Säkerhet i TCP/IP

Datorsäkerhet

- Plattformar:
  - Unix
  - Windows NT
  - Macintosh
  - PDA

- Varför behöver vi bry oss, vi har ju en brandvägg?:
  - Brandvaggen måste ju ha ett operativsystem alt köra på.
  - Minst 70% av alla datorintrång sker från insidan

Plattformar
De plattformar som oftast beror när det gäller datorsäkerhet är UNIX och NT. Anledningen är att de är de vanligaste server-systemen. Unix har varit del starkaste medan Windows NT har kommit den senaste tiden. När del gäller att deklarera säkerhetsproblem har dom valt två olika inriktningar. UNIX har hell öppen policy när nya buggar kommer, vilket leder till att uppdateringar i form av patchar skrivs mycket snabbt. När del gäller NT så har Microsoft en lite tillbakadragen filosofi. Först nekar man till att det existerar en bugg och därefter kan del dröja ett bra tag innan en uppdatering släpps. Denna filosofi kommer att behöva ändras dels för att möta kundernas behov samt att det finns ett antal hemsidor som listar de senaste buggarna till både UNIX och NT.

Hostsäkerhet
Anledningen till att man måste fokusera sin säkerhet-policy även på hostarna. Beror på att det är dessa som blir angripna. Delta gäller både det vi kallar bastion-host men lika väl server system på insidan, Flera studier visar all 70% av intrången på företag sker från insidan vilket leder till att brandvaggen man inskaffat inte har något resultat. En sak man inte far glömma är att även brandvaggen körs på ett operativsystem som har eller kommer alt ha buggar Delta gäller bade hårdvarubaserade likväl som mjukvarubaserade

Minimera komplexiteten

- Nätverkstjänster
  - Finns kända och okända m
- Förenkla
  - Ta bort alla onödiga tjänster
  - Ta bort onödig trafik
  - Ta bort onödiga hostar
- Spärra trafik
  - Spärra hellre för mycket än för lite

Nätverkstjänster:
Alla nätverkstjänster innehåller både kända och okända säkerhetsrisker. Med varje tjänst finns del en risk att del någon gång i framtiden uppdagas ett säkerhetsproblem.
Ta bort alla onödiga tjänster. "Det spelar ingen rolf om del finns säkerhetsrisker i en tjänst så large den inte körs".

Spärra trafik:
Del är bättre all spärra för mycket trafik än för lite. Spärrar vi för mycket kommer användarna att klaga, om vi spärrar för lite får vi inga samtal.

Säkerhet introduktion

- Allmänt ADB-säkerhet:
  Skydd av kapital i gjorda investeringar
  Skydd av funktioner i system
  Informationsskydd
  Skydd av informationens kvalitet

Vi ska inte tala om:
  Stöld, brand, vatten, elektriska problem, ...

- Vi ska tala om:
  Logiska säkerhetsproblem i TCP/IP-miljö
  Kanda problem i olika system
  Kanda problem med TCP/IP-protokoll
  Applikationsbundna problem
  Åtgärder
  Organisation

