Book
[129] Cipher Block Chaining
[130] Cipher Feedback Mode
[131] Output Feedback
[132] Data Encryption Algorithm
[133] Federal Information Processing Standard
[134] Advanced Encryption Standard (AES)
[135] *International Data Encryption Algoritm (IDEA)*

Ett block chiffer som arbetar på 64-bitars block av data. Nyckellängden kan vara upp till 448 bitar och datablocket går igenom 16 runder av kryptografiska funktioner.
RC5:
Ett block chiffer som har en blandning av parametrar. Det kan användas för blockstorlek, nyckelstorlek och antalet runder som används. Blockstorleken: 32/64/128 och nyckelstorlek upp till 2048 bitar.

7.6 Typer av asymmetriska system

7.6.1 RSA

Erbjuder autenciering, digital signatur, och kryptering. Säkerheten kommer från svårigheten vid faktorisering av stora tal, där nycklarna är funktioner av ett par stora primtal.
Används i många web browser som SSL, i PGP och myndighetssystem som använder publika kryptosystem.

7.6.2 El Gamal

Används för digital signatur och nyckelutväxling. Baseras på kalkyleringen av diskreta logritmer i ett begränsat fält.

7.6.3 Elliptisk kurv kryptosystem[136]

Erbjuder digitala signaturer, säker nyckeldistribution och kryptering. Kräver mindre andel av resurser än för andra system. Baseras på egenskaperna från eliptiska kurvor i deras publika nyckelsystem.

7.7 Hybrid Krypterings metoder

7.7.1 Publik Nyckelkryptografi

Använder två nycklar skapade av en asymetrisk algoritm för att skydda kryptering nycklar och nyckeldistribution och en hemlig nyckel skapas av en symetrisk algoritm och används för bulk kryptering.
- Asymmetrisk algoritm utför kryptering och dekryptering genom användade av publika och privata nycklar.
- Symmetrisk algoritm utför kryptering och dekryptering genom att användade av en hemlig nyckel.
- En hemlig nyckel används för att kryptera det verkliga meddelandet.
- En hemlig nyckel är synonym med en symetrisk nyckel.
- En asymetrisk nyckel refereras till en publik och privat nyckel.

Diffie-Hellman Nyckel Utväxling
Var först att introducera begreppet Publik Nyckel Kryptografi. Används för nyckeldistribution och det kan inte användas för kryptering och dekryptering av meddelande.
Sessionsnycklar
Är en hemlig nyckel som används för att kryptera meddelande mellan två användare. Är endast giltig för en session.

[136] Eliptic Curve Cryptosystem, ECC

7.8 Symmetriska kontra Asymmetriska System

Attribut	Symmetrisk	Asymetrisk
Nycklar	En nyckel delas mellan två eller fler enheter	En enhet är en publik nyckel och den andra enheten har en privat nyckel.
Nyckel utväxling	Ej tillämpligt	Symmetrisk nyckel krypteras och skickas med meddelande: sålunda, nyckeln distribueras genom inbordes medel.
Hastighet	Algoritmen är mindre komplex och snabbare	Algorithmen är mer komplex och långsamare.
Nyckellängd	Bestämd nyckellängd	Variabel nyckellängd
Användande	Bulk kryptering, vilket innebär kryptering av filer och kommunikationsvägar	Nyckel kryptering och distribution av nycklar
Säkerhetstjänst som erbjuds	Konfidentialitet och integritet	Konfidentialitet, integritet, autenciering och oavvislighet

7.9 Publik Nyckel Infrastruktur, PKI

Digitala certifikat – En referens som innehåller den publika nyckeln för individen tillsammans med annan identifierande information.
Certifikats auktoritet (CA) – En organisation som upprätthåller och utfärdar publika nyckel certifikat.
Certifikats revokerings lista (CRL) – En lista för varje certifikat som har blivit revokerade av en eller en annan orsak. Listan underhålls periodiskt.
Certifikat – Är mekanismen som används för att associera en publik nyckel med en samling av komponenter tillräckligt för att unikt autensiera den påstådda ägaren.
Registerings auktoritet (RA) – Utför certifikats registrerings uppgifter.
PKI enheter och funktioner – CA / RA / certifikats lagringsplats / certifikats revokerings system / nyckel säkerhetskopia och återställande system / automatisk nyckel uppdatering / hantering av nyckel historik / kors-certifiering med andra CA / tidsstämpling / klient mjukvara.
PKI erbjuder – Konfidentialitet/ Styrning av åtkomst / Integritet / Autenciering.

7.10 En-vägs funktion

Är en matematisk funktion som är enklare att beräkna i en riktning än i den motsatta riktningen.
Fallucka en-vägs funktion – Grunden för publik nyckel kryptografi. En publik nyckel krypterar och en privat nyckel (fallucka) dekrypterar.

7.11 Meddelande integritet

En-vägs hash
Är en funktion som tar en variabel-längd sträng av ett meddelande och komprimerar respektive transformerar det till ett värde med fixerad längd som refereras som ett hash värde.
Meddelandesammandrag – Hash värdet för en envägshash.
En-vägs funktion används i publik nyckel kryptografi – Hjälper krypteringsalgoritmen att erbjuda konfidentialitet och autenciering, krypterar i en riktning och dekrypterar i motsatt riktning.
En-vägs hash funktion – Det uförs aldrig omvänt / det erbjuder integritet för ett meddelande, inte konfidentialitet eller autenciering / resultatet av en en-vägs hash är ett hash värde / Det används vid hashberäkning för att skapa ett fingeravtryck för ett meddelande.
Digital signatur
Är ett krypterat hashvärde av ett meddelande.
Digital signatur standard[137]
En standard för digitala signaturer och dess funtioner och accepterade avnändande. Kräver Digital Signatur Algoritm (DSA) och Säker Hash Algortim (SHA).

7.12 Olika Hash algoritmer

MD4 – Skapar 128-bitars hash värden. Används för höghastighetes beräkningar i mjukvaru-implementationer och är optimerade för microprocessesorer.
MD5 – Skapar 128-bitars hash värden. Mer komplex än MD4. Bearbetar text i 512-bitars block.
MD2 – Skapar 128-bitars hash värden. Långsammare än MD4 och MD5.
SHA – Skapar 160-bitars hash värden. Detta infogas därefter i DSA, vilken beräkar signaturen för ett meddelande. Meddelandets sammandrag signeras istället för hela meddelandet.
SHA1 – Uppdaterad version av SHA.
HAVAL – Är en varibel längd en-vägs hash funktion och är en modifiering av MD5. Bearbetar text i 1024-bitars block.

7.12.1 Attacker mot en-vägs hash funktioner

Kollision – Om algoritmen skapar samma värden för två distinkt olika meddelanden.
Födelsedags attack – Är en attack på hash funktioner genom rå kraft. Attackeraren försöker hitta två meddelande med samma hashvärden.

7.12.2 En-gångs stämpel

Är oknäckbart och varje stämpel används exakt en gång.
Använder en sann icke repeterande uppsättning av slumpmässiga bitar som är kombinerade bit-vis XOR med meddelande för att skapa chiffertext.
Den slumpmässiga nyckeln har samma storlek som meddelandet och används endast en gång.
Svårigheter att distribuera stämplarna med slumpmässiga tal till alla nödvändiga parter.

7.13 Nyckelförvaltning

Kerberos – Ett nyckel distributions center (KDC) används för att lagra distribuera och underhålla kryptografiska sessions nycklar.
Diffie-Hellman – Använder en nyckelutväxlingsalgoritm (KEA).

[137] *DSS*

7.13.1 Nyckelförvaltningsprinciper

Bör inte vara i klartext utanför den kryptografiska enheten.
Säkerhetskopior bör vara tillgängliga och lättillgängliga när de behövs.
Ett företag kan välja mellan att ha flerparts kontroll för nödfallsnyckel återläsning. Detta betyder att om en nyckel behöver återläsas, krävs mer än en person för att vara involverad i processen.

7.13.2 Regler för nyckel och nyckelförvaltning

- Nyckellängden bör vara tillräckligt lång för att erbjuda nödvändig nivå av skydd
- Nycklar bör lagras och överföras genom säkra medel.
- Nycklar bör vara extremt slumpmässiga och använda hela spektrumet av nyckelutrymme.
- Nyckelns livstid bör överensstämma med känsligheten i data som den skall skydda.
- Ju mer nyckeln används, destu kortare bör livslängden vara.
- Nycklar bör säkerhetskopieras och deponeras i händelse av nödfall.
- Nycklar bör förstöras ordentligt när deras livslängd nått slutet.

7.14 Länk kontra ände-till-ände kryptering

7.14.1 Länk kryptering

Krypterar all data längs en specifik kommunikationsväg som en satellit länk, T3 linje eller telefonkrets.
Användarinformation, huvud, släp, adresser och transportvägsdata som är en del av paketet krypteras.
Erbjuder skydd mot paketsniffers och avlyssnare.
Paketet måste dekrypteras vid varje hopp och krypteras på nytt.
Förekommer på det fysiska lagret.

7.14.2 Början-till-slut krypteirng

Endast information krypteras.
Initieras vanligtvis i applikationslagret i den urprungliga datorn.
Förblir krypterat från början av sin resa till slutet.
Större grovkornighet i krypteringen är tillgänglig eftersom varje applikation eller användare kan använda olika nycklar.

7.15 E-post standards

7.15.1 Privat-utökad e-post[138]

Erbjuder autenciering, meddelande intgritet, kryptering och nyckel förvaltning
Specifika komponenter kan användas:
- Meddelanden krypteras med DES i CBC läge.
- Autenciering erbjuds av MD2 och MD5.
- Publik nyckelförvaltning erbjuds av RSA.
- X.509 standard används för certifikats struktur och format.

7.15.2 Meddelande Säkerhets Protokoll[139]

Kan signera och kryptera meddelande och utföra hash funktioner.

