Informasjonssikkerhet: Teori og praksis

Audun Jøsang
2. utgave 2023
Universitetsforlaget

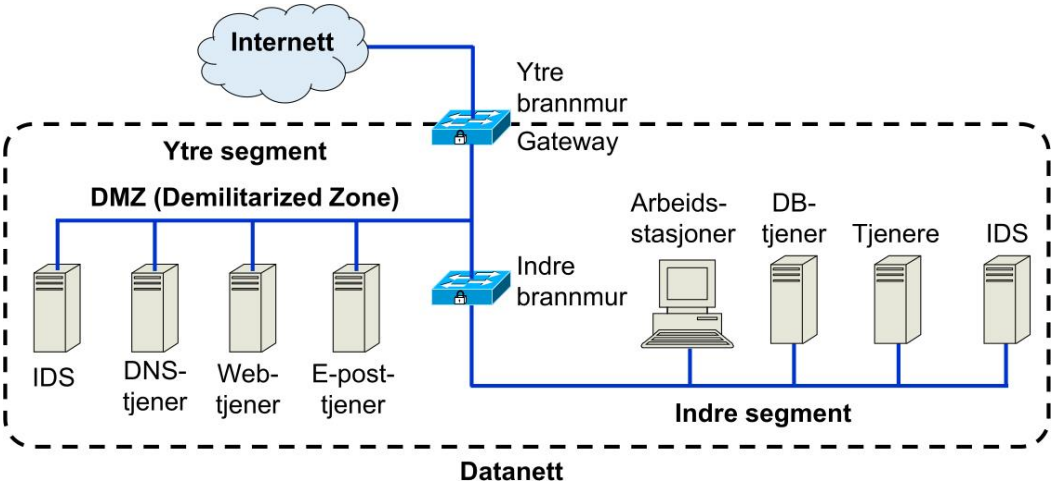
Oppgaver

Kapittel 6: Nettverkssikkerhet

Oppgave 1: Sikkerhetsprotokoller

a. Hva er en sikkerhetsprotokoll, og hva kan slike brukes til?
b. Gi eksempler på sikkerhetsfunksjoner/tjenester som støttes av sikkerhetsprotokoller.
c. Nevn minst fire velkjente sikkerhetsprotokoller.
d. På hvilke lag i internettstakken (og OSI-stakken) opererer TLS og IPSec? Hvorfor er det reservert et portnummer for HTTPS (HTTP med TLS) men ikke for IPSec?

Oppgave 2: Brannmurer



Se på figuren over som viser en enkel nettverksarkitektur med brannmurer.

a) Hva er formålet med DMZ? Hvilke tjenester fins typisk der?
b) Hvordan beskyttes indre nettverkssegmenter for angrep fra internett via DMZ?
c) På hvilke lag i internettstakken (og OSI-stakken) opererer en brannmur av typen pakkefilter?
d) Hvilken type brannmur kan filtrere trafikk basert på brukerdata i datapakker?

Oppgave 3: TLS-Inspeksjon

a. Beskriv legitime grunner for å benytte TLS-inspeksjon.
b. Beskriv trusselscenarioer for misbruk av TLS-inspeksjon.
c. Hvordan kan en bruker finne ut om TLS-inspeksjon brukes i en HTTPS nettforbindelse?

Oppgave 4: Fremoverhemmelighold (Forward Secrecy)

a) Hva menes med fremoverhemmelighold?
b) Hvordan oppnås fremoverhemmelighold?
c) Nevn en sikkerhetsprotokoll for nøkkeletablering som støtter «fremoverhemmelighold» (eng. «forward secrecy» eller «perfect forward secrecy»)?
d) Nevn en sikkerhetsprotokoll som **ikke** støttet fremoverhemmelighold. Si hvorfor ikke (dvs. hvordan den etablerer øktnøkler)

