Datasäkerhet och integritet

OH-5 v1

- OSI-modellen
- TCP/IP
- Nätverkssäkerhet
  - ett mycket stort område!
- Mer om TCP/IP
- Vanliga attacker på protokoll och mjukvara

Media och topologier i nätverk

- Koaxialkabel
- Partvinnad kopparkabel
- Fiberoptisk kabel
- Trådlös bärarvåg

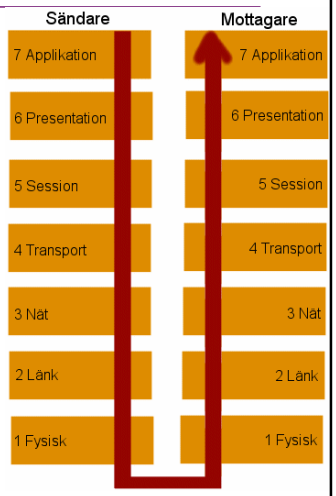
- CSMA/CD (C*arrier Sense Multiple Access with Collision Detection*) eller ethernet (används till 99,9% i LAN)
  - Broadcast
- Token ring (utdött)

- Avlyssning
- Trusted och untrusted nätverk
- Skalskydd
  - Firewall, Proxy, NAT

OSI-modellens 7 olika nivåer

- OSI-modellen är en referensmodell för datakommunikation
- Den har skapats för att visa hur olika system kan kommunicera med varandra

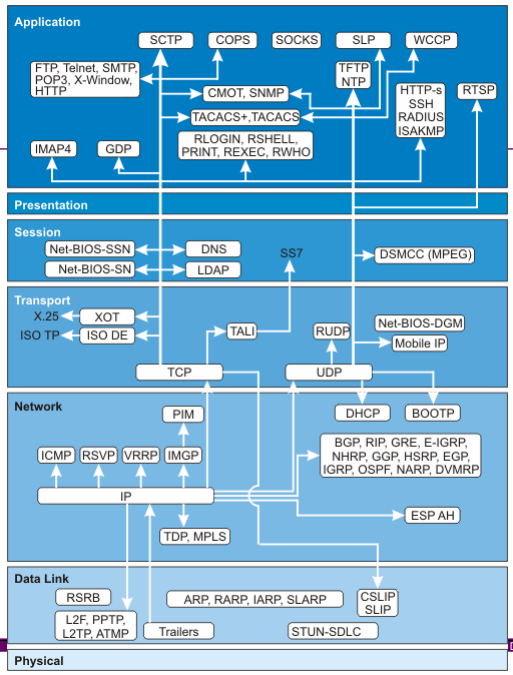
7. Applikationsnivå: Koppling till användaren, hur programmet skall visa den överförda informationen.
6. Presentationsnivå: Beskriver vilka koder som används i överföringen av data, behandling av komprimering och kryptering.
5. Sessionsnivå: Bestäms hur den logiska uppkopplingen och dialogen ska genomföras mellan sändare och mottagare, dvs. applikations protokollet, t.ex. HTTP.
4. Transportnivå: Här bestäms vilket bärarprotokoll som ska användas vid överföring av data från sändaren till mottagaren, t.ex. TCP.
3. Nätnivå: Adressering, vägval, anpassning till protokollet som används i det fysiska nätverket.
2. Länknivå: Kontrollerar att överföringen i kommunikationskanalen fungerar korrekt.
1. Fysisk nivå: Beskriver vilket gränssnitt som används.



Transmission Control Protocol/Internet Protocol (TCP/IP)

- Utgår från DARPA-modellen med 4 lager
  - 4. Applikationslagret
    - Motsvarar i stort sett de 3 översta lagren i OSI-modellen
  - 3. Host till host transportlager
    - Motsvarar i stort sett transportlagret i OSI-modellen
  - 2. Internetlagret
    - Motsvarar i stort sett nätverkslagret i OSI-modellen
  - 1. Nätverkskontaktlager
    - Motsvarar i stort sett de 2 nedersta lagren i OSI-modellen
  - Referens (till nästa bild)
    - http://www.protocols.com/pbook/tcpip1.htm

