NTNU

Kunnskap for en bedre verden

IT Grunnkurs

Nettverk

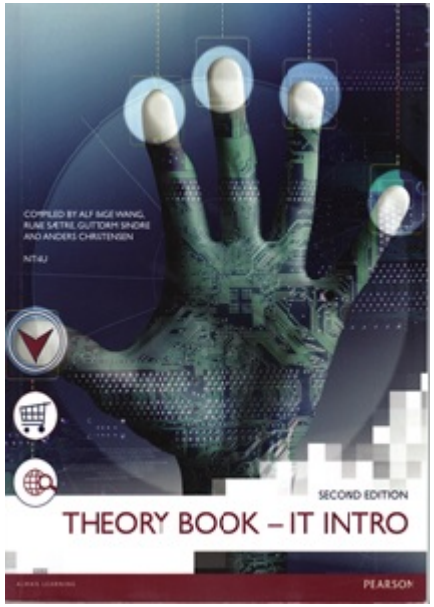
Foiler av **Bjørn J. Villa**, Førsteamanuensis II
bv@item.ntnu.no

Presentert av **Rune Sætre,** Førstelektor
satre@idi.ntnu.no

Kunnskap for en bedre verden

Innhold

- Del 1
  - Motivasjon, Analog/Digital
  - Meldingskomponenter, Feildeteksjon
  - Teknologisk utvikling
- Del 2
  - Internet historikk & arkitektur
  - Aksessteknologier
  - IP protokollen
- Del 3
  - Krav til nett
  - Sikkerhet
  - Sikker kommunikasjon



Side 177-255

Krav til nett

Avhengig av bruken

Når du skal bruke et nettverk til «et eller annet» så må du tenke gjennom følgende:

- Hvor mye informasjonstap er akseptabelt ?
- Hvor mye tidsforsinkelse er akseptabelt ?
- Er variasjon i tidsforsinkelse (jitter) problematisk ?
- Hvor mye kapasitet (bits/sek) er nødvendig ?

Dette er helt fundamentalt for at ting skal fungere….

Krav til nett

Avhenger av hver enkelt tjeneste

Krav fra telefoni

Informasjonstap	: ~1%
Tidsforsinkelse	: ~100ms (en vei)
Kapasitet	: 10-200Kbps

Krav fra VoD

Informasjonstap	: ~0%
Tidsforsinkelse	: ~2-5sek
Kapasitet	: ~100Kbps-10Mbps

Krav til nett

Avhenger av hver enkelt tjeneste

Krav fra email

Informasjonstap : 0%
Tidsforsinkelse : sekund - dager
Kapasitet : fleksibelt

Krav fra gaming

Informasjonstap : ~1%
Tidsforsinkelse : 0-10ms
Kapasitet : 0-100Kbps

Krav til nett

Avhenger av hver enkelt tjeneste

Krav fra **multimedia**

- Potensielt de strengeste kravene fra hver enkelt komponent

  Informasjonstap : 0%
  Tidsforsinkelse : 0-10ms
  Kapasitet : 10Kbps-10Mbps

- Det er «prisen» vi må betale for denne typen tjenesteintegrasjon i et felles nett, som f.eks Internet

Krav til nett

Intro

- **Skalerbarhet**
  - Evnen til å håndtere en stadig større mengde trafikk, antall kunder eller dekning – på en sømløs og kontrollert måte.
- **Tilgjengelighet**
  - Et nett sin evne til å tilby et sett av tjenester på et bestemt (eller vilkårlig) tidspunkt
- **Pålitelighet**
  - Et nett sin evne til å levere uavbrutt / kontinuerlig tjeneste
- **Ytelse**
  - Et nett sin evne til å levere de nødvendige ressurser til alle typer tjenester

Krav til nett

Intro

- **Skalerbarhet**
  - Evnen til å håndtere en stadig større mengde trafikk, antall kunder eller dekning – på en sømløs og kontrollert måte.
- **Tilgjengelighet**
  - Et nett sin evne til å tilby et sett av tjenester på et bestemt (eller vilkårlig) tidspunkt
- **Pålitelighet**
  - Et nett sin evne til å levere uavbrutt / kontinuerlig tjeneste
- **Ytelse**
  - Et nett sin evne til å levere de nødvendige ressurser til alle typer tjenester

17.06.2011:
Telenor har problemer - igjen!

Telenor mobil-kunder i store deler av landet har problemer med å ringe til hverandre.

Mellom to og tre millioner kunder ble rammet sist gang Telenor hadde problemer (en uke siden).

Hvor mange som er rammet denne gangen, er fortsatt usikkert

Krav til nett

Tilgjengelighet – forstår vi det ?

digi.no
IT-bransjens nettavis
Nyhetsbrev
Din e-postadresse
Ok!
Bedrifts-IT | Telekom | Utvikling | Karriere | Økonomi | Samfunn | Sikkerhet
Ubetjent

Det er full stans i togtrafikken over store deler av landet grunnet problemet med Jernbaneverkets GSM-baserte nødnett

Tog-nødnett klappet sammen

Førte til full stans i trafikken.

Tirsdag 10. september 2013 kl. 09:23
Av Norsk Telegrambyrå

OPPDATERT: NTB melder at problemene med nødnettet nå er rettet.

Nødnettet for tog, det såkalte GSM-R-nettet, er nede over store deler av landet. Dette rammer togtrafikken i hele landet.

– Radiosambandet mellom tog og togleder ligger nede over store deler av Sør-Norge. Nå er hele GSM-R-nettet nede for togtrafikk. Det betyr at alle tog får beskjed om å kjøre til nærmeste stasjon og stoppe der. Dette gjør vi av sikkerhetsmessige hensyn, sier pressevakt Arvid Bårdstu i Jernbaneverket til NTB.

Sentral i Trondheim
Han forteller at feilen i nødnettet skjedde i 9-tiden. Første melding gikk ut klokka 9.01.

– Det er togleder som oppdager en slik feil først. Nødnettet ledes av et operasjonssenter i Trondheim, og siden dette er kritisk for at vi skal kunne kjøre togtrafikk, har vi to systemer som kjøres parallelt. Det skal ikke gå tog hvis ikke radiosambandet fungerer. Togene skal stå hvis dette er ute av drift, sier Bårdstu.

Doble systemer
Han forteller at nødnettet har en garantert oppetid på over 99,9 prosent, og at operasjonssenteret i Trondheim nå jobber med å lete fram feilen og rette den.

– Vi har en datamaskinpark på Marienborg og en i en gammel ubåthangar på havna i Trondheim. Det er lagt ned store ressurser for at vi skal ha doble systemer. Vi vet foreløpig ikke om begge systemene er nede, sier han.

Han forteller at det er uvisst hvor lang tid det tar før man har fått nødnettet opp igjen.

Garantert oppertid på 99.9%

$$\overline{A} = 1 - \overline{U} = \frac{MUT}{MDT + MUT} = \frac{MUT}{MTBF}$$

$$A(T) = \frac{1}{T}\int_0^T A(t)dt$$

$$\overline{A} = \lim_{T \to \infty} A(T)$$

Tilgjengelighet må ses i sammenheng med observasjonsperiode...