[138] Privacy-enhanced mail - PEM
[139] Message Security Protocol - MSP

7.15.3 Pretty Good Privacy, PGP

Första spridda publika nyckel krypteringsprogrammet.
Använder RSA publik nyckelkryptering för nyckelförvaltning och IDEA symetriskt chiffer för bulkkryptering av data.
PGP använder passerfraser, som används för kryptering av användarens privata nyckel som lagras på hennes hårddisk.
Förlitar sig på ”web of trust” i sin nyckelförvaltnings angreppssätt.
Nyckelring – Varje användare behåller en samling av signerade publika nycklar han har mottagit från andra användare.

7.16 Internet Säkerhet

7.16.1 HTTP

Ligger på toppen av TCP/IP
Är ett tillståndfritt protokoll, klient och webserver skapar och avbryter en anslutning för varje bearbetning.

7.16.2 S-HTTP – Säker Hypertext Transport Protokoll[140]

Utvecklad för att erbjuda säker kommunikation.
Krypterar meddelanden med sessionsnycklar som beräknas.
Erbjuder integritet och avsändarens autencieringsförmåga.
Är inte ett tillståndsfritt protokoll.
Kan stödja multipla krypteringsläge och typer.
Kan använda publik nyckelteknologi och symetrisk kryptering.
Används när ett individuellt meddelande behöver krypteras.

7.16.3 HTTPS

Skyddar kommunikationskanalen mellan två datorer.
Använder SSL och HTTP för att erbjuda en skyddad krets mellan klient och server.
Används när all information som utbyts mellan två datorer behöver krypteras.

7.16.4 SSL – Säkert Fördjupningslager[141]

Skyddar en kommunikations kanal.
Använder publik nyckelkryptering.
Erbjuder datakryptering, server autenciering, meddelandeintegritet och som option klient autenciering.
Håller kommunikationskanal öppen tills en av parterna begär att avsluta sessionen.
Ligger mellan applikationslagret och ovanpå transportlagret.

7.16.5 MIME – Flerändamåls Internet E-post tillägg[142]

Indikerar hur multimedia data och e-post meddelande skall överföras.

[140] Secure Hypertext Transport Protocol
[141] Secure Sockets Layer
[142] Multipurpose Internet Mail Extension

7.16.6 S/MIME – Säker MIME[143]

Standard för kryptering och digital signering av elektronisk post som innehåller bilagor och erbjuder säker dataöverföring.
Erbjuder konfidentialitet genom användarens krypteringsalgoritm, integritet genom användarens hash algoritm, autenciering genom användande av X.509 publika nyckel certifikat och oavvislighet genom kryptografiskt signerade meddelanden.

7.16.7 SET – Säker Elektronisk Transaktion[144]

Utvecklat för att skicka krypterade kreditkortsnummer.
Omfattar tre huvudparter, den elektroniska plånboken, mjukvaran som körs på försäljarens server och på dennes website och betalningsservern som är placerad på försäljarens bank.

7.16.8 Cookies

Textfiler som en browser behåller på en användares hårddisk.
Används för demografi och annonsinformation.
Används som tidsstämpling för att försäkra sig om att en session mellan en användare och en server är begränsad till ett specifikt tidsutrymme.
Cookies som innehåller känslig information bör krypteras av servern på siten som distribuerar dem.

7.16.9 SSH – Säkert skal[145]

Fungerar som en typ eller tunnel mekanism som erbjuder terminal liknande åtkomst till fjärrdatorer.
Borde användas istället för telnet, ftp, rlogin, rexec eller rsh.
Två datorer går igenom en handskakning och en säker kanal etableras.

7.16.10IPSec – Internet Protokoll Säkerhet[146]

En metod för att etablera en säker kanal för att skydda data som utväxlas mellan två enheter.
En spridd accepterad standard för säker nätverkslager transport.
Har stark kryptering och autencierings metoder som använder publik nyckelkryptering.
Används vanligtvis för att etablera VPN.
Är ett öppet modulärt ramverk som erbjuder mycket flexibilitet.
Har två grund säkerhetsprotokoll:
- AH – Autencerings Huvudet[147]: Är autencierings protokollet.
- ESP – Inkapslings Säkerhets Nytto-last[148]: Är ett autencierings och krypterings protokoll som använder kryptografiska mekansimer som erbjuder källautenciering, konfidentialitet och meddelandeintegritet.

Kan arbeta i två lägen:
- Transport läge: Nytto-lasten för meddelande krypteras.
- Tunnel läge: Nytto-lasten och huvudinformationen för meddelandet krypteras.

SA – Säkerhetsassociation[149] – Kan innehålla autencierings och krypteringsnycklar, den överenskomna algoritmen, nyckellivslängden och källans IP address. En SA för varje

[143] Secure MIME
[144] Secure Electronic Transaction
[145] Secure Shell
[146] Internet Protocol Security
[147] Authentication Header
[148] Encapsulating Security Payload
[149] Security association

anslutning.
SPI – Säkerhet Parameter Index[150] – Ett index som håller kontroll över olika SA och talar om för enheten vilken som är lämplig att anropa.
ISAKMP – Internet Säkerhets Association och Nyckel Hanterings Protokoll[151] – En autencierings och nyckel utväxlings arkitektur som är oberoende av vilken nyckelmekanism som används.

7.17 Attacker

7.17.1 Chiffertext attack

Den som attackerar har chiffertexten för flera meddelande. Varje meddelande har krypterats med samma krypteringsalgoritm.

7.17.2 Endast känd klartext

Den som attackerar har klartexten och chiffertexten för ett eller flera meddelanden.

7.17.3 Vald klartext attack

Den som attackerar har klartexten och chiffertexten och kan välja den klartext som blir krypterad.

7.17.4 Vald chiffertext attack

Den som attackerar kan välja chiffertexten som skall dekrypteras och har tillgång resultatet av den krypterade klartexten.

7.17.5 Man-mitt-imellan attack[152]

Avlyssning av konversationer. Genom att använda digitala signaturer vid sessionens nyckelutbyte kan attacken kringgås.

7.17.6 Ordlista attack[153]

Tar en lösenordsfil med envängs funktionsvärde och tar sen de mest vanliga använda lösenord och kör dem genom samma envägsfunktion. Filerna jämförs därefter.

7.17.7 Repris attack[154]

An attackerare kopierar en biljett och knäcker krypteringen och försöker sen utge sig för att vara klienten och lämnar på nytt biljetten vid ett senare tillfälle för att få otillåten åtkomst till en resurs.

[150] Security parameter index
[151] Internet Security Association and Key Management Protocol
[152] Man-in-the-middle attack
[153] Dictionary attacks
[154] Replay attack

8 CBK#6 Säkerhetsarkitektur & Modeller

8.1 Säkerhetsmodell

Är ett uttalande som visar huvuddragen för krav som är nödvändiga för att ordentligt stödja en specifik säkerhetspolicy.

8.2 Dator arkitektur

8.2.1 CPU – Central processor enhet[155]

Är en microprocessor.
Innehåller en kontrollenhet, en ALU / aritmetisk logisk enhet och ett primärt. lagringsutrymme. Instruktioner och data bibehålls i den primära lagringsenheten som behövs av den centrala processor enheten.
Det primära lagringsutrymmet är en temporär lagringsarea för att bibehålla instruktioner som skall tolkas av CPUn och användas för data bearbetning.
Buffer överflöde – Data som skall bearbetas förs in i CPUn i block vid varje tillfälle. Om mjukvaruinstruktionerna inte definierar gränserna för hur mycket data som kan komma in som ett extra block, kan extra data följa med och utföras.
Verkligt lagringsutrymme – Allt eftersom instruktioner och data bearbetas, förflyttas de tillbaka till systemets minnesutrymme / verkliga lagringsutrymme.

8.2.2 Minne

RAM / Slumpartat åtkomstminne[156] – Är ett flyktigt mine eftersom information går förlorad när strömmen upphör.
Typer av RAM:
- Statisk RAM – När det lagrar data, förblir det där utan att det kontinuerligt behöver bli uppdaterat.
- Dynamiskt RAM – Kräver att data inom minnet periodiskt måste uppdateras eftersom data skickas och förfaller.

ROM / Endast läsminne[157]– Är ett icke flyktigt mine. Mjukvara som lagras inom ett ROM kallas för ”firmware”.
EPROM / Raderbart och programerbart endast läsminne[158] – Bibehåller data som elektriskt kan raderas eller skrivas till.

8.2.3 Cache minne

Är en del av RAM som används för höghastighets skrivning och läsning.

8.2.4 PLD – Prgramerbar logisk enhet[159]

Är en integrerad krets med anslutningar och interna logiska portar som kan förändras genom programmeringsprocessen.

[155] Central Processing Unit
[156] Random Access Memory
[157] Read-only memory
[158] Erasable and programmable read-only memory
[159] Programmable Logic Device

8.2.5 Minnes kartläggning

Verkligt eller primärt minne - Minne som direkt addresseras av CPUn och som används för lagring av instruktioner och data som hänger samman med programmet som håller på att exekveras.
Sekundärt minne – Är ett långsammare minne (så som magnetskivor) som erbjuder icke flyktigt lagringsutrymme.
Sekvensiellt minne – Minne från vilken information måste erhållas genom sekvensiell sökning från början istället för att direkt söka åtkomst till lagringsplatsen (magnet band, ...).
Virtuellt minne – Använder sekundärt minne i förening med primärt minne för att presentera en CPU med större, synbart addressutrymme av verkliga lagringsplatser.

8.2.6 Minnes adressering

Register adressering – Adresseringregistren inom en CPU eller andra för speciella syften register som anges i primära minnet.
Direkt adressering – Adresserar en del av primära minnet genom att specificera den verkliga adressen för minnesplatsen. Minnesadresserna är vanligtvis begränsade till minnes sidor som exekveras eller till sidan noll.
Absolut adressering – Adressering av hela det primära lagringsutrymmet.
Index adressering – Utveckling av en minnesadress genom att lägga till innehållet för adressen definierad i programmets instruktioner genom ett index register. Den beräknade, effektiva adressen används för att få åtkomst till det efterfrågade minnesutrymmet. Således, om ett index register växer eller minskar, kan ett område av minnesutrymme ges åtkomst.
Antydd adressering – Används när operationer som är interna för processorn måste genomföras som rensning av en bärande bit vilken var definierad som ett resultat av en matematisk beräkning. Eftersom beräkningen utförs på ett internt register som specificeras inom instruktionen själv, finns det inget behov att förse med en adress.
Indirekt adressering – Adressering där adressutrymmet som specificeras i programminstruktionen innehåller adressen för den avslutande önskade platsen.

