Inledning

- Applikationsnivåsäkerhet: att sköta säkerheten på applikationsnivå – till viss del av applikationen själv
- Kryptering: applikationsnivå eller nätnivå?
- Ökad användning av kryptering och tunnling gör det också svårare att upptäcka oönskad trafik
  - Vissa applikationer blir säkrare
  - Totala säkerheten riskerar att minska
- När vi bygger skydd på applikationsnivå måste vi förstå vad det innebär för säkerheten

Hur attackeras ett system?

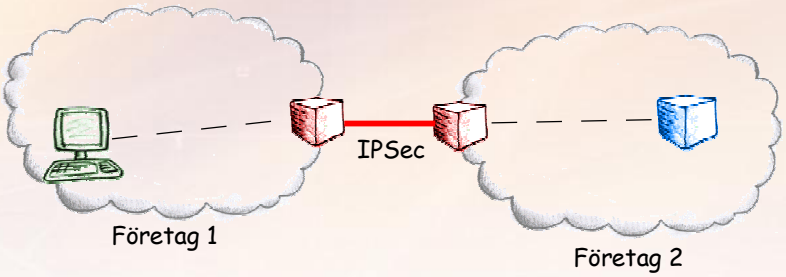
1. Nätnivå
   - Avlyssning och ”förbättring” av trafiken
   - Om krypterat på nätnivå: fortfarande möjligt från de maskiner som har kryptonyckeln
2. Operativsystemnivå
   - Attacker mot systemtjänster som DNS, fildelning, etc.
   - Applikationsservrar måste skyddas från angrepp (pers. brandvägg)
3. Applikationsnivå
   - Applikationerna angrips (mail, http, sql, legacy)
   - Typexempel på attackmetoder:
     - Buffer overflows
     - Publicerade buggar (”script kiddies”)
     - Obs: ingen hjälp av brandväggen, AV-program, operativsystem, mm.

Kryptering i applikationen eller globalt?

Finns i princip två huvudmöjligheter:

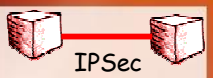
- Kryptering på nättnivå: IPSec
- Applikationsnivå: SSL/SSH

1: Kryptering på nätnivå



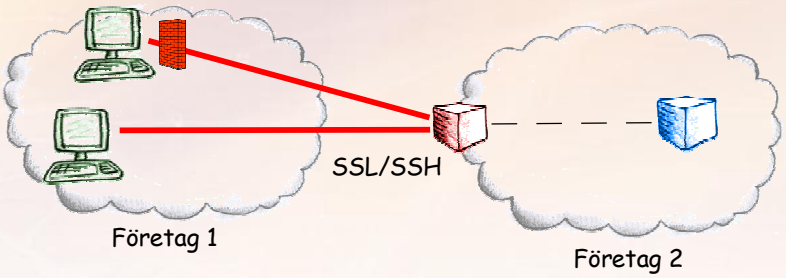
- Optimal för kryptering kontor ←→ kontor
- Applikations- och användaroberoende
- Bara kryptering del av sträckan

Kryptering på nätnivå



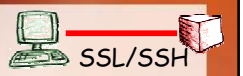
- Slipper vara beroende av programvaruleverantören
  - Passar många applikationer
  - Kan lägga på säkerhet i efterhand
  - Färre implementeringsproblem (buggar, säk-problem)
- Billigare (?)
- Hög hastighet, ev. med speciell hårdvara
- Men lösningen blir aldrig optimal
  - Inte end-to-end
  - Applikationerna får ingen hjälp med säkerheten (autentisering, accesskontroll, SSO, etc.)
- *Det kommer aldrig att bli bara en teknik som vinner!*

2: Kryptering på applikationsnivå



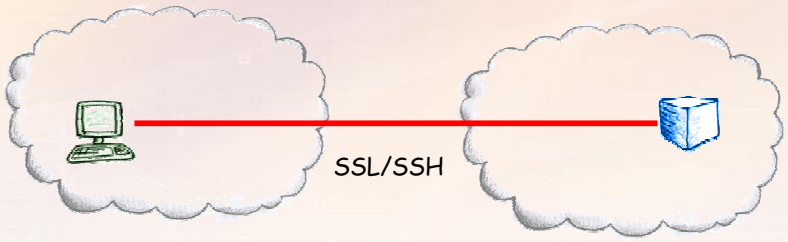
- Application-level VPNs
- Kryptering från klient till gateway
- Kan hantera tunna klienter (telefoner, applets, ...)
- Personlig brandvägg med fjärrpolicy

Application level VPNs



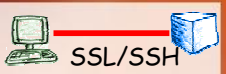
- Kan ge hög säkerhet och stor flexibilitet
- Klientprogramvaran är liten och enkel
  - Modifierar inte systemet (bra för externa användare & partners)
  - Klienter kan laddas ner från webbservrar
  - Klienter för bärbara enheter (telefoner, PDAs)
- Kan kombineras med brandväggsfunktioner
  - Klient
  - Server
- Kan erbjuda reducerat antal inloggningar (SSO)

3: Applikationskryptering



- Kan ge högsta applikationssäkerhet
- Dyrare
- Inflexibelt – varje applikation behöver säkras

