NTNU

Kunnskap for en bedre verden

IT Grunnkurs
Nettverk 4 av 4

Foiler av Yngve Dahl og Rune Sætre
Del 1 og 3 presenteres av Rune, satre@ntnu.no
Del 2 og 4 presenteres av Yngve, yngveda@ntnu.no

Kunnskap for en bedre verden

Nettverk Oversikt

- Del 1
  - 1. Introduksjon og oversikt
  - (2. Internett-trender)
  - 8. Pålitelighet og kanalkoding
- Del 2
  - 13. LANs, pakker, rammer og topologier
  - 20. Nettverk: Konsepter, arkitektur og protokoller
  - 21. IP: Adressering på Internett
- Del 3
  - 25. TCP: Reliable Transport Service
  - 27. Nettverksytelse. QoS og DiffServ
- Del 4
  - 29. Nettverkssikkerhet
  - 32. Internet of Things

Kunnskap for en bedre verden

Nettverk

29. Nettverkssikkerhet

Læringspunkter

Få en grunnleggende forståelse av:

- Sikkerhetsutfordringer i datanettverk.
- Ulike former for sikkerhetsangrep.
- Hva en sikkerhets-policy er.
- Ulike teknologier benyttet for å håndheve en sikkerhets-policy.

Sikkerhetstrusler

- Med økt digitalisering og tilgjengelighet av informasjon og tjenester på nett endres også trusselbildet.

- For mange organisasjoner og bedrifter er nettverkssikkerhet viktig mht. å unngå:
  - Omdømmetap
  - Tap av tillit blant f.eks. brukere eller kunder
  - Tap av åndsverk (*intellectual property*)

Sikkerhetsutfordringer

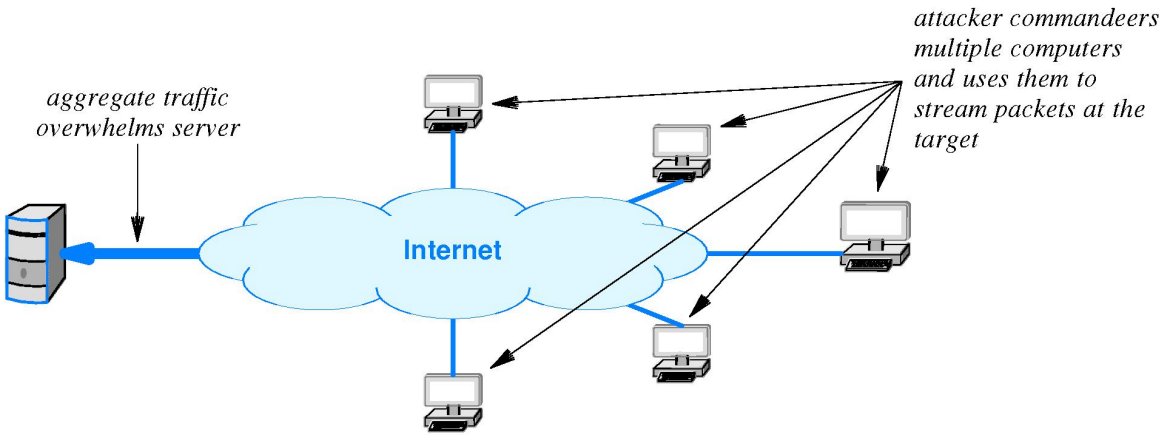
- **Phishing**: Opptre som en kjent nettside (f.eks. nettbank) for å få tak i personlig informasjon som f.eks. aksesskoder, kontonummer, etc.
- **Misrepresentation**: Oppgi feilaktige opplysninger om et produkt eller tjeneste eller levere produkter tjenester som er falsk eller av dårlig kvalitet.
- **Scams**: Lure brukere til å investere penger eller gjøre noe ulovlig.
- **Denial of service**: Bevist blokkere av tilgang til en nettside eller nettjeneste.
- **Loss of control**: Uvedkommende tar kontroll over en brukers datamaskin.
- **Loss of data**: Tap av åndsverk eller annen verdifull informasjon.