8.2.7 CPU lägen och skyddsringar

Skyddsringar – Förser strikta avgränsningar och definitioner avseende vad processen som arbetar inom varje ring kan få åtkomst till och vilka kommando som framgångsrikt kan exekveras. Processerna som bearbetas inom den inre ringen har större rättigheter, priviligerad / övervakande läge, än processorna som bearbetas i de yttre ringarna, användar läge.

8.2.8 Bearbetnings tillstånd

Redo tillstånd – En applikation är klar för att återuppta bearbetning.
Övervakande tillstånd – Systemet bearbetar ett sytem, eller högre rättighetsrutin.
Problem tillstånd – Systemet exekverar en applikation.
Vänte tillstånd – En applikation väntar på en specifik händelse för att fullfölja, så som en användare avslutar att registrera bokstäver eller väntar på att utskriftsarbete skall avslutas.

8.2.9 Flera trådar – uppgifter, bearbetning

Flera trådar – En applikation kan göra flera anrop på en gång, som använder olika trådar.
Flera uppgifter – CPUn kan bearbetar mer än en process eller uppgift åt gången.
Fler bearbetning – Om en dator har mer än en CPU och kan använda dem parallellt för att utföra instruktioner.

8.2.10 Inmatning/Utmatning enhetshantering

Dödläges situation – Om strukturer inte upplöses och frigörs efter användning. Resurser borde användas av andra program och processer.

8.3 System arkitektur

8.3.1 TCB – Betrodd Bearbetnings Bas[160]

Definieras som den totala kombinationen av skyddsmekanismer inom ett datorsystem.
Omfattar hårdvara, mjukvara och ”firmware”.
Ursrpungligen från den oranga boken.
Den oranga boken definierar ett betrott system som en hårdvara, mjukvara som utyttjar åtgärder för att skydda integriteten av icke klassificerad eller klassificerad data för ett utrymme av användare utan att bryta mot åtkomsträttigheter och säkerhetspolicy. Det ser på alla skyddsmekanismer inom ett system för att framtvinga säkerhetspolicy och förse en miljö som beter sig på ett sätt som förväntas.

8.3.2 Säkerhets omkrets

Definieras som resurser vilka faller utanför TCB.
Kommunikation mellan betrodda komponenter och icke betrodda komponenter behöver kontrolleras för att försäkra sig om att konfidentiell information inte flödar på icke avsedda vägar.

8.3.3 Referens övervakare

Är en abstrakt maskin, vilken förmedlar all åtkomst subjekt har till objekt för att försäkra att subjekt har nödvändiga åtkomsträttigheter och för att skydda objekt från otillåten åtkomst och destruktiv modifiering.
Är ett åtkomstkontroll koncept, inte en verklig fysisk komponent.

8.3.4 Säkerhetskärnan

Skapas av mekanismer som faller under TCB och inför samt framtvingar referens övervakar konceptet.
Är kärnan i TCB och är det vanligast använda angreppssättet för att bygga betrodda datorsytem.
Tre krav:
- Det måste erbjuda isolering av processer som utförs av referens övervakar konceptet och de måste vara säkra för manipulering.
- Referens övervakaren måste anropas för varje åtkomst forsök och måste vara omöjlig att kringgå. Sålunda, referens övervakaren måste införas på ett komplett och idiotsäkert sätt.
- Det måste vara tillräckligt litet för att kunna testas och verifieras på ett komplett och omfattande sätt.

8.3.5 Domäner

Definieras som en uppsättning av objekt som ett subjekt har möjlighet att få tillgång till.
Exekverings domän – Ett program som befinner sig i en priviligerad domän behöver ha möjlighet att exekvera sina instruktioner och beabeta dess data med en försäkran att program i en annan domän inte negativt kan påverka dess miljö.

[160] Trusted Computing Base

Säkerhets domän – Har ett direkt växelförhållande till skyddsringen som ett subjekt eller objekt är tilldelad. Ju lägre skyddsringens nummer är, destu högre är rättigheterna och större är säkerhetsdomänen.

8.3.6 Resurs isolering

Hårdvarusegmentering – Minne separeras fysisk istället för enbart logiskt.

8.3.7 Säkerhetspolicy

Är en uppsättning av regler och rutiner som talar om hur känslig information skall hanteras, skyddas och distribueras.
Flernivå säkerhetspolicy – Säkerhetspolicy som skyddar information från att flöda från en högre säkerhetsnivå till en lägre säkerhetsnivå.

8.3.8 Minsta rättigheter

Innebär att en resurs, process inte har mer rättigheter än vad som är nödvändigt för att kunna fullgöra sina funktioner.

8.3.9 Nivåer

En strukturerad och hierarkisk arkitektur som har den grundläggande funktionaliteten i lägre nivåer och mer komplexa funktioner i högre nivåer.

8.3.10 Data döljning

När det krävs att processer i olika lager inte kommunicerar, eftersom, de inte har något gränssnitt att interagera med varandra.

8.3.11 Abstraktion

När en klass av objekt är tilldelat specifika rättigheter och accepterade aktiviteter har definierats. Detta gör administrationen av olika objekt enklare eftersom klasser kan hanteras istället för att varje enskilt objekt hanteras.

8.4 Säkerhetsmodeller

Kartlägger de abstrakta mål i policyn för information systems termer genom att specificera explicita data strukturer och tekniker nödvändiga för att genomdriva säkerhetspolicyn.

8.4.1 Tillståndsmaskin[161] modellen

För att verifiera säkerhet i ett system, används tillståndet, vilket innebär att befintliga rättigheter och alla befintliga instanser av subjektet som skall ha åtkomst till objektet måste samlas.
Tillståndsövergång – Aktiviteter kan förändra ett tillstånd.
Ett system som använder en tillståndsmakin modell kommer att vara i ett säkert tillstånd i varje enskild fas av sin existens. Det kommer att starta i ett säkert tillstånd, utföra kommando och transaktioner säkert och det kommer tillåta subjekt att få åtkomstresurser endast i ett säkert tillstånd.

[161] State machine

8.4.2 Bell-LaPadula modellen

Beaktar bekymmer om systemsäkerhet och läckage av klassificerad information.
Flernivå säkerhetssystem – Ett system som använder Bell-LaPadula modellen, där användare med olika godkännande använder systemet och systemet bearbetar data med olika klassificeringar.
Nivån till vilken information är klassificerad bestämmer vilka hanteringsprocedurer som borde användas -> bildar ett spjälverk.
Spjälverk – Är en övre gräns och en lägre gräns för tillåten åtkomst.
Är en tillståndsmaskin modell som genomdriver konfidentialitets aspekter avseende styrning av åtkomst.
En åtkomstkontroll matris och säkerhetsnivåer används för att fastställa om subjekt kan ges åtkomst till olika objekt.
Modellen använder subjekt, objekt, åtkomst operationer (läs, skriv och läs/skriv) samt säkerhetsnivåer.
Är en informationsflödesmodell, vilket innebär att information inte flödar till ett objekt med lägre eller icke jämförbar klassficering.
Två huvudregler:

- Den enkla säkerhetsregeln – Ett subjekt i en given säkerhetnivå kan inte läsa data som befinner sig i en högre säkerhetsnivå. Refereras till ej ”läsa upp” regeln.
- *-egenskapen – Fastställer att ett subjekt i en given säkerhetsnivå inte kan skriva information till en lägre säkerhetsnivå. Refereras till ej ”skriva ner” regeln.

Definierar ett säkert tillstånd som en säker bearbetningsmiljö och tillåtna aktiviteter vilka är säkerhetsbevarande operationer.
Grundläggande säkerhetssats – Om ett system initieras i ett säkert läge och all tillståndsövergångar är säkra, då kommer varje efterföljande tillstånd att vara säkra oberoende av vilken indata som inträffar.
Modellen förser konfidentialitet, och beaktar inte integritet för den data som systemet upprätthåller.

8.4.3 Biba modellen

Är en informationsflödesmodell, bekymmrar sig om dataflöde från en säkerhetsnivå till en annan.
Använder sig av tillståndsmaskin modellen.
Beaktar att integriteten för data hotas när ett subjekt kan läsa data i en lägre nivå.
Förhindrar att data från vilken integritetsnivå som helst flödar till en högre integritetsnivå.
Två huvudregler:

- ”Skriv ej upp” – Ett subjekt kan inte skriva data till ett objekt i en högre integritetsnivå.
- ”Läs ej ner” – Ett subjekt kan inte läsa data från en lägre integritetsnivå.

8.4.4 Clark-Wilson modellen

Skyddar integriteteten för information genom att fokusera på att förebygga auktoriserade användare att göra icke auktoriserade förändringar av data, bedrägeri och felaktigeter i kommerciella applikationer.
Användare kan inte få tillgång till eller manipulera objekt direkt, utan måste få tillgång till objektet genom ett program.
Använder också uppdelning av uppgifter, vilket delar en operation i olika delar och kräver att olika användare utför varje del. Detta förhindrar auktoriserade användare att göra icke auktoriserade förändringar av data, vilket åter skyddar dess integritet.
Revision krävs också för att spåra information som kommer från utsidan av systemet.

8.4.5 Informationsflödes modell

Kan hantera vilken sorts informationsflöde som helst, inte enbart riktningen av flödet.
Tittar på osäkra informationsflöden som kan inträffa i samma nivå och mellan objekt tillsammans med flödet mellan olika nivåer.
Ett system är säkert även om det inte finns något otillåtet informationsflöde.

8.4.6 Ingen störnings modell

Försäkra att vilken aktivitet som helst som inträffar i en högre säkerhetsnivå inte påverkar eller stör aktiviteter som inträffar i en lägre nivå.

8.5 Säkerhetsformer för drift

8.5.1 Dedikerad säkerhetsform

Om alla användare har godkännande eller akuktorisation och behov-av-att-veta till all data som bearbetas inom systemet.
Alla användare har givits formellt tillstånd för åtkomst till all information i systemet och har signerat avtal för att inte avslöja något avseende denna information.
Systemet kan hantera en enskild klassificeringsnivå för information.

