Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver

T8 (Del 9): Kommunikasjonssikkerhet

Oppgave 1: Sikkerhetsprotokoller

a. Hva er en sikkerhetsprotokoll, og hva kan slike brukes til?
b. Gi eksempler på sikkerhetstjenester 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: Fremoverhemmelighold (Forward Secrecy)

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

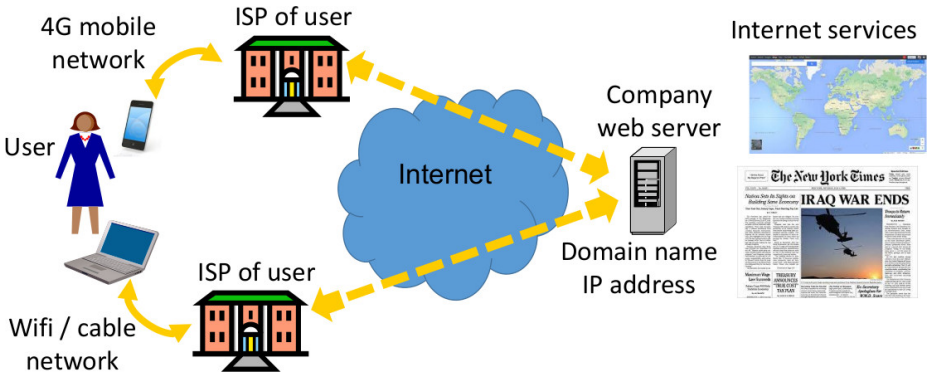
Oppgave 3: TLS

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 4: 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?