Sikkerhetsangrep

- **Wiretapping (avlytting)**: Kopiere datapakker som traverserer nettet for å få tak i informasjon.
- **Replay**: Sende pakker fanget opp fra tidligere sesjoner (f.eks. passord-pakker fra tidligere påloggінger).
- **Buffer overflow**: Oversende mer data enn hva mottaker forventer. Overskrider et databuffers grenser og skriver til nabolokasjoner i minnet.
- **Spoofing**: Bruke falsk IP-kildeadresse for å lure mottaker til å prosessere pakken. Bruke falske e-postavsendere, misbruke domenenavn. Avlede datatrafikk retter mot en server.

Sikkerhetsangrep (forts.)

- **Denial of Service (DoS/DDoS)**: Overøse en vert med datapakker (fra én eller flere kilder) for å ta bruke opp alle ressurser. Skaper lange forsinkelser.



- **SYN flood**: Form for DoS-angrep. Angriperen sender en serie med SYN-forespørsler (synkroniseringsforespørel om å opprette forbindelse) mot et datasystem for å forhindre annen trafikk.

Sikkerhetsangrep (forts.)

- **Password breaking**: Automatiserte systemer laget for å ”knekke” passord eller dekrypteringsnøkler for å få uautorisert aksess til en nettressurs.
- **Port Scanning**: Forsøk på å kople til åpne protokollporter på en vert for å finne en svakhet.
- **Packet interception**: Modifisering av pakker på vei fra avsender til mottaker.

Sikkerhetsrettningslinjer (policy)

- Det finnes ingen absolutt definisjon på et sikkert nettverk.
- I praksis må man balansere sikkerhet og enkelhet i bruk.
- En organisasjons nettverkssikkerhets-policy beskriver *hva* som bør beskyttes (ikke hvordan).
  - Komplekst. Involverer en kombinasjon av mennesker, datamaskiner og nettverk.
- Typiske sikkerhetsaspekter en organisasjon må vurdere?
  - Dataintegritet: Er dataene som sendes identiske med de som mottas?
  - Datatilgjengelighet: Er dataene tilgjengelige for personer som skal ha tilgang?
  - Datakonfidensialitet: Er dataene beskyttet mot uautorisert tilgang?
  - Personvern: Blir senderens identitet avslørt?

Ansvar og kontroll

- En organisasjon må også spesifisere hvordan ansvar for informasjon tildeles og kontrolleres:
  - Ansvar: Hvilken gruppe er ansvarlig for hvilke data? Hvordan loggføre av gruppen aksess og endringer?
  - Autorisasjon: Hvem har ansvar for hvor informasjon ligger? Hvordan tillater ansvarlig person aksess og endringer.

- Kontroll er sentralt mht til begge ovennevnte aspekter.
  - En organisasjon må kunne kontrollere tilgang til informasjon.
  - Autentisering (validering av identitet) er en viktig del av kontroll.
  - En autentiserings-policy forutsetter *autentiserings-mekanismer*
  - Eksempel: Rollebasert tilgang til informasjon forutsetter mekanismer som muliggjør å skille mellom bruker roller som f.eks. *student, stud.ass. og faglærer*.

Sikkerhetsteknologier

- **Hashing**: Dataintegritet
- **Aksesskontroll og passord**: Datakonfidensialitet
- **Kryptering**: Personvern
- **Digitale signaturer**: Meldingsautentisering
- **Digitale sertifikater**: Avsenderautentisering
- **Brannmurer (firewalls)**: Nettsteds-integritet
- **Inntrengingsdeteksjonssystem**: Nettsteds-integritet
- **Innholdsskanning og dyp pakkeinspeksjon**: Nettsteds-integritet
- **Virtuelle private nettverk (VPNs)**: Datakonfidensialitet

Hashing

- Paritetssjekker sørger ikke for dataintegritet
  - Feil kan resultere i endret sjekksum og endret dataverdi.
  - Kan få gyldig sjekksum for data som har blitt endret
  - En angriper kan endre data i pakker og likevel sørge for at sjekksum er gyldig.