Class	System type	Availability	Accumulated down time per year [Min.]	Comments
1	Unmanaged	$1 - 10^{-1}$	52 600	Home-computer
2	Managed	$1 - 10^{-2}$	5 260	
3	Well managed	$1 - 10^{-3}$	530	
4	Fault tolerant	$1 - 10^{-4}$	53	
5	High availability	$1 - 10^{-5}$	5	Telephone switch
6	Very high availability	$1 - 10^{-6}$	0.5	
7	Ultra high availability	$1 - 10^{-7}$	0.05	

Krav til nett

Intro

- **Skalerbarhet**
  - Evnen til å håndtere en stadig større mengde trafikk, antall kunder eller dekning – på en sømløs og kontrollert måte.
- **Tilgjengelighet**
  - Et nett sin evne til å tilby et sett av tjenester på et bestemt (eller vilkårlig) tidspunkt
- **Pålitelighet**
  - Et nett sin evne til å levere uavbrutt / kontinuerlig tjeneste
- **Ytelse**
  - Et nett sin evne til å levere de nødvendige ressurser til alle typer tjenester

NextGenTel

20.09.2011:
Nextgentel-kunder kom ikke inn på utenlandske nettsider

I tre timer i natt var ~200.000 nordmenn uten «internasjonal nettilgang».

I tillegg til at Nextgentels kunder ikke kom på internett, ble heller ikke e-poster mottatt og sendt over landegrensene.

Trolig har heller ikke tjenester som Skype eller MSN fungert.

Krav til nett

Intro

- **Skalerbarhet**
  - Evnen til å håndtere en stadig større mengde trafikk, antall kunder eller dekning – på en sømløs og kontrollert måte.
- **Tilgjengelighet**
  - Et nett sin evne til å tilby et sett av tjenester på et bestemt (eller vilkårlig) tidspunkt
- **Pålitelighet**
  - Et nett sin evne til å levere uavbrutt / kontinuerlig tjeneste
- **Ytelse**
  - Et nett sin evne til å levere de nødvendige ressurser til alle typer tjenester

ventelo

11-13.Mai 2011:
En ny forretningsmodell på nett

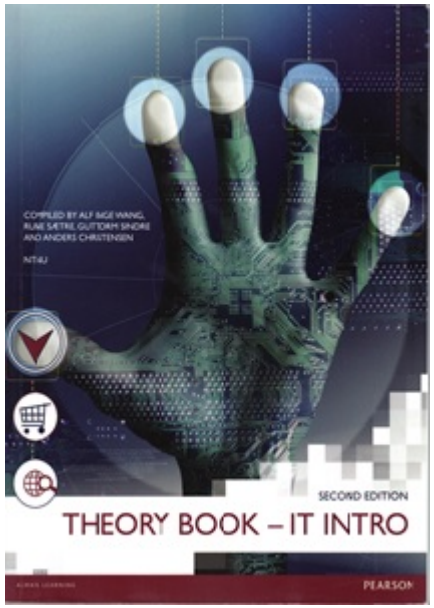
En eksplosiv vekst av levende bilder (video) på nettet oppleves. For internett- leverandørene er dette en utfordring.

Bredbåndsselskapene må hele tiden investere i ny teknologi for å øke kapasiteten i nettet.

Innholdsleverandører som vil ha tjenestekvalitet på internett må betale for det. Dagens forretningsmodell må revurderes

Innhold

- Del 1
  - Motivasjon, Analog/Digital
  - Meldingskomponenter, Feildeteksjon
  - Teknologisk utvikling
- Del 2
  - Internet historikk & arkitektur
  - Aksessteknologier
  - IP protokollen
- Del 3
  - Krav til nett
  - Sikkerhet
  - Sikker kommunikasjon



Side 177-255

Sikkerhet

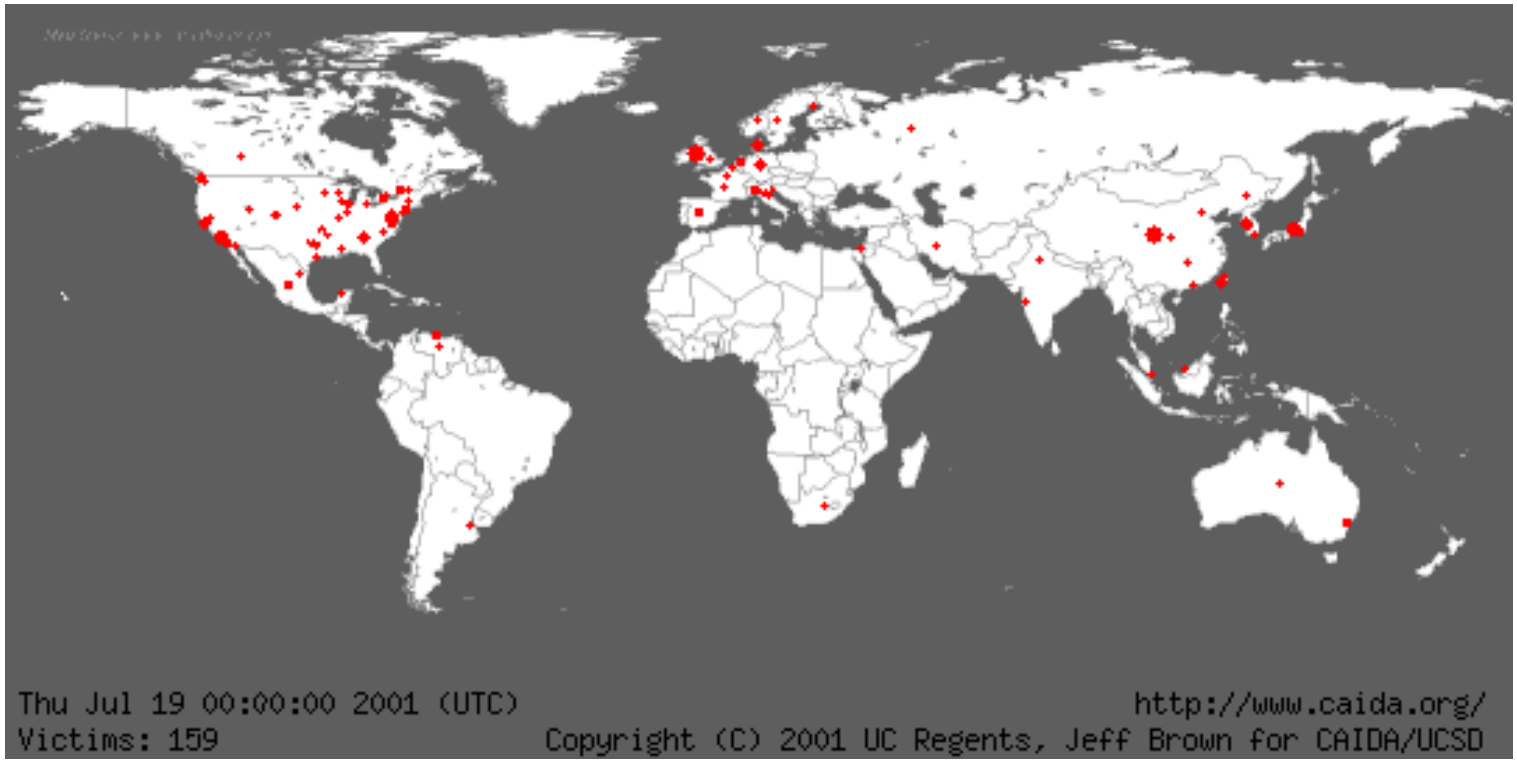
Intro

"In this world nothing can be said to be certain, except death and taxes."