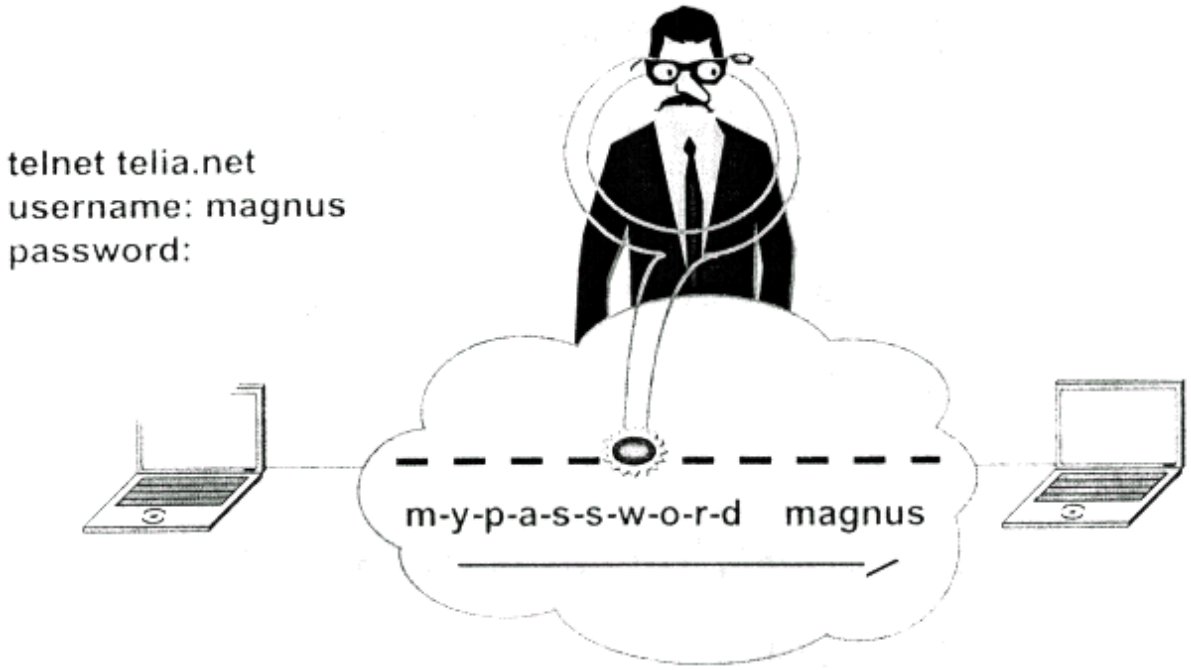
Hotbild

- Uppfångande av identitet
- Uppträdande under falsk identitet .
- Återuppspelning
- Uppfångande av data
- Manipulering
- Förnekande
- Funktionsförlust; Tillgänglighetsförlust
- Felaktigt vägval
- Trafikanalys

Hot vid överföring av information:

• Uppfångande av identitet (identity interception)
Identiteten för en användare, som deltar i kommunikation, avslöjas
• Uppträdande under falsk identitet (masquerade)
En användare utger sig for att vara en annan, i syfte att få tillgång till information eller för att få andra privilegier
• Återuppspelning (replay)
• Uppfångande av data (data interception]
Iaktta data som utväxlas
• Manipulering (manipulation)
Utbyte, borttagande eller instoppning av data
• Förnekande (repudiation)
Användare förnekar att ha mottagit eller sänt data
• Funktionsförlust; Tillgänglighetsförlust (denial of service)
Förhindra eller försämra kommunikationen for andra
• Felaktigt vägval (mis-routing)
Styr trafiken över nätet via fel vägar
•Trafikanalys (traffic analysis)
Analysers; förekomsten eller avsaknaden av trafik, trafikriktning, frekvens, typ av trafik osv.

Hot: Avlyssning



Avlyssning:
• Oönskad access av data under transport eller lagring.
• Möjlighet att avlyssna lösenord som ger åtkomst till ytterligare system.
• Allt som har ett nätverksgränssnitt kan användas för avlyssning.