- Hashing-mekanismer kan lage meldings-autentiseringskoder som ikke kan knekkes eller forfalskes.
  - Benytter en hemmelig nøkkel som bare avsender og mottaker har.
  - Nøkkelen brukes til å generer en hash-kode (kort bitsekvens) som avsender merker meldingen med.
  - Mottaker bruker nøkkel for å undersøke om hash-koden på pakken er riktig.
  - En angriper kan ikke modifisere pakken uten å introdusere feil.

Aksesskontroll og passord

- Aksesskontroll-mekanismer kontrollerer hvilke brukere eller programmer som kan aksessere data.
  - Passord som styrer hvilke data en bruker får tilgang til.
  - Aksesskontroll-lister (ACLs) per objekt som spesifiserer hvem som skal ha tilgang.

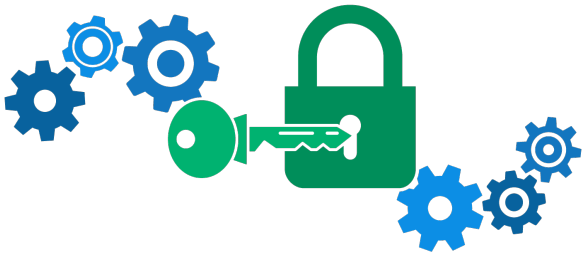
- Ukrypterte passord og ACLs som sendes over nettverk kan potensielt bli plukket opp av noen som ”avlytter” nettverket.

- Tiltak må gjøres for å sikre at passord ikke er for enkle å gjette (krav til lengde, tegninnhold, etc.)

Kryptering

- Endre på dataene i en melding, slik at kun riktig mottaker kan rekonstruere den opprinnelige meldingen.
  - Plaintext: Orginalmeldingen førkryptering.
  - Cyphertext: Den krypterete meldingen.
  - Encryption key: Bitsekvens som brukes til kryptering.
  - Decryption key: Bitsekvens som brukes til dekryptering.

- Kan garantere konfidensialitet, meldingsautentisitet og dataintegritet og forhindre *replay*-angrep.



Kryptering (som funksjon)

- Vi kan tenke på kryptering som en funksjon som tar i mot to argumenter (nøkkelen (K_1) og meldingen (M)) og som returnerer en kryptert variant av meldingen (C):

$$C = \textit{encrypt}(K_1, M)$$

- En dekrypteringsfunksjon reproduserer orginalmeldingen:

$$M = \textit{decrypt}(K_2, C)$$

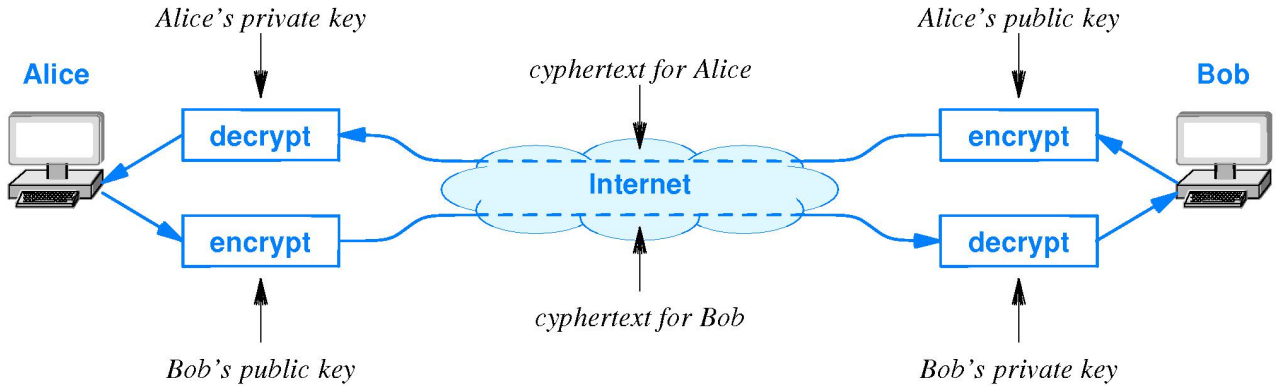
Kryptering med privat nøkkel

- Krypteringsteknikker kategoriseres etter hvordan de bruker krypteringsnøkler:
  - Private key systems (systemer med privat nøkkel)
  - Public key systems (systemer med offentlig nøkkel)

