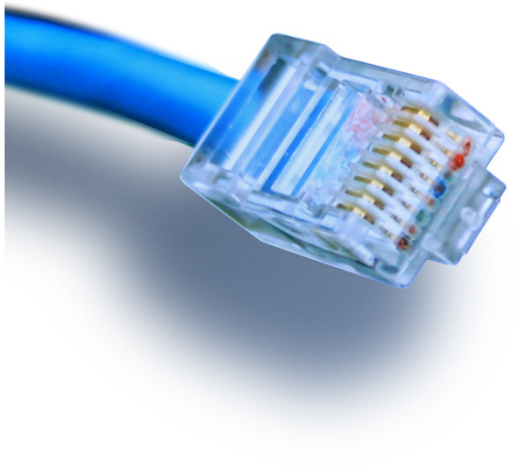
HOUSE OF TECHNOLOGY

– en del af mercantec+



Sikkerhed på net

- datasikkerhed, VPN, kryptering, vira, spyware ...

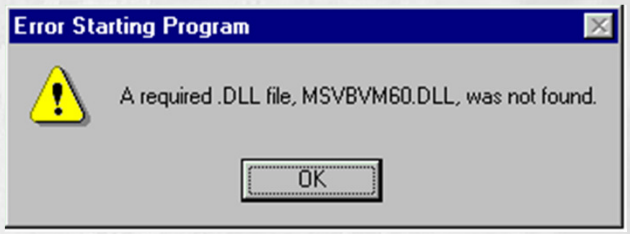
Netteknik 1

Svage punkter ved IT og net

HOUSE OF TECHNOLOGY

– en del af mercantec

- ’Altid’ fejl i helt ny hard- og software
- Den menneskelige faktor:
  - Sjusk, fejl og dovenskab



- Social hacking:
  - Medarbejdere snydes til udlevering af data
- Mangelfuld organisering af IT-området
  - Mangelfuld uddannelse af brugere og admins
  - Utilstrækkelige retningslinier for sikkerhed
  - IT Sikkerhedsmanual på 800 kedelige sider

Svage punkter ved IT og net

HOUSE OF TECHNOLOGY

– en del af mercantec

- Upålidelige softwaredesigns
  - Sikkerhed i programmel er en ny disciplin for mange programmører.
  - Manglende eller mangelfuld kryptering.

- Ubeskyttet hardware
  - Manglende UPS-anlæg (Nødstrømsanlæg)
  - Ubeskyttede tekniske installationer.
    - Fysisk adgang til udstyr giver hackere nem adgang
    - Servere, Routere og Switche i aflåste skabe/rum.

Sikkerhed på net er mange ting

HOUSE OF TECHNOLOGY

– en del af mercantec

- Datasikkerhed, VPN og kryptering
- Sikkerhedsproblemer med forskellige operativsystemer, kommunikations-protokoller og med World Wide Web
- Vira, orme og andet godt!
- SpyWare, Adware og Pop-ups
- Fysisk sikring af netværk og af maskiner