Benjamin Franklin, 1789

Sikkerhet

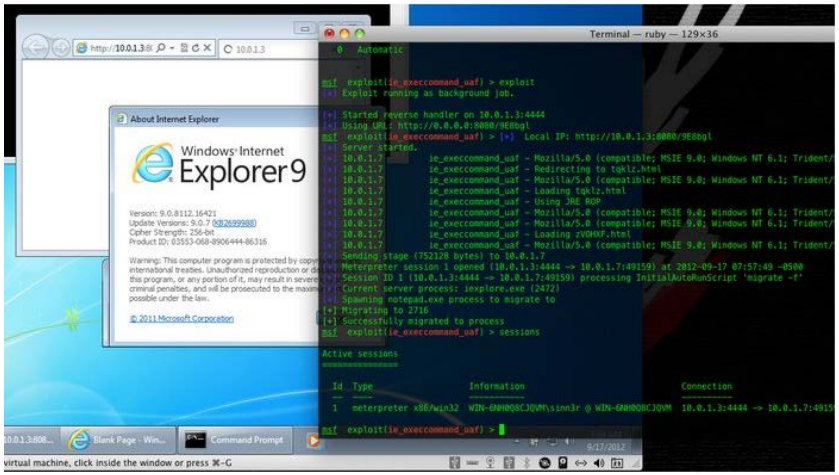
Allerede i 2001 innså vi at Internet var litt «skummelt»



En av de første (kjente) store sikkerhets-hendelsene på Internett var da **Code Red Worm** i 2001 infiserte 359.000 PC'er++ over hele verden i løpet av 15 timer

Sikkerhet

Hva er trygt ?



digi.no
IT-bransjens nettavis

18.Sept 2012

Internet Explorer angripes

Microsoft ber kundene installere eget sikkerhetsverktøy.

19.Sept 2012

- Velg en annen nettleser

Flere lands myndigheter advarer mot Internet Explorer.

digi.no
IT-bransjens nettavis

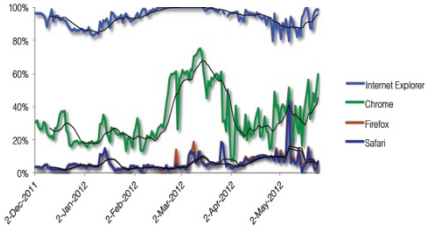
2.Okt 2012

IE suveren på sikkerhet

Mange ganger mindre risikabelt enn å surfe med Chrome, Firefox og Safari, ifølge NSS.

Torsdag publiserte NSS Labs, et kjent amerikansk testlaboratorium, de to første rapporter i en serie om sikkerhet i nettlesere.

I begge rapportene er konklusjonene entydig: Det er mange ganger større risiko å surfe med Safari, Firefox og Chrome enn med Internet Explorer (IE).



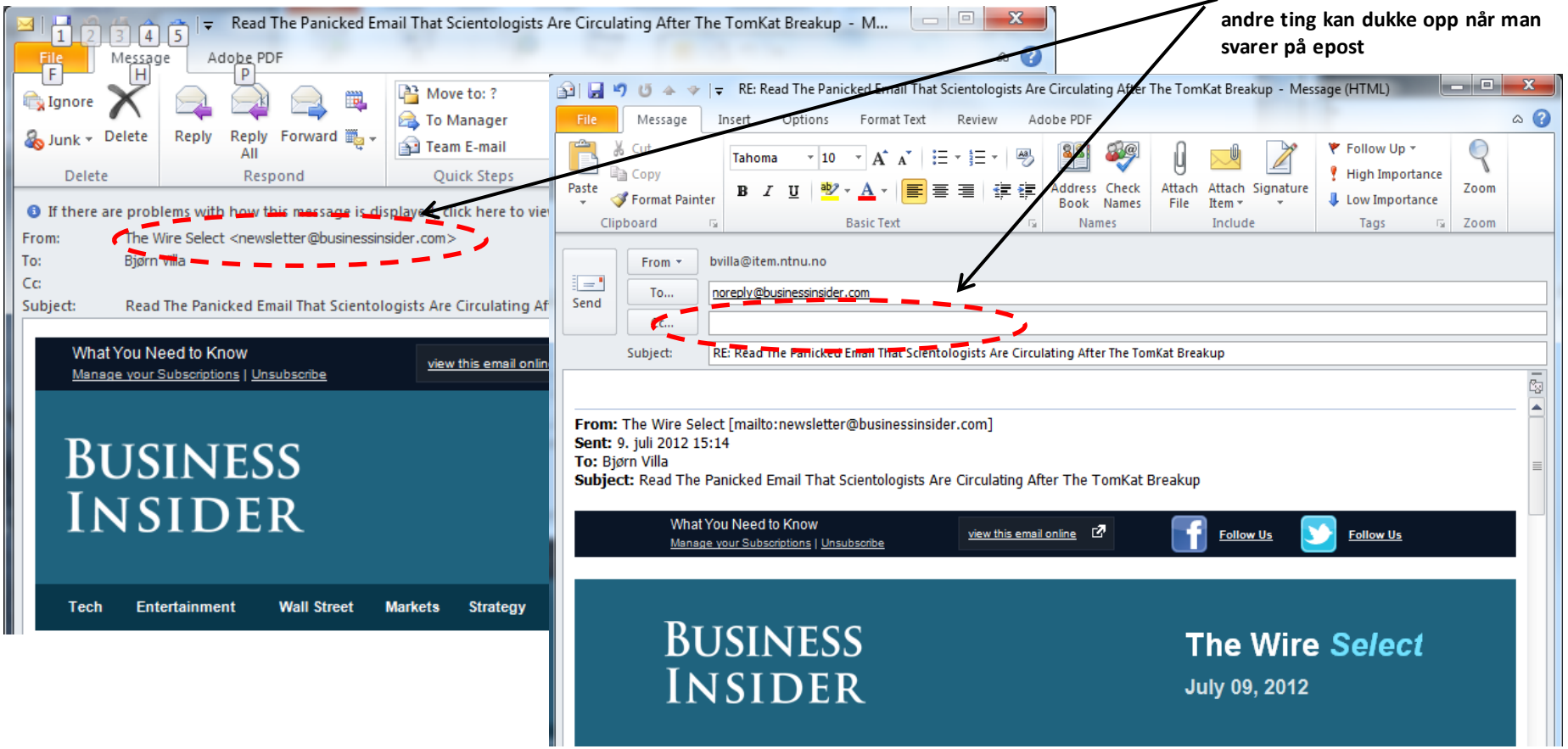
Kunnskap for en bedre verden

Sikkerhet

Spoofing

- For eksempel bruk av falske epost avsendernavn, slik at eposten ser ut til å komme fra et sted som gjør at vi stoler på innholdet

Feltet «From» address kan inneholde hva som helst. Helt andre ting kan dukke opp når man svarer på epost



Kunnskap for en bedre verden

NTNU

Sikkerhet

Phishing

- Bruk av kjente institusjonsnavn for å lokke frem konfidensiell informasjon
- Noen vanlige måter ser ut som om de kommer fra banken din eller eBay, og ber deg «oppdatere» kontoen din.

– Visste du at det finnes 512 falske sider med Alexander Rybak?

Motivene for å utgi seg for andre varierer, men er i alle tilfeller definert som identitetstyveri. Noe som er straffbart etter norsk lov

«For identitetstyveri straffes den som uberettiget bruker uriktig identitet ved elektronisk kommunikasjon. Som uriktig identitet anses identiteten til en annen fysisk eller juridisk person og identitet som ikke tilhører noen.

