**Universitetet i Oslo**
**IN2120 Informasjonssikkerhet**
**Høst 2018**
**Workshop-spørsmål**


# *Forelesning 4: Kommunikasjonssikkerhet*

## Spørsmål 1

a) Hva er en sikkerhetsprotokoll, og hva brukes de til?
b) Gi eksempler på sikkerhetstjenester som støttes av sikkerhetsprotokoller.
c) Gi eksempler på velkjente sikkerhetsprotokoller som brukes på Internett.

## Spørsmål 2

TLS er en sikkerhetsprotokoll som brukes på Internett, men TLS består egentlig av flere separate del-protokoller.

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) Forklare 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?
f) I Handshake-protokollen kan klienten og serveren forhandle om hvilke Chiffer-suite som skal brukes. Hvorfor er denne forhandlingen nyttig? Hvorfor utgjør forhandlingen en potensiell sikkerhetsårbarhet?

## Spørsmål 3

TLS er potensielt sårbar for TLS stripping.

a) Hva gjør at nettsteder er sårbare for TLS-stripping?
b) Forklar kort hvordan TLS-stripping fungerer.
c) Hva betyr forkortelsen HSTS?
d) Hvordan kan HSTS forhindre TLS-stripping?
e) Hvordan mottar nettleseren HSTS-policyen for et nettsted?
f) Hvordan kan HSTS-policyer slettes fra nettleseren?
g) Bruk et verktøy for å sjekke TLS-konfigurasjon av servere, for eksempel https://www.ssllabs.com/ssltest/
   Sjekk din nettbank og andre nettsteder som bruker https for å få en sikkerhetsrapport om deres TLS-konfigurasjon.
h) Forklar hvordan det er mulig å lure folk til å tro at et falskt nettsted er deres virkelige nettbank, til tross for at forbindelsen bruker TLS og HSTS for sterk server-autentisering.

## Spørsmål 4

IPSec er en åpen standard for IP-nettverk (Internet Protocol).

a) Beskriv kort tre viktige fordeler ved å bruke IPSec.
b) Tre sikkerhetstjenester støttes av IPSec er: meldings-konfidensialitet, meldings-integritet og beskyttelse mot trafikkanalyse. Forklare hvilke mekanisme som brukes for å gi hver av disse tjenestene.
c) Beskriv kort de tre VPN-arkitekturene som hovedsakelig støttes av IPSec. Beskriv et typisk scenario for hver arkitektur.

## Spørsmål 5

ESP (Encapsulating Security Payload) er en IPSec-protokoll som kan kjøres i to modi: transportmodus og tunnelmodus.

a) Forklar den største forskjellen i pakke-prosessering mellom disse to modiene.
b) Beskriv kort den mest typiske scenario for ESP i tunnelmodus.
c) Beskriv kort et scenario for ESP i transportmodus.
d) Forklare kort de ekstra sikkerhetstjenestene som støttes ved å bruke ESP i tunnelmodus, i motsetning til å bruke ESP i transportmodus.

## Spørsmål 6

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?