Datasikkerhed - begreber

HOUSE OF TECHNOLOGY

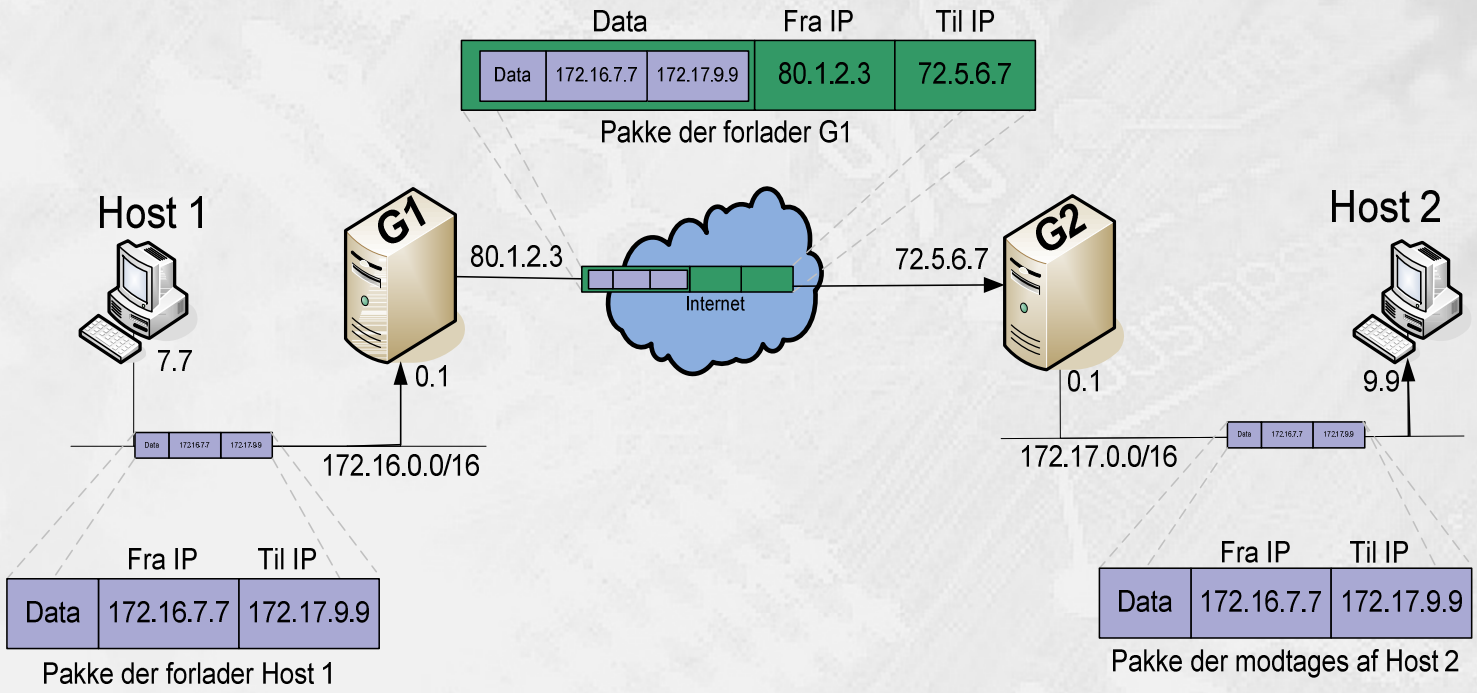
– en del af mercantec

- Confidentiality - Fortrolighed
  - Kun tiltænkte modtagere ser indhold
- Authentication – Pålidelighed
  - Sikkerhed for at afsenderen/modtageren er - og forbliver - den rigtige afsender/modtager.
- Integrity Checking – Helheds check
  - At data ikke er blevet ændret mellem afsender og modtager
- Non-Repuditation – Ikke fornægtelse
  - Afsender kan ikke senere nægte at have sendt data

VPN

HOUSE OF TECHNOLOGY

– en del af mercantec



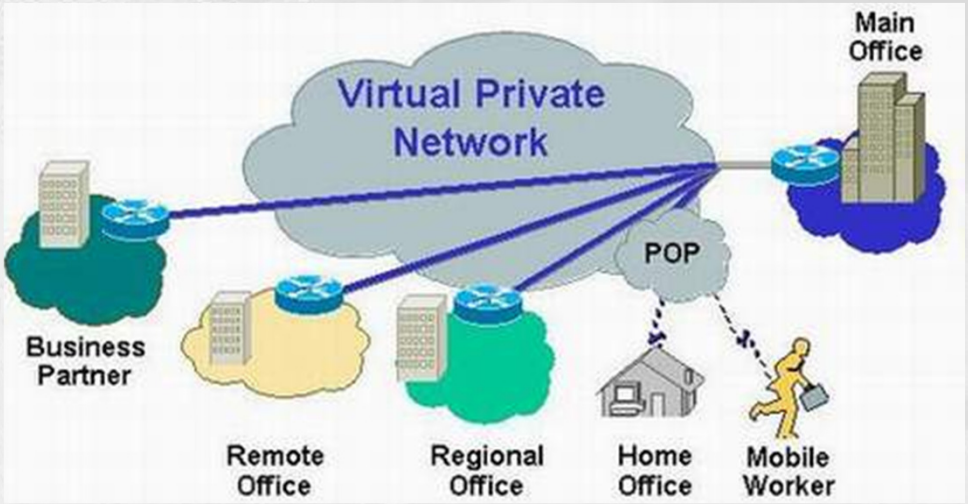
- - datasikkerhed på tværs af usikre netværk