Straffen er bøter eller fengsel inntil 3 år. For grov overtredelse er straffen fengsel inntil 6 år. For liten overtredelse er straffen bøter eller fengsel inntil 6 måneder. »

Sikkerhet

Utfordringer

- Pharming
  - Sender deg videre til en forfalsket web-side.
  - Sender deg videre til en forfalsket web-side selv om du skriver riktig URL
  - Hvordan?
    - Ondsinnet programvare på maskinen din.
    - «Fiendtlige» DNS-servere
      - Husk, bak en URL ligger det alltid en IP-adresse. URLen oversettes dynamisk av en (DNS) server som vanligvis tildeles til din maskin i det du kobler deg til nettet. Så hvis du er i et nytt/ukjent miljø…

Sikkerhet

Pharming – et eksempel fra Oktober 2012

Hacket rutere fra Nextgentel

Kunde fikk ruteren kapret av eksterne hackere. Selskapet bekrefter sårbarhet som gjør dette mulig.

BREDBÅND

Tildeling av DNS server

En PC eller smartphone får normalt sett tildelt informasjon om hvilken DNS server som skal brukes dynamisk gjennom DHCP protkollen. Det er denne protokollen som også gir deg IP adresse, subnet informasjon og gateway IP. I et typisk hjemmenett så ligger DHCP i den ruteren som du har fått fra din bredbåndsleverandør.

Primær og sekundør DNS

Det er vanlig å ha 2 DNS servere konfigurert, hvorav den første spørres først. Dersom den første ikke svarer, vil den neste «spørres».

Line Rate - Upstream (Kbps):	1020
Line Rate - Downstream (Kbps):	16810
LAN IP Address:	10.0.0.1
Default Gateway:	84.48.58.1
Primary DNS Server:	217.13.7.140
Secondary DNS Server:	217.13.4.24
Date/Time:	Tue Oct 23 07:23:14 2012

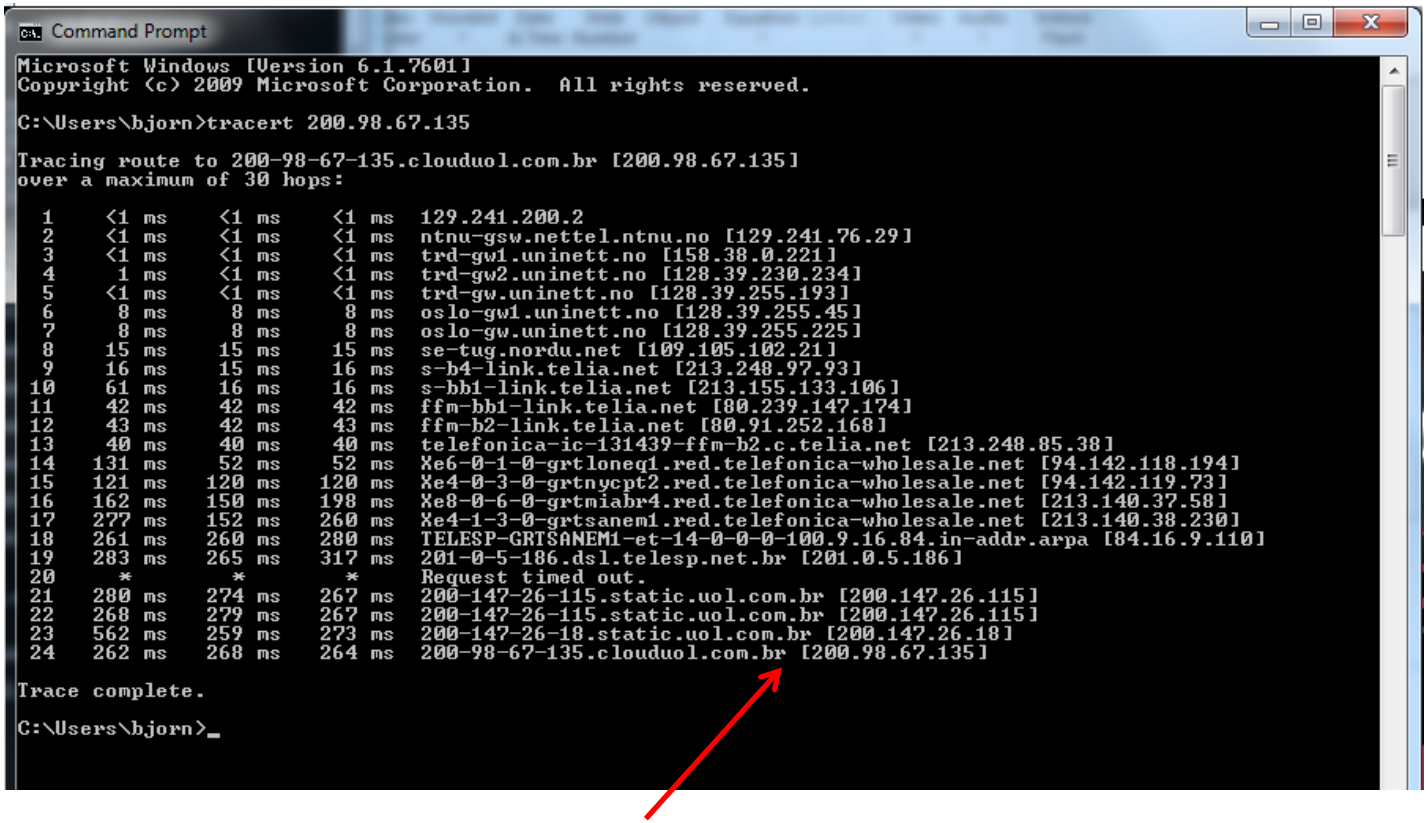
Observant kunde:

Etter å ha sjekket ruternes administrasjonsgrensesnitt fant han at primær DNS (domain name service) var endret til 200.98.67.135. Sekundær oppføring var endret til IP-adressen 8.8.8.8, som er Googles legitime DNS-tjener.

Hvor er «galt» med 200.98.67.135 ?

Sikkerhet

Pharming – et eksempel fra Oktober 2012



Den falske DNS serveren med IP 200.98.67.135 var i Brasil....

Kunnskap for en bedre verden

Sikkerhet

Utfordringer

- Cookies
  - Små tekstfiler som etterlates på harddisken av en del av de websidene du besøker
  - Kan inneholde ditt brukernavn, passord og browser-innstillinger
  - Kan være nyttig (slipper å logge inn for hver side)
  - Men kan også brukes til å samle informasjon om deg og nett-vanene dine

Velkommen tilbake til www.finn.no ☺

Sikkerhet

Utfordringer

Ny norsk lov ~~kan~~ lamme internett

En ny forskrift fra regjeringen truer livsgrunnlaget til norske nettmedier. - Hvis dette blir vedtatt, vil det sende internett tilbake til steinalderen, sier ekspert.

Opprinnelig forslag:

§ 7-3 skal lyde:
§ 7-3 *Opplysninger i brukers kommunikasjonsutstyr*
Lagring av opplysninger i brukers kommunikasjonsutstyr eller å skaffe seg adgang til slike opplysninger er ikke tillatt. Slik lagring eller adgang kan likevel skje dersom bruker har blitt informert av den behandlingsansvarlige i henhold til personopplysningsloven og har gitt sitt samtykke. Første punktum er likevel ikke til hinder for teknisk lagring eller adgang til opplysninger:

1. utelukkende for det formål å overføre eller lette overføringen av kommunikasjon i et elektronisk kommunikasjonsnett
2. som er nødvendig for å levere en informasjonssamfunnstjeneste etter brukerens uttrykkelige forespørsel

*Det er ikke alle tiltak som er like gjennomtenkte, i den forstand at det meste har både en **effekt** og en **bi-effekt**. Om dette hadde blitt iverksatt så ville Cookies vært forbudt og Internet hadde blitt vesentlig mindre brukervennlig*

Vedtatt og iverksatt per 01.07.2013:

Den nye loven er en revisjon av tidligere utgaver, og cookie-delen får følgende to hovedtrekk:

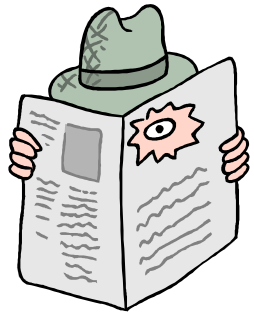
- Ansvarlige for nettsider må informere brukerne om cookie-bruk via en informasjonsside
- Brukeren gir samtykke ved å ikke skru av for cookies i nettleseren

Loven har dermed ingen egentlig praktisk innvirkning på sluttbrukeren. Hvis en bruker ikke godtar bruken av informasjonskapsler, kan han skru av funksjonen i nettleseren – noe som har vært mulig i årevis før den nye loven.