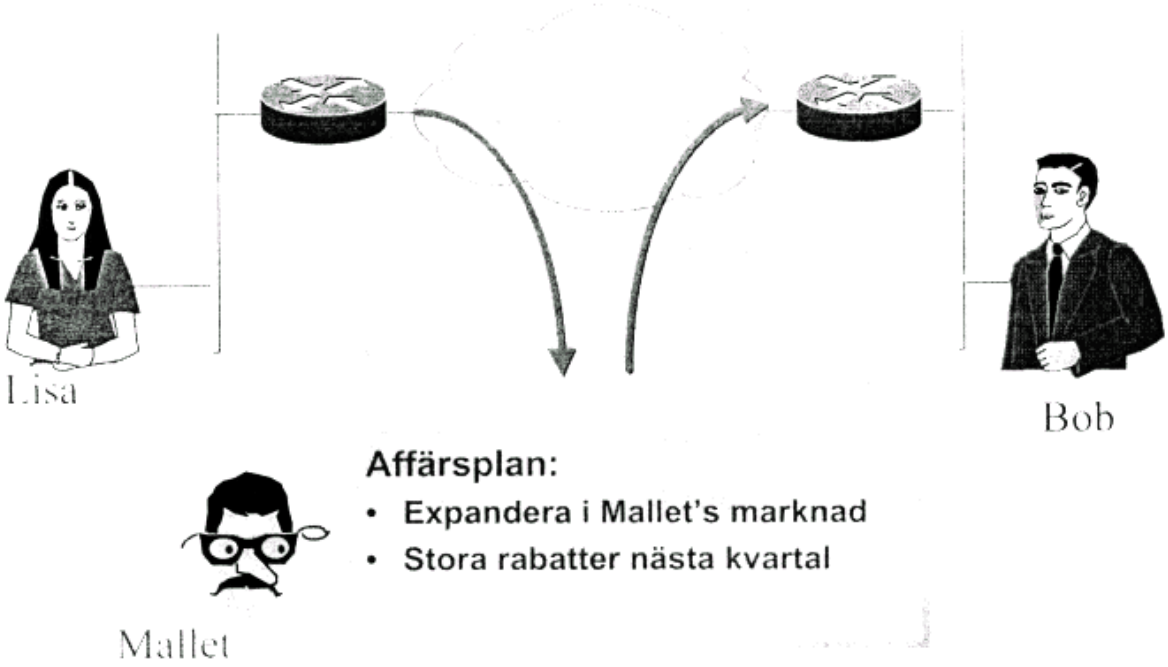
Lösenord

- Gissa lösenord
- Komma över och kracka password-fil
- Avlyssna lösenord
- Andra sätt:
  Social engineering
  Nedskrivna lösenord

Gissa lösenord:
1. Logga in med kända eller förmedlade användar-ID och gissa lösenord (använda program som inte loggar försöken: t.ex. ftp, rexec)

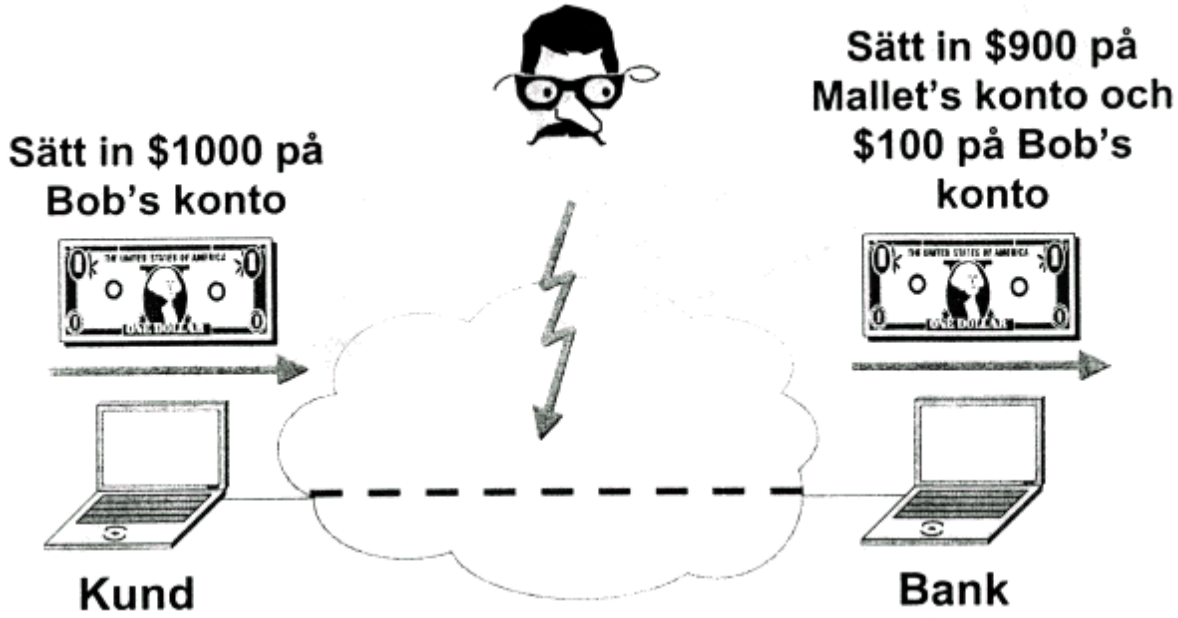
Passwordfilen:
2. Cracka stulen password-fil
(Om möjligt manipulera lösenordsfilen,
då man har legitim tillgång till systemet, för att återkomma senare)
3. Avlyssna nätet (packet sniffer) eller dator (keyboard monitor)
4. Erhålla lösenord från "hacker-kollega"
5. Social engineering
I 22% av alla incidenter till CERT/CC (1988-1995) förekom problem med lösenord.