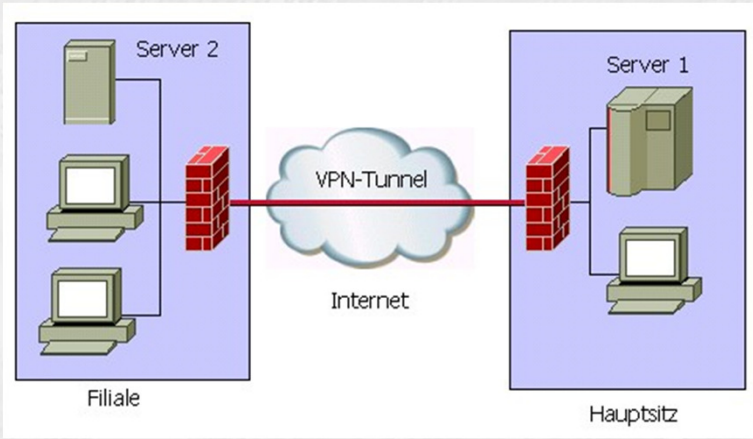
Hvad er et VPN?

HOUSE OF TECHNOLOGY

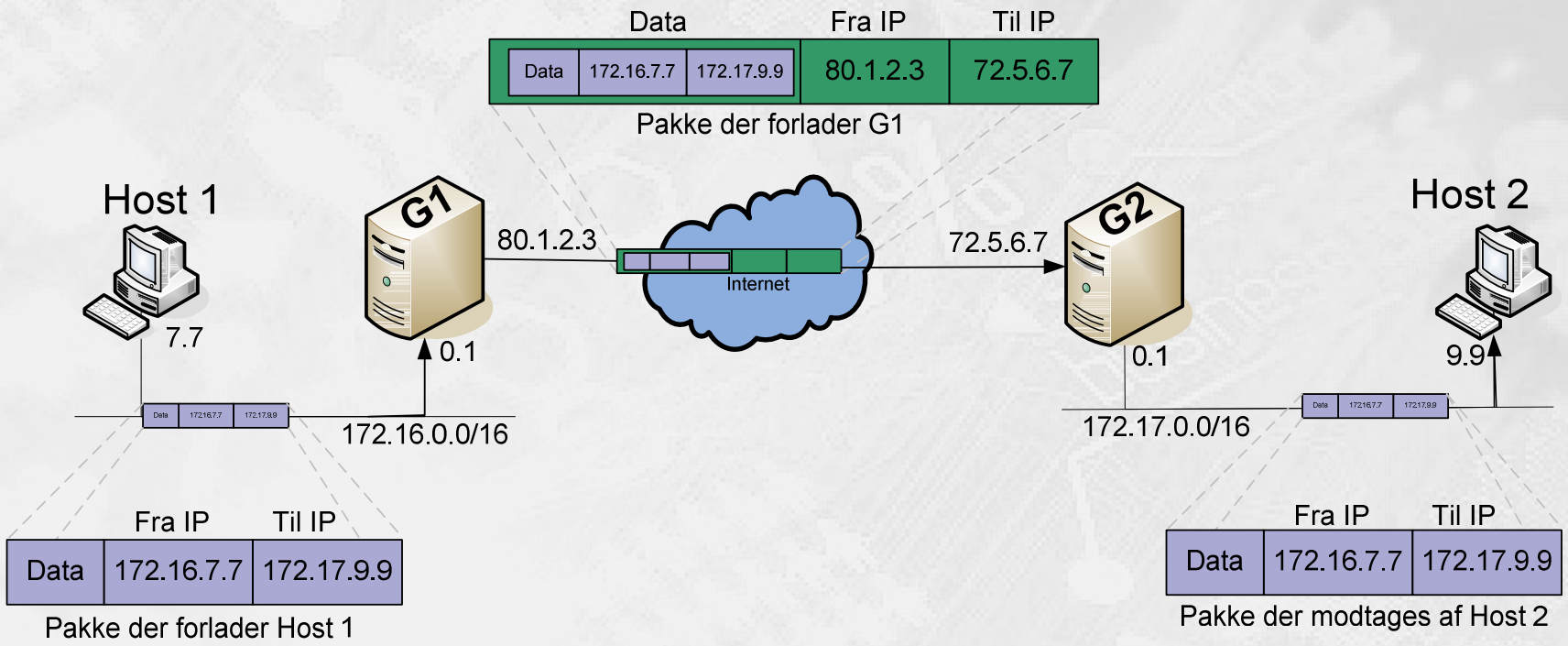
– en del af mercantec

- VPN - Virtual Private Network
- Et privat net (tunnel) gennem et offentligt net, fx Internettet
- Et VPN er et antal tilslutninger til et Backbone net som må udveksle trafik.
- Medlemmerne i et VPN må ikke udveksle trafik med andre.
- Et VPN er defineres af et sæt regler der
  - Definerer connectivitet og QoS mellem tilslutninger i VPN'et.





VPN Tunneling



- En tunnel er en vej mellem to enheder – typisk to Gateways – hvorigennem trafik kan passere uændret.

Tunneling protokoller

HOUSE OF TECHNOLOGY

– en del af mercantec

- Tunneling kræver 3 forskellige protokoller:
  - En bærer protokol (fx.IP) som anvendes til at transporterer informationen
  - Encapsulation (indpakning) protokol – Protokollen som de originale data er pakket ind i (fx GRE, IPSec, L2F, PPTP, L2TP).
  - En passager protokol – De originale data (IPX, NetBeui, IP) som overføres.