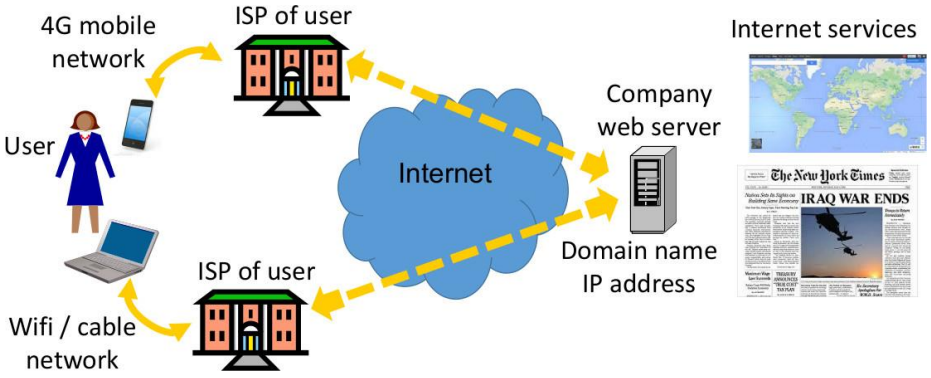
Oppgave 5: TLS

TLS er en sikkerhetsprotokoll som brukes på Internett, men TLS består egentlig av flere separate del-protokoller. Den nyeste versjonen er TLS 1.3 fra 2018.

a) Hvilken IP-port er reservert for http over TLS? Hvilken URL-prefiks indikerer at en applikasjon bruker http over TLS?
b) Beskriv kort hvor i OSI og TCP/IP protokollagene TLS opererer.
c) Forklar kort formålet med TLS Handshake-protokollen.
d) Nevn sikkerhetstjenestene som TLS Record-protokollen støtter i en TLS-forbindelse.
e) Hvordan er TLS Handshake-protokollen og TLS Record-protokoll relatert?

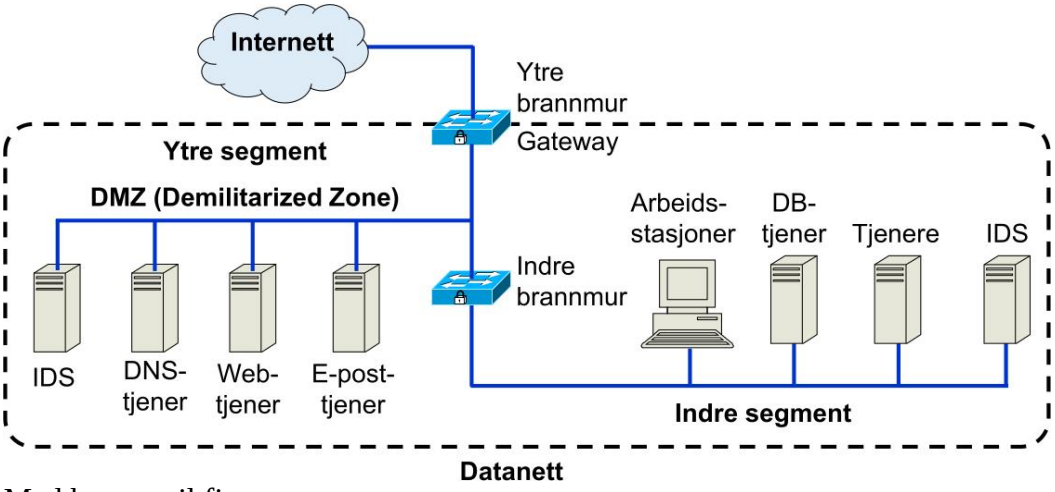
Oppgave 6: VPN

Brukerens ISP (Internet Service Provider) kan normalt se domenenavnet / IP-adressen til webserveren som brukeren aksesserer, som illustrert i figuren nedenfor. Dette kan være et personvernproblem hvis brukere ikke vil at noen tredjepart skal se deres internettaktivitet.



a) Når det brukes en sky-VPN, hvilke trafikkdata er skjult for brukerens ISP?
b) Når det brukes en sky-VPN, hvilke trafikkdata kan VPN-tilbyderen få tak i?
c) Når man bruker Tor, hvilke trafikkdata er skjult for brukerens ISP?
d) Når man bruker Tor, hvilke trafikkdata kan Tor acceess-serveren se?
e) Hvordan kan du forhindre at din ISP vet at du bruker Tor?

Oppgave 7: Pakkefilter og inntrengingsdeteksjon



Med hensyn til figuren over.

a) Hva er en typisk sikker konfigurasjon (filterregler) for brannmurene?
b) Hvor plasseres et nettverks inntrengingsdeteksjon (NIDS)?

Svarforslag

a) Ekstern brannmur:
   - Utgående forbindelser: tillat alle
   - Innkommende forbindelser: tillat port 80, 443 til webserver, port 53 til DNS-serveren, port 25 (kanskje også 143, 993) til e-postserver; forby alt annet

   Intern brannmur:
   - Utgående forbindelser: tillat alle
   - Innkommende forbindelser: forby alle; kanskje tillat tilkobling fra webserver til DB-server

b) NIDS kan plasseres både i DMZ og i det interne nettverket