Universitetet i Oslo
IN2120 Informasjonssikkerhet, høst 2025
T10 Nettverkssikkerhet
Teoretiske oppgaver med løsningsforslag



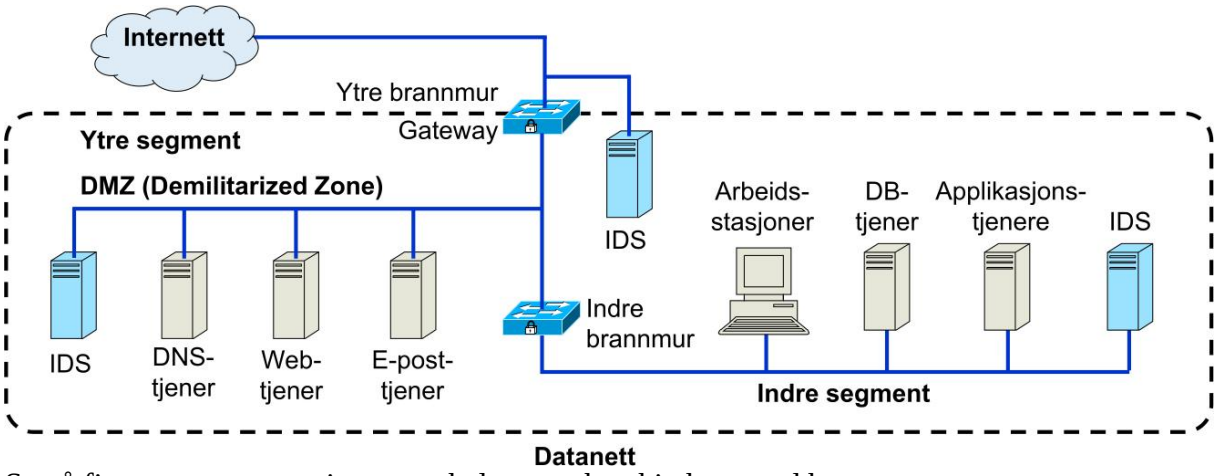
Oppgave 1: Sikkerhetsprotokoller

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?

Svarforslag

a. En sikkerhetsprotokoll er en type kommunikasjonsprotokoll kombinert med kryptografiske mekanismer, dvs. at det er en spesifikasjon på formater og sekvens for utveksling av meldinger mellom noder i et kommunikasjonsnett, inkludert kryptografiske funksjoner som utføres av hver node.
b. Typiske tjenester som støttes av sikkerhetsprotokoller er: konfidensialitet, node-autentisering, data-autentisering, dataintegritet, og nøkkelutveksling/etablering.
c. Velkjente sikkerhetsprotokoller er f.eks.: TLS (SSL), IPSec, Kerberos, SAML (som brukes i føderert identitetshåndtering), og OAuth (som brukes for autorisering og tilgangskontroll i online sosiale nettverk). Det fins mange andre sikkerhetsprotokoller, f.eks. e-valgprotokoller, e-betalingsprotokoller, osv.
d. TLS består egentlig av et sett ulike protokoller, der TLS handshake-protokollen ligger på applikasjonslaget (OSI-lag 7), mens TLS record-protokollen ligger på transportlaget (OSI-lag 4). IPSec ligger på internettlaget (OSI-lag 3). HTTPS (HTTP med TLS) har portnummer 443. IPSec har intet portnummer fordi portnummer er usynlig og irrelevant på internettlaget. Internettlaget kan støtte alle slags applikasjonsprotokoller og apper som kan ha forskjellige portnummer.

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?