- Kryptering med privat nøkkel
  - Partene deler en hemmelig nøkkel som brukes både for kryptering og dekryptering.
  - Partene kan både sende og motta krypterte meldinger (symetrisk system)
  - M = *decrypt*(K, *encrypt*(K, M))

Kryptering med offentlig nøkkel

- Hver part får én (hemmelig) privat og en offentlig nøkkel.
- En melding kryptert med offentlig nøkkel kan kun dekrypteres med den korresponderende private nøkkelen.
- Sikrer konfidensialitet. Man trenger den privat nøkkel for å dekryptere meldingen.



Digitale signaturer (autentisering)

- En melding kryptert med privat nøkkel kan kun dekrypteres med den korresponderende offentlige nøkkelen.
- Kryptering med en privat nøkkel brukes for å gi en melding en *digital signatur*.
- En mottaker kan autentisere avsender (den digitale signaturen) ved å bruke avsenders offentlige nøkkel for å dekryptere meldingen.
- Mottaker vet hvem som sendte meldingen fordi det kun er avsender som har nøkkelen for å gjennomføre krypteringen.

Digitale signaturer (autentisering)

- En melding kan også krypteres to ganger for å garanterer autentisitet (riktig avsender) og konfidensialitet (riktig mottaker).
- Først dekrypteres (signeres) meldingen ved at avsender bruker sin private nøkkel.
- Deretter krypterer avsender meldingen en gang til ved å bruke mottakers offentlige nøkkel.
- For å dekryptere meldingen må mottaker først bruke sin private nøkkel, deretter avsenders offentlige nøkkel.

Digitale sertifikater og utstedere

- For å forhindre at hvem som helst kan lage private og offentlige nøkler og dermed opptre som andre er det behov for en pålitelig tredjepart – en nøkkelutsteder/sertifikatutsteder.

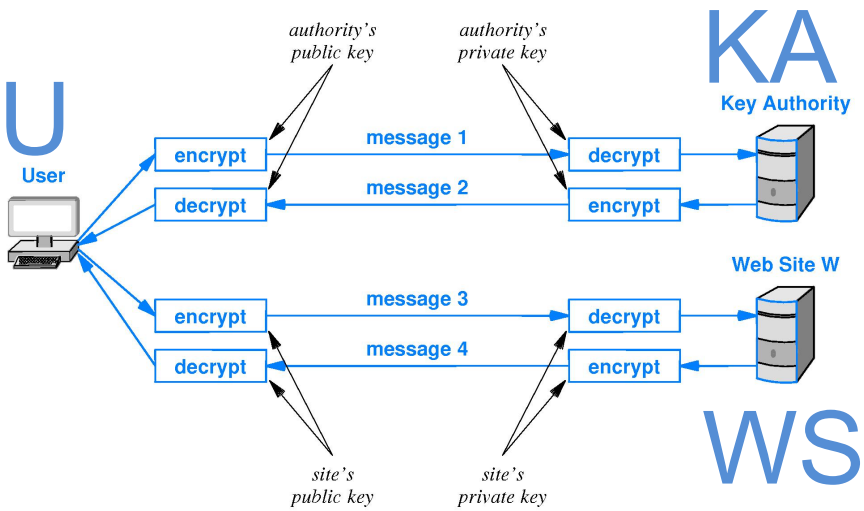
- Et digitalt sertifikat garanterer at identiteten knyttet til en offentlig nøkkel.

- Ved å ha tilgang utsteders offentlige nøkkel, kan man få tilgang til andre offentlige nøkler.

Digitale sertifikater og utstedere

Scenario: En bruker (U) vil gjennomføre en sikker transaksjon med en webside (WS).