TCP/IP & OSI



Några vanliga TCP/IP protkoll

Se bra film på: http://www.warriorsofthe.net

- IP (Internet Protocol)
  - Adresserar och routar paket mellan värddatorer (hosts)
- ARP (Adress Resolution Protocol)
  - Översätter hårdvaruadresser till IP-adresser
- ICMP (Internet Control Message Protocol)
  - Kontrollerar att paketleverans fungerar
- IGMP (Internet Group Management Protocol)
  - Hanterar hostar som är med i multicast grupp, kräver stöd från router, motsatsen till unicast
- TCP (Transmisson Control Protocol)
  - Pålitligt förbindelseorienterat, ACK skickas, använder portar
- UDP (User Datagram Protocol)
  - Opålitligt förbindelselöst, använder portar, snabbare än TCP

Nätverkstjänster

- För att fungera i nätverk måste OS ha vissa nätverkstjänster igång
  - Man bör sträva efter att **endast** ha de nödvändiga igång
- Standardtjänster har vissa ”portnummer” tilldelade
  - Portar, kan jämföras med TV eller radiokanaler, 65536 st.
  - Med kommandot netstat kan man se vilka portar som är aktiva
  - Vissa protokoll/applikationer kräver en viss port t.ex. WWW = 80, FTP (File Transfer Protocol)= 21, SMTP = 25, DNS = 53 (Domain Name System) samma funktion som vita sidorna i telefonkatalogen, se lista/referenser i läroboken
  - Med en nätverksskanner eller portskanner kan man från en annan dator se vilka portar ”victim” svarar på för att hitta svagheter
  - T.ex. ISS Internet Scanner, SuperScan, NMAP etc.
- Verifiera att det verkligen är din tjänst som svarar och inte en trojan!
- En personlig eller central brandvägg kan kontrollera vilka TCP/UDP portar som tillåts fungera på datorn eller in/ut i nätverket

IP-adresser, sub-netting och portar

- IP-adressen är 32 bitar lång och delas in i fyra oktetter (8 bitars fält), 0-255 ex. 192.168.12.1
- Adressklasser
  - Delas in a.b.c.d del, ex. C-nät 130.243.36.x, A-nät 130.x.x.x, 2113929216 möjliga adresser
- Framtidens Internet - IPv6
  - 128 bitar lång adress, http://www.ipv6.org
- Sub-netting dela upp ditt nät (segmentera) – Subnet Calculator
  - Lek med program på http://www.warriorsofthe.net
- IP-adress + port
  - 123.123.123.123:80 anropar WWW tjänsten på datorn med IP-adress 123.123…

Vilka är hoten mot nätverket?

- Skadlig kod
  - Virus, maskar, trojaner
- Denial of Service (DoS) eller bombardment och flooding
  - Ett samlingsbegrepp för attacker som slår ut tjänster på nätverket för användare, i huvudsak av 3 typer:
  - 1. Slå ut datarelaterade egenskaper som bandbredd, CPU, lagring
  - 2. Slå ut nätverkets konfiguration som t.ex. routerns information
  - 3. Slå ut fysiska komponenter i nätverket
- Distributed Denial of Service (DDoS)
  - Använder en mängd slavdatorer med bredbandsanslutningar som infekterats av en DoS-bot (trojan) av hackern
  - Styrs av hackern via en bot-master som är gömd bakom proxies eller bouncers (IP-studsare)
  - Slavdatorerna formar ett DoS-net eller bot-net, bot = autonom robot

Vilka är hoten mot nätverket?

- Bakdörrar (trap doors)
  - Syftar till en hemlig öppning som en programmerare eller trojan kan ha skapat i systemet för att komma in bakvägen (obemärkt)
- Phreaking
  - Ett samlingsbegrepp för manipulering av telefonlinjer (analoga och digitala), omprogrammering av SIM-kort etc. m.m.
- Cookies
  - Används på de flesta webbplatser med inloggning (även utan inloggning) för att spara information om användaren (sessionsdata) i syfte att snabba upp nästa besök
  - Cookien lagras lokalt på användarens dator i t.ex. ”C:\Documents and Settings\användarnamn\Cookies”
  - Risken ligger i att någon webbplats läser av cookies och kartlägger användarens datorvanor i syfte att sända spam etc.
  - Cookies går att stänga av i webbläsaren

Vilka är hoten mot nätverket?

