UKE-2

Opplegg

- Går igjennom nettverksdelen
- Ukesoppgaver – rettet mot datanettverk
- Mentimeter – datanettverk
- Går igjennom sikkerhetsdelen – Autentisering og sikkerhetstiltak
- Noen ukesoppgaver
- Mentimeter - sikkerhetsdelen

Komponenter i nettverk

UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Nettverkskomponenter

- Tjenere
- Klienter
- Switcher
- Routere



Tjenere: Ansvarlig for å oppfylle forespørsel fra klienter

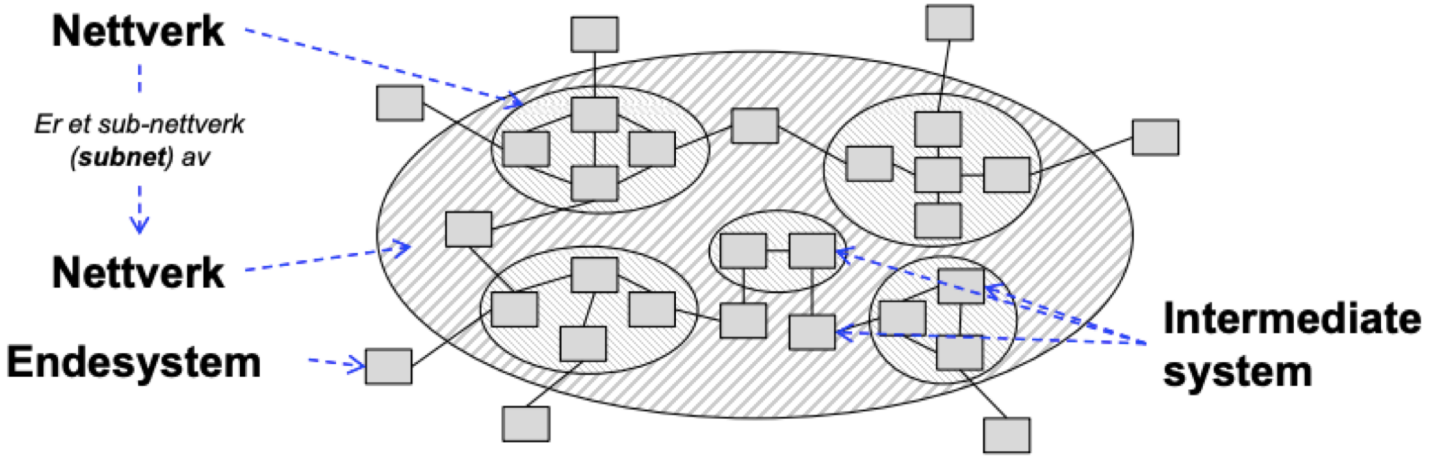
Klienter: Ber om forespørsler til tjenere (Ønsker å danne en forbindelse med nettside, hjelp)

Switcher: Knytter diverse enheter til et nettverk kun benyttes gjennom kabler. Overfører datatra gjennom koblingen til en annen node. Kobler to noder sammen

Router: Sørger for at flere datamaskiner kan de samme nettverk. Støtter trådløs nettverk, kan sees som tilgangspunktet for alle maskiner kob til det trådløse nettverket. Vet hvordan den skal overføre datapakker i nettverket. En innebygd Switch, men som er «smartere» enn switch.

Endesystemer og intermediate systemer

Nettverkskomponenter



Endesystemer:

- Endesystemer finnes helt ytterst i nettverket
- For eksempler: datamaskiner, mobiltelefoner, sensorer, skrivere

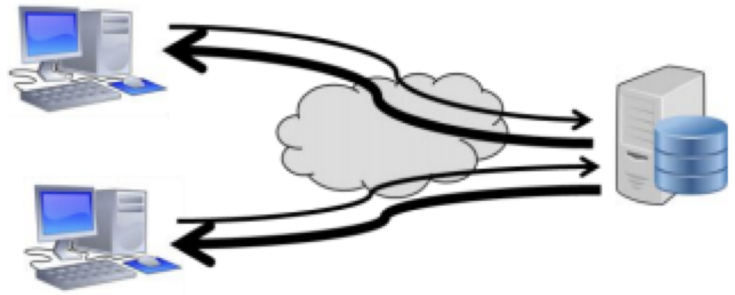
Intermediate system:

- For eksempel:
  - ruter, switch
  - gateway
  - repeater, bridge

Aksessmodeller – Modeller for datakommunikasjon

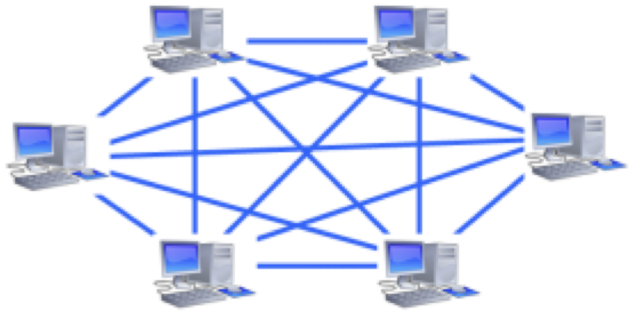
Klient-tjener:

- Klienter ber om en tjeneste (oppretter en forbindelse)
- Tjenere leverer tjenesten (svarer på forespørselen)



Peer-to-Peer (P2P)

- Alle noder er likeverdige
- Alle noder kan nå hverandre
- Eierskapet er distribuert



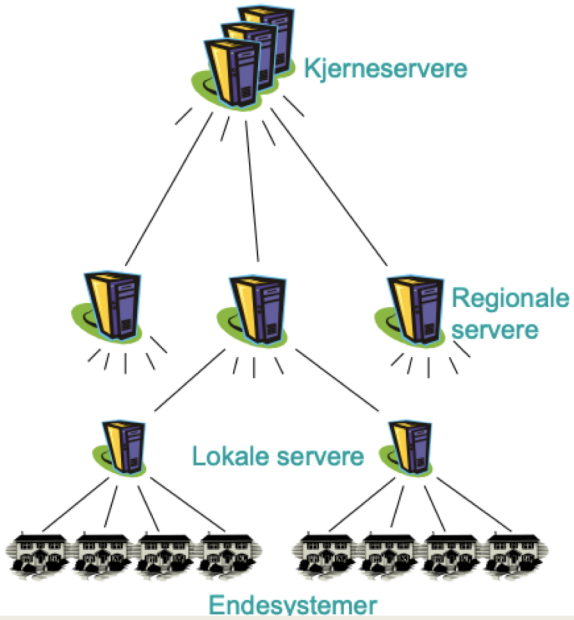
Content Delivery Network

UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Distribusjon med CDN

- **Hierarkiske systemer for å distribuere innhold**
  - Vanlig å "cache" populært innhold.

- Populære videoer blir lagret nærme sluttbrukerne
- Videoer som ikke er så populære lagres enten på eller nærme kjerneserveren.
- Spesielt viktig hvis båndbredden er begrenset.
  - For eksempel: WiFi på fly



Forskjellige typer nettverk – punkt til punkt

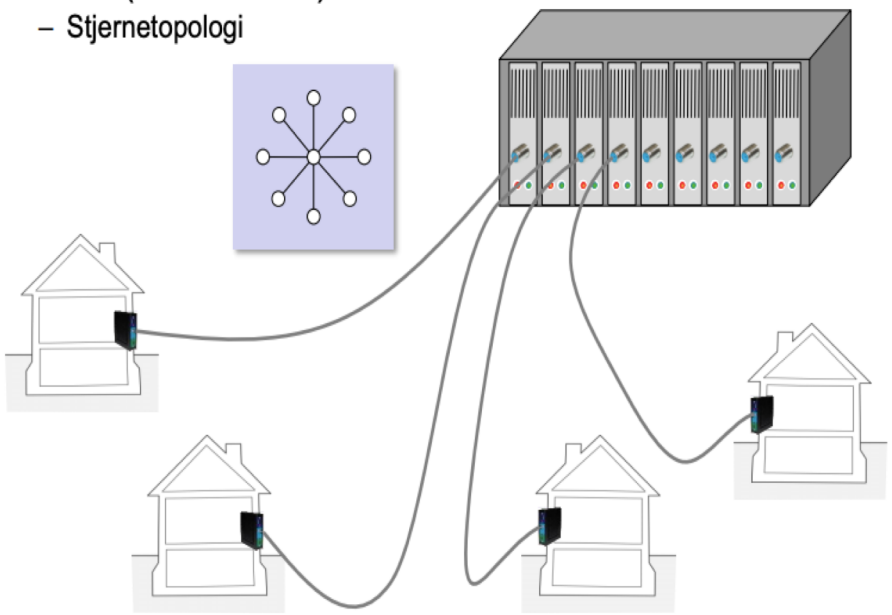
UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Nettverksstrukturer

