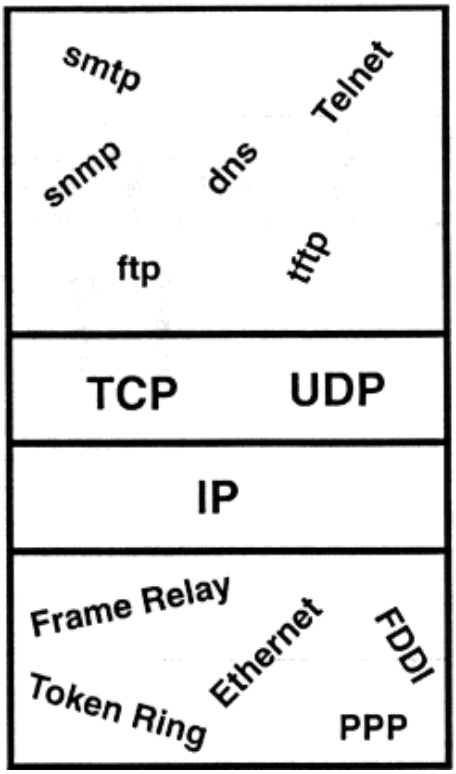
Säkerhetsproblem i TCP/IP

Grundprotokollen
- ARP
- ICMP
- IP
- TCP/UDP
- DNS

Routing
- Routrar
- Routingprotokoll

Applikationer
- SMTP
- TFTP
- WWW



TCP/IP - säkerhet
Säkerhetsproblemen i TCP/IP kan man dela in i olika delar som t ex :

Grundprotokoll:
Här tittar man på de mest grundläggande problemen i själva TCP/IP-slacken. TCP/IP designades för att kunna fungera i en svår miljö, men utan tankar på att man en dag skulle leta efter metoder att missbruka själva protokollen.

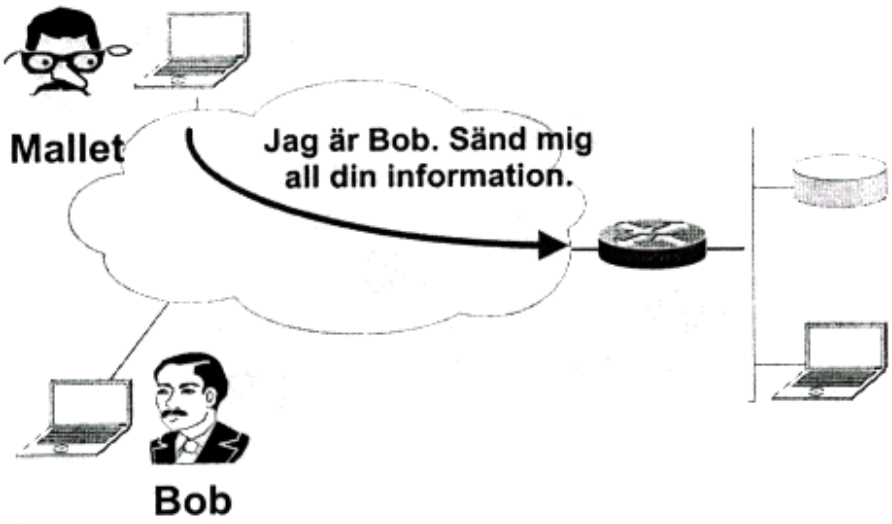
Routing:
Routingen är själva infrastrukturen inom TCP/IP-teknologin. Utan en fungerande routing kommer inget att fungera som tänkt. Routrar utgör också en del av näten och är med sina styrmekanismer ofta utsatta för attackförsök.

Applikationsprotokoll:
De flesta och mest kända attackerna riktar sig mot olika applikationstjänster. Ofta är syftet inget annat an att förhindra åtkomst av en viss service, sk DOS-attack.

Data-transport

- IP-spoofing Data spoofing
- Session hijacking Network sniffers

- **IP-spoofing** **Data spoofing**
- **Session hijacking** **Network sniffers**



IP-spoofing:
Innebär att man på olika sätt försöker att få privilegier med falsk IP-identitet, stjäla en IP adress.

Session hijacking:
När man lyckas att ta över eller agera "man in the middle" för en viss session.

Data spoofing:
Innebär att man förändrar data under pågående transport.

Network sniffers:
Innebär att man med hjälp av olika enheter på ett nät kan avlyssna trafiken.

Routingtabeller

Hur lär sig routrar sina tabeller ?
Hur görs vägval ?

RIP V1 och V2

Broadcast var 30 sekund till alla direktanslutna grannar.
Routing Information Protocol. Version 2 klarar av subnetmaskar och användaridentifikation. Lämpar sig endast för privata nätverk.

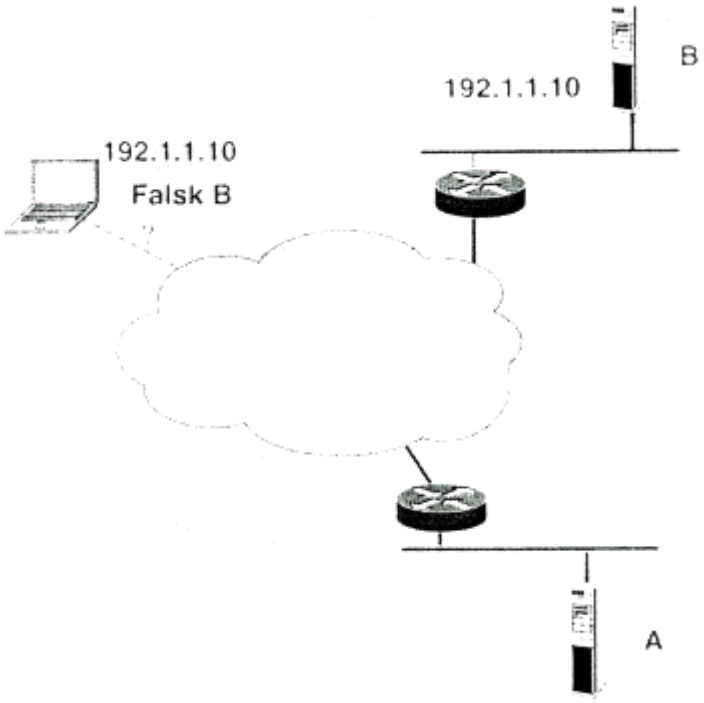
EGP

Exterior Gateway Protocol, meddelar var 15 sekund sin närvaro genom "advertisements" genom broadcast. Mera kompetent än RIP, handskakning förekommer.

OSPF

Open shortest path first, en hel familj med protokoll. Den mest kompetenta i samlingen router protokoll. Databaser till hjälp för statistiskt villkorsbetingade vägval och router meddelanden. Kryptering och handskakning med grannar. Nyttjas i backbone.

IP-spoofing



Vilket syfte ?
Hur förfalskar man sin adress ?
Vad kravs mer ?

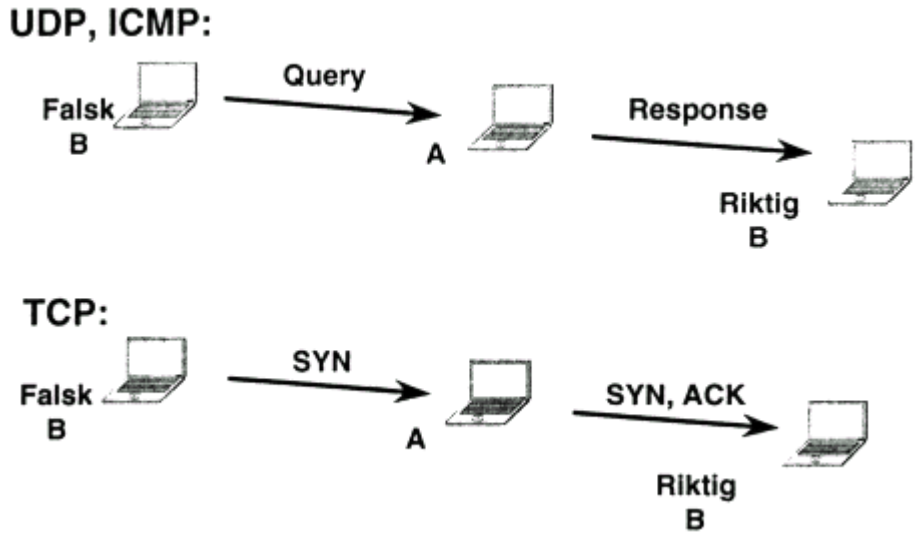
Spoofing:	parodi, drift, förfalskning
IP-spoofing:	Uppträda med falsk IP-adress i syfte att kringgå behörighetssystem

Varfor IP-spoofing:
- för att komma förbi filter i routrar och brandväggar
- for att ni tjänster på datorer som endast erbjuds viss IP-adress, t.ex. rlogin, rsh, ssh, nis+, ldap….