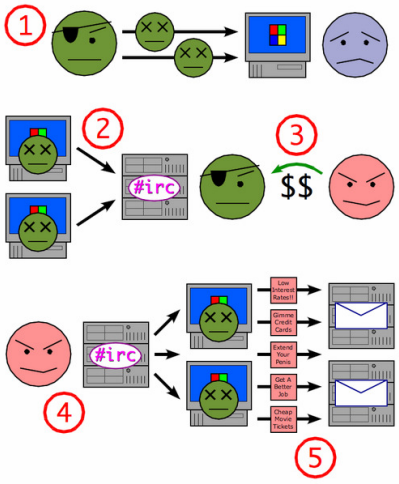
- Intrångsförsök/otillbörlig åtkomst
  - Med intrångsförsök menas att någon utifrån eller att en trojan inifrån försöker ta sig in i ditt system i syfte att komma åt användardata
  - På ett nätverk och i datorn går en väldig massa trafik in/ut från olika programvaror (spel, etc.) som ibland broadcastar ut information på vissa portar.
  - De flesta personliga firewalls gör ingen skillnad på legitima eller otillbörliga förfrågningar/utsändningar och varnar därför ofta i onödan
- Buffer-owerflow
  - När program sänder meddelanden som är större än väntat
- Spam (skräppost)
  - Är sedan flera år ett tilltagande problem
  - Global lagstiftning enda lösningen

DoS attacker

- IP broadcast attack
  - Sänd ett ping (kommandot) med datastorlek 1kB till t.ex. 192.168.255.255 (directed broadcast = remote broadcast)
  - Ger ett LAN broadcast på 192.168.0.0 och alla värdar kommer att försöka ge ett ICMP ”echo reply” svar
    - Ett visst arbete krävs trots att ”respond to ping” är avslaget
  - Om ”echo request” sänds varje tiondels sekund med 1kB data så floodar 100 värdar en 10 Mbit lina!
- Smurf attack (en variant på IP broadcast)
  - Attackeraren har spoofat sin egen adress att peka på victim, victim får därmed alla ICMP ”echo reply” svar!
- I de flesta routrar finns stöd att blockera directed broadcasts
  - Dvs. utnyttjas för smurf attack, men du kan fortfarande bli victim!
  - Brandväggar kan blockera ”echo reply”, men hjälper inte mot flooding

Diagram som beskriver hur virusinfekterade datorer kan användas för att sända spam eller till DDoS attacker

1. Virusskrivaren sänder ut ett virus som infekterar vanliga användares datorer
2. Infekterade datorer loggar in på IRC (Internet Relay Chat) eller annat kommunikationsmedium och formar tillsammans ett eget botnet/dosnet
3. Spammaren eller DDoS användaren köper access till bot-net/DoS-net av virsusskrivaren eller ”dealer”
4. Spammaren eller DDoS hackaren sänder instruktioner till de infekterade datorerna att sända spam eller ”flooda” ett nätverk
5. De infekterade datorerna sänder spam-meddelanden till Internetanvändares mailservrar eller en massa meningslösa kommandon till t.ex. en webbserver



Vad är buffer-overflow?

- Är ett tillstånd i datasäkerhet och programmeringsvärlden där en process försöker placera mer data i en minnesbuffert än den har fått tilldelat sig
  - Kallas även för buffer overrun
- Resultatet är att programkod eller att variablers data kan bli överskrivet
- Följdresultatet är att datorn kraschar eller ger felaktiga resultat
- Vad attackeraren är ute efter är att endera:
  - Genom att skriva över en annan variabel etc. nära bufferten i minnet kan han påverka programmet att göra något som gynnar honom
  - Genom att skriva över speciella variabler (en funktions returadress t.ex. på stacken) kan attackerarens få programmet att börja exekvera dennes kod och då göra i stort sett vad som helst

Vad är buffer-overflow?

- Finns det skydd mot dessa attacker?
  - Välja ett programspråk som inte tillåter ”out of bounds” adressering, nästan alla andra programspråk än C/C++ kastar ett exception om detta görs
  - Designa sitt program så dessa attacker ej är möjliga
  - Använda programmeringsbibliotek som är skyddade
  - Stack-smashing protection - algoritmer som detekterar stack overflow
  - Executable space protection – skydd från operativsystemet
  - Address space layout randomization – lägger ut processen slumpmässigt i minnet
  - Deep Packet Inspection – detekterar attacker över nätet

DNS attacker

- DNS servern översätter värdnamn till IP-adress
  - En mycket viktig tjänst!
- Attacker kan anta två former
  - Modifiering av informationen i DNS servern
  - DoS attack för att effektivt sänka hela nätet eller t.ex. låta en egen DNS server ”ta över”
- Skydd (de flesta servar kör programvaran BIND)
  - Uppdaterad och rätt konfigurerad
  - DNSSEC - BIND 9.x och högre
    - Skyddar mot ej auktoriserad ändring i DNS databasen genom ett publikt krypteringssystem PKI