Hot: Stöld av data



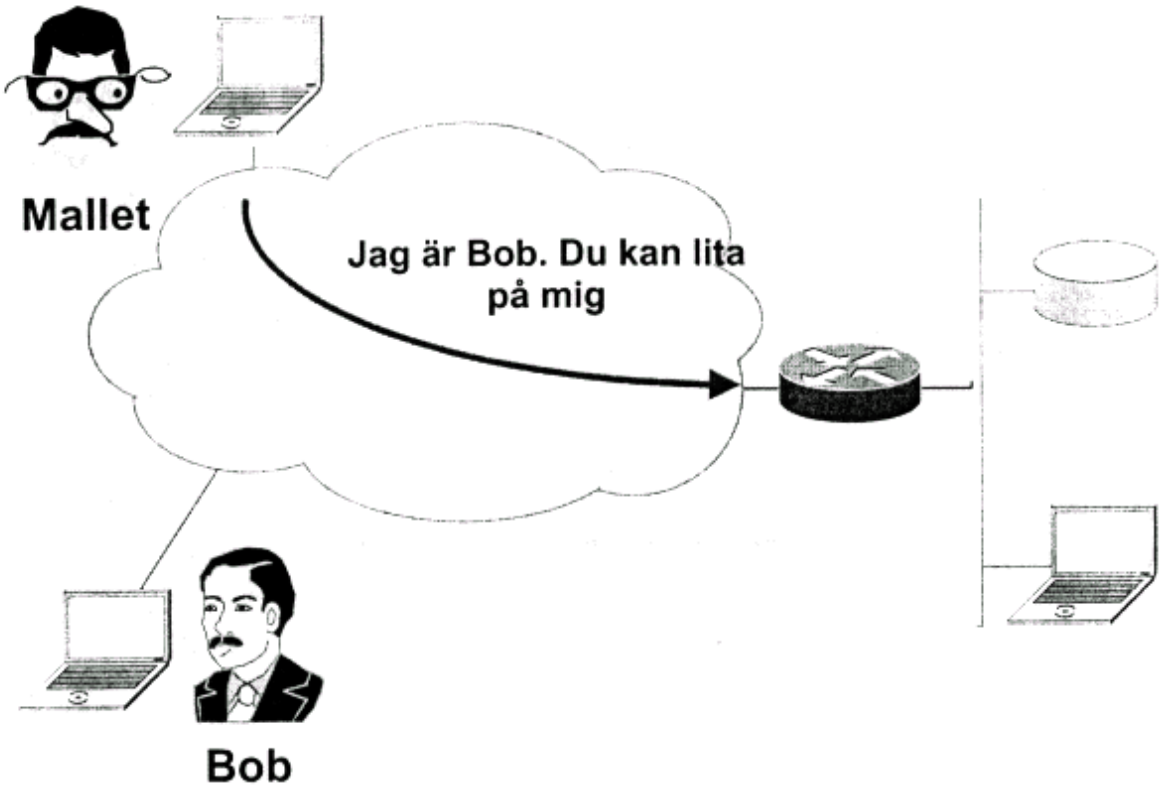
Stöld eller avlyssning av data:
Data som är under transport över ett publikt nät utsätts alltid för risken att drabbas av avlyssning. Man måste alltid värdera om del aktuella transportsättet erbjuder tillräckligt hög säkerhet for del data som skall sändas.
Det finns som regel ingen som helst möjlighet att upptäcka att avlyssning har skett,
Lösningen är oftast att använda någon form av kryptering som gör att datainnehållet blir oanvändbart for den som avlyssnar.