Falsk sourceadress

Skillnad mellan TCP och UDP

Ping



SYN-flooding

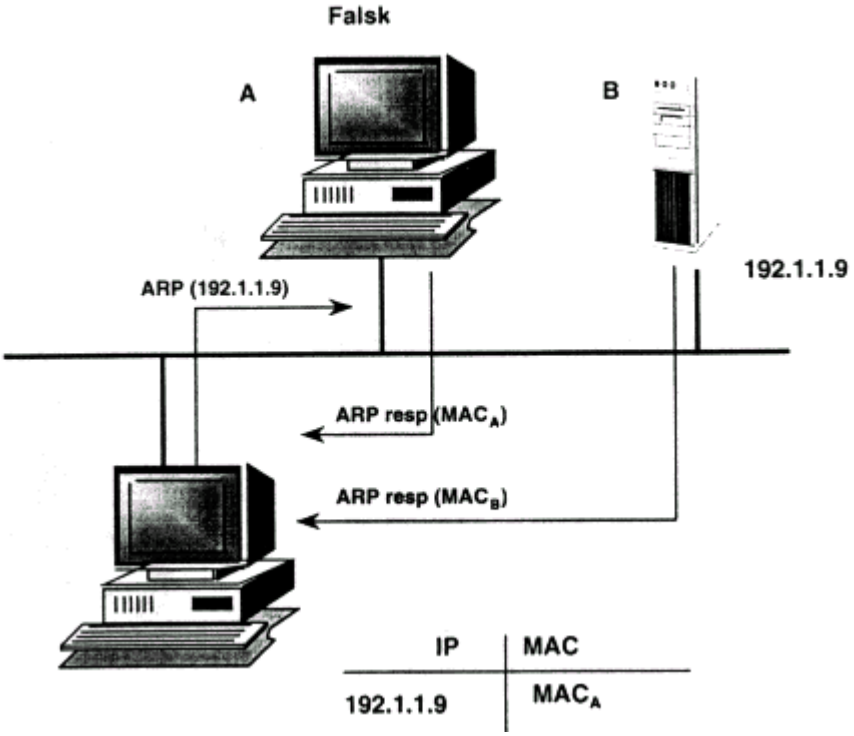
Trots att svaret går till "fel" dator kan man ända få problem med till exempel:
SYN-flooding (Flöda en dator med många TCP-uppkopplingspaket)
Ping of death: (Ett ICMP echo som innehåller en felaktig paketstorlek)

Vad händer om följande sänds:

- SNMP set
- Fråga till Character generator protocol med source addr = broadcast

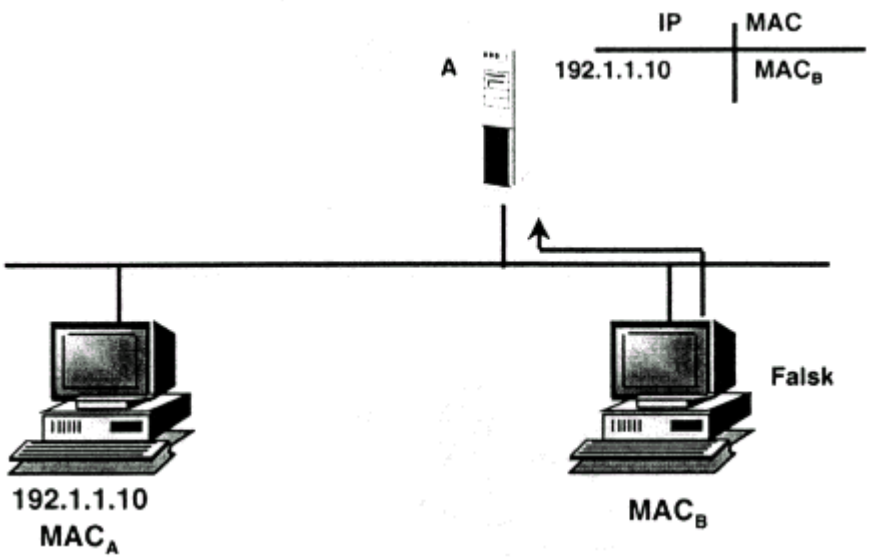
Falsk ARP-response

Exempel 1;

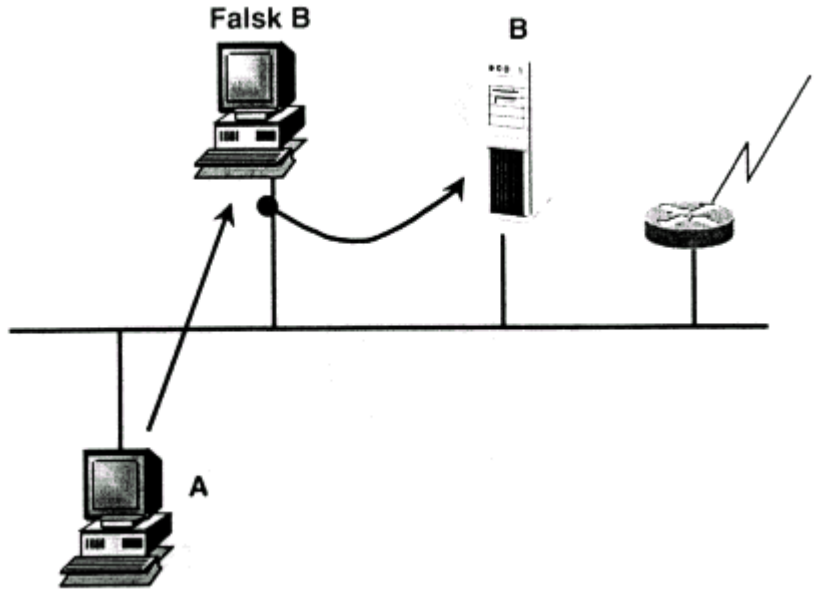


Falsk ARP-response

Exempel 2;

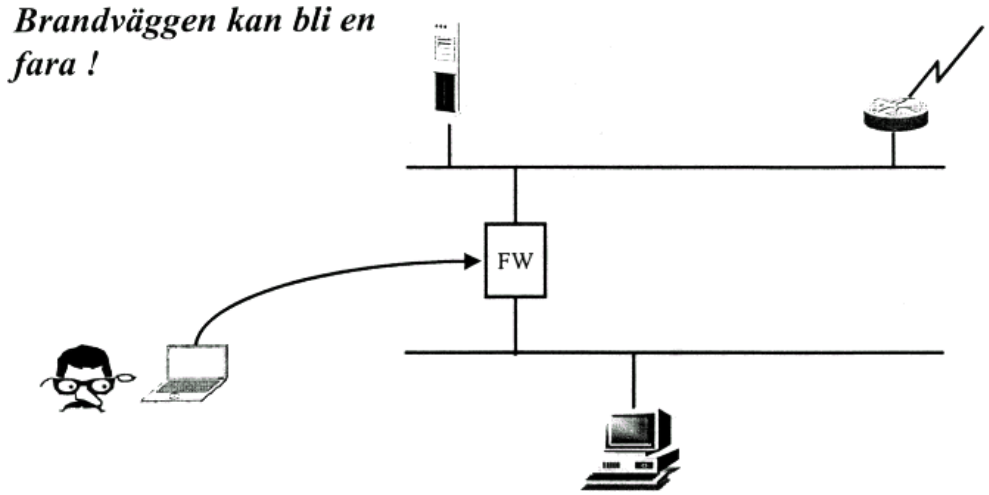


Man in the middle



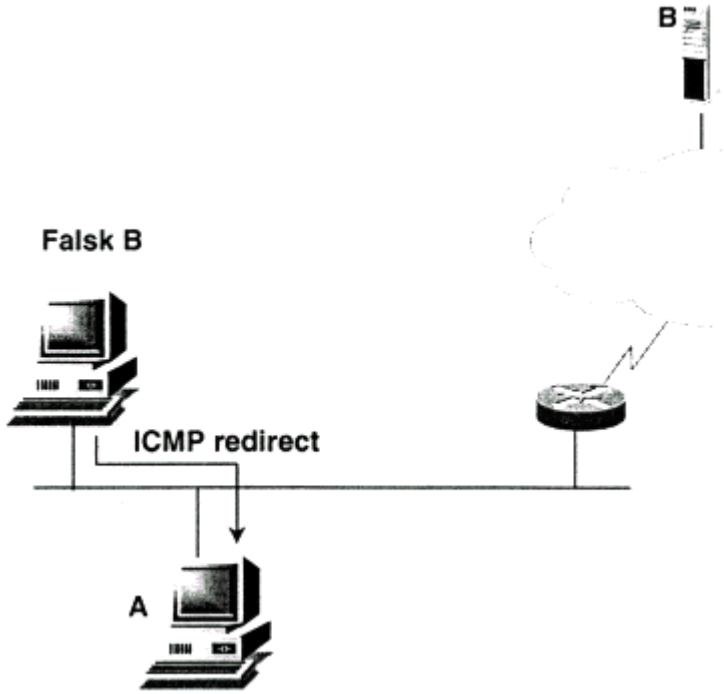
Kan t.ex. användas för:
- session hijacking
- modifiera data

Man in the middle



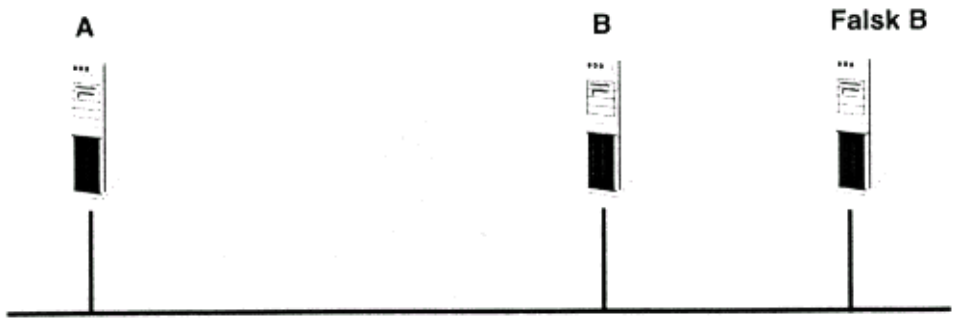
ICMP

ICMP kan användas felaktigt
Man litar på ICMP



ICMP

Vad kan man göra med **ICMP** *1* Vad bör förbjudas ?