Punkt til punkt:

DOCSIS (kabelmodem)

– Stjernetopologi



UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

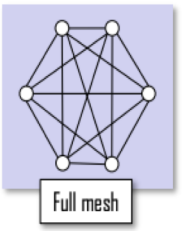
Nettverksstrukturer

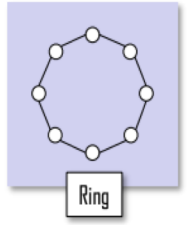
Punkt til punkt:

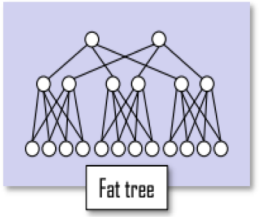
DOCSIS (kabelmodem)

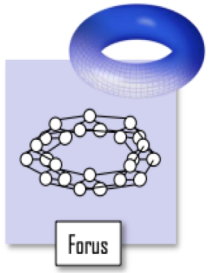
– Stjernetopologi

- Gigabit Ethernet ("1GB Ethernet")
  - Stjernetopologi eller tretopologi
- IEEE 802.5 "Token Ring" (utdatert)
  - Ring
- Noen «supermaskiner»:
  - Full mesh
  - Torus
  - Fat tree







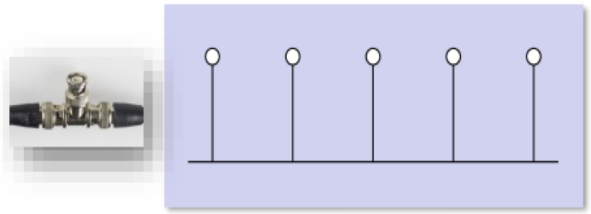


Forskjellige typer nettverk - broadcasting

UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Nettverksstrukturer

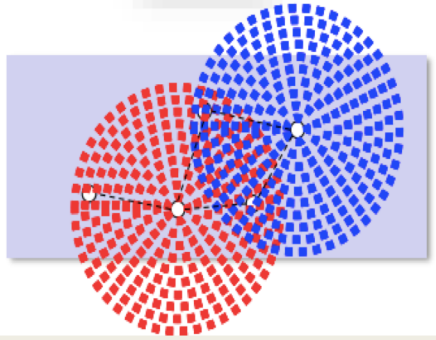
Broadcast-systemer:



- *Kabel:*
  - Gammeldags Ethernet
- *Radio:*
  - Aloha (første generasjon trådløs)
  - WiFi (IEEE 802.11)
  - Mobiltelefoni: 3G, 4G
  - Satellitt



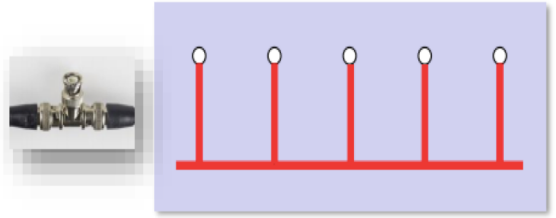
- ***Egenskaper:***
  - Når en node sender kan potensielt alle høre!
  - Kan bli problemer hvis to noder sender samtidig…
  - Feildeteksjon er viktig!
  - Sending bør koordineres…



UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Nettverksstrukturer

Broadcast-systemer:



- *Kabel:*
  - Gammeldags Ethernet
- *Radio:*
  - Aloha (første generasjon trådløs)
  - WiFi (IEEE 802.11)
  - Mobiltelefoni: 3G, 4G
  - Satellitt



- ***Egenskaper:***
  - Når en node sender kan potensielt alle høre!
  - Kan bli problemer hvis to noder sender samtidig…
  - Feildeteksjon er viktig!
  - Sending bør koordineres…

Nettverket fordelt mellom alle datamaskiner gjennom f.eks, en ruter.