Router attacker

- Ändra i routingtabellens konfiguration (intrång)
- Göra routingtabellen korrupt (sända felaktig data)
  - Ganska enkelt då det inte finns någon autentiseringsmekanism i RIP (Routing Information Protocol)
  - Felaktig routertabell innebär att IP-paket anländer till fel destination
- RIP v2 och OSPF (Open Shortest Path First) har ett autentiseringsfält men det sänds okrypterat med varje meddelande
- Ett annat protokoll BGP (Border Gateway Protocol) sätter upp en TCP länk och är svårare att hacka
  - En attackerare kan dock sända felaktiga ICMP (Internet Control Message Protocol) ”redirect” meddelanden och därigenom få routern att skapa en ny path till en viss destination
  - ICMP ”destination unreachable” är också ett hot
- Bästa skyddet är att ha statiska (manuella) tabeller för alla externa hostar och blockera inkommande utomstående router meddelanden

Mer om TCP/IP

- Pålitlig leverans av data i ordning över ett nätverk mellan två anslutna värdar
- Applikationer sänder byte-strömmar av data och TCP hackar sönder dessa till lämpliga segment, MTU (Maximum Transmission Unit)
- IP levererar paketet till andra änden där det packas upp
- TCP ser till så att inget paket förloras genom att ge det ett sekvensnummer
- Ett ACK sänds tillbaka om sändningen lyckades
- CRC (checksumma) används, sänds med och beräknas
- Om sändningen misslyckades eller om RTT (Round-Trip Time) gick ut så sänds paketet om

Mer om TCP/IP

- En socket (anslutningsport) har följande tillstånd
  - LISTEN, väntar på anslutning från remote TCP & port
  - SYN-SENT, väntar på att remote TCP skall sända paket med SYN & ACK
  - SYN-RECEIVED, väntar på att remote TCP skall sända tillbaka ACK efter att lokal TCP sänt connection ACK
  - TIME-WAIT, väntar tillräckligt länge på att remote TCP skall ha fått ACK på dess connection termination request
  - Övriga tillstånd
    - ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK, CLOSED
- TCP har 3 tillstånd
  - Anslutning etablering
  - Data sändning
  - Anslutning terminering

TCP/IP - Anslutning etablering

- TCP anslutning använder 3-vägs handskakning
  - Passive Open
    - Innan en klient försöker ansluta till servern så måste servern binda en port för att kunna öppna den för anslutningar
    - När passive open är klart kan klienten initiera active open
  - Active Open
    1. Active Open görs genom att sända SYN till servern
    2. Servern svarar med SYN-ACK
    3. Klienten sänder slutligen ACK till servern
- Iom. detta har både klient och server mottagit ACK för anslutningen