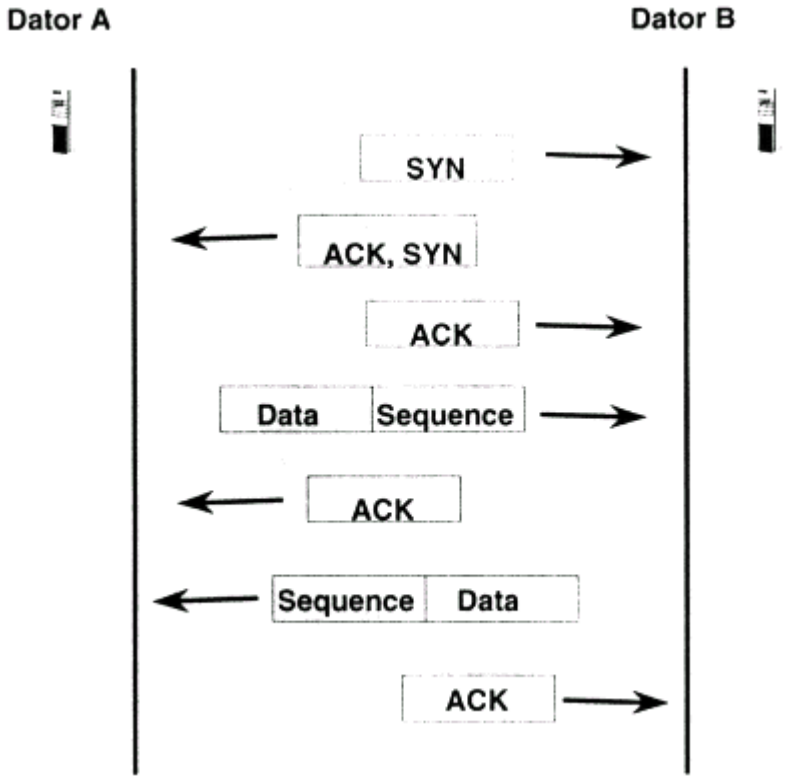


ICMP-meddelanden:

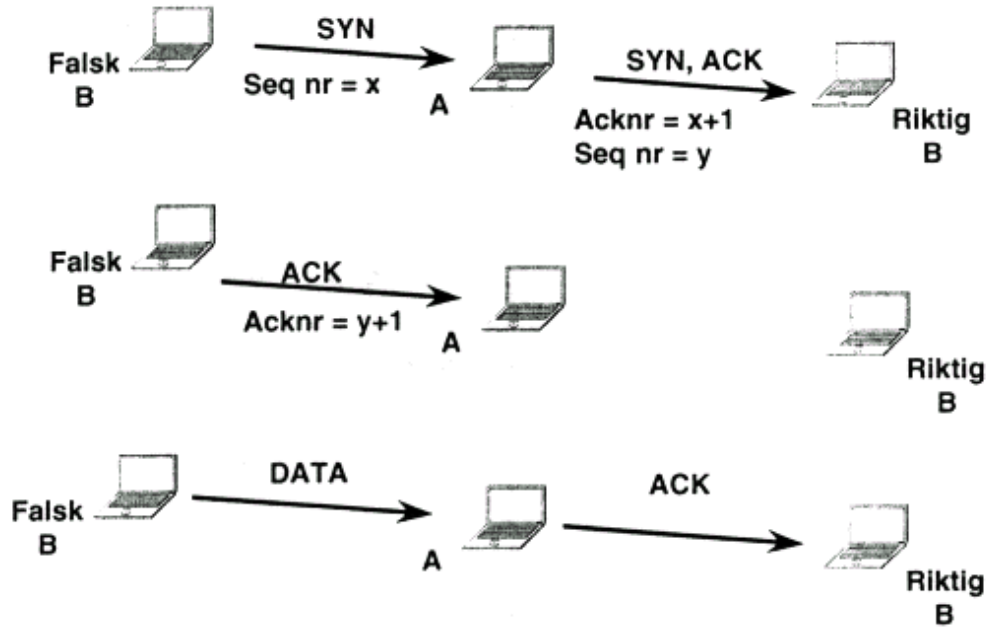
Echo reply
Destination unreachable
Source Quench
Redirect
Echo request
Router advertisement
Route solicitation
Time exceeded
Parameter problem
Timestamp request
Time stamp reply
Address-mask request
Address-mask reply

TCP-uppkoppling

Vad kontrolleras i TCP ?



TCP Sequence-number attack

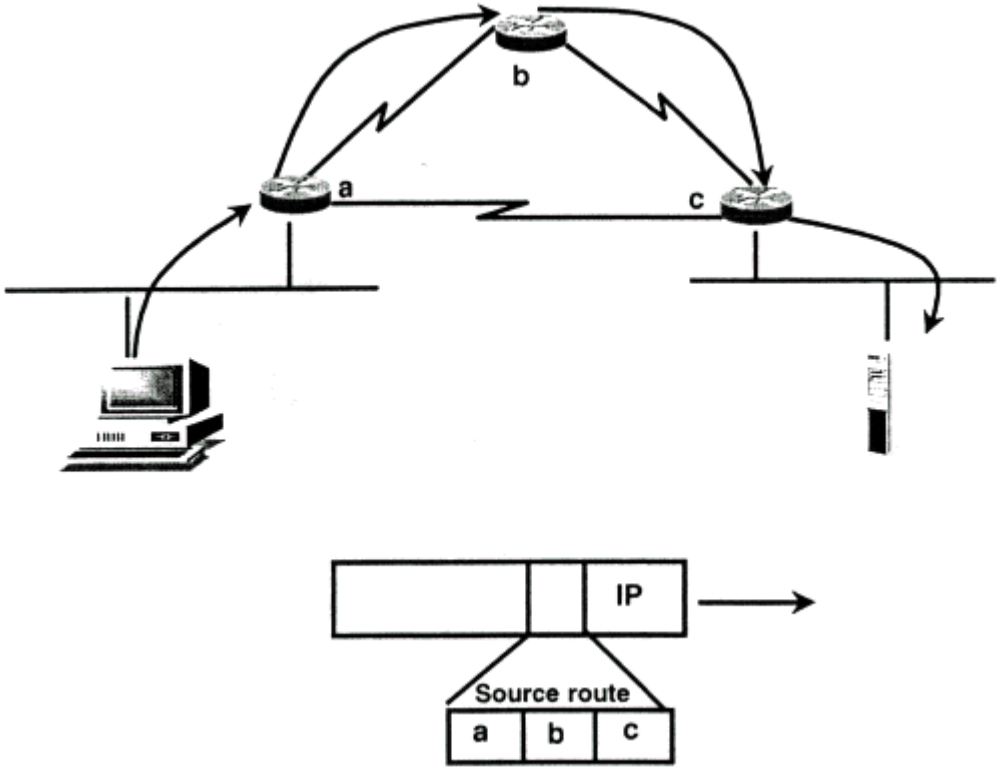


Hur vet den falske B vilket ack nr den skall använda i paket nr 3 ?

- Enligt specen ska A välja initialt sekvensnummer "slumpmässigt" (uppdatera seqnr var 4 mikrosek). Detta görs inte av alla implementationer!
- Koppla upp en förbindelse till en godkänd port, t.ex. SMTP. Beräkna därefter vad nasta TCP-koppel kommer att få för initialt! sekvensnummer.
- Attackera efter att B eliminerats!

Ser inte output, men kan ge input.

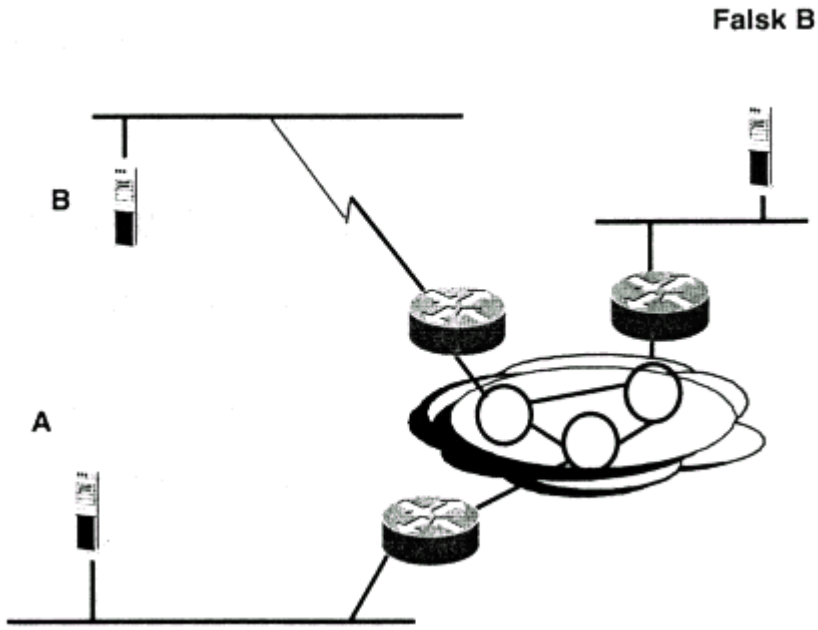
IP source routing option



Ett bitmappat fält bestämmer vilka av de i optionsfältet, sist i IP huvudet, medföljande ip-adresserna som skall besökas enl nedan:
0=Loose Source Routing
1=Strict Source Routing
Metoden användes för att på förhand bestämma paketets väg genom Internet, eller för att nå in bakom en NAT server till icke routebara IP adresser.

