1)

Flyttkontrollen på TCP-protokollen tar hovedsakelig utgangspunkt i at avsender ikke overrumpler mottakeren med datapakker. Altså at flere pakker enn mottakeren kan håndtere blir sendt. For å løse dette slik at pakkene flyter i en mengde som både mottaker og avsender kan håndtere bruker TCP-protokollen denne metoden:

En forbindelse mellom mottaker og avsender blir opprettet før noe som helst data blir sendt. Mottakeren har en buffer som fylles opp etter hvert som datapakker kommer inn. (I andre enden av denne sendes pakkene videre opp i systemet). Dette bufferet er også av en viss størrelse. Størrelsen av hvor mye plass det er igjen i dette bufferet blir målt av mottakeren. Informasjonen (ang plass) sendes tilbake til avsender som evt kan bremse opp hvis det er lite plass igjen i bufferet. Slik oppnås en viss flytkontroll.

2)

Kø oppstår ofte lett når det er kontinuerlig dataoverføring over et stort sendevindu. TCP vet I utgangspunktet ikke hvor stor kø det er i nettverket. (Kø oppdages ikke før det evt blir et tap av pakker) Protokollen må derfor begynne med å sjekke hvor stort sendevindu den kan bruke. Dette gjøres på denne måten:

Den begynner med et vilkårlig sendevindu. Deretter økes sendevinduet for hver gang, helt til det blir pakketap. TCP-protkollen ender dermed opp med å finne ut hvor stort sendevinduet kan være, og en viss kø-kontroll blir oppnådd.

3)

Det finnes en rekke forskjeller mellom UPD- protokollen og TCP-protokollen for det første er TCP- en «connection- oriented» som vil si at en forbindelse mellom avsender og mottaker blir opprettet før data blir utvekslet. UPD- protokollen benytter seg ikke av forbindelse, og har ingen flytkontroll eller kø-kontroll for datapakkene slik TCP har. Det gjør denne protokollen veldig effektiv i forhold til TCP. (Pakkene ankommer nødvendigvis ikke i rekkefølgen de blir sendt heller)

TCP er mest brukt da den er mest pålitelig, men UPD har også sine bruksområder. Da spesielt taleoverføring, video-streaming og gaming. (Dette er forbindelser som trenger rask/ effektiv overføring av data).

4)

UDP- headeren består av følgende deler:

Source port: Her ligger informasjon om port-nummer til avsenderen. (Dette feltet blir satt til 0 hvis mottakeren ikke trenger å svare.

Destination port: Dette er portnummeret til enheten som skal ta imot dataen. (Disse kan være mellom 0 og 65 535.

Length: Denne delen spesifiserer antall byte pakken er på. (Her inngår både headeren og data-delen).

Checksum: Feilsjekk metode. Dette gjør det mulig for mottakeren og avgjøre om riktig (intended) data er mottatt.

5)

Source port: 16-bits felt som spesifiserer port nummeret til avsenderen av pakken.

Destination port: 16- bits felt som spesifiserer port- nummeret til mottakeren av datapakken.

Sequence number: 32 bits-felt som indikerer hvor mye data som er sent under TCP- session.

Acknowledgment number: Dette er et 32 -bits felt som blir brukt av mottaker til å forspørre det neste TCP-segmentet. (Overnevnte verdi inkrementert med 1)

DO: Også kjent som header length. Dette indikerer bit-lengden på headeren. Denne er med så vi skal kunne skille mellom data og headeren i pakken.

RSV: 3 bit for ubrukte / reserverte felt. Alltid satt til 0.

Flags: 9 bit er satt av til dette. Kalles også for kontroll bits. De brukes til å etablere koblinger, sende data og avslutte koblinger. (Finnes flere typer av denne)

Window: 16- bit felt som spesifiserer hvor mange bytes mottaker er villig til å ta imot. Eksempelvis kan mottakeren fortelle at den vil motta mer enn det den allerede gjør.

Checksum: 16-bits felt som blir brukt for å feilsjekke TCP- header.

Urgent pointer: 16-bit felt. Brukes til å indikere hvor «urgnt data» slutter.

Options: Dette feltet er valgfritt, og kan være alt mellom 0 og 320 bit.

6)

Det finnes en rekke utfordringer ved å bruke skytjenester. For det første er de aller fleste skytjenester basert i utlandet. Vi blir da avhengig av utlandet. Disse landene kan kanskje ha andre praksiser for håndtering av data enn det vi har i Norge.

I tillegg til at andre land ofte ikke kan tilby samme standarder for håndtering av data som Norge, vil det også kunne bli slik at vi til slutt er helt avhengig av utenlandske skytjenester. Det vil da blir vanskelig og vurdere om disse kan tilby tilgjengelighet og sikkerhet som forventes hele tiden.

7)

De tre angrepsmetodene man kan utsettes for er:

-**Angrep på konfidensialitet**: Angriperen leser informasjonen som sendes.

-**Angrep på Integritet:** Angriperen modifiserer informasjonen som sendes.

-**Angrep på tilgjengelighet:** Angriperen blokkerer informasjonen som sendes.

8)

Kombinasjonen av trussel, verdi og sårbarhet kalles ofte for risikotrekanten.