Hot: Förändring av data



Förändring av data:
Data som sänds över ett publikt nät utsätts också for risken att en tredje part förändrar innehållet så att effekten av meddelandet ändras. I princip kan detta drabba alla former av dataöverföringar, men ses oftast när del gäller e-post.
För att försvåra for en förövare kan man använda;
- Kryptering
- Digital signatur
- Tidsstämpling
- Tunnling, VPN-nät

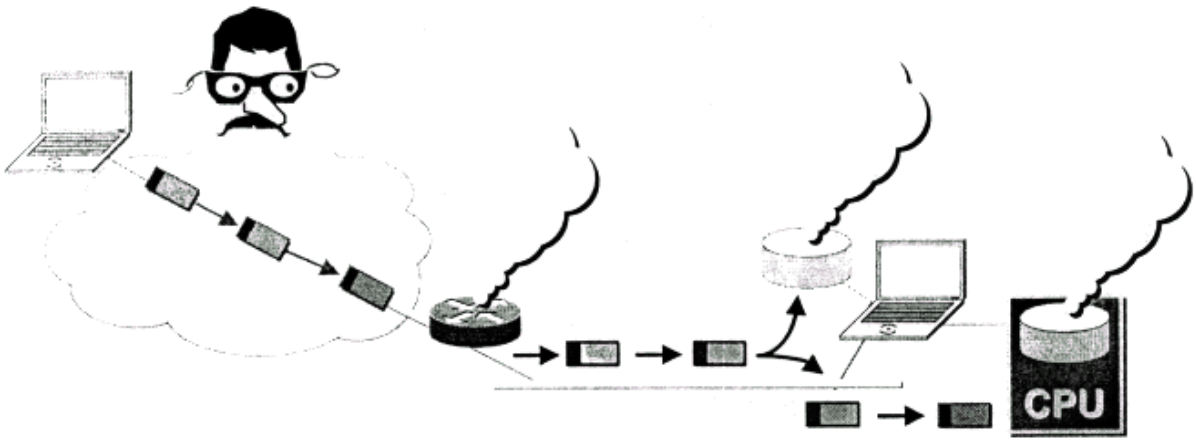
Hot: Falsk identitet



Falsk identitet:
Att sända data på ett sådant sätt att mottagaren luras att tro att avsändaren är någon annan kan ses som ett allvarligt hot. Ofta anses detta vara mest förekommande när det gäller elektronisk post, där del finns uppenbara skäl till att göra detta. Det är också inom e-post-applikationerna man ser de största bristerna.

Lösningen på problemet är att antingen nyttja någon form av digital signatur eller också ha en annan starkare autenticering före överföringen av informationen.

Hot: Tillgänglighetsförlust



Tillgänglighetsförlust:
- Överbelasta offrets processor
- Överbelasta offrets nätverk
- Fylla offrets lagringsyta
- TCP SYN-flooding
- Utnyttja Applikationsbundna brister

Tillgänglighetsförlust

- Uppnås genom att:
- Filer eller hela filsystem förstörs Filsystemet fylls, t ex genom mailbombning
- Degradering av processförmåga genom att;
  - starta många processer
  - överlasta CPU:n
  - belasta applikationer eller TCP/IP-stacken
  - Döda processer
  - Döda systemet

Exempel:
The Internet worm, sänkte ca 5% av hostarna pa Internet. Sedan dess har det inte förekommit någon slorskalig DOS-attack (i genomsnitt 3,7 siter per incident)
DOS-attacker (ökar 50% snabbare än vad Internet växer

Den enskilt vanligaste DOS-attacken var mailbombning. DDOS attacker börjar också sprida sig.

Buggar

- Alla program innehåller buggar.
- större program innehåller proportionellt fler buggar
- Utsatta datorer ska köra så få program som möjligt - de som körs ska vara så små som möjligt.
- Buggar utgör det mest spännande sättet att cracka ett system, men det är inte det vanligaste

Exempel:
November 1988 the "Internet worm Denial-of-Service attack, där över 2000 datorer drabbades (av 60.000)
Flera buggar utnyttjades (Sendmail, finger, gissa lösenordet)
Observera att vi är mer sårbara idag:
Ökad komplexitet i programvaror (t ex active code och multimedia)
Buggigare programvaror, "Time to market" allt viktigare (tiden for test av program allt kortare)

Balans mellan behov och risk: Säkerhetspolicy

Low Security
Connectivity
Performance Ease of
Use Manageability
Availability

Security balances the risks of providing access with the need to protect network resources.