Sikkerhet i nettverket

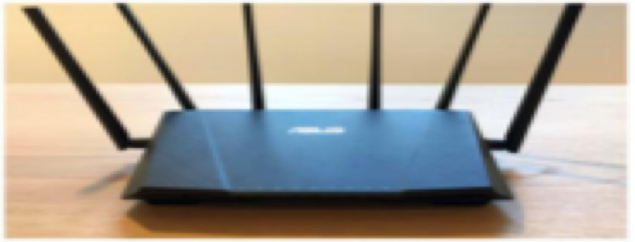
UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Sikkerhet i trådløse nettverk

- All trafikk i trådløse nett uten passord er åpen
- Svakhet i protokoller og algoritmer
  - Key Reinstallation Attacks (KRACK)
  - Svakheter i implementasjoner
- "Brute-force"
  - Teste alle mulige kombinasjoner
  - Moderne maskiner kan teste over millioner av passord i sekundet
    - 8 siffer = 28 timer
    - 6 bokstaver = 4 dager
  - Ordbokangrep

16. Oktober 2017

Dinside



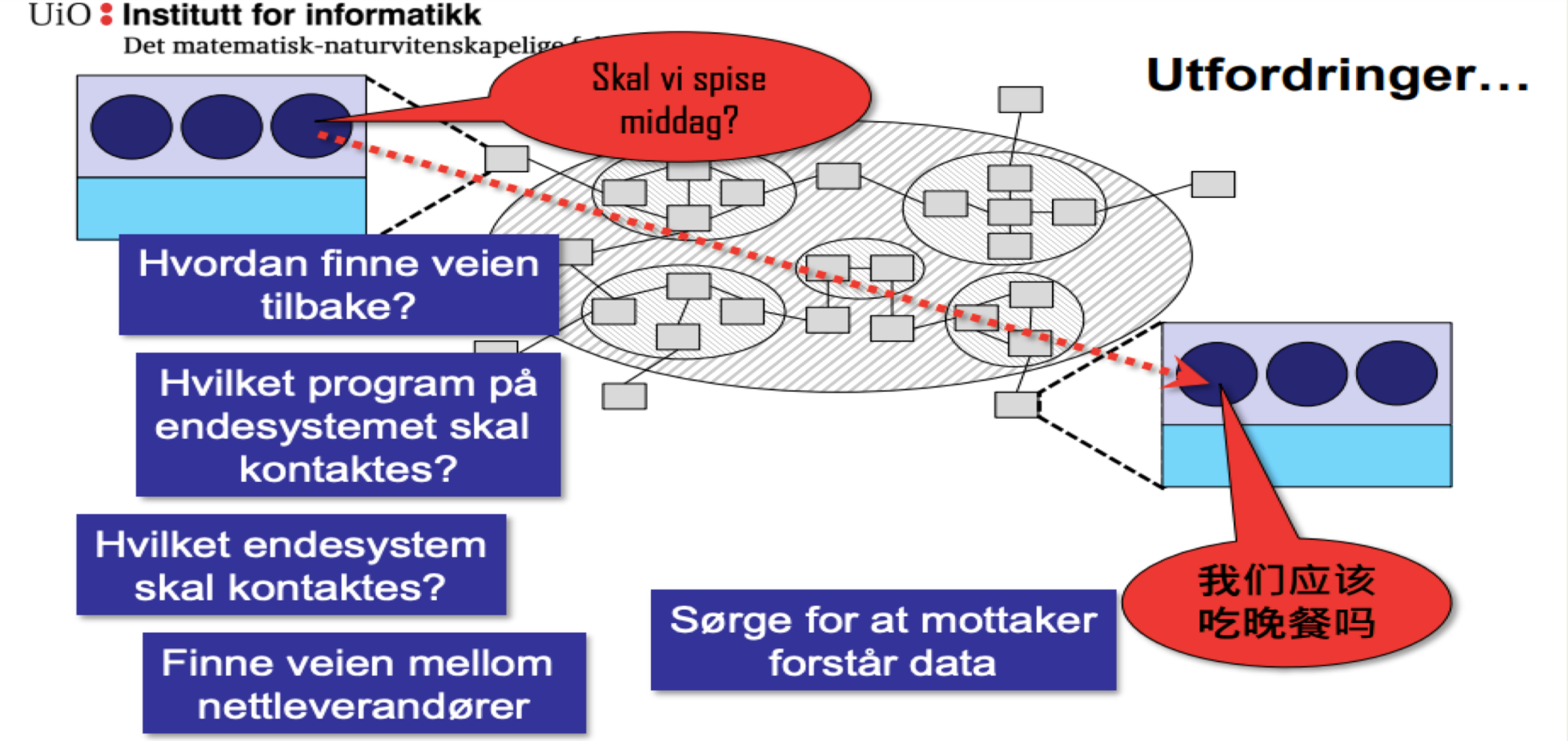
Plutselig ble alle trådløse nettverk utrygge