Routingprotokoll

Är routrar kritiska till information ?



Åtgärder;

Statisk routing
Passive interface
Route filtrering

Hur kritiska är routingprotokoll till falsk routinginfo?

- RIP saknar användaridentifikation för RIPv1, beslut fattas av den lokala routern enkom på basis av mottagen tabellinformation, utan att verifiera informationen. Fel sprider sig snabbt.
- OSPF En hel familj med protokoll för utbyte av routinginformation, kryptering och nyckelutbyte (MD5) är vanligt förekommande. Beslut fattas med hjälp av statistik och tabellutbyten.
- BGP/EGP/IGP Samma som för OSPF.

Domain Name System - DNS

- DNS är en distribuerad katalogtjänst
- Mappar namn mot IP-adresser
- Rekursiv sökning i domanstrukturen
- Servrar ansvarar for en eller flera zoner
- Servrar cachar information
- Reverse lookup används för att mappa en IP-adress mot ett namn
- DNS-namn används ibland för autenticering
- Utan DNS faller allt...

DNS används för:

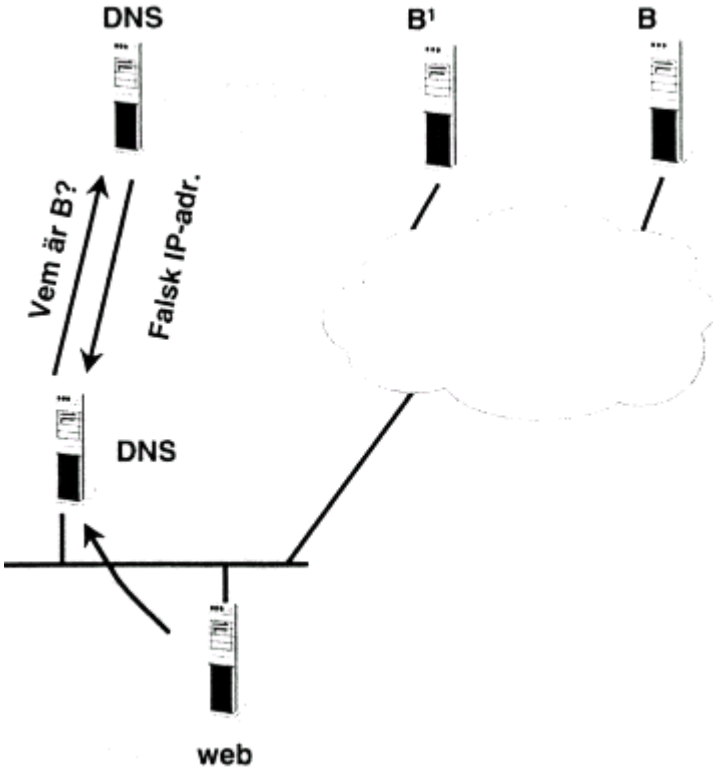
Uppkoppling mot datorer med hostnamn. DNS mappar hostnamn mot IP-adress, t ex www.lraining.telia.se til! 194.52.54.36

Baklangesuppslagning (Reverse Lookup):
194.52.54.36 mappas mot www.training.telia.se

Leverans av elektronisk post:
DNS mappar domändelen av en mailadress till ett postkontor, t ex:
training.telia.se till mail.training.telia.se

DNS kan även mappa applikationer, det görs via sk. taggar

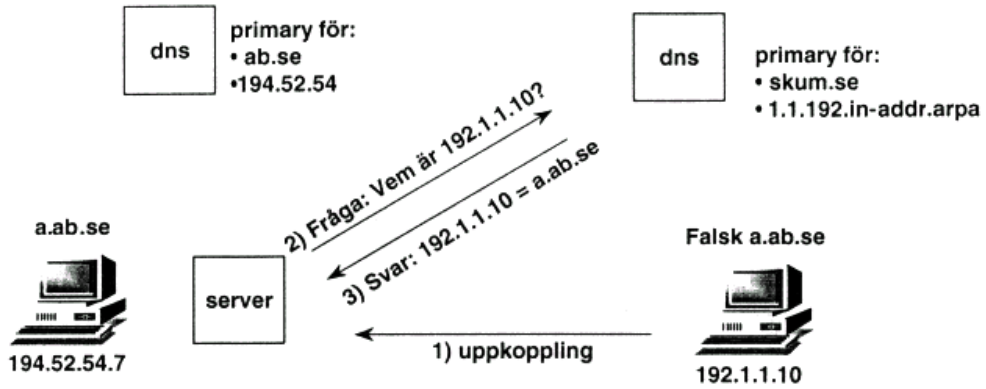
Falsk DNS-information



Hur kan DNS-info förfalskas ?
Vilka skador kan uppstå ?
Olika tjänster påverkas olika

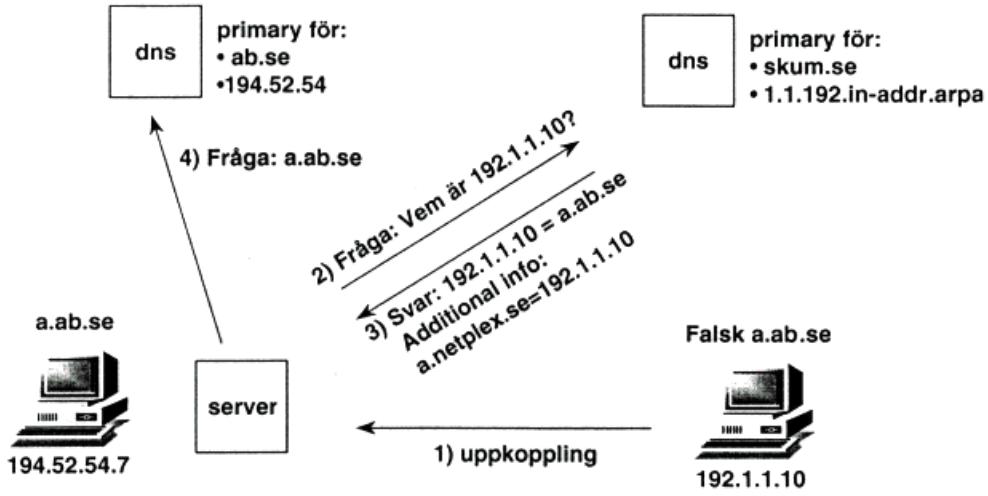
Falsk DNS-information

Den som kontrollerar domänen för baklängesuppslagning (in-addr.arpa), kan lägga in godtyckliga hostnamn.



Dubbel DNS-uppslagning

Additional info ifrågasätts inte och kan användas for att "smutsa" ner DNS-cachar.



Några problem med DNS:

Världens största distribuerade databas. Dessutom utan någon egentlig kontroll.
Ingen autenticering sker av vem etc DNS-svar kommer ifrån.
Programmet är välkänt, vilket gör att eventuella buggar kan utnyttjas "optimalt"

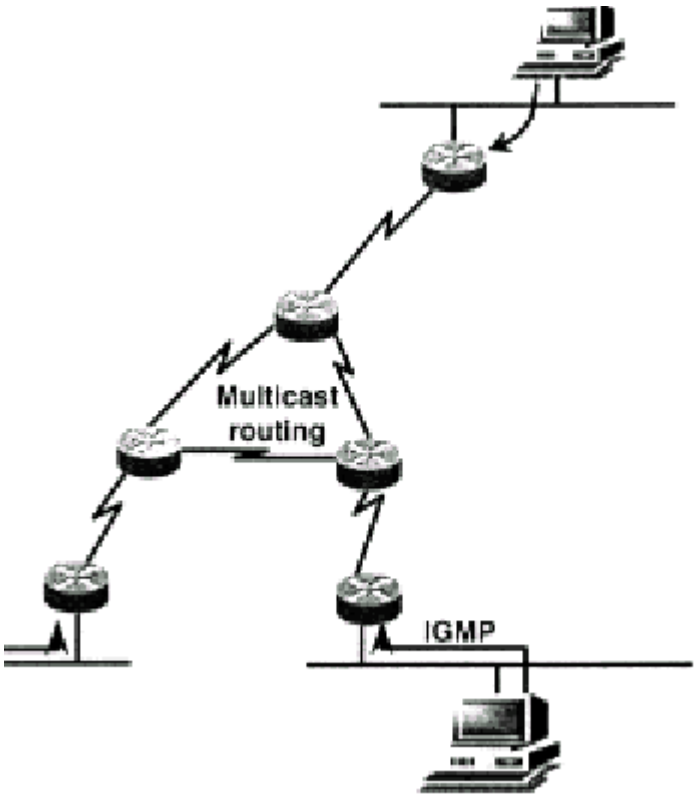
Tänkbara attacker:

Flöda klienten med svar - sänd in tusentals falska svar, då den ställer en fråga. (Även vid uppstart).
Förorena klientens cache - förse klienten med falsk information (additional information) i samband med svar på andra frågor.
Ändra i DNS-konfigurationsfilerna.
Buggar i BIND-paketet.