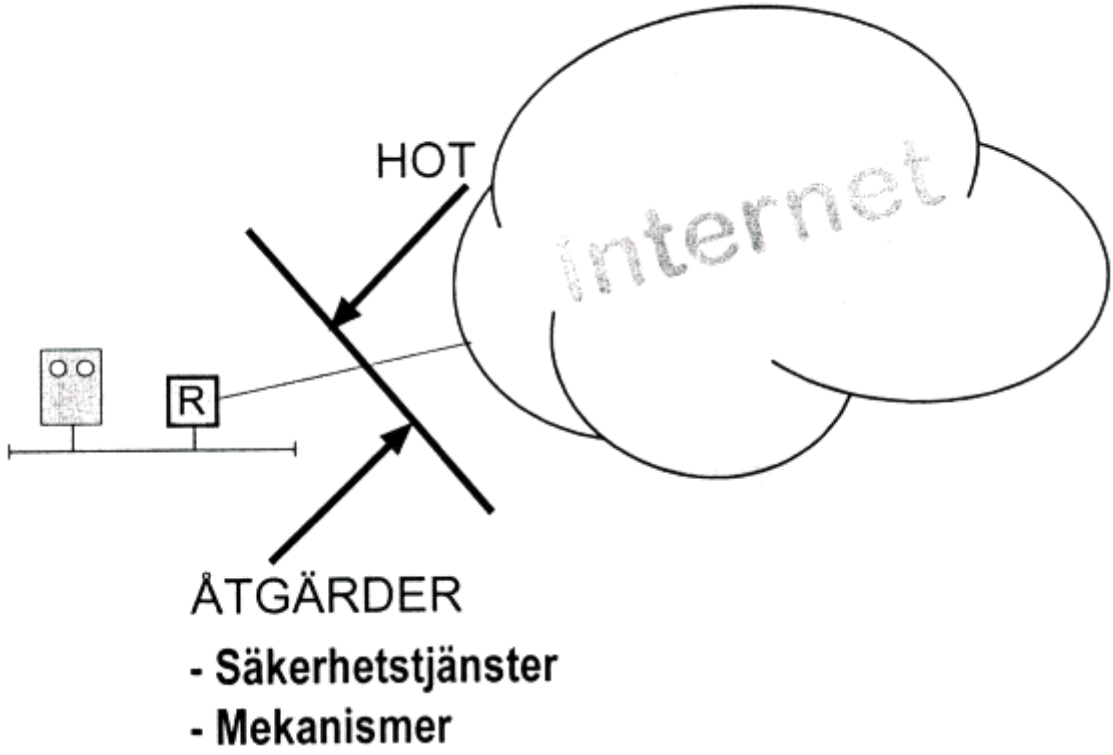
Creating a security policy involves evaluating the risks, defining what's valuable, and determining whom you can trust. The security policy plays three roles to help you specify what you must do to secure company assets.

It specifies what is being protected and why, and the responsibility for that protection.

It provides grounds for interpreting and resolving conflicts in implementation, without listing specific threats, machines or individuals. A well-designed policy does not change much over time. It addresses scalability issues Confidentiality—information is protected form unintended disclosure. Availability means that systems, data and other resources are usable when needed, despite system outages etc. Availability is enhanced through measures to prevent malicious denials of service. Trade off—employees expect access but enterprise requires **security—**Plan with scalability and deployment of layered technologies in mind.

High Security
Authentication
Authorization
Accounting Assurance
Confidentiality Data
Integrity

Åtgärder



Säkerhetstjänster
Autenticering (peer entity authentication) -identifiering av den vi talar med
Åtkomstkontroll (access control)
Sekretess (data confidentiality)
Dataintegritet (data integrity) -Data överförs oförändrat
Oavvislighet (non-repudiation) -Bevis för att data verkligen kommer från angiven källa (-alterativt mottagningsbevis)

Mekanismer
Utbyte av autenticeringsinfo. (authentication exchange)
Kryptering (encipherment)
Dataintegritet (data integrity) -checksumma bifogas med data
Digital signatur (digital signature)

TCP/IP-nät

- Typiska säkerhetsproblem med:
  - Dåliga lösenord
  - Buggar
  - Konfigurationsfel
  - Designfel
  - Osäkra applikationer
  - Avlyssning

Den nya situationen:
"Allt" sitter samman i ett sammanhängande nät. Även kopplingar mellan företag, modem, Internet, ...