KRACK: Svakheter i WPA:
https://www.krackattacks.com/

Password Calculator:
http://lastbit.com/pswcalc.asp

Med kabla nett så vil vi hindre problemene nevnt over med mindre inntrengere har tilgang til den fysiske porten

Utfordringer ved nettverk



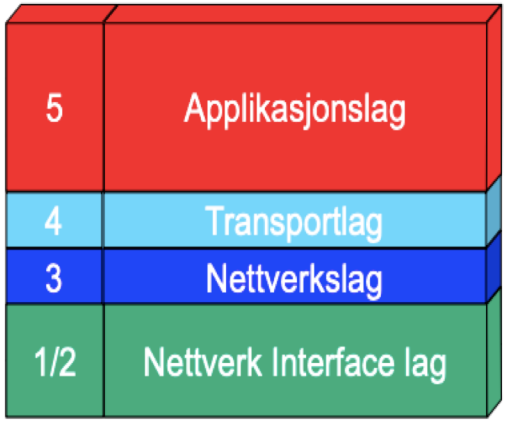
Protokoller og lagdeling

UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Fem-lags referansemodellen – TCP/IP modellen

TCP/IP (Internett)

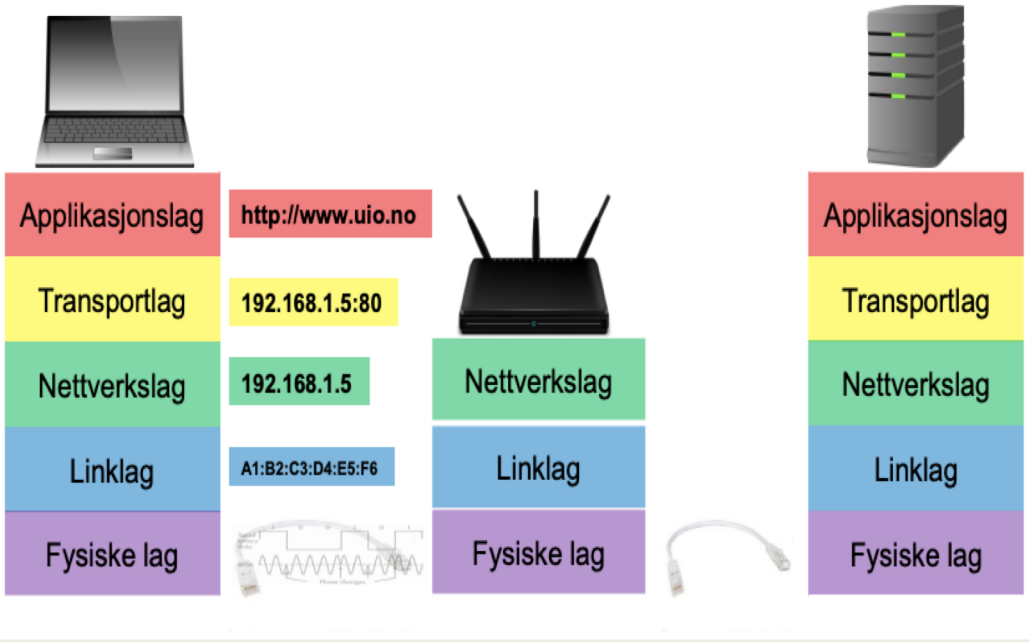
- TCP/IP er overalt: WWW, E-post, filoverføring, tjenester på nettet...