De senaste versionerna av bind har utökats med ett Autentieringsprotokoll, dock ej särskilt använt ännu.

Multicasting mm

Introducerar en rad nya problem, multicasting har funnits ett tag men inte utvecklats riktigt ordentligt och ej heller blivit riktigt populärt.



Nya tjänster kommer emellertid, några som sett dagens ljus är:

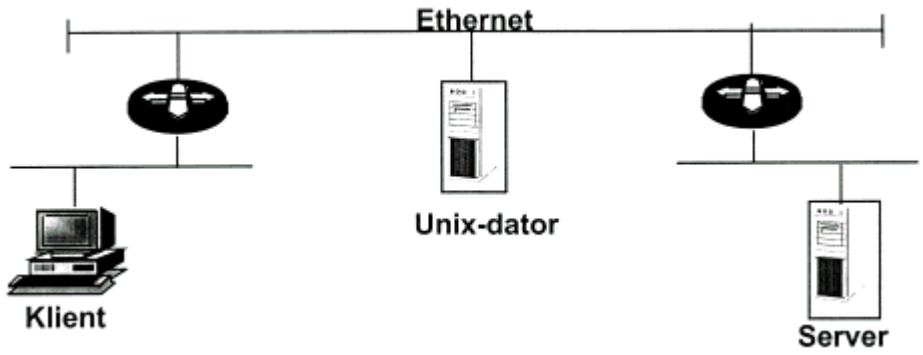
VoIP
Mobile IP
Media on demand
Multicasting

Det finns också ett MBONE nätverk över hela världen med avsikt att kunna leverera multicast med världsperspektiv, dock ej särskilt nyttjat.

En del programvaror för replikering av information nyttjar multicast för att spara bandbredd.

Säkerhetsproblem med applikationer

Avlyssning av nät

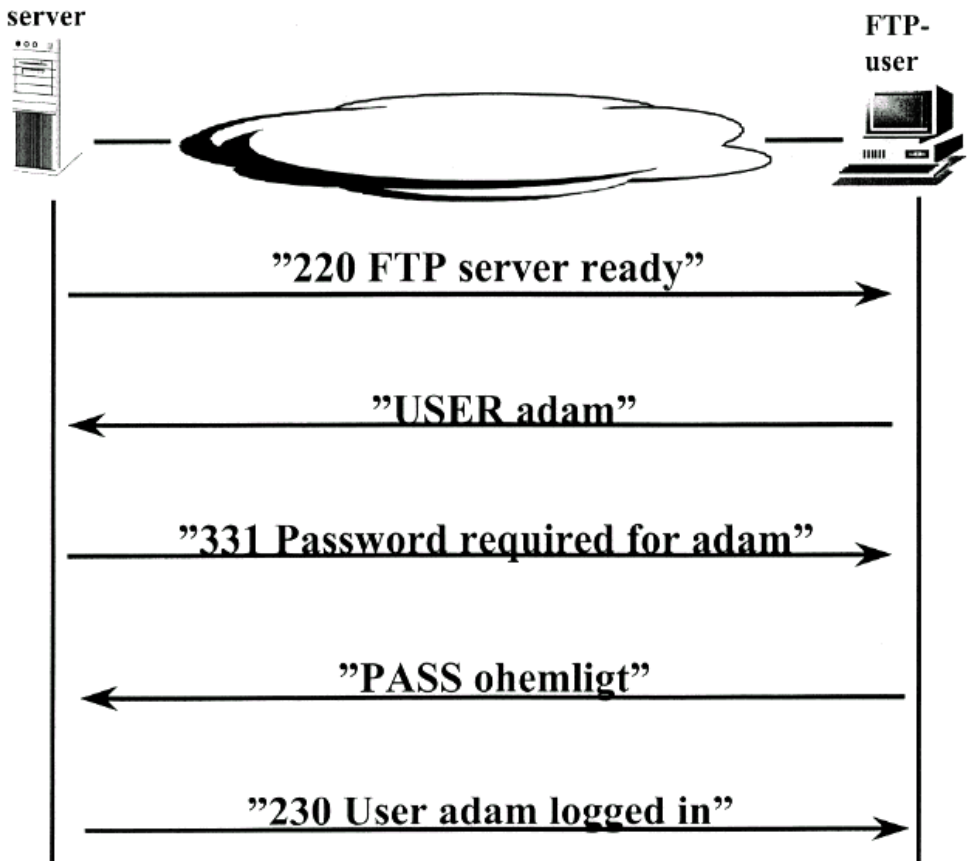


Packet sniffers:
- Unix dator som står och "skräpar". Den kanske används.
- Inga säkerhetspatchar inlagda.
- Utnyttjas av crackers för att lyssna på nätet och samla användarnamn och lösenord i klartext.
- Färdiga program finns som bara sparar undan information om konto och lösenord.
- Mycket vanligt hackerverktyg.
- En switchlösning kan vara första steget mot ett säkrare nät

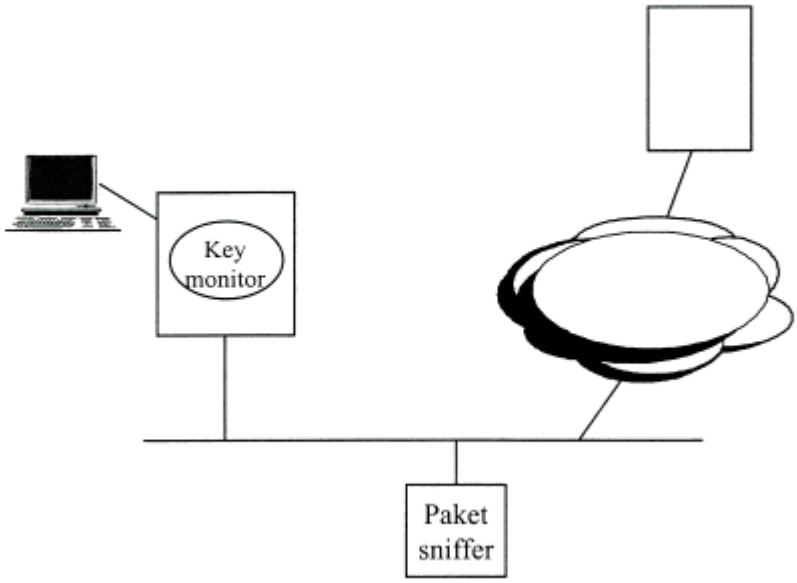
Lösenord i klartext

Flera vanliga protokoll sänder användarnamn och lösenord i klartext vid inloggning, t.ex.

- RLOGIN.
- TELNET.
- FTP.
- POP.



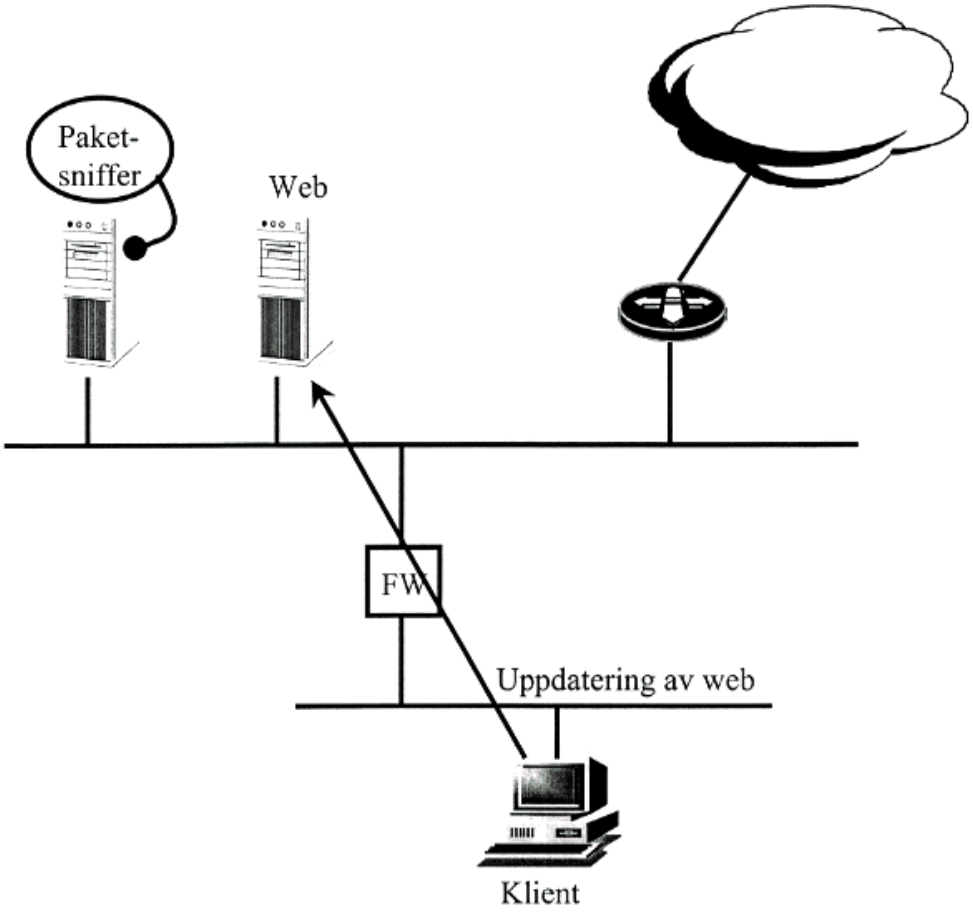
Keystroke monitors



- lösenord till andra datorer
- engångslösenord och kryptering hjälper inte

Finns flera olika typer av dessa verktyg, en del monteras mellan tangentbord och dator, andra som mjukvara i den avlyssnade datorn. Installationen kan ske med virus eller trojan som leveransmetod. Nedtryckta tangenter kan sparas i lokal fil eller sändas direkt till vem som helst på nätverket.