Tunnel IP-header (bærer protocol)
Encapsulation protocol (fx GRE, IPSec, L2F, PPTP, L2TP)
Indkapslet IP-datagram

Tunneling protokoller

HOUSE OF TECHNOLOGY

– en del af mercantec

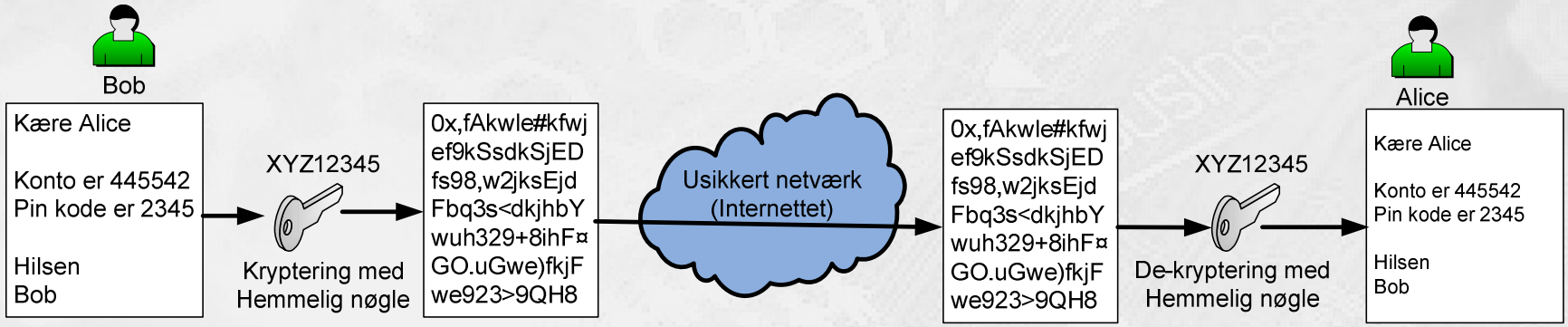
- **GRE** (generic routing encapsulation) traditionel tunneling beskrevet i RFC1701 og 1702.
- **PPTP** (point to point tunneling protocol)
  Client-Server protokol som er meget benyttet i forbindelse med Microsoft klienter. Understøttes af Windows 95, 98 og nogle versioner af NT4.0, samt Windows 2000 og Windows XP. Benytter Microsoft MPPE kryptering.
- **L2TP** (layer 2 tunneling protocol)
  Client-Server protokol som kombinerer mange faciliteter fra PPTP og L2F (layer 2 forwarding). Benyttes i Windows 2000 og XP.
- **L2F** (Layer 2 Forwarding) – Udviklet af Cisco, L2F kan bruge alle type authentication som understøttes i PPP.
- **IPSec** (IP Secure Connection)
  Benytter 3DES kryptering (168bit) og betragtes som den mest sikre protokol.