8.5.2 System med hög säkerhetsform

Alla användare har ett säkerhetsgodkännande eller auktorisation för att få åtkomst till information men inte nödvändigtvis behov-av-att-veta till all information som bearbetas i systemet (endast viss data).
Kräver att alla användare har den högsta nivån för godkännande, men en användare begränsas genom åtkomstkontroll matrisen.

8.5.3 Avdelningsvis säkerhetsform

Alla användare har godkännande att få åtkomst till all information som bearbetas av systemet, men har kanske inte behov-av-att-veta och formellt godkännande för åtkomst.
Användare är begränsade till att kunna få åtkomst till viss information eftersom de inte behöver ha åtkomst till det för att kunna utföra funktioner i sina arbeten och de har inte fått formellt godkännande att ha åtkomst till denna data.
Avdelningar är säkerhetsnivåer med begränsat antal av subjekt, säkerhetsgodkända att ha åtkomst till data i varje nivå.
CMW / Avdelningar – Gör det möjligt för användare att bearbeta flera avdelningar av data på samma gång, om de har nödvändigt säkerhetsgodkännande.

8.5.4 Flernivå säkerhetsform

Tillåter två eller flera klassficeringsnivåer för information att bearbetas samtidigt när alla användare inte har säkerhetsgodkännande eller formellt tillstånd att ha åtkomst till all information som bearbetas av systemet.

8.5.5 Förtroende och försäkran

Förtroende – Berättar för kunder hur mycket de kan förvänta sig av detta system, vilken säkerhetsnivå det erbjuder.
Försäkran – Systemet kommer att fungera korrekt och på ett förutsägbart sätt i varje enskild bearbetnings situation.

8.6 Systemutvärderings metoder

Undersöker säkerhetsrelevanta delar av ett sytem, vilket innebär TCB, styrning av åtkomst mekanismer, referens övervakaren, kärnan, skyddsmekanismer.

8.6.1 Den Oranga boken / TCSEC

TCSEC – Betrott Dator System Utvärderings Kriterie[162].
Utvärderar produkter för att bedömma om de innehåller säkerhetegenskaper som de påstår sig att ha och utvärderar om produkten är lämplig för en specifik tillämpning eller funktion.
Tittar på funktionalitet, ändamålsenlighet och försäkran om ett system under dess utvärdering och det använder klasser som är uttänkta för att beakta typiska mönster av säkerhetskrav.
Fokuserar på operativsystem.
Hierarkisk uppdelning av säkerhetsnivåer -
A – Verifierat skydd
B – Obligatoriskt skydd
C – Godtyckligt skydd
D – Minimalt skydd
Ämne – Säkerhetspolicy, ansvarighet, försäkran och dokumentation.
Områden –
Säkerhetspolicy – Måste vara explicit och väldefinierad och framtvingad av mekanismer inom systemet.
Identifiering – Individuella subjekt måste vara unikt identifierade.
Etiketter – Åtkomstkontroll etiketter måste vara associerade ordentligt inom objekt.
Dokumentation – Omfattar test, design, specifikation av dokument, användarguider och manualer.
Ansvarighet – Revisionsdata måste samlas och skyddas för att framtvinga ansvarighet.
Livscyckel försäkran – Mjukvara, hårdvara och firmware måste kunna testas individuellt för att vara säker på att var och en framtvingar säkerhetspolicyn på ett ändamålsenligt sätt genom dess livstid.
Kontinuerligt skydd – Säkerhetsmekanismer och systemet som helhet måste fungera förutsägbart och acceptabelt i olika situationer kontinuerligt.
Utvärderingsnivåer –
D – Minimalt skydd
C1 – Godtyckligt säkerhetsskydd
C2 – Kontrollerat åtkomstskydd
B1 – Etikett skydd
B2 – Strukturerat skydd
B3 – Säkerhetsdomäner
A1 – Verifierad design

[162] Trusted Computer System Evaluation Criteria

8.6.2 Den röda boken[163]

TNI – Betrodda Nätverks Tolkningar[164].
Beaktar säkerhetutvärderingsämnen för nätverk och nätverkskomponenter.
Beaktar isolerade lokala nätverk och utspridda Internet nätverkande system.
Säkerhetspunkter som beaktas:
* Kommunikations integritet.
— Autenciering
— Meddelande integritet
— Oavvislighet
* Förebyggande avseende vägran av service[165].
— Kontinuitet i drift
— Nätverks administration
* Äventyrande av skydd.
— Data konfidentialitet
— Trafikflödes konfidentialitet
— Selektiv routing
Klasser -
- Ingen
- C1 - Minimal
- C2 - Rättvis
- B2 - God

8.6.3 ITSEC

ITSEC – Informations Teknologi Säkerhets Utvärderings Kriteria[166].
Används endast i Europa
Två huvudattribut – Funktionalitet och försäkran.
Är ett kriterie för både säkerhetsprodukter och säkerhetssystem och refererar båda till målet för utvärdering[167].

8.6.4 Common Criteria

Är en internationell utvärderings standard.
EAL – Utvärderings försäkrans nivå.
Skyddsprofil – Samlingen av säkerhetskrav, deras avsikt och argumentation och den motsvarande EAL klassen.
Två huvudattribut – Funktionalitet och försäkran.
Fem sektioner avseende skyddsprofilen –
- Beskrivande beståndsdelar.
- Logisk grund.
- Funktionella krav.
- Krav avseende utvecklings förtroende.
- Krav avseende utvärderingens försäkran.

[163] The Red Book / TNI
[164] Trusted Network Interpretation
[165] Denial of service
[166] Information Technology Security Evaluation Criteria
[167] target of evaluation, TOE

8.7 Certifiering <-> Ackreditering

8.7.1 Certifiering

Är den tekniska utvärderingen av säkerhetskomponenter och deras efterlevnad avseende syftet med ackrediteringen.
Är processen för att bedömma de säkerhetsmekanismer och kontroller och utvärdering av deras ändamålsenlighet.

8.7.2 Ackreditering

Är den formella acceptancen av lämpligheten för ett systems övergripande säkerhet av ledningen.
Är ledningens officiella acceptans av information i certifieringsprocessens finnande.

8.8 Öppna system <-> Slutna System

8.8.1 Öppna System

Har en arkitektur som har publicerade specifikationer, vilka gör det möjligt för tredje parts leverantörer att utveckla tilläggskomponenter och enheter.
Erbjuder möjlighet till samverkan mellan produkter av olika leverantörer för olika operativsystem, applikationer och hårdvaruenheter.

8.8.2 Slutna System

Använder en arkitektur som inte följer industristandard.
Möjlighet till samverkan och standard gränssnitt används inte för att möjliggöra enkel kommunikation mellan olika typer av system och tilläggs funktioner.
Är patentskyddat, vilket innebär att systemet endast kan kommunicera med liknande system.

8.9 Hot mot säkerhetsmodeller och arkitekturer

8.9.1 Hemliga kanaler[168]

Är en väg för en enhet att ta emot information på ett icke auktoriserat sätt. Det är ett informationsflöde som inte kontrolleras av en säkerhetsmekanism.
Hemliga tid kanaler – En process vidarbefordrar information till en annan genom att anpassa dess användning av systemresurser.
Hemliga lagringskanaler – När en process skriver data till ett lagringsutrymme och en annan process direkt eller indirekt läser det. Problemet uppstår när processerna befinner sig i olika säkerhetsnivåer och därför inte förväntas dela känslig data.
- Motåtgärder:
Det finns inte mycket en användare kan göra för att motverka dessa kanaler.
För trojanska hästar som använder HTTP, intrångs detektering och granskning kan upptäcka hemliga kanaler.

[168] Covert Channels

8.9.2 Bakdörrar[169]

Kallas även underhållshakar.
Är instruktioner inom en mjukvara som endast utvecklaren känner till och kan anropa.
- Motåtgärder.
Kodgranskning och enhets- och integrations tester bör alltid leta efter bakdörrar.
Preventiva motåtgärder mot bakdörrar –
Värd intrångs detekterings system.
Använd filsystem rättigheter för att skydda konfigurations filer och känslig information från att bli modifierade.
Strikt åtkomst kontroll
Filsystems kryptering.
Revision

8.9.3 Anpassningsproblem

Kallas även asynkron attack.
Behandlar tidsdifferensen i följden av steg ett system använder för att fullgöra en uppgift.
En tid-att-kontrollera i motsats till en tid-att-använda attack, kallas också kapplöpningsvillkor, kan ersätta autexec.bat.
- Motågärder:
Värd intrångsdetekterings system.
Fil systems rättigheter och kryptering.
Strikt åtkomstkontroll
Revision.

8.9.4 Buffert Överflöde[170]

Refereras ibland till “spränga stacken”.
När program inte kontrollerar längden på data som förs in i ett program och sen bearbetas av CPU.
- Motåtgärder.
Ordentlig programmering och goda kodningsrutiner.
Värd intrångs detekteringssystem.
Fil systems rättigheter och kryptering.
Strikt åtkomstkontroll.
Revision.

[169] Back Doors
[170] Buffer Overflows

9 CBK#7 Operativ Säkerhet

9.1 Kontroller och Skydd

För att skydda hårdvara, mjukvara och media resurser från
- Hot i den operativa miljön.
- Interna och externa inkräktare.
- Operatörer som olämpligt har åtkomst till resurser.

9.1.1 Kategorier av Kontroller

- Preventativa Kontroller:
Är utformade för att minska omfattning och påverkan efter oavsiktliga fel som förs in i system och för att skydda ej auktoriserade inkrätare internt eller externa att få åtkomst till system.
- Detektiva Kontroller:
Används för att upptäcka fel när det har inträffat.
- Korrektiva Kontroller / Återställnings Kontroller:
Är införda för att mildra påverkan efter ett förlusttillfälle genom dataåterställnings procedurer.
- Avskräckande Kontroller / Anvisande Kontroller:
Används för att uppmuntra efterlevnad avseende externa kontroller.
- Applikations Kontroller:
Är de kontroller som är utformade i en mjukvaruapplikation för att minska och upptäcka mjukvarans operativa oregelbundenhet.
- Transaktion Kontroller:
Används för att förse kontroll över de olika stegen i en transaktion. Typer av kontroller är: Inregistrering, bearbetning, förändring och test.

