Datasäkerhet och integritet

OH-7 v1

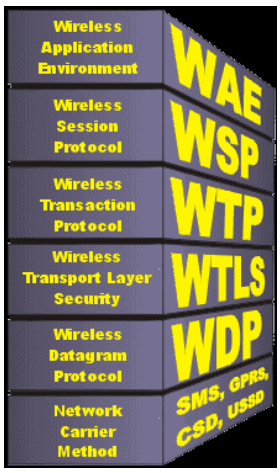
- Mobiltelefon
- Trådlösa nätverk
- Peer-to-peer
- Web services
- Computer Forensics

Trådlös säkerhet

- Trådlösa nät är i allmänhet mer känsligt än fasta ledningar
- Trådlösa enheter är oftast mobila vilket medför risker
- GSM (Global System for Mobile communication)
  - SIM-kort – autentisering mot nätet - pinkod
  - IMEI-kod – unikt id på telefonen
- GPRS (General Packet Radio Services)
  - Förädlat GSM (kretskopplat) till paketförmedlande nät
  - Lediga tidsluckor i nätet används - upp till 40 kbit/s
- UMTS/3G (Universal Mobile Telecommunication System)
  - Förädlat GSM/GPRS - datahastigheter upp till 2 Mbit/s
  - Utökad säkerhet vid autentisering mot nätet – AES krypto med 128 bitar

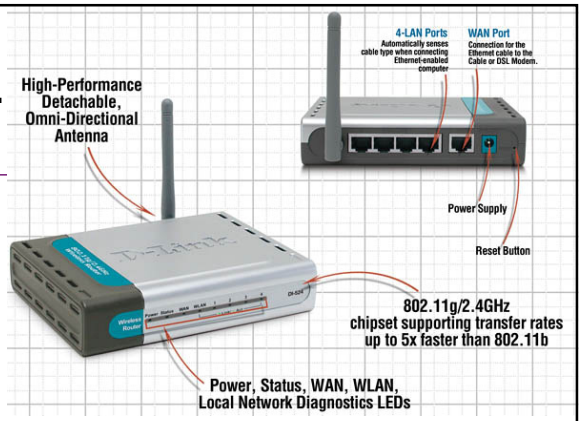
WAP (Wireless Application Protocol) stacken

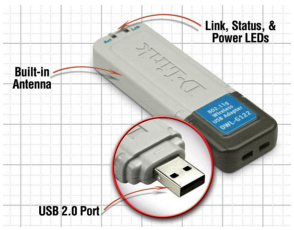
- WAE
  - Scripts etc. – motsvarar t.ex. Javascript
- WSP
  - Specificerar förbindelsen – sessionens olika faser, start, transfer och stop
- WTP
  - Trafikpolisen – hanterar packet loss osv.
- WTLS
  - Autentisering, kryptering, integritet – motsvarar TLS i TCP/IP
- WDP
  - Arbetar mot ett utbytbart bärarlager – adresserar och sätter ihop paketen



Utan en tråd...

- Vanliga märken:
  - D-link
  - Netgear
- En router kostar ca 600:-
- Ett nätverkskort kostar ca 300:-

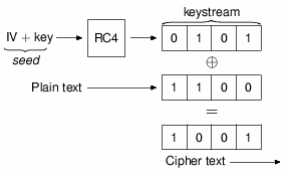




Trådlöst Ethernet (WLAN)

- Enkelt (för det mesta) att få igång men svårare med säkerheten
  - Se dokument - flödesbeskrivning för uppkoppling av en dator i ett skyddat trådlöst nätverk
- Ett stort antal gratis hackerverktyg finns speciellt för WLAN
- Potentiella risker med otillåtna gäster i nätet - skyddsåtgärder:
  - Basstationen
    - Byt namn på adminkontot och lösenordet
    - Tillåt inte administration via wireless eller IP-adresser utifrån
  - SSID
    - Dölj och byt SSID (Service Set IDentifier) namnet, ett namn som sätts på basstationen och klienterna, vilket läggs till varje header på paketen som sänds i WLANet, SSID namnet broadcastas annars ut i nätet
  - MAC-adresser (Media Access Control)
    - Alla enheter som kan anslutas till nätverk har en unik hårdvaruadress
    - Ta reda på vilka MAC-adresser dina enheter har och tillåt endast dessa att ansluta till basstationen
    - Kom dock ihåg att en MAC-adress kan via mjukvara sättas till vad man vill…