Kryptering

HOUSE OF TECHNOLOGY

– en del af mercantec

- At kryptere en besked er at *prøve* at gøre beskeden umulig at læse mellem afsender og modtager
- At de-kryptere en besked er at gøre den læselig igen.



HOUSE OF TECHNOLOGY

– en del af mercantec

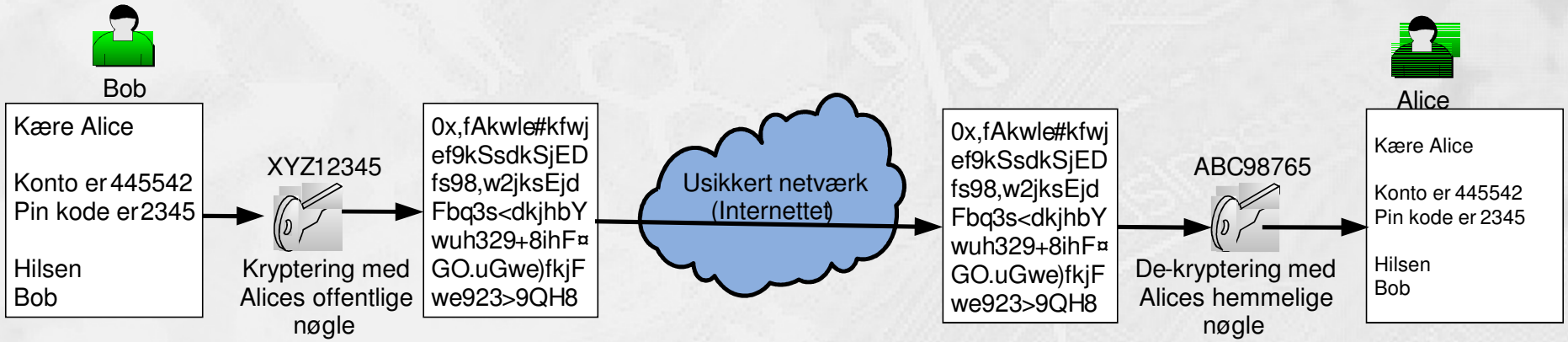
- Symmetrisk nøgle
  - Samme nøgle anvendes til kryptering og dekryptering
  - Udveksling af hemmelige nøgler en sikkerheds risiko
- Asymetriske nøgler
  - Forskellige nøgler - en privat *og* en offentlig - anvendes til kryptering og dekryptering
  - Udveksling af offentlige nøgler *ingen* sikkerheds risiko.