Svarforslag

a) Alle tjenester som skal være tilgjengelige for å motta direkte forespørsler/meldinger fra internett (f.eks. oppslag på nettsider eller mottak av epost), bør plasseres i eget nettverk (DMZ) bak en ytre brannmur som nettopp tillater den type trafikk.
b) Indre brannmurene er konfigurert slik at tilgang fra DMZ videre til indre segmenter er strengt kontrollert med en eller flere indre brannmurer som har mer detaljerte og strengere regler for å kontrollere trafikken. Dette gjør det vanskelig å gjennomføre angrep fra internett via DMZ mot indre segmenter.
c) Pakkefiltre opererer på transportlaget (OSI-lag 4), internettlaget (OSI-lag 3), og delvis på linklaget (OSI-lag 2). Det betyr at regler for filtrering kan baseres på parametere i pakkehodene på disse tre lagene.
d) Applikasjonsbrannmurer kan filtrere trafikk basert på brukerdata. Slike brannmurer kan dermed operere på applikasjonslaget (OSI-lag 7). Det betyr at regler for filtrering kan baseres på brukerdata, i tillegg til parametere fra pakkehoder i de underliggende lagene. Filtrering basert på brukerdata kan gi høy belastning, slik at applikasjonsbrannmurer må ha høy ytelse.

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?

Svarforslag

a. En virksomhet kan vurdere det som en stor trussel at angrep og skadevare kan nå inn til virksomhetens datanett gjennom en kryptert HTTPS-forbindelse. Dette kan gjøre at virksomheten vurderer det som nødvendig å kunne filtrere/inspisere kryptert trafikk ved bruk av TLS-inspeksjon.
b. TLS-inspeksjon er en svært invaderende teknologi som kan dekryptere trafikk på en måte som gjør det vanskelig for brukeren å oppdage. Det er legitimt når en virksomhet informerer ansatte om at TLS-inspeksjon benyttes og hvorfor. Imidlertid kan angripere benytte TLS-inspeksjon uten at brukere forstår at det skjer. Hvis en bruker er koblet til internett gjennom en offentlig wifi kan de som administrerer wifi-nettet gjennomføre TLS-inspeksjon. Nettleseren vil typisk informere brukeren om at den har mottatt et ukjent sertifikat, men mange brukere er kondisjonert til å ikke bry seg om slike advarsler, og godta sertifikatet.
c. Brukeren må vite forskjellen mellom det eksterne PKI-rotsertifikatet og det interne proxy-rotsertifikatet som brukes til å validere det mottatte serversertifikatet. Brukeren kan sjekke sertifiseringsstien/signaturstien fra serversertifikatet til rotsertifikatet. Rotsertifikatet øverst i sertifiseringsstien angir om det mottatte serversertifikatet er ekte eller falskt. Hvis rotsertifikatet er et ekte eksternt PKI-rotsertifikat, er det mottatte serversertifikatet ekte, og den krypterte trafikken er ende-til-ende. Hvis rotsertifikatet er proxy-roten, tilhører det mottatte serversertifikatet proxyen, noe som betyr at trafikken dekrypteres og leses på proxyen. Imidlertid er det teknisk mulig at tilogmed proxy rotsertifikatet er spoofet, og at organisasjonen gir rotsertifikatet et spoofet navn som f.eks. "VeriSign.com". Selv om det unike navnet på rotsertifikatet sier "VeriSign.com" er det ikke nødvendigvis "VeriSign.com". Organisasjonen som drifter proxy-serveren, bestemmer hva de de ulike attributtene til proxy-root-sertifikatet skal være. Hvis brukeren ikke vil stole på noen av attributtene i rotsertifikatet, må hun være i stand til å skille mellom det ekte eksterne rotsertifikatet og proxy-rotsertifikatet basert på den offentlige nøkkelen. En offentlig nøkkel er omtrent 2000 bit lang, som er noen få linjer med HEX-sifre. Siden proxyen kan kopiere alle attributtene fra det ekte eksterne rotsertifikatet til proxy rotsertifikatet, med unntak av den offentlige nøkkelen, kan den offentlige nøkkelen brukes til å bestemme om rotsertifikatet er falsk eller ekte, men det ville kreve at brukeren har en autentisk kopi av den offentlige nøkkelen for det eksterne rotsertifikatet, og sammenligner denne med den offentlige nøkkelen i rotsertifikatet på den interne hosten.

