Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver med løsningsforslag

T8 (Del 9): Kommunikasjonssikkerhet

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: 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 tjeners private nøkkel) 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 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.

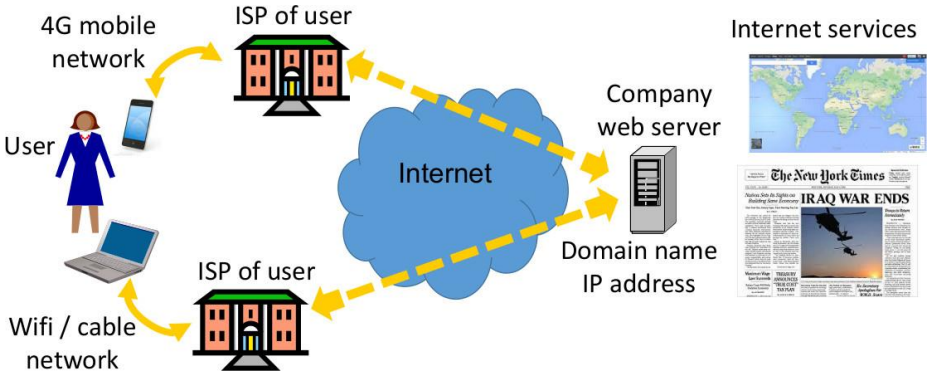
a) Hvilken IP-port er reservert for http over TLS? Hvilken URL-prefiks indikerer at en applikasjon bruker http over TLS?
b) Beskriv kort hvor i OSI og TCP/IP protokollagene TLS opererer.
c) Forklar kort formålet med TLS Handshake-protokollen.
d) Nevn sikkerhetstjenestene som TLS Record-protokollen støtter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

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 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?

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.