9.1.2 Den Oranga Bokens Kontroller

Operationell försäkran:
- Systemarkitektur.
- System integritet.
- Analys av hemliga kanaler.
- Hantering av betrodd anordning.
- Betrodd återställning.

9.1.3 Livscyckel försäkran

- Säkerhets test.
- Specifikation av utformning och test.
- Konfigurations hantering.
- Betrodd distribution.

9.1.4 Analys av hemliga kanaler

- B2:
Systemet måste skydda mot hemliga lagringskanaler. Det måste utföra analys av hemliga kanaler för alla hemliga lagringskanaler.
- B3 and A1:
Systemet måste skydda mot både hemliga lagrings och tids kanaler. Det måste utföra en analys av hemliga kanaler för båda typer.

9.1.5 Hantering av betrodda anordningar

B2:
System måste stödja separata operatörer och system administratörsroller.
B3 and A1:
System måste tydligt identifiera funktioner för säkerhets administratören att utföra säkerhets relaterade funktioner.

9.1.6 Uppdelning av uppgifter och arbetsrotation

- Minsta rättighet:
Innebär att ett systems användare bör ha den lägsta nivån av rättigheter och privilegier nödvändiga för att utföra deras arbete och borde endast ha dem under kortast möjliga tidsperiod.
- Två-personer kontroll:
Två operatörer granskar och godkänner vara andras arbete, för att ge ansvarighet och för att minimera bedrägeri i starkt känsliga och hög-risk transaktioner.
- Dubbel kontroll:
Båda operatörer behövs för att fullfölja en känslig uppgift.
- Arbetsrotation:
Processen för att begränas det tidsutrymme en operatör är tilldelad att utföra en säkerhetsrelaterad uppgift innan han eller hon förflyttas till en annan uppgift med annan säkerhets klassificering.

9.1.7 Betrodd återställning

Försäkrar att säkerhet inte bryts vid händelse av en systemkrasch eller att annat systemfel inträffar.
Krävs endast för B3 och A1 nivå system.
- Framkallande av fel:
Ta säkerhetskopia på alla kritiska filer på regelbunden basis.
- Systemåterställning.
I common criteria tre hierarkiska återsällnings typer -
- Manuell återställning.
- Automatiserad återställning.
- Automatiserad återställning utan onödig förlust.

9.1.8 Konfiguration / Förändrings hanterings kontroll

Procedurer för att införa och stödja förändrings kontroll processen:
- Ansök om att införa en förändring.
- Katalogisera den tilltänkta förändringen.
- Planera förändringen.
- Inför förändringen.
- Rapportera förändringen till lämpliga parter.

9.1.9 Avklippsnivåer

Trösklar för specifika typer av fel och misstag som tillåts och antalet av dessa misstag som kan inträffa innan det betraktas som misstänkt. När avklippsnivån har överträtts, dokumenteras ytterligare överträdelser för granskning.

9.1.10 Administrativa Kontroller

Kontroller som är införda och underhållna av administrativ ledning för att hjälpa till att minska hotet eller påverkan av överträdelser avseende datorsäkerhet.

- Personalsäkerhet.
  - Undersökning vid anställning och bakgrundskontroller.
  - Obligatoriskt uttag av en veckas semester.
  - Arbetsvarningar och avsked.
- Uppdelning av uppgifter och ansvar.
- Minsta rättigheter.
- Behov av att veta.
- Förändrings/Konfiguration hanterings kontroll.
- Post bevarande och dokumentation.

9.1.11 Post Bevarande

Dataminne -
Refererar till data som blir kvar på media efter att mediat har blivit raderat.

9.1.12 Operativa Kontroller

Dag-för-dag procedurer som används för att skydda dator bearbetningar.
Resursskydd:
Är konceptet för att skydda en organisations bearbetnings resurser och tillgångar från förlust eller äventyrande. Omfattar hårdvara, mjukvara och data resurser.

9.1.13 Hårdvaru Kontroller

- Hårdvaru underhåll.
- Underhållskonton.
- Diagnostisk portkontroll.
- Hårdvaru fysisk kontroll.

9.1.14 Mjukvaru Kontroller

- Antivirus hantering.
- Mjukvarutester.
- Mjukvarufunktioner.
- Säker mjukvarulagring.
- Säkerhetskopierings kontroller.

9.1.15 Privilegerad Enhetskontroll / Privilegerade operativa funktioner

- Speciella åtkomstkommando till system.
- Åtkomst till speciella parametrar.
- Åtkomst till systemets kontrollprogram.

9.1.16 Media Resurs Skydd

Införs för att skydda vilket säkerhetshot genom medveten eller omedveten exponering av känslig data -
- Säkerhetskontroller för media:

Bör utformas för att förebygga förlust av känslig information och kan vara:
- Loggning.
- Åtkomstkontroll.
- Ordentligt bortskaffande.

- Användbarhetskontroll för media.

Bör användas för att skydda användbarheten av datalagrings media.
Krävs vid händelse av en sytemåterställningsprocess -
- Märkning.
- Hantering.
- Lagring.

9.1.17 Fysisk Åtkomstkontroll

Omfattar:
- Hårdvara.
- Mjukvara.

Speciella arrangemang för övervakning måste göras när externa support leverantörer träder in i datacenter.
Följa med på ryggen: Är när en icke auktoriserasd person går igenom en dörr bakom en auktoriserad person. Konceptet ”människofälla” är utformat för att förhindra det.

9.2 Övervakning och revision

9.2.1 Övervakning

Innehåller mekanismer, verktyg och tekniker vilka tillåter identifiering av säkerhetshändelser vilka skulle kunna påverka driften av en datorverksamhet.
Övervaknings tekniker -
- Intrångsdetektering.
- Penetrationstest.
  - Scanning och undersökning.
  - Demon Uppringning.
  - Sniffning.
  - Avfalls dykning.
  - Social Genomgång.
- Överträdelser i bearbetning genom att använda tröskelvärde.

9.2.2 Revision

Är grunden i övervakning av operativa säkerhetskontroller.
Revisionsspår.
Möjliggör en säkerhetsutövare att spåra en transaktionshistorik.
Problem hanteringskoncept:
- Minska felaktigheter till en hanterbar nivå.
- Förebygga inträffande eller återinträffande av ett problem.
- Lindra den negativa påverkan av problem avseende datortjänster och resurser.

9.3 Hot och sårbarheter

9.3.1 Hot

Oavsktlig förlust:
Är en förlust som man har utsatt sig för oavsiktligt, även om det inte beror på brist av dator utbildning eller skicklighet eller av funktionsstörning i en applikations bearbetningsrutiner.
- Operatörers inregistrerings fel eller utelämnande.
- Transaktions bearbetnings fel.

Olämpliga aktiviteter:
Är ett datorbeteende som, vilket inte uppnår nivån för kriminella aktiviteter, kan kanske ligga till grund för arbetsvarning eller avsked.
- Olämpligt innehåll.
- Slösande av företagets resurser.
- Sexuella eller ras trakasserier.
- Missbruk av privilegier och rättigheter.

Illegala Dator operationer och avsiktliga attacker:
Dator aktiviteter som anses som avsiktliga och illegala dator aktiviteter för personlig finansiell vinning avseende förstörande.
- Avlyssning.
- Bedrägeri.
- Stöld.
- Sabotage.
- Externa Attacker.

9.3.2 Sårbarheter

- Trafik / Trend analyser
- Underhållskonton.
- Data sopnings attacker.
- IPL sårbarheter.
- Nätverksadress kidnappning.

9.4 E-post och Internet Säkerhets frågor

9.4.1 E-post

- SMTP – Fungerar som en agent för överföring av meddelanden.
- POP – Är ett Internet e-post server protokoll som stödjer inkommande och utgående meddelanden. När meddelandet har lästs ner från POP server, tas de vanligtvis bort från denna server.
- IMAP – Är ett Internet protokoll som möjliggör för användare att få tillgång till e-post på en e-post server. Meddelande kan läsas ner eller låta dem vara kvar på e-post servern inom dennes fjärr folder, refererad som postlåda.

9.4.2 Hack och Attack Metoder

- Port Scanning och nätverkskartläggning:

Nätverkskartläggnings verktyg skickar ut skenbara inlednings paket till många olika system i ett nätverk.
Port scanning identifierar öppna portar på en dator.
- Superzapping:

Är en funktion som används i IBM stordator center och har förmågan att kringgå kontroll avseende åtkomst inom operativ system.

- Bläddrande:
Är en generell term som används av inkräktare för att få tillgång till information de inte är auktoriserade att få åtkomst till.
Kan uppnås genom att söka igenom en annan persons filer som lagras på en server eller arbetsstation, söker igenom papperskorg sökande efter inforamtion som oförsiktigt har kastats eller granska information som har sparats på disketter.
- Sniffers
Verktyg som övervakar trafik allt eftersom det passerar.
Verktyget är antingen en hårdvara eller en mjukvara som körs på en dator med dess nätverks gränssnitts kort (NIC) i planlöst läge.
- Sessions kidnappning.
En attackerare placerar sig själv i mitten av en konversation utan att bli upptäckt.
- Lösenordsknäckning.
Insamling och avslöjande av lösenord -
- Ordboks attack: Är när en stor lista av ord förs in i ett intrångs verktyg. Detta verktyg kör en en-vägs hash på de insamlade lösenorden och för varje ord i listan. Verktyget jämför hashings resultatet för att se om de stämmer med varandra. Om de stämmer överens har verktyget upptäckt lösenordet, om inte flyttar det till nästa ord i listan.
- Attack med rå styrka: Ett verktyg kommer att testa många olika variationer av karaktärer, köra ett hashvärde på varje variation och jämföra detta med det hash värde för de insamlade lösenorden.
- Bakdörrar
Är ett program som installeras av en inkrätare för att möjliggöra för denne att komma tillbaka in i datorn vid ett senare datum utan att behöva ange inloggningsreferenser eller att gå igenom någon typ av auktorisationsprocess.