Kunnskap for en bedre verden

Sikkerhet

Utfordringer

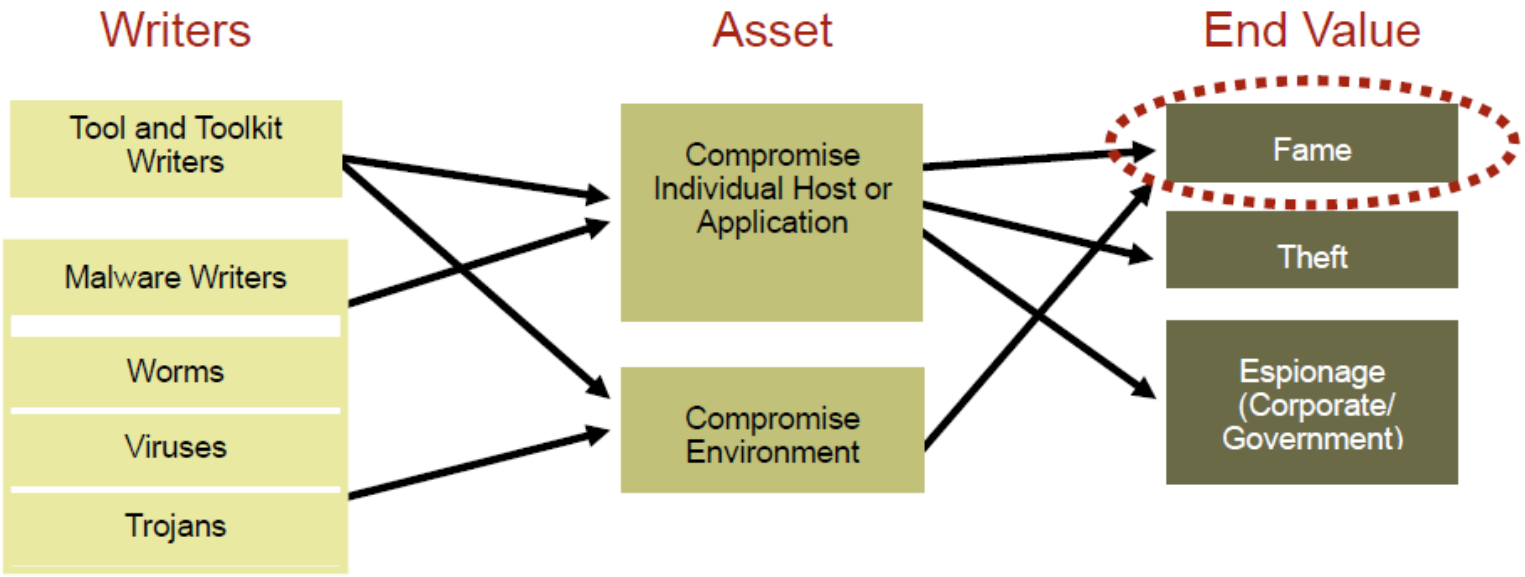


- Spyware
  - App'er som lastes ned uten at du vet om det
  - De gjemmer seg på PCen, og fanger informasjon om hva som er på PCen og hva du driver med
  - Den informasjonen sendes så til en Spyware-side på nettet
  - Informasjonen kan bli brukt mot deg, for eksempel til å stjele identiteten din, få Kredittkort med ditt navn på, eller andre forbrytelser

Installerer du ofte App'er fra nettet?
Er du sikker på at du vet om (alt) det disse gjør?

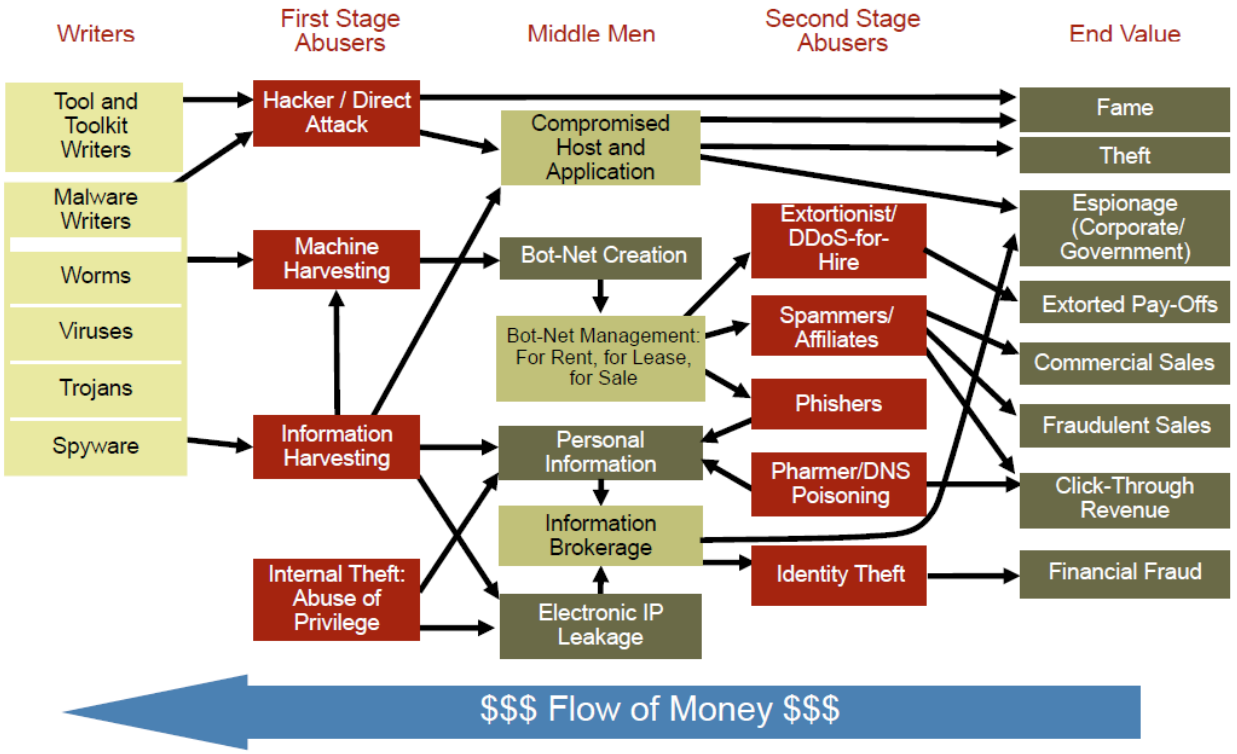
Sikkerhet

I gamle dager...



Sikkerhet

Idag...



Ser ut som organisert kriminalitet?

Kunnskap for en bedre verden

Sikkerhet

Naivitet – kanskje det største problemet ?