	Lag	Funksjon
5	Applikasjon	Applikasjonsrelaterte tjenester (HTTP, Mail)
4	Transport	Kobler sammen systemene ende-til-ende (TCP/UDP)
3	Nettverk	Sende data fra ende-til-ende systemer (IP)
2	Link	Pålitelig overføring mellom to noder (LAN/WiFi)
1	Fysisk	Sender bit ut på mediet (kablet eller trådløst)

UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Lagene i Internett (TCP/IP referansemodellen)



Nettverksprotokoll: Sett med regler som beskriver hvordan nettverket skal fungere.
Sørger for å løse problemene som ble nevnt istad.

Mentimeter innenfor datanettverk

- https://www.mentimeter.com

Autentisering og autentisitet

- Autentisitet: Forteller noe om ekteheten eller opprinnelsen av noe. Motsatte av en kopi eller falsk informasjon
- Autentisering: Bekrefter at noe er autentisk. I IT-sammenheng kan dette være å bekrefte at en bruker faktisk er en bruker.
- Autentisering av dataopprinnelse: Bekrefte at dataen faktisk er ekte, at en bruker f.eks ikke mottar uriktig informasjon gjennom e-mail.

Autorisering

«Å autorisere er å godkjenne eller gi løyve»

snl.no

- Å autorisere er å spesifisere en *tilgangs-policy*.
- Autorisering er altså **ikke** teknologi, men policy.
- Eksempel på en slik policy:
  «En ansatt i lønnsavdelingen skal ha tilgang til lønnssystemet.»

Hvilke rettigheter entiteter/systemer får ved innlogging. Studenter får rettigheten til å se karakterene deres f.eks,

Tilgangskontroll

«Tilgangskontroll innebærer å sjekke om et subjekt har tilgang til å utføre en ønsket handling på et objekt, etter forhåndsdefinerte regler»

Eksempler på forespørsler fra *subjekter*:

- Anne vil lese innholdet i en fil
- Per vil oppdatere kontobalansen på en bankkonto
- En applikasjon vil opprette en nettverksforbindelse mot en annen maskin

Tilgangskontroll = autentisering + autorisasjon

Eksempel: https://www.uio.no/studier/emner/matnat/ifi/IN2010/h21/ukeplan/

Sees som en dørvakt som avgjør hvem som skal slippe inn

Sikkerhetstiltaket - Kryptering

Kryptering: Et sikkerhetstiltak som sørger for at informasjonen blir uleselig for andre lyttere når dataen skal overføres mellom to noder eller når dere tilkobles til nettverket osv.

Sikkerhetsmål som oppnås:

Konfidensialitet – Hvis jeg sender en e-mail til dere så er det kun mellom oss, ingen andre skal få vite om det

Integritet – Modifikasjon av data går ikke hvis dataen er kryptert. Får ikke muligheten til å røre dataen rett og slett.

Relevant for obligen – 7, hvis UiO nettverket var åpent og det ikke var innført noe kryptografi, hva ville konsekvensene ha vært for oss da?

Sikkerhetstiltaket - Sikkerhetskopi

Ta vare på data: Sikkerhetskopi

- Sikkerhetskopiering er en strategi for å ta vare på informasjon over tid.
- **Mål**: Bidra til økt tilgjengelighet ved å være i stand til å gjenopprette systemer og data ved uønskede hendelser som endrer eller sletter informasjon.

Viktig ved sikkerhetskopiering:

1. Ta vare på *flere ulike versjoner* av informasjon.
2. Sikkerhetskopien må også sikres: Lagres trygt adskilt fra opprinnelige disker/data, utilgjengelig for uvedkommende.
3. Sikkerhetskopi =/= datasynkronisering

Mentimeter innenfor sikkerhetsdelen

- https://www.mentimeter.com