Asymmetriske nøgler

HOUSE OF TECHNOLOGY

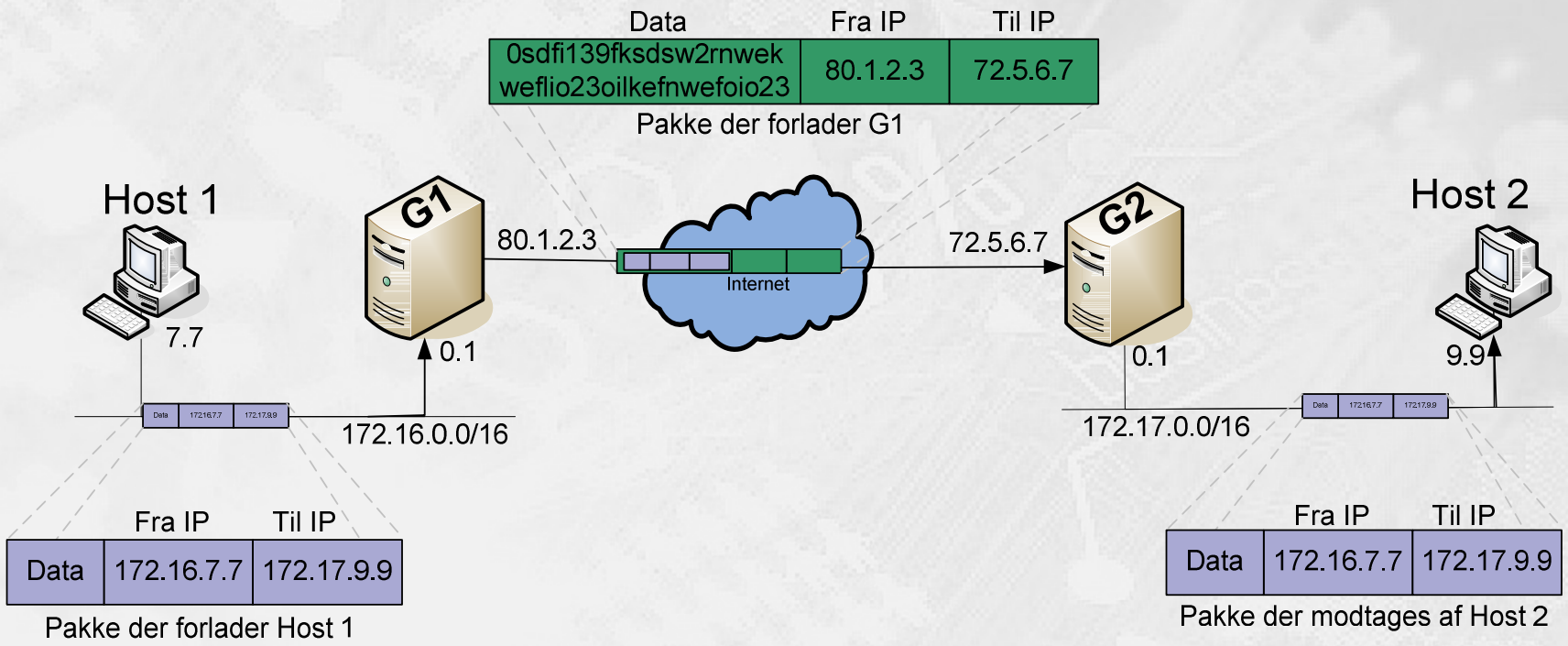
– en del af mercantec

- Alice sender Bob sin offentlige nøgle i en almindelig mail



- Nøglerne fungerer matematisk ved at anvende meget store primtal. (200 cifre eller mere)
- Alice kan sende data til Bob, ved at få hans offentlige nøgle

Kryptering og Tunneling



- Kryptering sikrer at uvedkommende ikke tyder data
- Kryptering af hele IP pakken sikrer hemmeligholdelse af identitet på afsender og modtager (Originale IP adresser)

IPsec: IP Security Architecture

HOUSE OF TECHNOLOGY

– en del af mercantec

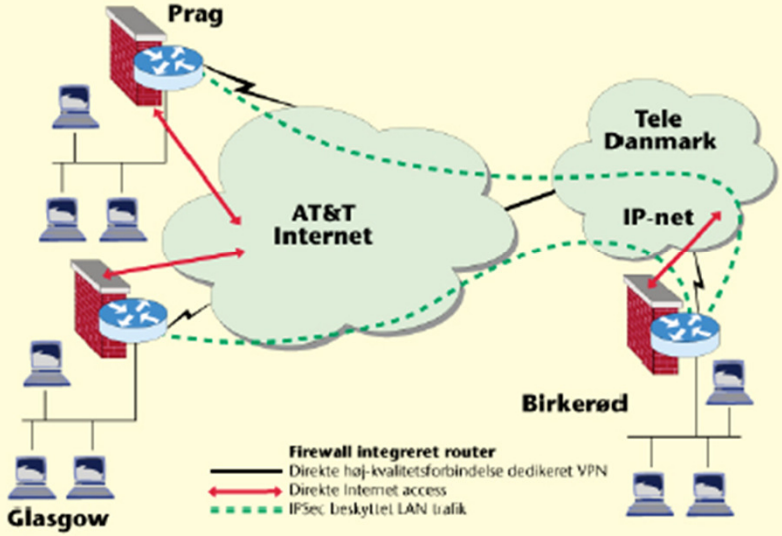
- IPsec er en tilføjelse til IPv4
- IPsec er indbygget i IPv6 som standard
- IPsec anvendes ofte i forbindelse med L2TP
  - Layer 2 Tunneling Protocol
  - PPP protokollen som er en data link protokol sendes også gennem tunnelen. (Validering PAP, CHAP)
- IPsec kan anvendes med en Preshared Key
  - Forhåndsdelt nøgle som indtastes.