Den gamla traditionella att "Säkerheten ska och kan uppratthallas på varje datorsystem, nätet ska vara öppet" är föråldrad!

Olika “brottslingar”

- Hackers
- Vandaler
- Spioner
- Terrorister
- Bedragare
- Bror duktig

Hackern:
Skryter med vad han gör
Många "wanna bees"

Vandaler:
Vill bara ställa till oreda och förstöra, kan vara före detta anställda och andra med intresse av att sätta käppar i hjulet.

Spionen:
Vill komma åt information, finns inom och utom verksamheter som skyddas

Terroristar:
Har politiska mål

Bedragaren:
Intern personal eller organisersd brottslighet, har en affarsmassig syn där dalorn är ett nytt verktyg.

Bror Duktig:
Livsfarlig typ
Inget personligt intresse
Blir allt vanligare

Hackern

- Intrång förorsakar skada, även om inga filer tas bort, konfidentiell info förändras, hemlig information läses av förövaren (hackern)
- Vad är kostnaden för att återställa tilltron till systemet?
- Även om förövaren inte har for avsikt att förstöra, så bryr han sig förmodligen inte om del, om delta sker.
- Han vet inte heller vilka konsekvenser som han kan förorsaka.

Hur arbetar hackern ?

1) Kartlägga och analysera målet, genom all inhämta tillgänglig information. Använda verktyg, få information från "kollegor" eller social ingenjörskonst.
2) Tar sig in på en dator genom att:
gissa/fånga/ett lösenord eller utnyttja konfigurationsfel eller bugg.
3) Val inne på datorn:
hämta hackerverktyg for att leta efter mer svagheter. Syftet är all bli "superuser".
Kolla vad som loggas och försöka sopa igen sina spar.
Försöka ta reda på fler användarnamn och lösenord. Installera bakdörrar, d.v.s. lägga till program eller förändra befintliga program.

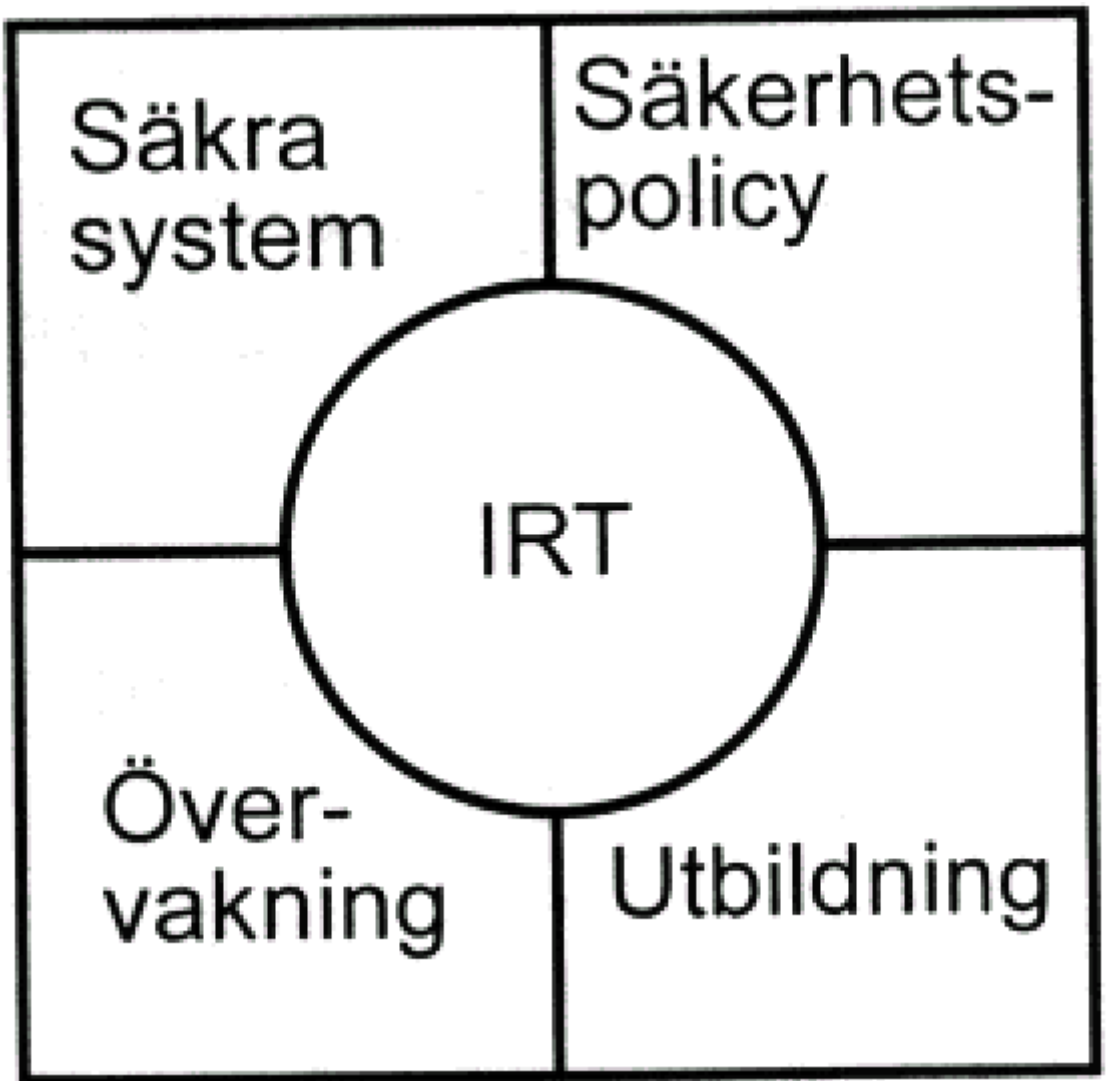
4) Ta sig vidare till andra datorer.