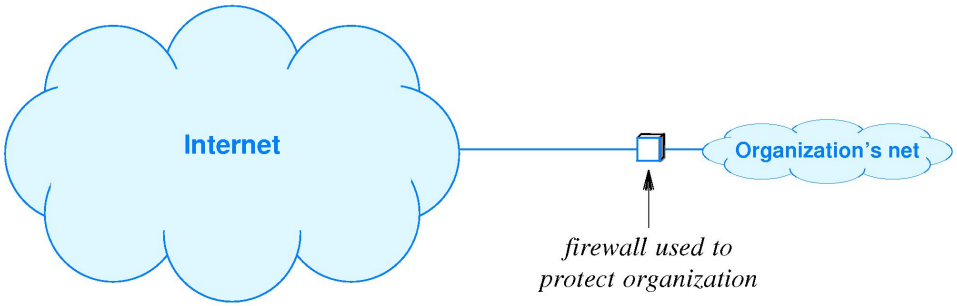
1. U benytter utsteders (KA) sin offentlige nøkkel for å sende forespørsel om WS sin offentlige nøkkel.
2. KA returnerer WS sin nøkkel i melding kryptert med KAs private nøkkel. U dekrypterer denne med KA's offentlige nøkkel.
3. U kan kan da sende en kryptert forespørsel til WS ved å bruke WS sin offentlige nøkkel.
4. U kan da vite at kun WS kan generere respons siden det kun er WS som besitter den private nøkkelen for å dekryptere forespørselen U sendte.



Kunnskap for en bedre verden

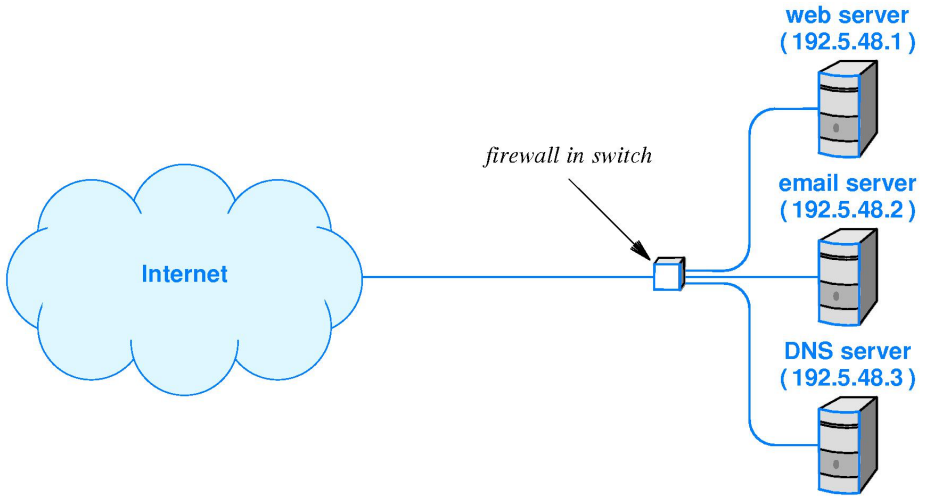
Brannmurer (firewalls)

- Overvåker og kontrollerer trafikk inn og ut av et internt nettverk for å beskytte mot problemer som kan komme utenfra (f.eks. fra internett).
- Typisk innebygd i switcher og rutere.
- Sentraliserer kontroll over nettverkstrafikken som går inn og ut.
- Implementerer sikkerhetsretningslinjene til en organisasjon og stopper trafikk (pakker) som ikke er i tråd med disse.



Brannmurer og pakkefiltrering

- En brannmur har et pakkefilter som undersøker informasjonen i pakkehodet og avgjør om pakken skal få passere gjennom ruteren eller ikke.
- Kan brukes for å kontrollere aksess til spesifikke tjenester på spesifikke datamaskiner.