10 CBK#8 Kontinuitets planering & Avbrotts planering

10.1 BCP / Kontinuitets Planering[171]

Viktigaste beståndsdelar:
- Omfattning och initiering av plan.
- Bedömning av påverkan på verksamheten.
- Utveckling av verksamhetens kontinuitetsplanering.
- Godkännande av plan och införande.

10.1.1 Omfattning och initiering av plan

Markerar början på BCP processen.
Det medför skapande av omfattning av planen.

Roller och ansvar -
BCP Kommitté:
Bör formeras och tilldelas ansvaret att skapa, implementera och testa planen.
Skapas av representanter från högsta ledningen, alla funktionella affärsenheter, informations system och säkerhets administratör.
Högsta ledningens roll:
Är ytterst ansvarig för alla fyra faser i planen.

10.1.2 BIA / Bedömning av påverkan på verksamheten[172]

Är en process som används för att hjälpa affärsenheter att förstå påverkan av ett avbrottstillfälle.
Påverkan kan vara finansiell (kvantitativ) eller operationell (kvalitativ, så som oförmåga att svara kunder).
En sårbarhetsanalys är ofta en del av BIA processen.
Det identifierar företagets kritiska system som är nödvändiga för överlevnad och uppskattar den utslagna tid som accepteras av företaget som ett resultat av en katastrof eller störning.

Tre huvud primära mål med BIA -
- Prioritering av vad som är kritiskt:
Varje kritisk verksamhetsenhets process måste identifieras och prioriteras och påverkan av en störande händelse måste utvärderas.
- Nertids uppskattning
Uppskatta MTB / Maximalt tillåten nertid[173] som verksamheten kan acceptera och fortfarande vara ett livskraftigt företag.
- Resurskrav:
Resurskrav för kritiska processer är också identifierade vid denna tidpunkt, med de mest tidskänsliga processerna ges den mesta resursallokeringen.

Fyra steg i BIA -
- Samla behovet av bedömnings material:
Identifiera vilka verksamhetesenheter som är kritiska för att kunna bibehålla en acceptabel nivå på driften.

[171] Business Continuity Planning
[172] Business Impact Assessment
[173] Maximum Tolerable Downtime

- Genomför sårbarhetsanalysen:
Är mindre än en fullständig riskanalys och är fokuserad på att ge information som används uteslutande för BCP och DRP.
En funktion är att genomföra en påverkan av förlust analys.
Kritiska supportområden måste definieras
- Analysera information som sammanställts.

10.1.3 Utveckling av verksamhetens kontinuitetsplanering

Refererat till att använda information som samlats in i BIA för att ta fram den verkliga kontinuitetsplanen.
Detta innefattar områden som införande av plan, test av plan och pågående underhåll av plan.

Två huvudsteg -
- Definiera kontinuitets strategi:
Hur verksamheten förväntas hantera en katastrof störning.
- Dokumentera kontinuitets strategin:
Skapande av dokumentation för utfallet.

10.1.4 Godkännande av plan och införande

Involverar att få slutliga ledningen att signera, skapa verksamhetsövergripande medvetenhet om planen och införa underhållsrutiner för att updatera planen efter behov.

10.2 DRP / Avbrottsplanering[174]

Är ett omfattande uttalande och överenstämmande aktiviteter som skall vidtas före, under och efter en störande händelse som orsakar en betydande förlust av informationssystems resurser. Huvudmålen är att förse förmågan att införa kritiska processer på en alternativ driftsplats och återgå till huvuddriftsstället och normal bearbetning inom en tidsram som minimerar förlusten för organisationen, genom att exekvera snabba återställnings rutiner.

Katastrof planerings process faser:
- Databearbetnings kontinuitets planering.
- Dataåterställningsplan underhåll.

10.2.1 Data bearbetnings kontinuitets planering

Vanliga alternativa bearbetningstyper -
- Ömsesidiga hjälpavtal / Ömsesidiga avtal:
Är ett arrangemang med ett annat företag som kanske har liknande bearbetningsbehov.
Fördelar är låg kostnad.
Nackdelar är att det är högst osannolikt att varje organisations infrastruktur kommer att ha extra kapacitet för att möjliggöra fullständig operativ bearbetning under händelsen.

- Abonnemangs tjänster:
  - Varm plats:
Är en fullständigt konfigurerad datorenhet med el, värme, ventilation och luftkonditionering (HVAC) och fungerande fil/skrivar servers och arbetsstationer.
Fördelen är 24/7 tillgänglighet

[174] Disaster Recovery Planning

Nackdelen är att det är dyrt, att tjänsteleverantören kanske säljer över sin kapacitet, säkerhetsexponering när information lagras på två olika platser och kan kanske vara administrativt krävande när kontroller måste implementeras två gånger.

- Varm plats:

Är en enhet redo att få tillgänglig med el och luftkonditionering och datorer, men applikationer är kanske inte installerade.
Fördelen är att kostnaderna är mindre än för en varm plats, mer flexibel i val av plats och mindre administrativa resurser än för en varm plats.
Nackdelarna är skillnaden i tiden och ansträngningen som det kräver för att starta produktionen på den nya platsen.

- Kall plats:

Är redo för utrustning att föras in under ett nödläge, men ingen hårdvara finns på plats.
Fördelen är låg kostnad.
Nackdelen är att det kanske inte fungerar när en katastrof inträffar.

- Flera centra:

Bearbetningen är spridd över driftscenter, skapar ett distribuerat angreppssätt avssende redundans och delning av tillgängliga resurser.
Fördelen är låga kostnader
Nackdelen är att en större katastrof kan enkelt ta över bearbetnings förmågan för platsen.

- Servicebyrå:

Kontrakt med en servicebyrå för att säkerställa alla alternativa reserv bearbetningsstjänter.
Fördelen är snabbt gensvar och tillgänglighet
Nackdelen är kostnaden och resursstrider under ett större nödläge.

- Andra datacenter reserv alternativ:
  - Rullande/mobila reservplatser.
  - Interna eller externa leveranser av hårdvara för ersättning.
  - Prefabricerade byggnader.

Tre koncept används för att skapa en nivå av feltollerans och redundant överförings bearbetning:
- Elektroniska hopp:
Refererar till överföringen av säkerhetskopierad data till en off-site plats. Detta är primärt en batch process avseende dumpa data genom kommunikations linjer till en server på en alternativ plats.
- Fjärr dokumentation:
Refererar till parallell bearbetning av transkationer till en alternativ plats. En kommunikationslinje används för att överföra live när det inträffar.
- Databas skuggning:
Använder realtids bearbetning av fjärrdokumentation, men skapar även mer redundans genom att duplicera databas set till multipla servrar.

10.2.2 Underhåll av dataåterställningsplan

Upprätthålla planer updaterade och relevanta.

Testa DRP / Avbrottsplaner:
Typer av tester -
- Checklistor:
Kopior av planer distribueras till ledningen för granskning.
- Strukturerad genomgång:
Verksamhetsenhetsledning möts för att granska planen.
- Simulationstest:
All supportpersonal möts för en praktisk utförande session.
- Parallelltest:
Kritiska system körs på en alternativ plats.

- Full-Avbrottstest:
Normal produktion stängs ner, med verkliga avbrottsplanerings processer.

Huvudelement för avbrottsplaneringsprocessen -
- Återställningsteamet:
Definieras tydligt med mandat att införa återställnings processer när en katastrof har deklarerats.
Huvudmålet är att få de fördefinierade kritiska verksamhetsfunktionerna i drift i en alterantiv reserv bearbetnings plats.

- Räddningsteamet:
Kommer att skickas tillbaka till den primära platsen för den normala bearbetnings miljöns villkor.
Detta team ges ofta auktoritet att kunngöra när platsen kan återupptas eller inte.

- Normal drift återupptas:
Fullständiga rutiner avseende hur företaget kan återgå med produktionsbearbetning från en alternativ plats till den primära platsen med ett minimum av störning och risk.
Nödläget är inte över förrän all drift är tillbaka i fullt produktionsläge på den primära platsen.

- Andra återställnings frågor:
  - Gränssnitt med externa grupper.
  - Relationen med anställda.
  - Bedrägeri och brott.
  - Finansiella utbetalningar.
  - Media relationer.

11 CBK#9 Lagar, Utredningar& Etik

11.1 Etik

11.1.1 ISC2

"Code of Ethics Canons" -
- Skydda samfundet, samhället och infrastrukturen.
- Agera hedersvärt, ärligt, rättvist, ansvarigt och legalt.
- Erbjuda arbetsamma och kompetenta tjänster till uppdragsgivare.
- Utveckla och skydda professionen.

11.1.2 IAB – Internet Aktivitets Styrelsen[175]

Oetiskt och oacceptabelt beteende -
- Avsiktligt sökande för att få oaktoriserad åtkomst till Internet resurser.
- Störa det avsedda användande av Internet.
- Slösa resurser genom målmedvetna aktiviteter.
- Förstöra integriteten för datorbaserad information.
- Äventyra privatlivet för andra.
- Involvera försumlighet vid genomförande av Internet spridda experiment.

11.1.3 GASSP – Generellt Accepterade System Säkerhets Principer[176]

Försöker utveckla och bibehålla GASSP med riktlinjer från säkerhetsproffs, IT produkt utvecklare, informationsägare och andra organisationer som har betydande erfarenhet när det gäller att definiera och fastställa principer för informationssäkerhet.

11.1.4 MOM – Motiv, Möjligheter, Skicklighet[177]

Motiv – Vem och varför ett brott
Möjligheter – Var och när ett brott.
Skicklighet – Den skicklighet en kriminell behöver för att lyckas.

11.2 Operativ säkerhet

11.2.1 Salami

Innefattar att dra av ett litet belopp av medel från ett konto i hopp om att ett sådant obetydligt belopp skall förbli ouppmärksammat.

11.2.2 Data Spratt

Refererar till förändring av existerande data och många gånger inträffar denna modifiering innan det förs in i systemet eller så snart den avslutar bearbetning och skickas ut från en applikation.