Kunne stoppet vanntilførselen med mobilen

**** Knusende, hemmelig rapport avslører store svakheter ** Latterlig lett passord beskyttet vann- og avløpssystemet**

RENSEANLEGG: Oset vannbehandlingsanlegg og andre bygg som er kritiske for vann- og avløpsnettet i Oslo kunne inntil i vår åpnes ved hjelp av blåtannteknologi. Foto: Heiko Junge / SCANPIX .

Sitat VG Nett 28.09.11:
"Uvedkommende har, med en mobil og ett lett passord, både kunnet overta kontrollen av vannforsyningen og fysisk komme seg inn og forgifte vannet etter at det har vært gjennom rensing"

Kunnskap for en bedre verden

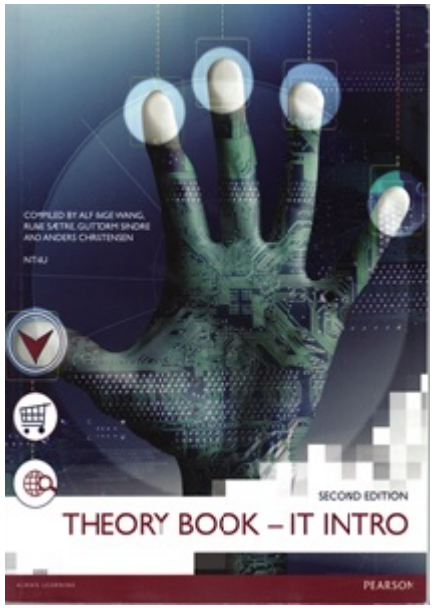
Naivitet er skummelt

Hvordan står det til med oss ?

www.vg.no

Innhold

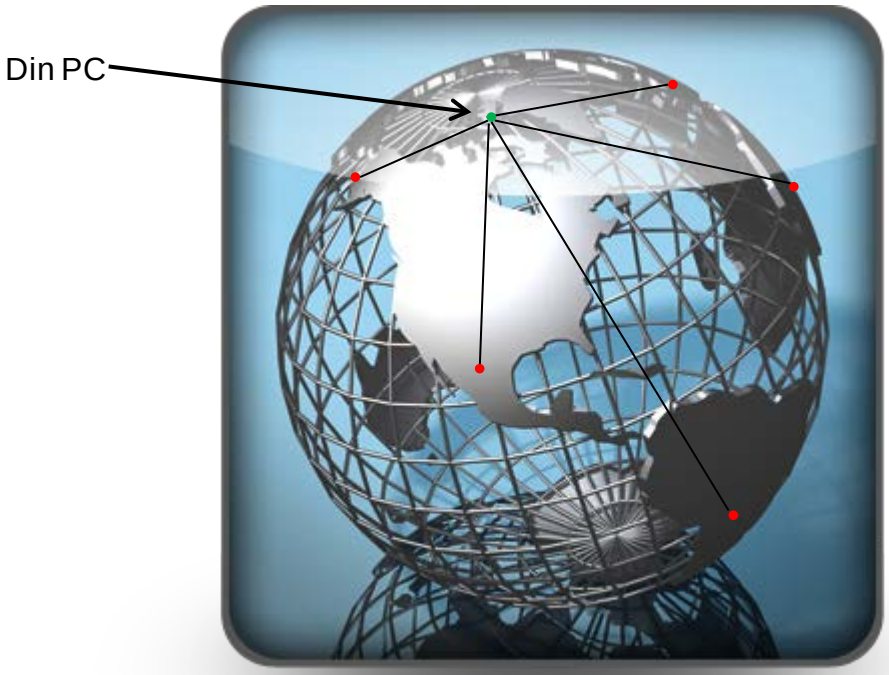
- Del 1
  - Motivasjon, Analog/Digital
  - Meldingskomponenter, Feildeteksjon
  - Teknologisk utvikling
- Del 2
  - Internet historikk & arkitektur
  - Aksessteknologier
  - IP protokollen
- Del 3
  - Krav til nett
  - Sikkerhet
  - Sikker kommunikasjon



Side 177-255

Sikker kommunikasjon

Hvorfor nødvendig ?



Sikker kommunikasjon

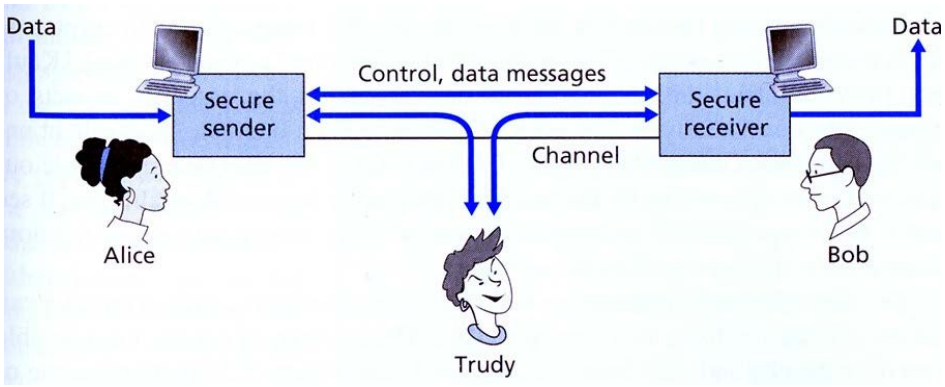
Konfidensialitet og autentisering

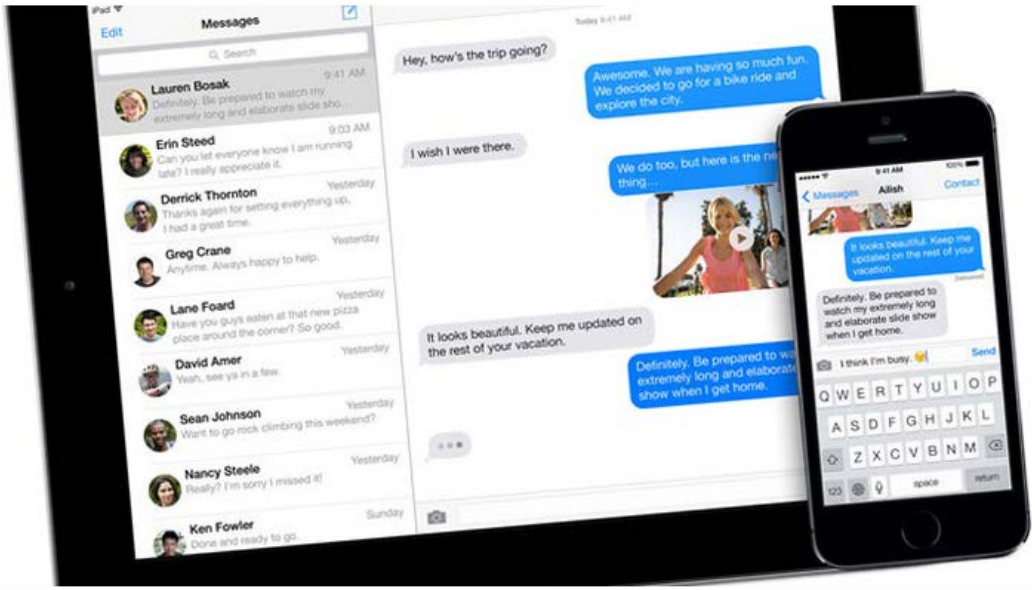
Konfidensialitet

- Et budskap er som regel kun tiltenkt avsender og mottaker
- Kryptering / dekryptering er nødvendig for å skjule innhold.