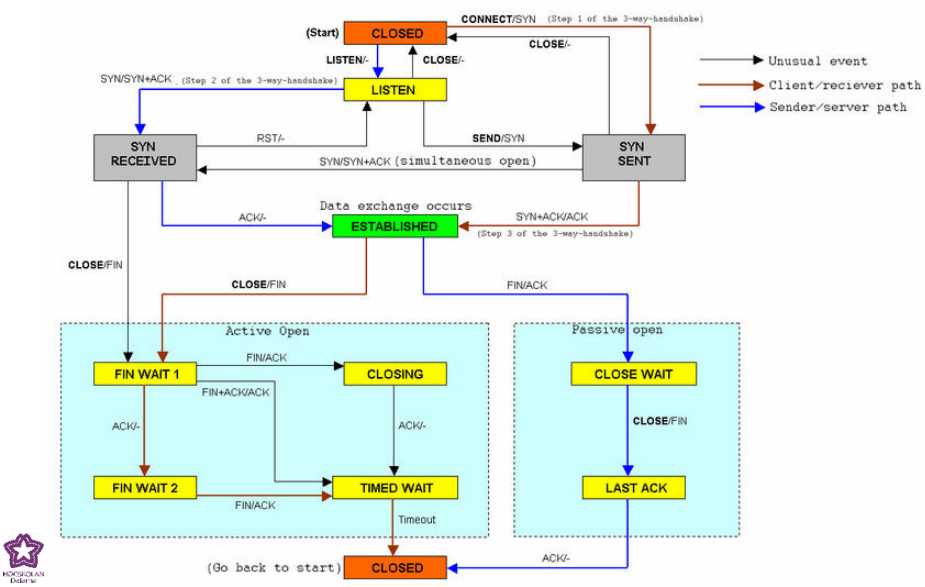
TCP/IP – Data sändning

- Nyckelfunktioner
  - Felfri datasändning som är ”i ordning”
  - Omsändning av ”tappade” paket och uteslutning av duplicerade paket
  - ”congestion throttling” – flödes kontroll
  - I de 2 första stegen (3 vägs handskakning) så utväxlades ett ISN (Initial Sequence Number) som identifierar ordningen m.m. på sändningarna, räknas upp för varje sänd byte
- TCP window size
  - Mängden mottagen data som kan buffras upp innan ACK sänds från mottagande värd
- Window scaling
  - Öka/minska storleken av window size i nätverk med hög/låg bandbredd

TCP/IP – Anslutning terminering & TCP-portar

- TCP terminering använder 4-vägs handskakning
  - Oberoende terminering av varandra
  - När någon ändarna vill avsluta sessionen sänder den ett FIN-paket som besvaras med ACK, dvs. 2 FIN och 2 ACK behövs
  - En connection kan vara ”half-open”, dvs. en sida har terminerat
- En half-open anslutning brukar tima ut efter omkring 3 minuter
- Det finns 2^16 (65535) TCP-portar
  - Vissa protokoll är som standard bundet till vissa portar
  - HTTP = 80, FTP = 21, SMTP = 23 osv…

TCP/IP funktion



SYN floods

- Attacken går ut på att klienten använder en IP-adress som inte svarar servern – vilket skapar en halvöppen anslutning
- Varje halvöppen anslutning konsumerar resurser hos servern och till slut kan de vara helt förbrukade
  - Endera för applikationen eller hela servern
- Det är svårt att skydda sig mot SYN flood attacker
  - Vissa OS kan dynamiskt sänka time-out tiden under tung belastning
- Vissa routrar och brandväggar har delvis inbyggt skydd
  - Intercept mode
    - En mjukvara svarar klienten (i stället för servern) och om klienten sänder ACK så kopplar den transparent upp klienten och servern på riktigt
  - Watch mode
    - En mjukvara övervakar förbindelsen, om allt går rätt till så gör den inget, om inte så sänder den ”reset” till servern

Ett regelsystem för att indela hoten

- Hot mot systemet
  - Få access till systemet eller data utan att ha blivit autentiserad
  - Köra program utan att ha korrekta rättigheter
  - Sänka systemet (DoS attacker)
- Hot mot nätverket
  - Få tag i information från nätet - eavesdropping (sniffa och kunna tolka data)
  - Hota integriteten av (modifiera) data
  - Sänka nätverket (DoS attacker)
- Attacker mot systemet kan ske inifrån systemet själv eller utifrån
- Attacker mot nätet sker nästan alltid utifrån

Attacker beror normalt på 8 olika orsaker

1. Protokoll-svagheter
   beror på svagheter i designen eller egenskaperna i nätverksprotokollen som kan utnyttjas av attackeraren, detta är allvarligt eftersom det påverkar alla system oberoende av operativ.
2. Protokoll-buggar
   beror på buggar i implementationen eller egenskaper i protkollen som kan utnyttjas av attackeraren. Tenderar oftast till att påverka ett operativsystem.
3. Operativsystem-svagheter
   beror på svagheter i designen eller vissa egenskaper i operativsystemet som kan utnyttjas av attackeraren. Är operativsystem specifika.
4. Operativsystem-buggar
   beror på buggar i operativsystemet som kan utnyttjas av attackeraren. Är operativsystem specifika.

Attacker beror normalt på 8 olika orsaker

5. Program-svagheter
   Beror på svagheter i designen eller av vissa egenskaper i programmet som kan utnyttjas av attackeraren för att t.ex. få superuser access i operativsystemet.
6. Program-buggar
   Beror på buggar i programmet som kan utnyttjas av attackeraren för att t.ex. få superuser access i operativsystemet.
7. Virus eller mask
   Virus och relaterade mekanismer är en form av DoS attack. De kan resultera i skador på systemet eller nätverket.
8. Bristfällig konfiguration
   Användaren har inte konfigurerat tjänster som t.ex. nätverk, operativsystem eller programvaror på ett säkert och korrekt sätt. **Detta är den vanligaste orsaken till att system blir penetrerade!**