Praktisk andvändning av paketsniffer



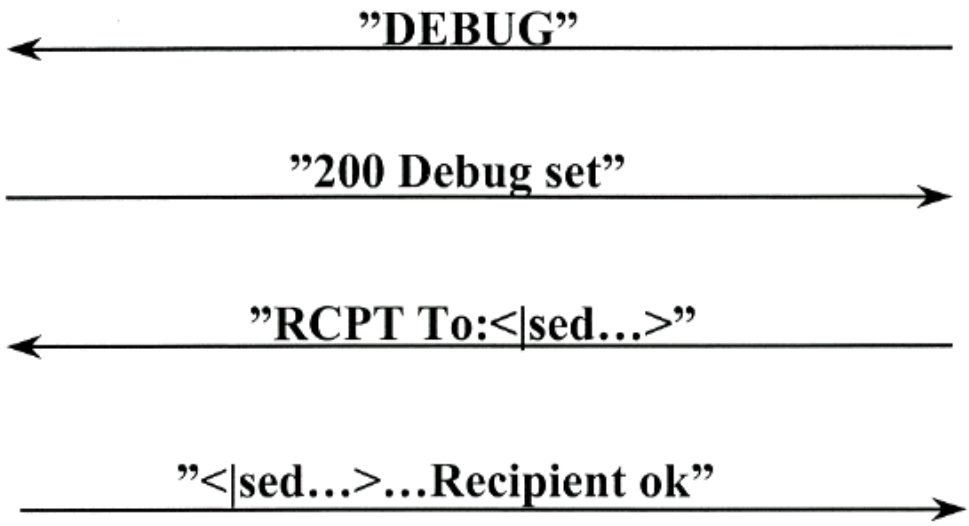
Sendmailbuggar genom åren

• Skicka mail till filer på systemet
• "wizard's password", möjliggjorde åtkomst till systemet
• "debug mode", med DEBUG kommandot gavs utomstående åtkomst
• Skicka mail till program som mottagare
• Undermålig validering av argument, vilket har gett möjlighet att skriva över i minnet

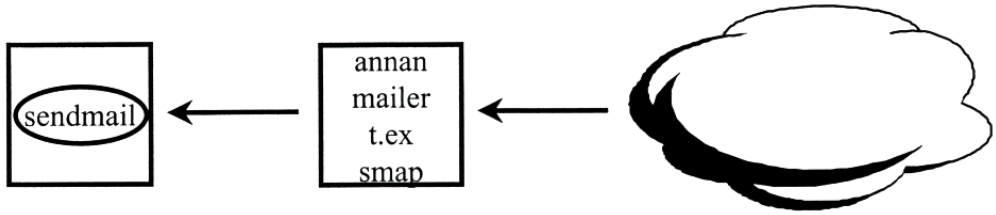
Grundproblem med Sendmail:
stort, komplicerat, flexibel programvara
kors av superuser
tar emot kopplingar från alla

Man kan köra en vanlig telnet session till sendmail och skriva post manuellt med godtycklig avsändare.

- Ett trick som Internet-masken använde:



Undvik att exponera Sendmail



Vad händer när brevet kommer fram till "Sendmail"?

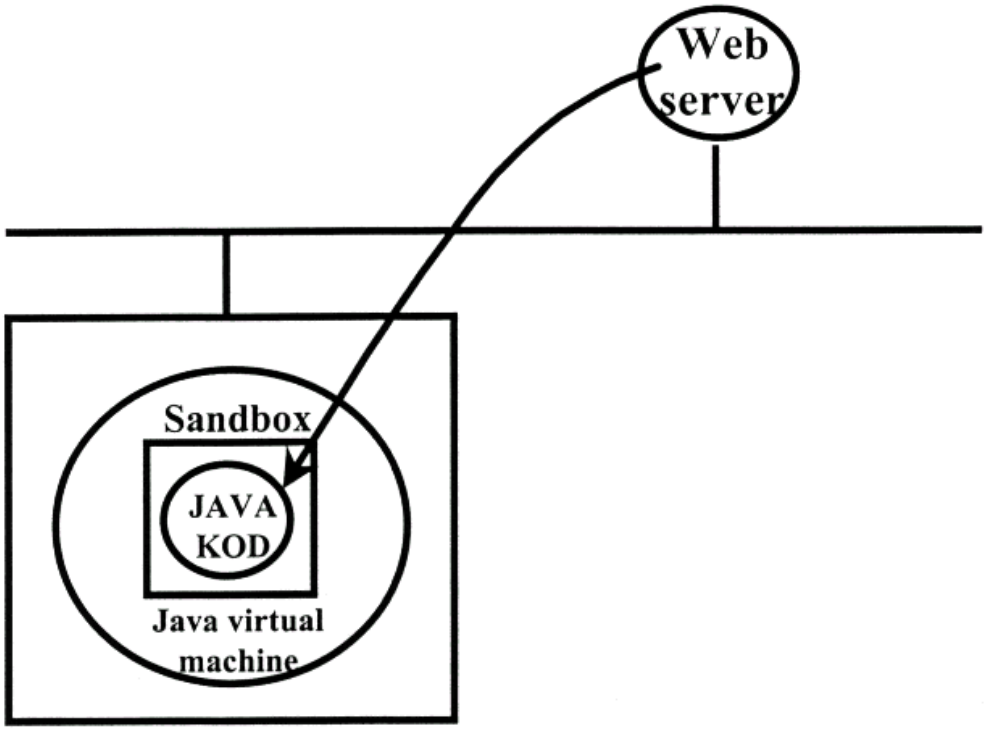
Det finns flera aspekter, någon form av content check av e-post bör göras, flera trojaner och virus kommer in i våra system denna väg.

Sendmail är helt öppet och behöver hjälp av andra programvaror för att bli säker.

Uppkoppling med telnet

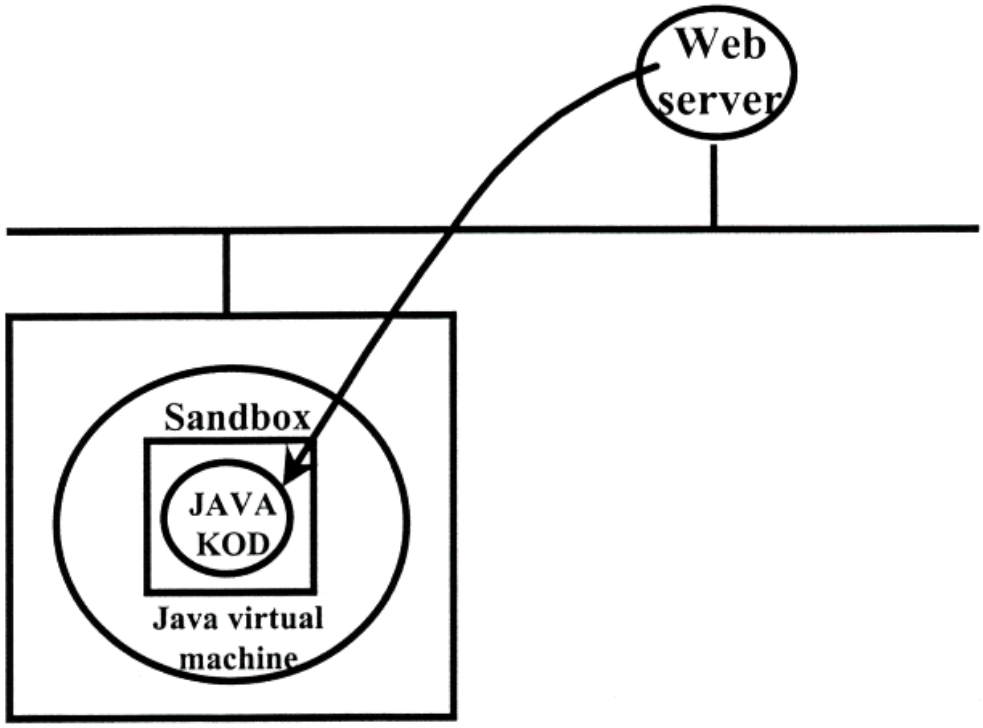
```
>telnet 10.2.1.1 25
 Trying 10.2.1.1...
 Connected to ariadne.offer.se.
 Escape character is '^]'.
 220 offer.se Server ESMTP ready at Thu, 17 Jul 1997 19:10:09 +0100
>HELO mailhub.rask.se
 250-That hostname is inconsistent with your address to name mapping.
 250 offer.se expected "HELO mailhub.ljusskygg.se"
>MAIL FROM:<skum@rask.se>
 250 Ok
>RCPT TO:<bobo@offer.se>
 250 Ok
>DATA
354 Start mail input; end with <CRLF>.<CRLF>
>
>FROM:skum@rask.se
>TO:bobo@offer.se
>
>Du kan lita på mig!
>
>.
>
250 Roger
```