Internationalt VPN

HOUSE OF TECHNOLOGY

– en del af mercantec

IVPN med internet access. Routeren er installeret og konfigureret med IP-Sec SW. samt en Cisco IOS firewall med lokal tilgang til internettet via AT&T nettet og der er opsat de ønskede tuneller.



Eksemplet viser et Internationalt VPN med tre lokationer, hvor der samtidig er etableret direkte internet-adgang. Trafikken mellem de tre lokationer er beskyttet af IPSec. mans downloading m.m. fra internettet sikres gennem firewall.

TDC VPN kunde løsninger

HOUSE OF TECHNOLOGY

– en del af mercantec

- Routerbaseret VPN
  - VPN forbindelsen etableres imellem CPE (Costumer Premises Equipment) routerne dvs. kunde routere.
  - Kan anvendes på alle tilslutninger til Internet
- Netbaseret VPN
  - Anvender MPLS VPN mellem kundens sites
  - Giver større sikkerhed

Styresystemer og sikkerheden

HOUSE OF TECHNOLOGY

– en del af mercantec

- Angreb på forskellige styresystemer til netværk kan groft opdeles i følgende typer:
  - Konto- og adgangskode-angreb
  - Netværksangreb
  - Angreb ved udnyttelse af applikationer
  - Sabotageangreb

- Af styresystemer til netværk kan nævnes
  - UNIX, Linux, Solaris, Novell NetWare, WindowsNT, Windows2000, Windows2003 ...

HOUSE OF TECHNOLOGY

– en del af mercantec

- Hackerens største gevinst:
  - En 'overtaget' maskine på et større netværk!
  - En maskine, hvor hackeren kender administrator- eller root-pasordet kan være af stor betydning - og til megen nytte - for en enkelt eller en hel gruppe af hackere.
  - Maskinen benyttes (misbruges) ofte som **server** for gruppens lyssky foretagender: Angreb på andre maskiner eller distribution af illegale data, f.eks. børneporno og hackerværktøjer

Styresystemer og sikkerheden

HOUSE OF TECHNOLOGY

– en del af mercantec

- Konto- og adgangskode-angreb
  - Formålet er helt klart at skaffe sig adgang til hele maskinen eller dele heraf
  - Metoderne varierer fra simpelt gætteri til avancerede hacker-programmer
- Netværksangreb
  - Formålet er det samme som ovenstående
  - Metoderne udnytter svaghederne i de anvendte netværksstyresystemer og -protokoller

- Angreb ved udnyttelse af de svagheder der altid er i programmerne på maskinen:
  - Formålet varierer fra sabotage over indbrud & overtagelse til lækage af følsomme data.
  - Metoderne her er knyttet til de forskellige programmer.
  - Mest kendt er nok de sikkerhedsproblemer der har været med Microsofts Messenger og lignende programmer som direkte 'annoncerer' sig selv til alle de andre på Internettet.