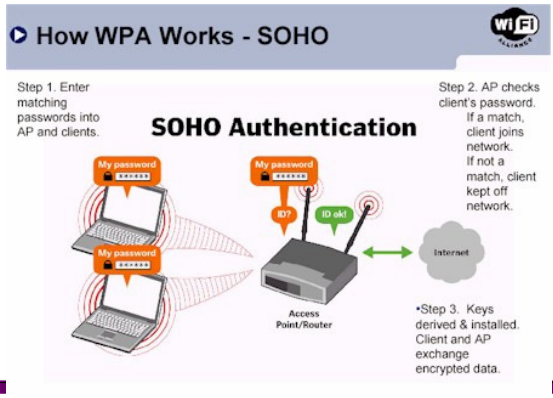
Trådlöst Ethernet (WLAN)



- WEP (Wired Equivalent Privacy)
  - Kryptering med 40, 64, 128, 152 eller 256 bitars RC4 strömchiffer
  - Sätt en statisk WEP passkey – måste sättas på alla enheter
    - En del av nyckeln - IV (initieringsvektorn) är 24 bitar lång
  - Standarden är dock bristfällig – kan forceras på 1-7 dagar
    - Nycklarna för olika paket liknar varann för mycket (byts ej dynamiskt)
- WPA/WPA2 (Wi-Fi Protected Access)
  - WPA = 802.11x + EAP + TKIP + MIC
  - Adresserar bristerna med WEP och förbättrar autentisering, kryptering och nyckelhantering
  - Autentisering sker med 802.11x och EAP mot en autentiseringsserver som t.ex. RADIUS-servertjänst i större nätverk (WPA-PSK annars)
  - Kryptering av dataöverföringen sker med ett av två olika protokoll, TKIP (WPA) och AES (WPA2)

Trådlöst Ethernet (WLAN)

- I privata mindre nätverk används oftast WPA PSK (Pre-Shared Key)
  - En statisk nyckel eller lösenord (Network key/pass phrase) på 8 - 63 tecken sätts på alla enheter

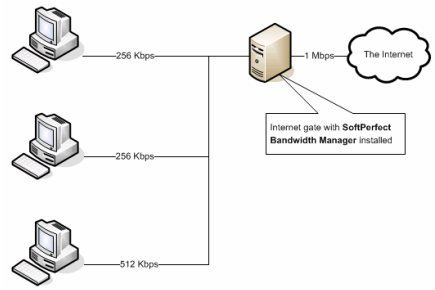


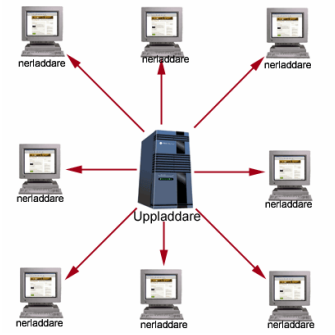
Trådlöst Ethernet (WLAN)

- Temporal Key Integrity Protocol (TKIP)
  - Har per paket nyckel mixning och byter även nycklarna efter en viss tid (Rekey Interval) eller efter ett visst antal paket sänts, använder RC4 strömchiffer
- MIC (Message Integrity check)
  - Förhindrar att paket fångas och förändras över nätet – en hash beräknas på varje paket
- EAP (Extensible Authentication Protocol)
  - En utökning av PPP – alltså ett punkt till punkt protokoll med stöd för flera typer av autentisering som Kerberos, engångs-lösenord m.m.
- 802.11x
  - En metod för att paketera EAP protokollet i Ethernet-ramar
  - 802.11b - 11 Mbit/s, 802.11g - 54 Mbit/s, 802.11n – 540 Mbit/s (ej klar)
  - WPA är en delmängd av IEEE 802.11i (WPA2)
  - WPA2 support kräver en uppdatering av OS, drivrutiner och basstation (om det ens går, endast de nyaste enheterna har support)

Peer-to-peer (P2P)

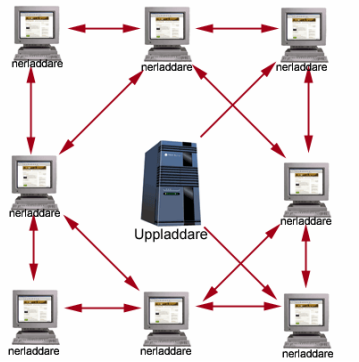
- Protokoll som tillåter fildelning utan att filerna går via någon central server (varje klient kan agera server efter fullständig fil laddats ner)
- Napster var först, Kazaa, Direct Connect, DC++, eDonkey osv…
- Trafiken kan enkelt shapas (prioriteras) efter protokoll, adress, QoS etc.