Java



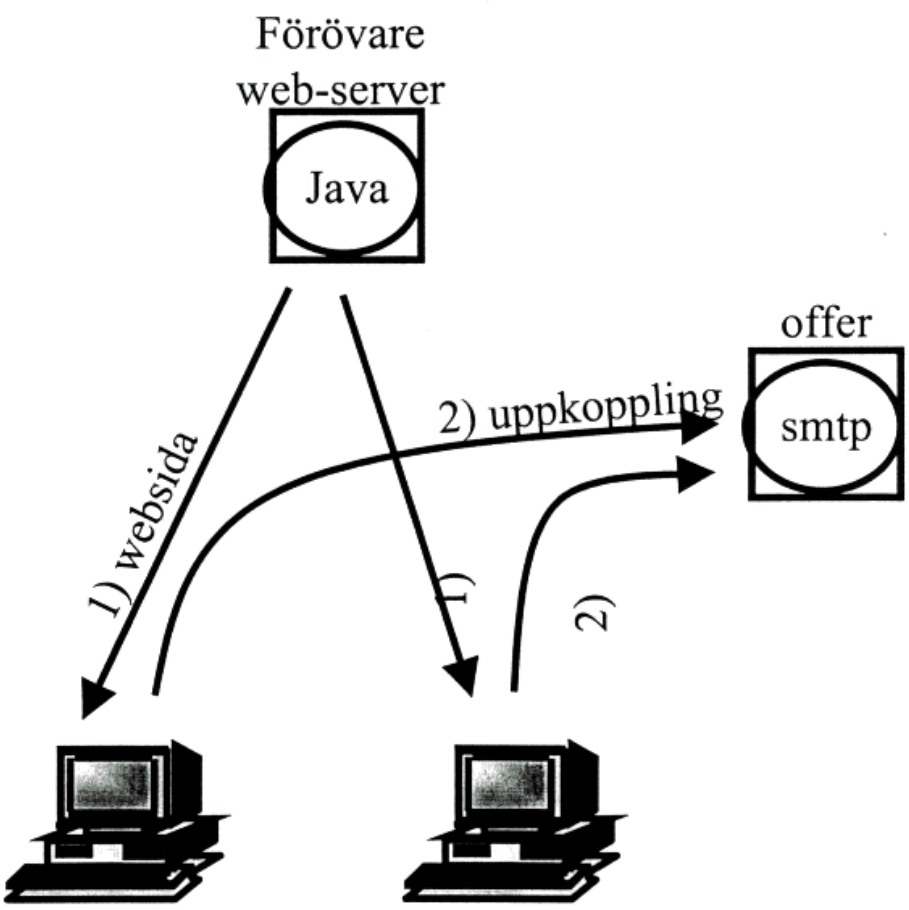
• Utvecklat av SUN 1995, tog fart under 1996
•C++ liknande
•Portabelt (byte code)
• "Designat med tanke på säkerhet", men flera allvarliga buggar i Java-implementationer har rapporterats, t.ex. har det varit möjligt att:
  - öppna godtyckliga förbindelser till andra system
  - modifiera filter på den lokala datorn
  - hämta en lista över URL:er som användaren har besökt
• Strider mot principen "utsatta datorer ska köra så få program som möjligt, de som körs ska vara så små som möjligt".
• Ett kraftfullt programspråk at hackers!

ActiveX



- Binär objektkod baserad pa Microsofts OLE (Object Linking and Embedding) och COM (Component Object Model).
- Möjliggör for programkomponenter att samverka i nätverksmiljö.
- Begränsas inte av webbrowsern (jmf Java).
- Da den körs, kan den utföra OLE-baserade operationer.
- Klienten ska skyddas genom att endast signerad kod från pålitliga servers ska valjas att exekveras.
  Om koden inte är signerad av pålitlig port ska den inte laddas ner. (kra'ver nyckel administration)

Utnyttja 3:e part i en attack

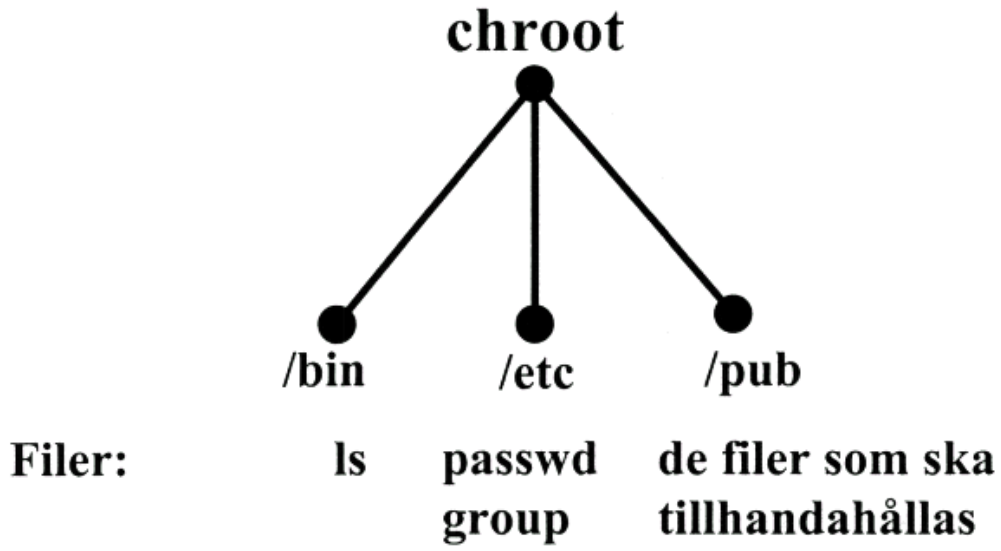


CGI-script

CGI scripten körs på servern, även känt som SSI server side includes. Riskerna är många och allt är upp till programmeraren. CGI är vilket körbart program som helst, ex batchfiler, shellscript, c program, perlscript, php med mera.

- CGI (Common Gateway Interface), för att kunna ha program bakom websidorna
- Samma möjlighet till buggar som traditionella serverapplikationer
- CGI-script utgör en möjlighet att få obehörig åtkomst till filer på servern, alternativt få kontroll över servern.
  T.ex. genom att CGI-scriptet tillåter läsning av filer på andra kataloger än vad webbservern ursprungligen konfigurerats för
- CGI-script innehåller en bug som möjliggör för externa användare att köra godtyckliga kommandon på servern
- I många fall ovana programmerare
- Egenutvecklade, ej "publika" program, bör hemlighållas, för att förhindra upptäckt av säkerhetshål

Installation av anonym FTP på Unix



- Använd ett "restricted filesystem", vilket åstadkoms med chroot. FTP arkivets rootkataloger är inte den verkliga rootkatalogen utan en underkatalog till denna.
- Skrivbara kataloger kan utnyttjas av programvarupirater. Om skrivbara kataloger måste finnas, se till att:
  - katalogen inte är läsbar for ftp-anvandare
  - se till att begränsa diskutrymmet (filequota)
  - flytta kontinuerligt (t.ex. var 15 min) inkomna filer till andra kataloger, ej nåbara for ftp-anvandare (med hjälp av ett script)
- Blanda inte anonym FTP och Webbkataloger. Detta ger FTP-anvandare möjlighet att nå webfiler (t.ex. script).

TFTP
(Trivial File Transfer Protocol)

- Används typiskt for att hämta konflgurationsfiler
- UDP-baserat
- TFTP saknar autenticering av användaren
- Ska konfigureras så att överföring endast kan ske från vissa kataloger. Om inte, klassiskt trick att hämta /etc/passwd (Unix).
- CERT rapporterade problem med AIX TFTP demon redan oktober 1991. Trots delta inträffade en incident där minst 140 siter drabbades 1993, där svagheten hot TFTP utnyttjades.

NTP (Network Time Protocol)

- För att synkronisera klockor
- Tar hänsyn till transmissionsfordröjningar
- UDP-baserat
- Inte designat for att motstå attacker
- Att andra systemklockor kan fa konsekvenser for säkerheten:
  - log filer kommer inte att ha ratt tid, ev kan även loginfo fas att raderas då den är "gammal"
  - filers datum (skapad, andrad, ...) kommer inte att vara ratt
  - batchjob kommer ev inte att startas
  - tid är viktigt for vissa autenticering system, t.ex. Kerberos

rlogin

• Typiskt Unix
• Använder IP-nummer och hostnamn for autenticering.
Känslig for IP-spoofing och DNS-manipulering
/etc/hosts.equiv anges "trusted hosts", användare på dessa anger inte lösenord då de loggar in med rlogin eller rsh
• Se upp for plus-tecken (+), gör alla datorer till trusted.
SUNOS hade per default ett plus-tecken i hosts.equiv, vilket gjorde alla till trusted hosts. Klassiskt hack!
.rhosts varje användare kan ange "trusted hosts"

X Windows

- Fönstersystem, används på Unix arbetsstationer, X-terminaler eller PC:s
- X Window-servern körs på arbetsstationen (ej serven)
- Applikationer kopplar typiskt upp sig mot arbetsstationens fönstersystem (X Window-servern)
- X Window-servern använder TCP portnummer >6000

Säkerhet

- X-servern skyddas typiskt endast med (x host) en lista över godkända hostar
- De godkända hostarna får oinskränkt kontroll över fonstersystemet, t.ex. - kan ta över tangentbord, monitorers
  tangenttryckningar och sanda dem till lämpligt
  ställe
- Andra säkerhetsmekanismer finns, (SUN Secure RFC och Kerberos) men används typiskt inte

Se upp med reflection och exeed samt liknande programvaror då de oftast nyttjar rlogin och telnet. SSH (secure shell) börjar dock bli allt mera populärt, där krypteras inloggning och session via publik/privat nyckel.