- Sabotageangreb
  - Også kaldet Denial of Service (DoS) Attacks
  - Formålet er at gøre modtagersystemet ustabilt - og helst at få det til at gå helt ned!
  - Metoderne varierer fra begrebers som Ping of Death, SYN Flooding, CPU-angreb og til SMB-crashes
  - Der findes en speciel variant af DoS Attacks, nemlig Distributed DoS Attacks (DDoS)
    - Mange angriber samtidigt. (Evt. via en virus)

De forskellige typer vira

HOUSE OF TECHNOLOGY

– en del af mercantec

- Boot-vira
  - angriber en computers boot-sekvens
  - resultatet er ofte en computer der nægter at starte op
- System-vira (klynge-vira)
  - angriber typisk File Allocation Table
  - resultatet er ofte en computer med rod i filsystemet
- Program-vira
  - den klassiske type, nemlig et program der skjuler sig
  - udfører skumle aktiviteter uden brugeren ved det!
- Polymorfe vira
  - almindelig virus der kan ændre 'udseende' så antivirus programmerne ikke kan finde det
  - angriber computere ganske som andre vira, men de er næsten umulige at udrydde helt

De forskellige typer vira

HOUSE OF TECHNOLOGY

– en del af mercantec

- Stealth-vira
  - almindelig virus der kan 'skjule sig' i f.eks. Boot- eller filområdet på en harddisk
  - angriber computere ganske som andre vira, men de er svære at udrydde helt
- Retro vira
  - almindelig virus der målrettet går efter at slette antivirus programmerne!
- Data-vira
  - en nyere type vira, der typisk udnytter makrokommandoer eller PostScript, begge programmeringssprog, der ofte findes på Pc'er
  - Resultaterne spænder fra uskyldig selvkopiering til sletning af systemfiler!

De forskellige typer vira

HOUSE OF TECHNOLOGY

– en del af mercantec

- Trojanske heste
  - når et angreb lykkes bliver Pc'en, som navnet antyder, angrebet indefra! Der installeres diskret et lille spion-program på maskinen.
  - resultatet kan være at der diskret indsamles kodeord og andre login informationer, som efterfølgende elegant sendes til hackeren med en e-mail!
- Worms
  - en bestemt type virus der kan 'formere' sig over datanetværk
  - er ofte i brug før et større 'angreb' af f.eks. DoS

Beskyttelse mod vira

HOUSE OF TECHNOLOGY

– en del af mercantec

- Virksomheder bør oprette en **virus-handlingsplan,** og gennem den
  - få styr på alle fjern-dataforbindelser, f.eks. Internet og Dial-Back
  - få styr på alle softwarekilder
  - få styr på gæsteindgange og samarbejdspartnere
  - installere antivirus software
  - have effektiv backup!
  - kunne fjerne vira hurtigt og effektivt (beredskab)

SpyWare is watching you!

HOUSE OF TECHNOLOGY

– en del af mercantec+

- Det er umuligt at surfe rundt på Internet med en Browser i dag uden at få installeret en masse spion-programmer (SpyWare) på sin maskine

- SpyWare'n opsamler informationer om brugerne og denne information sælges herefter til en masse forskellige firmaer verden over der handler over Internet

Adware & Malware

HOUSE OF TECHNOLOGY

– en del af mercantec

- Begrebet **adware** anvendes om programmer, som viser reklamer.

- Begrebet **malware** anvendes om programmer, som f.eks. ødelægger andre programmer på pc'en.

SpyWare is watching you!

HOUSE OF TECHNOLOGY

– en del af mercantec

- Det er heldigvis forholdsvis nemt at komme af med spionerne. Man skal downloade og installere et program der scanner, identificerer og fjerner uønsket SpyWare:
  - Ad-Aware fra LavaSoft i Sverige
    http://www.lavasoftusa.com/software/adaware/
  - SpyBot Search&Destroy fra Patrick M. Kolla
    http://beam.to/spybotsd
  - Dansk forening til bekæmpelse af ADWARE
    http://www.spywarefri.dk

Mere information

HOUSE OF TECHNOLOGY

– en del af mercantec

- Hvis du vil finde mere information om sikkerhed, vira mv. kan du prøve følgende hjemmesider:
  - http://www.icsalabs.com/ og
  - http://www.symantec.com/avcenter/

- Her kan du også følge med i den aktuelle situation omkring sikkerhedstruslerne på 'nettet'