Autentisering

- Må kunne stole på den andre sin identitet
- Metoder basert på krypto er brukt også til dette





Sikkerhetsforskere hevder at Apple selv vil kunne avlytte iMessage-meldinger dersom selskapet velger eller tvinges til å gjøre dette. (Foto: Apple)

Kan iMessage avlyttes?

Stol på oss, sier Apple.

Mandag 21. oktober 2013 kl. 10:24

Av Harald Brombach

I sommer, rett etter at PRISM-programmet ble avslørt, skrev Apple at samtaler som finner sted i selskapets iMessage- og FaceTime-tjenester er beskyttet med ende-til-ende-kryptering, noe som skal kunne sikre at ingen andre enn sendere og mottakeren skal kunne lese meldingene, heller ikke selskapet selv.

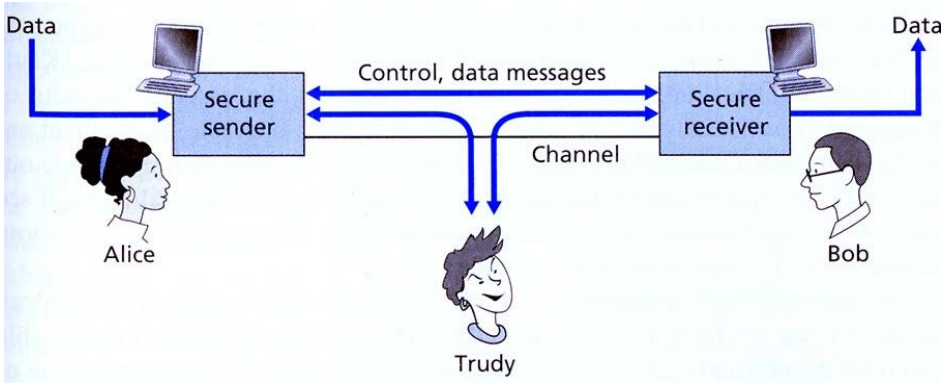
Men under Hack in the Box-konferansen i forrige uke la to sikkerhetsspesialister ved Quarkslab fram bevis på at slik avlytting vil være mulig, i alle fall for Apple. Presentasjon og flere detaljer er tilgjengelige her.

– Som Apple hevder, er det ende-til-ende-kryptering. Svakheten er i nøkkelinfrastrukturen som er kontrollert av Apple. De kan bytte en nøkkel når de måtte ønske, og derfor lese innholdet i våre iMessage-meldinger, skriver Quarkslab-ekspertene.

Sikker kommunikasjon

Meldingsintegritet, aksesskontroll

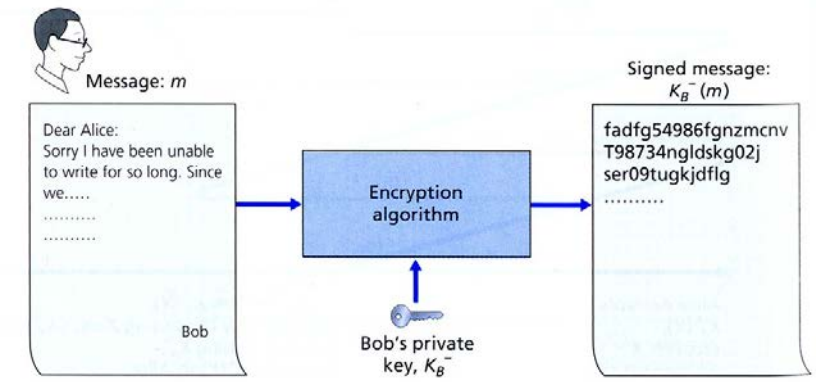
- Meldingsintegritet og ikke-fornekting
  - Må kunne stole på at en melding ikke er endret
  - En mottaker må kunne påvise at en melding faktisk er sendt fra avsender
  - Kryptering/nøkler kan brukes
- Tilgjengelighet og aksesskontroll
  - Denial of Service – angrep (f.eks. på webserver eller mailserver) som hindrer kommunikasjon for mange
  - Mål: Tillate adgang kun til de som har rett til det, stenge andre ute
  - Adgangskontroll nødvendig



Sikker kommunikasjon

Digital signatur

- Vi trenger å bekrefte at en melding er fra den påståtte avsender
- Digital signatur må være
  - Mulig å verifisere
  - Umulig å forfalske
  - Umulig å fornekte



- Kun Bob har K_B^-, og kan kryptere meldinga m med denne nøkkelen
- Bob sender kryptert melding $K_B^-(m)$
- K_B^+ Offentlig nøkkel, alle har denne og kan dekryptere på denne måten: $m = K_B^+(K_B^-(m))$
- Dvs. kun Bob kan ha sendt denne!
- **Krypteringen i seg selv kan altså også betraktes/fungere som en signatur**

- **Ulempe ?**
  - **Krevende å kryptere hele melding for å oppnå signatur**

Sikker kommunikasjon

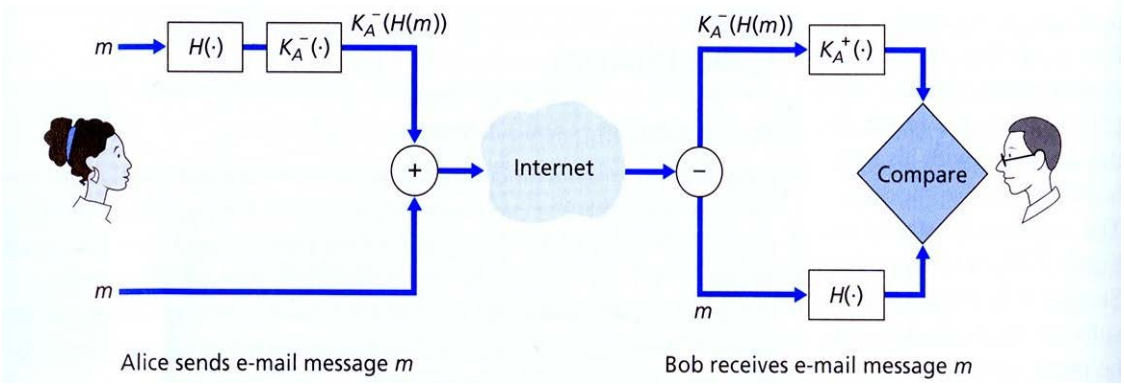
Digital signatur

Autentisering og meldingsintegritet

- Alice bruker en hash-funksjon H(.) på meldinga m, og krypterer denne vha sin **private** nøkkel
- Resultatet sendes sammen med meldingen
- Bob kjenner H(.), og har Alice sin **offentlige** nøkkel

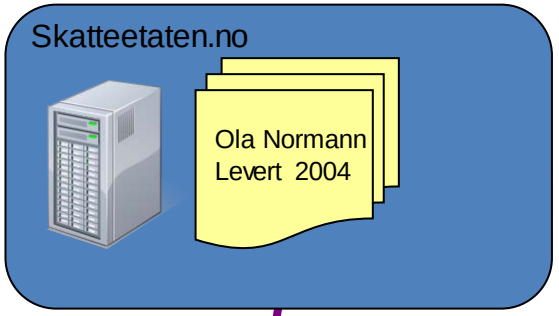
- Dette er grunnlaget for **Pretty Good Privacy (PGP)**, som er en *de facto* standard for sikker e-post

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Bob:

Can I see you tonight?