Dir	Frame Type	IP Src	IP Dest	IP Type	Src Port	Dest Port
in	0x0800	*	192.5.48.1	TCP	*	80
in	0x0800	*	192.5.48.2	TCP	*	25
in	0x0800	*	192.5.48.3	TCP	*	53
in	0x0800	*	192.5.48.3	UDP	*	53
out	0x0800	192.5.48.1	*	TCP	80	*
out	0x0800	192.5.48.2	*	TCP	25	*
out	0x0800	192.5.48.3	*	TCP	53	*
out	0x0800	192.5.48.3	*	UDP	53	*

Inntrengings-deteksjonssystem (IDS)

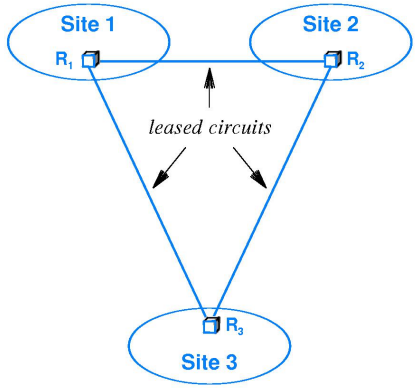
- Mekanisme som monitorer pakker og gir administrator beskjed når sikkerhetsbrudd avdekkes (en brannmur kan kun forhindre at angrep).
- Kan typisk konfigureres til å se etter spesielle typer angrep.
- Kan koples sammen med brannmur slik at nye konfigurasjoner/regler kan opprettes på bakgrunn av hva som detekteres.
- I motsetning til en brannmur kan et IDS loggføre hvor pakker kommer fra, f.eks. om flere SYN pakker kommer fra samme kilde.

Innholdsskanning og dyp pakkeinspeksjon

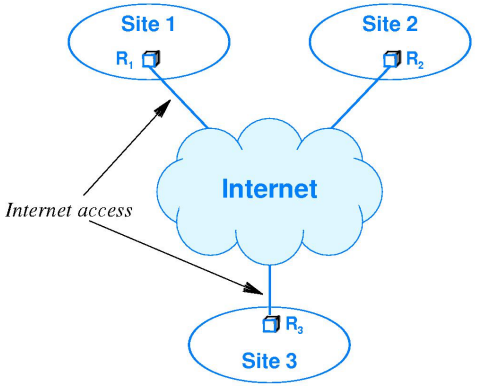
- En brannmur sjekker kun pakkehodet – ikke pakkeinnholdet.
- Innholdsanalyse kan sjekke pakkeinnhold for skadelig programvare, som f.eks. virus.
- *File scanning*: Skanner hele filer på jakt etter ”fingeravtrykk” (kjente byte-mønstre), som kan indikere virus.
- *Dyp pakkeinspeksjon (DPI)*: Analyserer innhold i pakker (i tillegg til hodet)
- DPI er ressurskrevende:
  - Rammen er gjerne 20 ganger større enn hodet.
  - I motsetning til hodet er ikke pakkeinnholdet organisert i felter.

Virtuelle private nettverk (VPN)

- Bruker kryptering for å tilby sikker aksess (via internett) til et lokalt nettverk for klienter som befinner seg utenfor (f.eks. tilgang NTNUs nettverk hjemmefra).
- Opprinnelig laget for å kople sammen lokale nettverk til en organisasjon som er fysisk distribuert.
- Sikker løsning for lav kostnad (bruker internett i stedet for å leie dedikerte linjer).
- VPN-funksjonen kan knyttes til dedikerte rutere med brannmur for økt sikkerhet.
  - Brannmuren kan sjekke om innkomne pakker er merket med IP-adresser som korresponderer med til en annen spesifikk VPN-ruter .



(a)



(b)

Kunnskap for en bedre verden

NTNU

Bruk av VPN i telekommunikasjon

- To former for VPN.

- *Stand-alone device:*
  - Bruker får egen ruter VPN rutersom automatisk etablerer sikker kommunikasjonskanal med VPN server.