Sårbarhetsstudier

- DISA
- DISA (Defence Information Systems Agency) utförde 38.000 attacker mot militära siter under 1992-1995
- 35% av attackerna spärrades av skyddsanordningar
- Av de 24.700 lyckade attackerna förblev 96% oupptäckta
- Telia Tiger Team utför sårbarhetsstudier i Sverige och är kända för att kunna ta sig in överallt.
- AFIWC (Air Force Information War force Center) attackerade 1.248 hostar i januari 1995
- Pa 23% av hostarna erhölls root access
- Pa 23% erhölls åtkomst till något konto (ej superuser)
- Pa resterande 54% erhölls ingen åtkomst
- Bara 1 av 8 attacker rapporterades

Attackera dina egna system för att kolla upp dem innan någon annan gör det.

Utforma skyddet



- Bade verktyg och organisation
- Kostnadseffektivt
- Inför säkerhet stegvis

What is FIRST?
Since November of 1988 an almost continuous stream of security-related incidents has affected thousands of computer systems and networks throughout the world. To address this threat, a growing number of government and private sector organizations around the globe have established a coalition to exchange information and coordinate response activities. This coalition, the Forum of Incident Response and Security Teams (FIRST), brings together a variety of computer security incident response teams from government, commercial, and academic organizations. FIRST aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large. Currently FIRST has nearly 70 members.
Från: http://www.first.org

Säkerhet i Internet

- Bygger pa samarbete mellan operatörer, anslutna nät, användare och tillverkare.
- Frivilligt att vara med. Förutsatts följa vissa regler, annars föreligger grund för sanktioner.
- RFC 1281, Guidelines for the secure operation of the Internet

RFC1281:
1) Anv3ndare är individuellt ansvariga för att respektera de regler som gäller för de resurser som de använder
2) användare har ansvar för att skydda sin egen data
3) Nätoperatorer och de som till handhar datorresurser är ansvariga f6r att upprätthålla säkerheten pa sina system. De är även ansvariga för att informera sina användare
4) Tillverkare av programvara och system ansvarar för att implementera adekvata mekanismer för säkerhet
5) Användare, tjänsteproducenter och tillverkare är ansvariga för att samarbeta kring säkerhet
6) De som är med om att vidareutveckla protokoll och tjänster för Internet, förutsätts ta hänsyn till säkerhetsfrågor i design och utvecklingsarbete.