Passionately yours, Alice

-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJhFEvZP9t6n7G6m5Gw2
-----END PGP SIGNATURE-----
```



Sikker kommunikasjon

Web

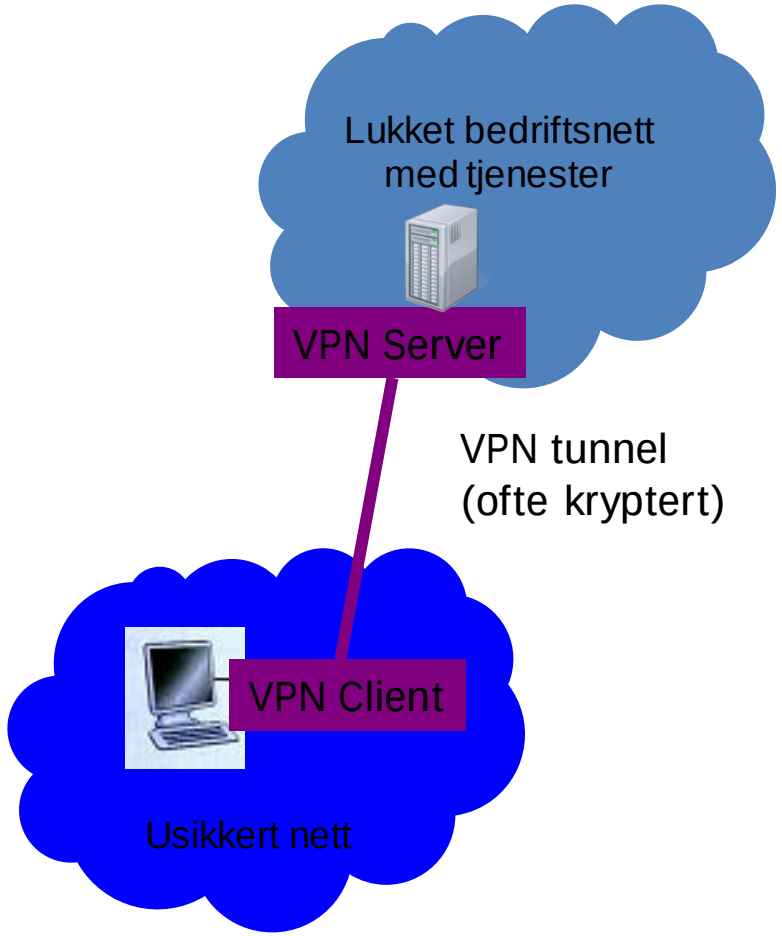


Kryptert og autentisert samband over SSL/TLS

- **SSL** (Secure Sockets Layer) ble utviklet for sikker kommunikasjon mellom web-server og web-klient. For kryptering av data og autentisering
- Siste generasjon av SSL er **TLS** (Transport Layer Security)
- **HTTP + SSL/TLS = HTTPS**
- Bruker både symmetriske nøkler og public key

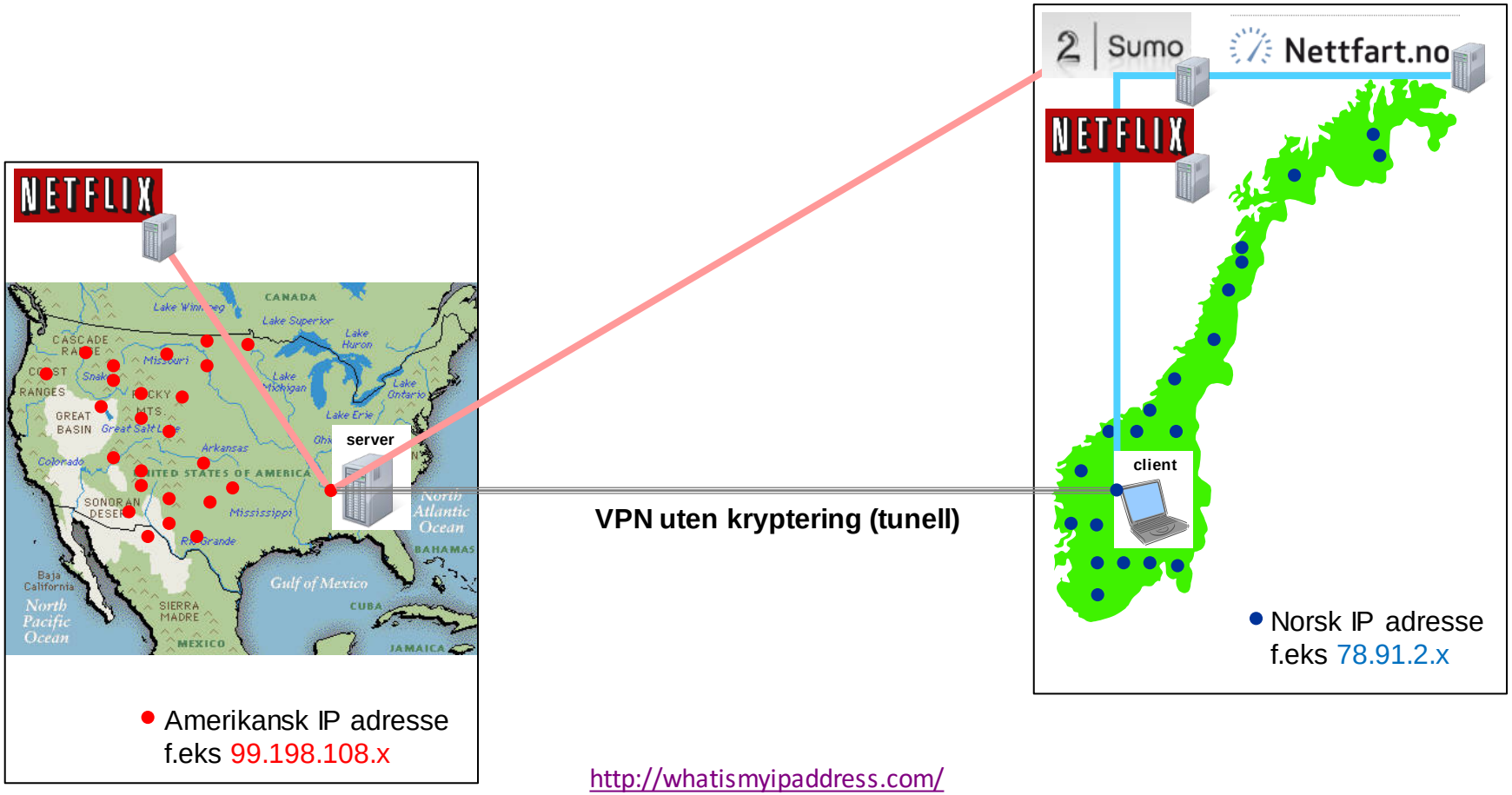
Virtual Private Network - VPN

- Ofte har vi behov for å ”utvide” et bedriftsinternt nett
  - Inkluderer personer som ikke har direkte fysisk tilgang til bedriftsnettet
  - Gir tilgang til tjenester i bedriftsnettet (kataloger, programvare, e-post, …) fra andre usikre lokasjoner
- For disse formål kan permanente eller dynamiske forbindelser (tunneler) opprettes
- VPN ved NTNU
  - Studenter og ansatt kan koble seg opp vha en SW-basert VPN klient
  - Din PC får da tildelt IP-adresse fra NTNU og du er dermed «inne i varmen»



IP adresse som aksesskontroll

VPN som «triks» for å få USA versjon av Netflix



http://whatismyipaddress.com/
http://nettfart.no

Innhold

- Del 1
  - Motivasjon, Analog/Digital
  - Meldingskomponenter, Feildeteksjon
  - Teknologisk utvikling
- Del 2
  - Internet historikk & arkitektur
  - Aksessteknologier
  - IP protokollen
- Del 3
  - Krav til nett
  - Sikkerhet
  - Sikker kommunikasjon