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)

Svarforslag

a) Når en langtidsnøkkel (typisk tjenerens private nøkkel for digital signatur) benyttes for etablering av øktnøkler (f.eks. i TLS) er fremoverhemmelighold egenskapen at tidligere øktnøkler forblir beskyttet og hemmelige fremover i tid selv om langtidsnøkkelen kompromitteres/lekkes en gang i fremtiden. Uten fremoverhemmelighold vil tidligere økter kunne dekrypteres hvis den private nøkkelen lekkes/stjeles en gang i fremtiden.
b) Fremoverhemmelighold støttes f.eks. når øktnøkler etableres med Diffie-Hellman (DH). Merk at den såkalte «private delnøkkelen» i DH ikke er det samme som en privat nøkkel som brukes til digital signatur eller for asymmetrisk dekryptering.
c) En sikkerhetsprotokoll som gir fremoverhemmelighold er f.eks. TLS (1.3)
d) I TLS 1.2 var DH bare en opsjon for nøkkeletablering, slik at TLS 1.2 ikke alltid støttet fremoverhemmelighold. SSL er en tidligere versjon av TLS som ikke støttet fremoverhemmelighold fordi hemmelig (frø-verdi for) øktnøkkel ble oversendt kryptert med tjeners offentlige nøkkel.

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.

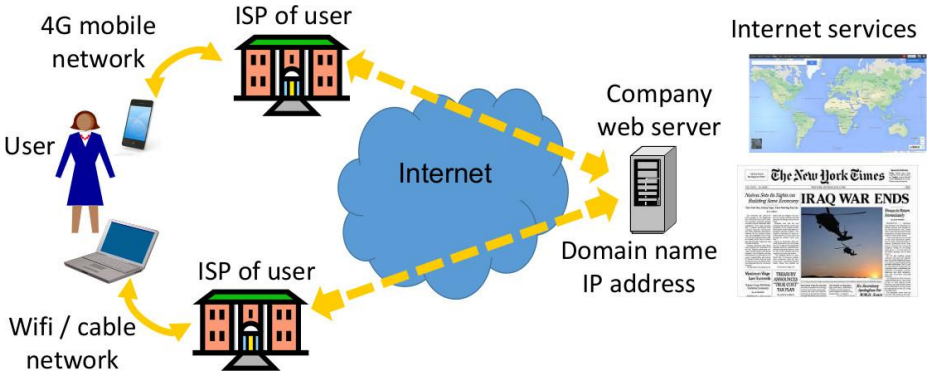
a) Hvilken IP-port er reservert for http over TLS? Hvilken URL-prefiks indikerer at en applikasjon bruker http over TLS?
b) Beskriv kort hvor i OSI og TCP/IP protokoll-lagene TLS opererer.
c) Forklar kort formålet med TLS Handshake-protokollen.
d) Nevn sikkerhetstjenestene som TLS Record-protokollen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

Svarforslag

e) Port 443 er reservert for TLS. «https» er prefikset for TLS/SSL-forbindelser.
f) TLS består av flere del-protokoller.
   - Record-protokollen ligger over TCP-protokollen.
   - Handshake-protokollen, Change Cipher Suite-protokollen, og Alert-protokollen ligger på samme lag som http-protokollen.
g) Handshake-protokollen: forhandler krypto-parametere, etablerer sesjonsnøkkel (øktnøkkel) og utfører server-autentisering (eventuelt også klient-autentisering).
h) Meldings-konfidensialitet og meldings-integritet
i) Krypto-algoritmene og nøkkelen som utveksles i Handshake-protokollen brukes av Record-protokollen for å beskytte dataene som overføres.

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.