Applikationskryptering



- Applikationen gör själv arbetet
  - Bäst möjlighet att få kontroll över säkerheten
  - Ger “end-to-end security”
- Kan vara optimal lösning
  - Endast här ser man alla säkerhetskraven
  - Man slipper förlita sig på externa moduler
  - Kan skräddarsy säkerheten – inget extra behövs (ekonomi)
- Kan medföra problem
  - Bygger in sig i ett hörn? Många olika lösningar att administrera, svårt att samordna (PKI, IDS, loggar, ...)
  - Flera lösningar = dyrare och mindre flexibelt
  - Mindre testade implementeringar – fler angreppspunkter, kan man lita på alla applikationer?
  - Central nätverksövervakning blir allt meningslösare

Trender

- Applikationer körs allt mer på andra sätt
  - Webbifiering av applikationer – inbyggd kryptering i webbläsaren
  - Körning via Microsoft Terminal Server eller Citrix-lösningar
- Tunnling av applikationsdata i annat etablerat protokoll
  - Främst för att kringgå nätverksbegränsningar (!)
  - T.ex. mail och filflyttning via http – är det bra?
- Säkerheten sköts av applikationen själv
  - Autentisering – t.ex. Stöd för PKI
  - Auktorisering
  - Sekretess och integritet (kryptering)
  - Tillgänglighet

För- och nackdelar

- Applikationer kan köras på godtyckliga system från centrala servrar
- Applikationer kan laddas ner och köras på klienten (aktiva script)
- Tunnling = enklare att få trafiken in/ut genom brandväggar
- Hög säkerhet om trafiken även krypteras

- Ofta skickas bara grafiska anrop till klienterna – mycket svårt att analysera
- Systemägarna får svårt att veta vad och vilka applikationer som körs
- Svårt för brandväggar och IDS-system att analysera och förstå trafiken
- Omöjligt att se vad som skickas om krypterat

Tunnling – på gott och ont

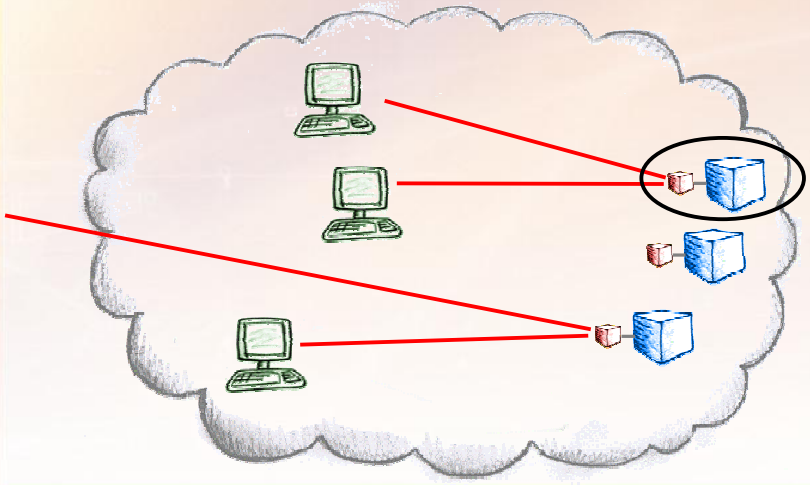
- Sätt att kringgå begränsningar i nät och brandväggar
  - Ibland bara av ”slentrian” eller okunskap
- I t.ex. webbtrafik kan mycket döljas:
  - Aktiva script (Active/X, Java, etc.)
  - Dokument som körs av lokala applikationer, t.ex. Word med makron
  - Filer kan laddas ner och skickas iväg
  - Virus och maskar kan tas emot och skickas
  - Mail kan läsas, chat, …
  - Attacker mot applikationsservrar och klienter kan göras (t.ex. mot säljsystemet eller Internet Explorer)
  - Även till synes oskyldiga dokument som t.ex. PDF-filer kan ha aktivt innehåll

Tänk extremfallet

- Alla applikationer tunnlar trafiken, t.ex. i HTTP
- Alla applikationer krypterar sin trafik (SSL/SSH)

Blir detta säkert och bra?

Kombination av ”application level VPN” och applikationskryptering



Skydd – var?

- Det är först när vi börjar analysera applikationsprotokollen vi kan se vad som pågår
  - Data skickas i klartext
  - Lösenord hanteras dåligt, dåliga administrationsverktyg, ...
  - Applikationsservrar är dåliga på att skydda sig, både mot nätverksattacker och dataattacker (som buffer overflow)
- Det är nära applikationen skydden måste finnas
  - Autentisering, kryptering av data, accesskontroll, loggning
  - Andra skydd, typ skärmlås
- Litar vi på att infrastrukturen och nätverks-utrustningen skyddar oss, är vi illa ute

Sammanfattning

- Multidimensionellt säkerhetstänkande
- Skydda arbetsstationer och servrar mot angrepp
  - Av icke-autentiserade användare
- Undvik ovanliga protokoll
  - Svårt eller omöjligt att hitta brandväggar som skyddar dom
  - Mindre sannolikhet att felaktigheter blir kända av användaren
- Begränsa applikationens möjlighet att flytta/ändra data
  - Skydda data där det lagras (kryptering, accesskontroll, auktorisering, roller,)
  - Nätverksskydd och bra loggar
- Välj applikationer som kan något om säkerhet och som begränsar användarnas möjligheter
  - Endast här kan bra och mycket detaljerade kontroller göras

Frågor?