Peer 2 peer

- Bittorrent är nyaste P2P protokollet, filerna laddas kors och tvärs!
- Bygger på en indexeringsserver (tracker) som håller reda på vilka klienter som har vissa filer eller fragment av filer
- Bittorrent står för minst 1/3 av all trafik på Internet!
- De nyaste klienterna tillåter kryptering vilket gör att traffic shaping inte fungerar längre!
- Blockera portar i FW är det sällan någon mening med
- Trackerlösa bittorrent nätverk är också på gång
- P2P program kan innebära många risker för företag, privatpersoner etc.

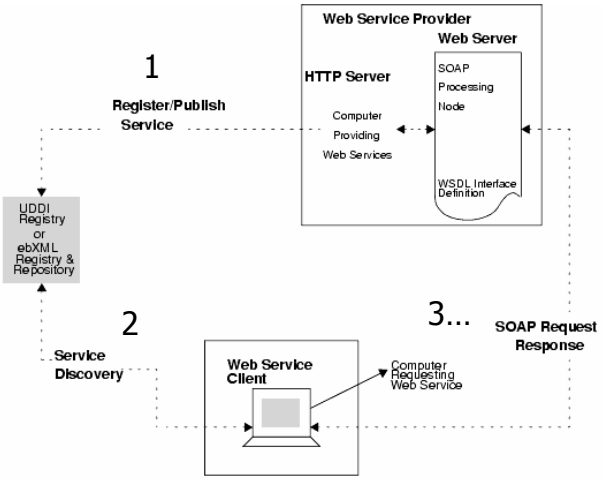


Web services

- Programvara som pratar med annan programvara över nätverk
- Baseras på (öppna) Internetstandarder och utvecklingsmodeller
- Fungerar oberoende av operativsystem och systemgeneration
- Kan integreras innanför eller utanför brandväggen
- Har (just nu) en bred uppslutning i branschen
- eXtensible Markup Language (XML)
  - W3C standard att strukturera dokument, liknar HTML-taggar
- Simple Object Access Protocol (SOAP)
  - XML för kommunikation endera som information eller RPC
- Web Services Descriptor Language (WDSL)
  - Definierar en Web Service
- Universal Description Discovery Language (UDDI)
  - En katalog över Web Service beskrivningar

Web services scenario

1. Once the Web service application is ready to accept requests, the Web service is registered with a registry, such as a UDDI registry and repository. Describe the Web service using a WSDL.
2. Another service or a user locates this registered service and requests by querying the registry.
3. The requesting service or a user writes an application to bind the registered service using SOAP.
4. The client discovers the Web service that is registered with the registry.
5. The request from a client to a Web service arrives in the form of an XML document.
6. The Web service receives the request and processes the request.
7. The Web service calls one or more components to perform business data processing.
8. The components perform their processing calling external systems.
9. The components return data to the service.
10. The Web service then marshals this return value into an XML document.
11. The Web service returns the XML document to the client on a response.



Web services utmaningar

- SOAP är inte beroende eller begränsad till HTTP/HTTPS utan kan använda underliggande protokoll som t.ex. SMTP
- SOAP-meddelanden kan därför behöva skyddas mot insyn
- WS-Security (säkra meddelanden via SOAP)
  - Multipla säkerhetsnycklar för autentisering och auktorisering
  - Multipla förtroendedomäner
  - Multipla krypteringstekniker
  - End-to-end-säkerhet för meddelanden (ej bara transportskiktet)
- SAML (Security Assertion Markup Language)
  - Ramverk för att utväxla säkerhetsinformation via XML
  - Fungerar över domängränser som en försäkran om ett påstående av betrodd part, ungefär som ett pass fungerar för en medborgare i andra länder

Web services utmaningar

- XKMS (XML Key Management Specification)
  - Gränssnitt mot bakomliggande PKI-infrastrukturer för program och klienter, även mobila
  - Består av två web services
    - XML Key Registration Services Specification (X-KRSS), hanterar livscykeln för innehållet i publika nyckeln
    - XML Key Information Services Specification (X-KISS), hanterar förfrågningar för att hämta/verifiera publika nycklar
  - Key Binding Association är en funktion som ger en försäkran om ett påstående av betrodd part som t.ex. att innehavaren av en privat nyckel (som tillhör en specifierad publik nyckel) är associerad med en viss eller vissa identiteter eller IP-adresser etc.
- XML Encryption
  - Behövs om något annat protokoll används där SSL/TLS eller IPSec inte ingår, tillåter persistent och selektiv kryptering