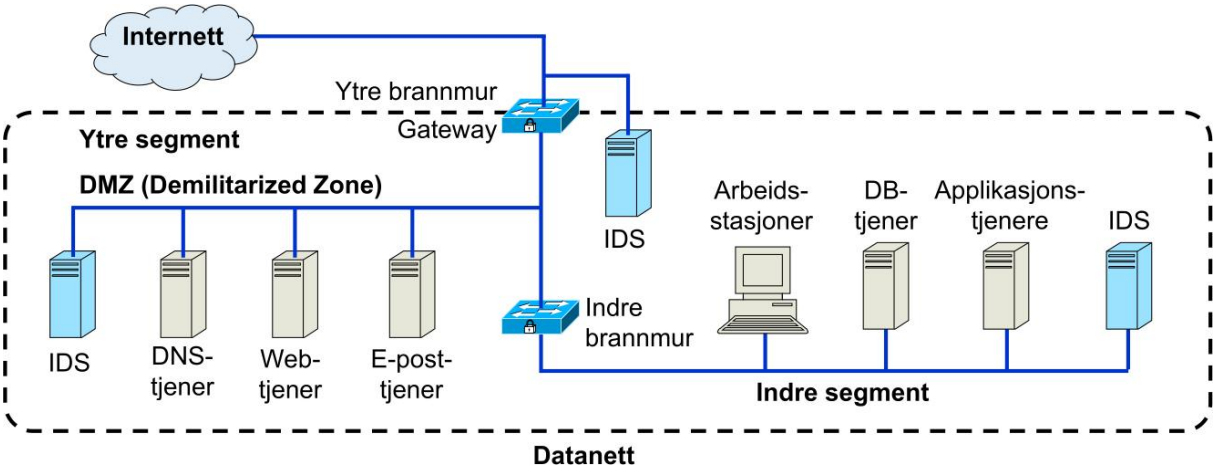


a) Når det brukes en sky-VPN, hvilke trafikkdata er skjult for brukerens ISP?
b) Når det brukes en sky-VPN, hvilke trafikkdata kan VPN-tilbyderen få tak i?
c) Når man bruker Tor, hvilke trafikkdata er skjult for brukerens ISP?
d) Når man bruker Tor, hvilke trafikkdata kan Tor acceess-serveren se?
e)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

Svarforslag

a) Brukerens ISP kan ikke se innholdet og kan ikke se den egentlige destinasjonens domenenavn / IP-adresse. ISP kan bare se at brukeren får tilgang til en sky-VPN.
b) VPN-tilbyderen kan se domenenavn / IP-adresse som brukeren aksesserer. Hvis det ikke brukes ende-til-ende-kryptering (https) kan VPN-tilbyderen også se innholdet. Med ende-til-ende-kryptering med TLS kan ikke VPN-tilbyderen se innholdet.
c) Samme som for sky-VPN. ISP kan se at brukeren får tilgang til en Tor-server.
d) Tor access-serveren ser ikke innholdet og kan ikke se destinasjonens nettadresse. Tor access-serveren kan bare se brukerens IP-adresse.
e) Å forhindre at ISP får vite at bruker går gjennom Tor kan gjøres ved å aksessere Tor gjennom en sky-VPN, men da vil VPN-tilbuderen se at Tor brukes.

Oppgave 7: Pakkefilter og inntrengingsdeteksjon



Med hensyn til figuren over.

a) Hva er en typisk sikker konfigurasjon (filterregler) for brannmurene?
b) Hvor er det fornuftig å plassere IDS for nettverks-inntrengingsdeteksjon (NIDS)? Forklar hvorfor.
c) Hva er hensikten med å plassere et IDS utenfor gatewayen, når det meste av angrepstrafikk likevel filtreres bort i gatewayen/ytre brannmur?

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) IDS kan plasseres utenfor gatewayen, i DMZ og i indre produksjonssegmenter. Det er nyttig å ha IDS utenfor gatewayen fordi all (skade)trafikk mot virksomheten er synlig slik at (mulige) angrep kan varsles selv om de kanskje stoppes i gateway-brannmuren. Det er nyttig å ha IDS i DMZ for å detektere angrep mot tjenester i DMZ. Det er nyttig å ha IDS i indre segmenter for å detektere angrep mot tjenester der. Generelt er det nyttig å ha IDS i ulike soner for å kunne detektere korrelasjon mellom angrepsaktiviteter, noe som gir bedre synlighet.

c) En god grunn til å plassere et IDS utenfor gatewayen er at det kan logge forsøk på angrep som filtreres bort, men som likevel kan korreleres med angrepstrafikk som detekteres i DMZ eller indre segmenter.