11.2.3 Överdrivna privilegier

Inträffar när en användare har mer datorrättigheter, tillstånd och privilegier än vad som krävs för uppgiften han eller hon behöver fullfölja.

[175] Internet Activites Board
[176] Generally Accepted System Security Principles
[177] Motivations, Opportunities and Means

11.2.4 Lösenords sniffning

Sniffning av nätverkstrafik i hopp om att fånga lösenord som skickas mellan datorer.
IP Spratt[178]:
Förändrar IP adressen manuellt inom ett paket för att peka på en annan address.

11.2.5 Förnekan av tjänst[179]

Förneka andra den tjänst som det utsatta systemet vanligtvis använder.

11.2.6 Avfalls dykning

Refererar till någon som letar igenom en annan person avfall efter bortkastade dokument, information och andra värdefulla saker som sen skulle kunna användas mot denna person eller företag.

11.2.7 Fånga utströmning

Avlyssning av elektriska vågor som skickas ut av varje elektrisk enhet.

11.2.8 Avlyssning

Avlyssning av kommunikationskanler.

11.2.9 Social genomgång

Konsten att lura människor och använda informationen de känner till att ovetande förse dem på ett uppsåtligt sätt.

11.2.10 Maskerad

En metod som en inkräktare kan använda för att lura andra avseende hennes riktiga identitiet.

11.3 Skadestånd och dess förgrening

11.3.1 Försiktighet[180]

Steg som vidtas för att visa att ett företag har tagit ansvar för de aktiviteter som inträffar inom företaget och har tagit de nödvändiga steg för att hjälpa till att skydda företaget, dess resurser och anställda.

11.3.2 Due Diligence

Kontinuerliga aktiviteter som säkerställer att skyddsmekanismer kontinuerligt underhålls och är operationella.

11.3.3 Regeln om klok man

För att utföra uppgifter som kloka människor skulle utöva under liknande omständigheter.

11.3.4 Nerströms skadestånd

När företag sluter sig samman för att arbeta på ett integrerat sätt, speciell försiktighet måste vidtas för att försäkra att varje part lovar att förse den nödvändiga säkerhetsnivån, skadestånd och ansvar som behövs vilket tydligt borde definieras i kontrakt som varje part undertecknar.

[178] *Spoofing*
[179] Denial of Service – DoS
[180] Due Care

11.3.5 Legalt erkända skyldigheter

Det finns en ställning avseende beteende som förväntas av företaget att skydda andra från orimliga risker. Företaget måste misslyckas att anpassa sig till denna standard, vilket resulterar i skada eller förstörelse för en annan.

11.3.6 Orsakad i omedelbar närhet[181]

Någon kan bevisa att skadan som orsakade, var företagets fel.

11.4 Typer av lagar

11.4.1 Civilrätt

Kallas även Tort.
Hanter felaktigheter mot individer eller företag som resulterar i skador eller förlust.
En civil rättegång skulle resultera i finansiellt återställande istället för fängelsedom.

11.4.2 Kriminalrätt

Används när en individs beteende bryter mot offentliga lagar, vilka har utvecklats för att skydda allmänheten.
Fängelsedommar är vanligtvis straffet.

11.4.3 Administrativ rätt

Hanterar regelmässiga standardarder som reglerar utförande och beteende.
Offentliga instanser skapar dessa standards, vilka vanligtvis tillämpas på företag och individer, inom dessa företag.

11.5 Intellektuella upphovsrättsliga lagar

11.5.1 Handels hemligheter

Resurser som påstas vara en handelshemlighet måste vara konfidentiell och skyddas med vissa säkerhets försiktighetsåtgärder och aktiviteter.

11.5.2 Copyright

Skyddar utrycket av en idé för en resurs.

11.5.3 Varumärke

Används för att skydda ett ord, namn, symbol, ljud, form, färg, enhet eller kombination av dessa.

11.5.4 Patent

Ges till individer eller företag för att garantera ägaren legalt ägandeskap och möljliggöra för ägaren att utelämna andra från att använda och kopiera innovationen som omfattas av patentet.
Ett pantent garanterar en begränsad äganderätt i 17 år.

[181] Proximate causation

11.6 Utredning av datorbrott

11.6.1 Incident hanterings team

Grundfrågor -
- Lista på externa byråer och resurser att kontakta eller rapportera till.
- Lista på dator eller rättsexperter att kontakta.
- Steg för hur att säkra och skydda bevis.
- Steg för hur bevis skall sökas.
- Lista på frågor som bör inkluderas i rapporten.
- En lista som indikerar hur olika system bör hanteras i denna typ av situation.

11.6.2 Dator rättsutredning

Rättsutredning -
1a steget: Ta frisk kopia av det attackerade system och genomför en rättsanalys på denna kopia. Detta kommer att göra det möjligt att bevismaterial förblir oskadat på originalsystemet i fall att något steg i utredningen fördärvar eller förstör data. Även minnet för systemet bör dumpas till en fil innan något arbete utförs eller att systemet stängs ner.
2a steget / Kedjan av förvar: Måse följa en strikt och organiserad procedur när bevis samlas in och märks.
Dikterar att alla bevis skall märkas med information som indikerar vem som säkrat och validerat det.
Kedjan av förvar är en historia som visar hur bevis samlades in, analyserades, transporterades och bibehölls för att presenteras som bevis i en rättegång. Eftersom elektroniska bevis enkelt kan modifieras, kan en tydligt definierad kedja av förvar påvisa att beviset är trovärdigt.

11.6.3 Livscykeln för bevis[182]

Inkluderar följande:
- Insamling och identifiering.
- Lagring, bevarande och transport.
- Presentation i rättegång.
- Retur till offret eller ägaren.

11.6.4 Bevis

Bästa bevis – Är det primära beviset som används i en rättegång eftersom det erbjuder bästa tillförlitlighet. Det används för att dokumentera bevis så som kontrakt.
Sekundära bevis – Det anses inte lika tillförlitligt och starkt när det gäller att erbjuda oskyldighet eller skyldighet när det jämförs med bästa bevis.
Direkt bevis - Kan bevisa fakta av sig själv istället för att behöva backup information att referera till.
Avgörande bevis - Är obestridligt och kan inte emotsägas.
Indicier bevis – Kan bevisa ett mellanliggande fakta som sen kan användas för att härleda eller anta förekomsten av andra fakta.
Bekräftande bevis – Är stödjande bevis som används för att hjälpa till att bevisa en ide eller ståndpunkt. Det kan inte stå för sig själv, med det används som kompletterande verktyg för att hjälpa till att bevisa en primär del av bevis.
Åsikts bevis – När ett vittne intygar, åsiktsregeln dikterar att hon måste endast intyga fakta i frågan och inte hennes egen åsikt om fakta.

[182] The lifecycle of evidence

Hörsägen bevis – Gäller muntliga eller skriftliga bevis som presenteras i rättegång som är andrahand och som inte har förstahands bevis när det gäller riktighet eller tillförlitlighet.

11.6.5 Karaktärsdrag för bevis

Måste vara
Tillräckliga – De måste vara tillräckligt övertalande för att övertyga en resonabel person om giltighet av fynd. Innebär också att det inte kan tvivlas på enkelt.
Tillförlitlig / Kompetent – Det måste konsistent med fakta, måste vara faktiska och inte indicier.
Relevant – Det måste ha en relevant och vettigt relation med fyndet.
Legalt tillåten – Om det samlades in på ett legalt sätt.

Lockelse[183] <-> *Lura*[184]:
Lockelse -
Är legalt och etiskt.
Lura -
Är varken legalt eller etiskt.

11.7 Telefon Knäckare

Blå boxar – Är en enhet som simulerar en ton som lurar telefonbolagets system att tro att användaren är auktoriserad att använda långdistanstjänster, vilket möjliggör för honom att göra samtalet.
Röda boxar – Simulerar ljudet av mynt som deponeras i en betaltelefon.
Svarta boxar – Manipulerar voltstyrkan på linjen för att ta emot ett avgiftsfritt samtal.

[183] *Enticement*
[184] *Entrapment*

12 CBK#10 Fysisk Säkerhet

12.1 Fysiska säkerhetskontroller

Typer av kontroller:
- Administrativa kontroller:
  - Byggnadsval eller konstruktion.
  - Byggnadshantering.
  - Kontroll av anställda.
  - Utbildning.
  - Nödfalls svar och procedurer.
- Tekniska kontroller:
  - Åtkomstkontroller.
  - Intrångsdetektering.
  - Larm.
  - Övervakning (CCTV).
  - Värme, ventilation och luftkonditionering (HVAC).
  - Kraftförsörjning .
  - Brand detektering och bortträngning.
  - Säkerhetskopior.
- Fysiska kontroller:
  - Staket.
  - Lås.
  - Ljus.
  - Byggnadens konstruktionsmaterial.

12.2 Byggnadshantering

12.2.1 Frågor vid val av lokal

- Synlighet.
- Närliggande area och externa enheter.
- Åtkomlighet.
- Naturkatastrofer.

12.2.2 Konstruktionsfrågor vid design och konstruktion av en byggnad

- Väggar.
- Dörrar.
- Tak.
- Fönster.
- Golv.
- Uppvärmning och luftkonditionering.
- Kraftförsörjning.
- Vatten och gaslinjer.
- Branddetektion och bortträngning.

12.2.3 Saker som kan innebära bekymmer

Bördan – Hur mycket vikt som kan bäras av byggnadens väggar, golv och tak behöver uppskattas och planeras för att försäkra sig om att byggnaden inte skall kollapsa i olika situationer.
Positivt flöde (vatten och gaslinjer) – Material bör flöda ut ur byggnaden, inte in.
Interna partitioner – Många byggnader har hängande tak, vilket innebär att den inre partitionen kanske inte sträcker sig ovanför taket, vilket innebär att en inkräktare kan lyfta på takpanelen och klättra över partitionen.

12.3 Urvalsprocessen för fysiska säkerhetskomponenter

12.3.1 Säkerhets-måsten

Tillmötesgående av lagar för att lyda vissa säkerhetskrav.

12.3.2 Säkerhets-bör

Skyddsprocedurer som bör sättas på plats för att hjälpa skydda företaget från förödande aktiviteter och deras resultat.