Computer Forensics
Cyberdetektiv på Svenska

- Nätundersökning
  - Loggar från brandvägg, proxyserver, värddatorer och liknande enheter analyseras för att få en bild av nätverkstrafiken
  - Ofta måste stora textmassor gås igenom
- Datorundersökning
  - En värddators hårddisk eller andra enheter med lagringsminne analyseras i detalj och information återskapas i syfte att finna spår
  - Ofta krävs specialistkompetens och specialverktyg för att genomföra en korrekt undersökning

Computer Forensics
Tillvägagångssätt

1. Dokumentera arbetsplatsen
2. Bryt strömmen till enheten genom att dra ur sladden
   - Avvägning: undersöka live eller förhindra radering?
3. Avlägsna lagringsmediat från enheten
4. Total kopia av lagringsmediat - ta hashsummor på original och kopia
5. Analysera kopian och verifiera funna bevis med andra programvaror
6. Sammanställ resultatet så att icke experter förstår
7. Presentera rapporten

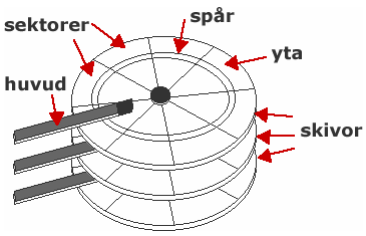
Computer Forensics
Vanliga misstag

- Låta egna IT-avdelningen göra undersökningen
- Vänta för länge med att agera, bevis kan skrivas över om det raderas
- Söker för snävt efter en viss typ av bevis och missar andra
- Att jobba med originalet – bevis kan förstöras eller hävdas ogiltigt – arbeta alltid med kopior!
- Välja fel företag för genomföring av undersökning

Computer Forensics
Hårddisken uppbyggnad

http://www.jonasweb.nu/sidor/datorn/tekniskt/harddisk.html

- Operativsystem skriver filer till ”byte blocks” av en viss storlek kallat sektorer
- Kluster byggs upp av n antal sektorer
- En fil består av n antal kluster som ofta är spridda över hela hårddisken
- FAT (File Allocation Table) håller reda på vilka kluster som är lediga m.m. (som ett adressregister)
  - DOS/Windows fyller ej helt fyllda kluster med data
  - En raderad fil finns kvar
  - FAT-12, 16, 32
- UNIX filsystem, NTFS och WinFS fungerar annorlunda



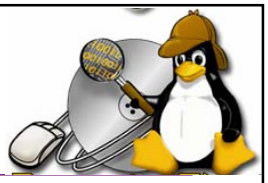
Computer Forensics
FAT - File, RAM och drive Slack

- File Slack innehåller information från datorn som den ”paddar upp” filen med för att den skall fylla ut sektorerna
- Anta att en hårddisk ser ut som nedan med en fil som innehåller texten ”Hello” och att den upptar två sektorer

Hello++++++++++++++|----------(EOC)

- RAM Slack indikeras av "+” och är slumpmässigt data från RAM och buffertar i OS
- Drive Slack indikeras av "-" och är gammal data som låg i sektorn tidigare
- Med speciella verktyg kan file slack läsas och eventuellt avslöja lösenord, kryptonycklar etc.

Computer Forensics
Verktyg etc.



- Radera hårddisk?
  - Enda sättet är att skriva skräp till varje byte
- Kommersiella verktyg
  - EnCase (www.guidancesoftware.com), det mest kända verktyget, dyrt
  - Forensic Tool Kit (www.accessdata.com/products/ftk/)
  - ILook (www.ilook-forensics.org)
  - Paraben (paraben.com)
- UNIX/Linux har en stor mängd fria verktyg som kan användas för både nät och datorundersökning, baseras oftast på knoppix (www.knoppix.org)
  - Security Tools Distribution - http://s-t-d.org
- Belgian Computer Forensic Website/FCCU (Federal Computer Crime Unit) Boot CD
  - http://www.lnx4n6.be/ och http://www.d-fence.be/
  - En mycket bra beskrivning (hacklu.pdf) finns som visar hur man samlar in bevis med CD’n
- Forensic Discovery (bok)
  - http://www.porcupine.org/forensics/forensic-discovery/
- The Sleuth Kit – med stöd av The Autopsy Forensic Browser
  - http://www.sleuthkit.org