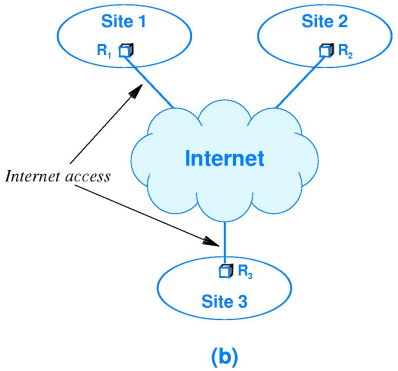
- *VPN software:*
  - *VPN* programvare kjører på brukerens datamaskin,
  - Krypterer alle pakker som så sendes til VPN serveren koblingen er knyttet mot.
  - Dekrypterer alle innkommende pakker.

Pakkekryptering kontra tunnelering

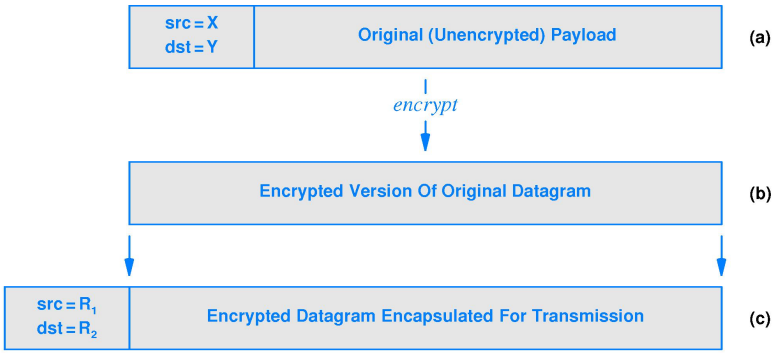
- Det finnes hovedsakelig tre valgmuligheter mht. hvordan pakker som skal sendes over Internett kan krypteres: *Payload encryption*, *IP-in-IP tunneling* og *IP-in-TCP tunneling*.

- Payload encryption:
  - Krypterer kun meldingsinnholdet i pakken (ikke pakkehodet).
  - Kilde- og destinasjonsadresse, pakkestørrelse m.m. kan fanges av uvedkommende.

- IP-in-IP tunnelling:
  - Krypterer både meldingsinnholdet og hodet og plasserer resultatet i en ny pakke, som så kan sendes over Internett.



(b)



Pakkekryptering kontra tunnelering

- IP-in-TCP tunneling:
  - To parter etablerer en TCP forbindelse.
  - Forbindelsen brukes til å sende en strøm av krypterte datapakker.
  - Små hoder markerer skillet mellom datapakkene i strømmen.
  - Kryptere hode og melding og legger til et lite hode som spesifiserer lengden på datagrammet.
  - VPN programvare på mottakersiden leser hodet og antall spesifiserte bytes for å finne datapakken.
  - Når en komplett kryptert melding er mottatt dekrypteres denne.
  - Pakkene må leveres i riktig rekkefølge.

Ytelsesutfordringer tilknyttet VPN

- *Latens/forsinkelser*:
  - Bruk av VPN resulterer gjerne i at datapakker må traversere internett mange ganger mellom en bruker og det lokale nettverket har er koplet opp til.
  - Medfører gjerne økt tidsforbruk for å gjennomføre en transaksjon.

- Throughput:
  - Raten data kan sendes på gjennom Internett kan være en begrensning.
  - Kan medføre at en får gjort færre transaksjoner per tidsenhet.

- ”Overhead”/fragmentering:
  - Tunnelering gjør at det blir mer data å sende og motta (f.eks. krypterte pakker som puttes i nye pakker)
  - Dersom ny pakke overstiger grensen for hvor mye data som kan kommuniseres per transaksjon (MTU) må pakken deles opp videre.
  - Øker sannsynligheten for forsinkelser og tap av pakker.

Oppsummering kapittel 29

- Kommunikasjonsnettverk er utsatt for flere typer trusler.
  - Phishing, misrepresntation, scamas, DoS, etc.
- Det finnes mange forskjellige typer sikkerhetsangrep
  - ”Avlytting”, spoofing, buffer overflow, denial of service, ”knekking” av passord og nøkler, pakkemanipulering, etc.
- Sikkerhet er en relativ term.
- En sikkerhetspolicy spesifiserer en organisasjons data-integritet, -tilgjengelighet, -konfidensialitet og personvern.
- Ulike teknologier håndterer ulike sikkerhetsaspekter.
  - Kryptering, hashing, digitale signaturer og sertikater, brannmurer, IDS, pakkeinspeksjon, VPN, etc.