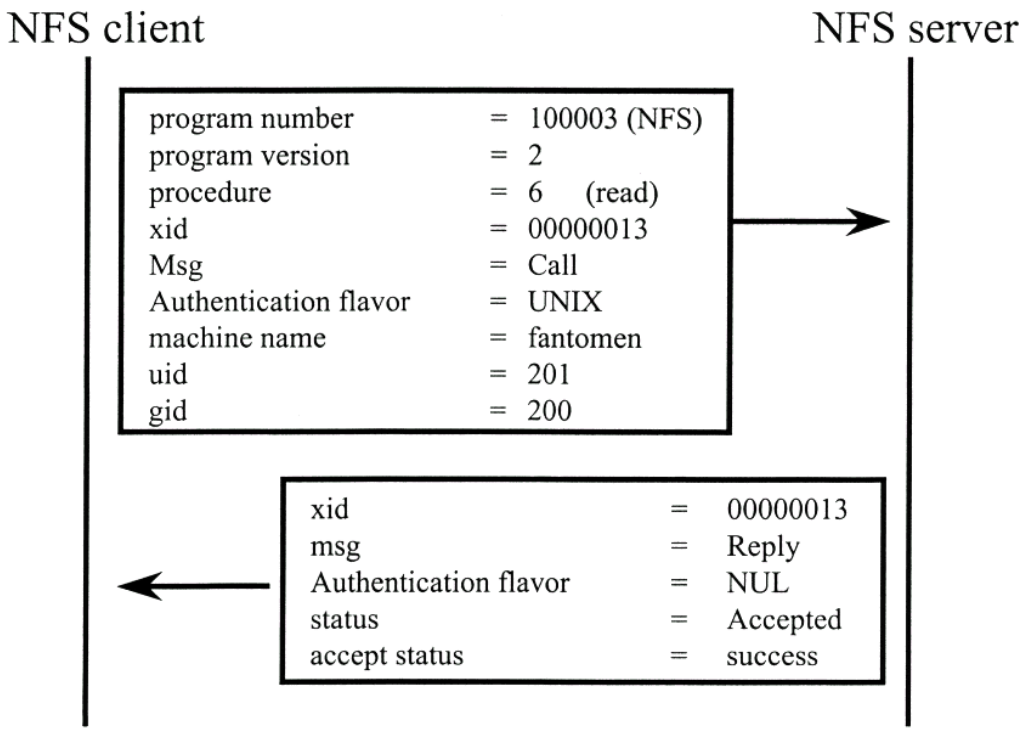
RPC, NIS, NFS

- Utv. av SUN vid mitten av 80-talet
- NIS, katalogtjänst for systemadmin, t.ex. central lagring av:
  - /etc/hosts
  - /etc/passwd
- NFS, Network File System, har fått stör acceptans bland flera leverantörer.
- NIS och NFS baserade på RFC
- RPC utvecklades for att erbjuda ett enkelt programatiskt gränssnitt åt applikationsutvecklare for utveckling av nätverksapplikationer
- RPC kör typiskt över UDP men kan idag även köras över TCP

Se upp med dessa protokoll, inloggning och informationsutbytet sker i klartext, dock kan de flesta nyttja Kerberos med litet handpåläggning.

RPC – Protokollet

RPC - protokollet gör del möjligt for en "client" att:
1) Ange vilken procedur som skall exekveras på servern
2) Para ihop ett svar från servern med en fråga som tidigare tällts till servern.
3) Identifiera sig for servern NFS client



Hot E-post - liten checklista

Tillgänglighetsförlust

Efter hand som e-post används blir del en allt viktigare funktion inom företaget och ut mot Internet. Da e-post ofta startar i "liten **skala"** glöms ofta konsekvenserna av en tillgänglighetsförlust bort

- genom att den externa e-postservern/brandvaggen/routern slås ut eller blockeras med trafik
- genom att mailbomba, t ex genom att anmäla en person till manga mail-listor eller att göra anmärkningsvärda debattinlägg i den personens namn.

Avlyssning av data

E-postmeddelanden sands ofta i klartext, varför någon med tillgång till nätet mellan er och sändaren/mottagaren av posten kan avlyssna denna, t ex:

- genom att ha en linjelyssnare på något nät mellan er och sändaren/mottagaren av post
- genom att läsa post som passerar en e-postserver, t ex hos en operator

Virus

Virussmittade filer kan mottas eller sands via e-post.

Omstyrning av trafik US falsk mottagare

E-post adresserad till/från Internet kan levereras till en falsk mottagare, t ex genom att manipulera DNS-information eller IP-routing

Manipulering av brev

Om e-post kan styras om till en falsk mottagare, är det även tänkbart att e-post i transit över nätet manipuleras.

Förnekande

Mottagaren av ett brev som ni sänder förnekar mottagandet av delta. Alternativt kan någon hävda att de har sänt ett brev till en av era användare, men att denne inte vill kannas vid delta. En orsak är att vissa personer får ansenliga mängder post (från maillistor), och slarvar med alt läsa igenom och klassificera det inkomna.

Hot E-post - liten checklista, forts.

Falsk avsändare

Avsändaren av brevet är inte den som den utger sig for; kan t ex användas for att:

- sprida påståenden for att trakassera en person eller ett företag
- sprida desinformation
- beställa varor i falskt namn

Otillbörlig åtkomst

- "sendmailbuggar"
- genom att exekvera mottagen kod

Trafikanalys

- Någon kartlägga med vilka ni utbyter information

Hot

Bombhot och dylikt, t ex via en remailer.

Hantering av virus

- Straffa inte folk, be dem berätta så snabbt sorn möjligt.
- Se till att ha uppdaterade antivirusprogram. Vem bar vad?
- Rekommendera antivirusprogram både på WS och Server, samt ev. hem-PC.
- Automatisk uppdatering av antivirusprogram vid inloggning.
- Boota antivirusprogrammet från skrivskyddad diskett.
- Scanna av arbetsstationerna en gång per vecka (t.ex.)
- Vid angrepp är det naturligtvis bättre att a

återinstallera programvaran an att desinficera den.

- Hantering vid angrepp:
  1) Koppla bort WS från server
  2} Städa server
  3) Städa WS, se till att WS inte kopplas in före det.
- Backuphantering även viktig for att mota virushotet.
- Vilken akut hjälp garanterar leverantören vid nya virus?
- Utbilda användarna om virus; varför antivirusprogram skall köras, berätta om problem som uppstått på företaget.

CGI-script

Några enkla regler for CGI-script:

1) Tillåt endast CGI-script på servern efter det att de har granskats av säkerhetskunnig
2) Script skall klara av att hantera godtyckligt (elakartat) indata, lita inte på restriktioner av indata (kan kringgås)
3) CGI-script ska antingen utföra den förväntade funktionen eller returnera felmeddelanden
4) Kör inte scriptet som superuser (Unix)
5) Användare ska inte tillåtas ha program eller kommandon på servern
6) Om webbservern faller, ska inte förövaren kunna nå längre in i organisationen

Hot mot Webbserver Liten checklista

Tillgänlighetsförlust

- genom att den externa www-servern slås ut
- genom att brandväggen slås ut
- genom an nätet blockeras med trafik

Manipulering av Webb information

- någon obehörig ändrar information i er WWW-server
- information andras medan den 6'verrors på Internet
- Internetanvändare kopplar upp sig mot en falsk webbserver i tron om att de bar kopplat upp sig mot er Webbserver, t ex genom att manipulera DNS- eller routing- information.

Avlyssning av Webbinformation

- avlyssning av information medan den överförs på Internet är möjlig, men vanligtvis inget problem då det rör sig om publik information.

Speciella problem när beställningar via Webb erbjuds

- kund förnekar gjord beställning
- en kunds riktiga beställning återuppspelas
- en falsk kund gör en beställning

Otillbörlig åtkomst till det skyddade nätet

- uppdatering av webben från det inre nätet görs, så att ett säkerhetshål öppnas upp i brandväggen mot det inre nätet

Trafikanalys

- utomstående kan kartlägga vilka som söker information

Webbklienter - Liten checklista

Otillbörlig åtkomst till information

- genom att utnyttja buggar eller features i Java, ActiveX, eller i någon plug-in, t ex genom att information från den lokala disken sands ut utan användarens vetskap.
- ett nerladdat program utfor otillbörliga operationer

Tillgänglighetsförlust

- buggar eller features i klienten
- genom att den externa webbservern slås ut
- genom att brandväggen slås ut
- genom att nätet blockeras med trafik
- ett nerladdat program utfor otillbörliga operationer

Avlyssning av Webbinformation

- avlyssning av information medan den överförs på Internet är möjlig
- era användare kopplar upp sig till en falsk Webbserver i tron att de får information från den riktiga Webbserver.
- "man in the middle"-attack
- era användare kopplar upp sig till en falsk Webbserver i tron att de får information från den riktiga Webbserver, t ex genom att manipulera IP eller DNS, eller att URL skrivs om under transit.
- felaktig information hämtas från en riktig server, då någon obehörig bar manipulerat informationen
- information andras medan den overförs på Internet

Speciella problem om beställningar via Webb erbjuds

- leverantör förnekar gjord beställning
- er beställning uppfångas av obehörig och återuppspelas

« en falsk kund gör en beställning i ert namn

- ert kreditkortnummer uppfångas och används sedan av obehörig

Trafikanalys

- någon kartlägger vad era användare söker information