12.3.3 Hårdvara

SLAs / Servicenivå avtal[185] – Försäkra att leverantörer erbjuder den nödvändiga skyddsnivån.
MTBF / Genomsnittligt tid mellan fel[186] – Används för att fastställa den förväntade livstiden för en enhet eller när ett element inom den enheten är förväntad att gå ut.
MTTR / Genomsnittlig tid att reparera[187] – Används för att uppskatta tiden mellan reparationer.

12.3.4 Kraftförsörjning

Kraft skydd -
- Realtids system: Använder en bank av batterier
- Standby UPS: Är inaktiva tills dess en kraftlinje sviktar
- Reservkraftsenheter: Används för att försörja huvudkraften eller ladda batterier i ett UPS sytem.
- Volt regulatorer och linje rensare: Kan användas för att försäkra en ren och jämn distribution av kraft.

[185] Servicelevel agreements
[186] Mean Time Between Failure
[187] Mean Time To Repair

Elektriska Kraft Definitioner:

Jord	Vägen till jorden för att möjliggöra överdrivna volt tal för att skingras.
Ljud	Elektromagnetiska eller frekvens störningar som störa kraftflödet och kan orsaka fluktationer.
Transient ljud	Korta uppehåll av störningar i kraftlinjen
Ren kraft	Kraft som inte fluktuerar
Fault	Ögonblicklig förlust av kraft
Blackout	Fullständig / förlängd förlust av kraft
Sag	Ögonblickligt lågt volttal
Brownout	Förlängt lågt volttal
Spike	Ögonblickligt högt volttal
Surge	Förlängt högt volttal
Inrush	Initial våg av kraft i början

12.4 Miljömässiga frågor

Positiv avledning – Innehållet flödar ut istället för in.
Relativ fuktighet - 40 to 60 % är acceptabelt.
Hög fuktighet – Kan orsaka korrosion.
Låg fuktighet – Kan orsaka omfattande statisk elektricitet.
Postivt tryck - När en anställd öppnar en dörr, luften går ut och luften utanför kommer in.

12.4.1 Brand detektorer

Rök aktiverade – Fotolelektriska enheter.
Värme aktiverade – Andel av stignings temperatur sensorer och fixerade temperatur sensorer.
Flamm aktiverade – Känner av infraröd energi.
Automatiskt uppringningslarm – Anropar den lokala brandstationen för att rapportera en upptäckt brand.

12.4.2 Brandsläckning

Bärbara släckare bör finnas inom 15,2 meter (50 feet) från vilken elektiskt utrustning som helst och placerade nära utgångar.

12.4.3 Brandklasser och släckningsmedium

A	Vanligt brännbart material	Vatten eller Sodavatten
B	Vätskor	CO2, Sodavatten eller Halon
C	Elektriskt	CO2 eller Halon

Vatten – Minskar temperaturen som krävs för att understödja elden.
SodaVatten – Minskar bränslet som understödjer elden.
CO2 – Minskar luften som krävs för att understödja elden.
Halon – Minskar brännbara material genom en kemisk reaktion.

12.4.4 Ersättningslista för Halon

FM-200, NAF-S-III, CEA-410, FE-13, Vatten, Inergen, Argon, Argonit.

12.4.5 Vatten Sprinklers

Våta rör - Innehåller alltid vatten i rören och utlöses av temperaturmätare som kontrollerar värmenivån.
Torra rör- Vattnet finns i ett valv tills dess att en specifik temperatur uppnås. Det finns en tidsförskjutning mellan när den fördefinierade temperaturen uppnås och att vattnet frisläpps
Preaktion – Kombinerar användandet av system med våta och torra rör. Vattnet finns inte i rören och frisläppps in i rören när den fördefinierad temperatur uppnås. När denna temperatur uppnås, fylls rören med vatten, men det släpps inte iväg direkt. En länk måst smälta innan vattnet utlöses från sprinklerhuvudet.
Övervämning – Samma som torra rör men där sprinklerhuvudet är öppet.

12.5 Närområdets säkerhet

12.5.1 Åtkomstkontroll till fastighet

Framtvingas genom fysiska och tekniska komponenter.
Lås:
Är den billigaste mekanismen för åtkomstkontroll.
Anses som avskräckande för mellanseriösa inkräktare och fördröjande för seriösa inkräktare
Förinställda lås – Är lås som vanligtvis används på dörrar.
Chiffer lås / Programerbara lås – Använder nyckeldyna för att kontrollera åtkomst till ett område eller en byggnad.
Val som är tillgängliga på många chifferlås:
- Dörr fördröjning: Om dörren hålls öppen under lång tidsperiod kommer ett larm att startas för att varna personal om misstänkt aktivitet.
- Nyckel upphävande: En specifik kombination kan programmeras för att användas i en nödfallssituation för att upphäva vanliga rutiner eller för övervaknings upphävande.
- Master-nyckel: Möjliggör övervakning av personal att ändra åtkomstkoder och andra funktioner på chifferlåset.
- Gisslan larm: Om en individ är under tvång och/eller hålls som gisslan, kan det finnas en kombination han eller hon kan kommunicera denna situation till vaktstationen och/eller polisstation.

Enhetslås – För att skydda enheten genom att använda ändringskontroller, öppningslås, portkontroller, periferi ändringskontroller och kabelfällor.

12.5.2 Åtkomstkontroll för personal

Ordentlig identifiering för att verifiera om personen som försöker att få åtkomst till en byggnad eller område verkligen skall vara tillåten att befinna sig i denna.
Rida på ryggen – När en individ skaffar sig oauktoriserad åtkomst genom att använda någon annans legitima referenser eller åtkomsträttigheter.

12.5.3 Magnetkort

Minneskort – Läsaren kommer att dra information från det och ta ett åtkomstbeslut.
Smarta kort – Individen kommer kan bli uppmanad att ange ett PIN eller lösenord, vilket läsaren jämför mot informationen som finns på kortet.

12.5.4 Trådlösa närhetsläsare

Användaraktiverade – Överför en sekvens av värden till läsaren.
System avkänning – Känner igen närvaron av kodade enheter inom ett specifikt område.
- Transponders: Kortet har en mottagare, överförare och batteri.
- Passiva enheter: Kortet har inte någon kraftkälla själv.
- Fält-försörjda enheter: Kortet och läsaren innehåller en överförare och aktiv elektronik.

12.5.5 Externa områdesskydds mekanismer

Staket:
0,9 – 1,2 meter (3-4 feet) – Avskräcker vanliga inkräktare.
1,8 – 2,1 meter (6-7 feet) – Anses för höga att enkelt klättra över.
2,4 meter (8 feet) med 3 strängar av taggtråd – Avskräcker inkräktare.
Människofälla – Ingången styrs genom en uppsättning av dubbla dörrar som kan övervakas av en vakt.

12.5.6 Belysning

Borde användas för att avskräcka inkräktare och ge säkerhet för personal, ingångar, parkeringsområde och kritiska sektioner.
Kritiska område borde belysas 2,4 meter (8 feet) högt och 0,6 meter (2 feet) ut.

12.5.7 Övervaknings enheter

Tre huvudkategorier -
- Patrullerings styrkor och vakter – Kan ta beslut.
- Hundar – Är lojala, tillförlitliga och är känsliga för lukter och ljud.
- Visuella inspelningsenheter: Kamera, CCTV, …

12.5.8 Upptäckande

Områdes upptäckande system / kapacitans detektorer -
Utger ett magnetiskt fält som kan mätas när det används. Detektorn övervakar detta elektriska fält och ett larm låter om fältet störs.
Fotoelektriska eller fotometriska system –
Detekterar förändringar i nivån av ljus inom ett område.
Vågmönster –
Genererar ett vågmönster som skicaks över ett område och reflekteras tillbaka till mottagaren.
Passiva infraröda system –
Identifierar förändringar i värmevågor inom området det är konfigurerat att skydda.
Aukustiska-Seismiska detektions system –
Är känsliga för ljud och vibrationer och detekterar förändringar i ljudnivåer inom området det är placerat i.

12.6 Media lagrings krav

Data som inte längre behövs eller används måste förstöras.
Återanvädning av objekt – Konceptet att återanvända media efter dess inledande användning.
Återstående data – Är problemet med kvarvarande information som blir kvar på media efter radering.
Steg i dataförstöring –
- Radering: Skriva över datamedia med avsikt att återanvändas i samma organisation eller i övervakad miljö.
- Rensning: Avmagnetisering eller överskrivning av media med avsikt att ta bort denna från den övervakade miljön.
- Förstörelse: Fullständigt förstörande av media och därmed återstående data.

13 Relaterade länkar

På Internet kan du hitta många siter som omfattar säkerhet. Alla av dem är inte en relvant studieguide för specialister, men kan innehålla väldigt intresant material. Länkarna nedan är bara några av alla dessa.

(ISC)2
www.isc2.org
Startpunkten för CISSP
CCCURE
www.cccure.org
Den bästa studieguiden för CISSP examinationen, dokument och länkar
ISACA
www.isaca.org
Stiftelse för informationssäkerhet,
Administrerar CISA certifieringen.
CERT Koordination
www.cert.org
Ett centrum för Internet säkerhet
Incidents.org
www.incidents.org
En virtuell organisation för avancerade intrångsanalytiker, brottsexperter och hanterare.
NIST CSRS
www.csrs.nist.gov
Datorsäkerhets resurscenter vid NIST

14 Referenser

Vid förberedelse inför CISSP examen, finns det många böcker och referenser du kan använda. Inför min förberedelse har nedanstående referenser använts.

CISSP all-in-one Certification Exam Guide
Shon Harris
Har varit huvudstudieguiden för mig. Övningsfrågor ingår i boken och på en CD
The CISSP Prep Guide
Ronal L. Krutz och Russel Dean Vines
Var kompletterande studieguide för mig. Övningsfrågn ingår i boken
ISO/IEC 17799
ISO standard (tidigare den brittiska standarden BS7799)
Ledningssystem för informationssäkerhet. Grunden för ISO certifiering i Informationssäkerhet
CCCURE
www.cccure.org
Redan nämnd. Du kan ändå hitta referensmaterial till dina förberedelser här.