Nettverk

32. The Internet of Things

Læringspunkter

- Få innsikt i den grunnleggende motivasjonen bak ”The Internet of things” (IoT).

- Få en forståelse av viktige hensyn som må tas i forbindelse maskin–til–maskin-kommunikasjon (M2M) og IoT.

Integrerte systemer (embedded systems)

- Kommunikasjon mellom ”ting” vi omgir oss med i hverdagen, som f.eks, lysbrytere, alarmsystemer, termostater, og overvåkningsutstyr.
  - Automatisering.
  - Maskin–til–maskin-kommunikasjon (M2M)

- Noen sentrale områder for M2M
  - Smart grid (strømstyring).
    - Eksempel: Lading av el-utstyr når strømmen er billigst
  - Online sikkerhetssystemer.
    - Automatiske varsler ved ulike hendelser (dør, vindu og beveglesessensorer).
  - Handel
    - Skreddersydde reklamer og tilbud.
    - Fange opp kunde oppførsel.

IOT og valg av nettverksteknologi

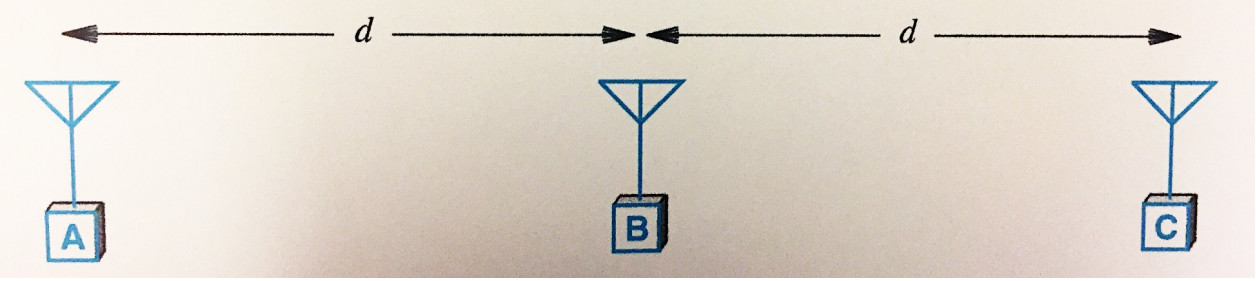
- Ulike nettverksteknologier gir ulike fordeler og ulemper mht. til IoT. Typiske hensyn:
  - Trafikkvolum: Dataorientere- kontra kontrollorientere applikasjoner.
  - Mobilitet: Kablet kontra trådløst.
  - Energiforbruk: Batteritid kontra strømkostnad.

- *Energy harvesting*: Nyttiggjøre energi fra omgivelsene for å lade batterier
  - F.eks. bruke bevegelses energi for å lade et armbåndsur.

- Tråløs teknologi med lavt energiforbruk er viktig for mange IoT-applikasjoner.
  - Lavt energiforbruk begrenser hvor langt radiosignalene rekker, gjør kommunikasjonen mer sensitiv mht til forstyrrelser og øker sannsynligheten for pakketap.

IOT og valg av nettverksteknologi

- Mesh-nettverk muliggjør trådløse kommunikasjonsnettverk bestående av noder med lavt energiforbruk.
- Hver node opprettholder en liste over hvilke nabo-noder som er innen radiorekkevidde.
- Nodene samarbeider om å få frem en melding sendt fra en node (A) til en node som ligger utenfor radiorekkevidde (C).



Oppsummering

- IoT brukes for å beskrive sammenkoplete integrerte systemer hvor datamaskiner kommuniserer med andre datamaskiner.

- Valg av nettverksteknologi i M2M styres gjerne av krav til trafikkvolum, mobilitet, og energiforbruk.

- Lavt energiforbruk er en viktig faktor i mange IoT-applikasjoner.