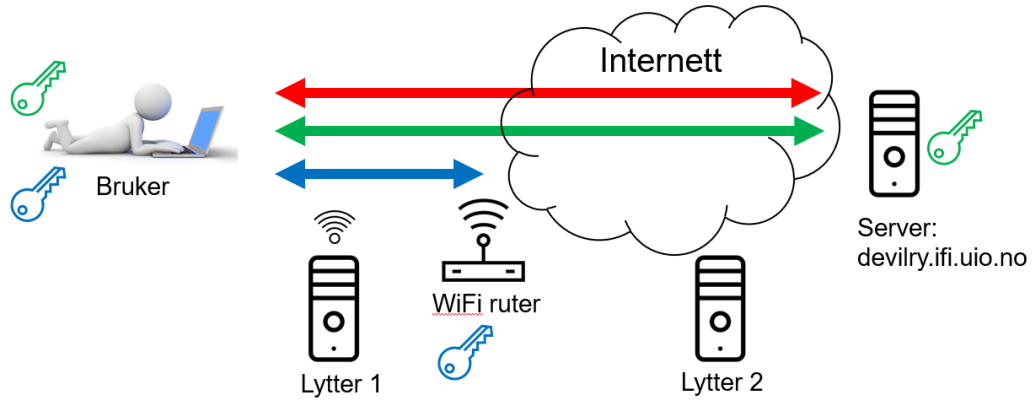
IN1020 - Datasikkerhet:
Øvingsoppgaver gruppetime 5 (uke 39)

1. Kommunikasjon i datanettverk



Rød = http-forbindelse
Grønn = https-forbindelse
Blå = Kryptert mellom bruker og WiFi-ruter

Figuren over illustrerer en bruker som aksesserer nettsiden devilry.ifi.uio.no på laptopen sin, der laptopen er koblet til et trådløst aksesspunkt (WiFi-ruter). I tillegg til bruker og server er det tre andre aktører (noder) i bildet: Lytter1, koblet på samme WiFi-ruter som Bruker, selve WiFi-ruteren, samt Lytter2, som er koblet på nettet et eller annet sted mellom WiFI-ruteren og Server.

Hvem av disse aktørene, i tillegg til Serveren, kan fange opp denne «samtalen» i klartekst i følgende tilfeller:

   (a) Usikret forbindelse mellom Bruker og WiFi-ruter, og http som protokoll mellom Bruker og Server.

   (b) Sikret (kryptert) forbindelse mellom Bruker og WiFi-ruter, http som protokoll mellom Bruker og Server

   (c) Usikret forbindelse mellom Bruker og WiFi-ruter, og https som protokoll mellom Bruker og Server.

   (d) Sikret (kryptert) forbindelse mellom Bruker og WiFi-ruter, https som protokoll mellom Bruker og Server

   (e) Spiller det noen rolle om man bruker sikker forbindelse til et trådløst aksesspunkt når man uansett bruker https som protokoll i kommunikasjonen?

2. Bruk av HTTPS som sikkerhetstiltak

   Hvordan beskytter bruk av https og digitale sertifikater i internettrafikk oss mot svindel og utnyttelse, og hva beskytter det evt. ikke mot?

3. Tjenestenektangrep er en form for angrep som gjerne forbindes med herverk og sabotasje, eller økonomisk kriminalitet i form av utpressing.

(a) Hvilke sikkerhetsmål påvirkes av denne type angrep?

(b) Hvilke ulike former for tjenestenektangrep benyttes ofte av hackere i dag?

(c) Hva kan virksomheter gjøre for å sikre seg mot denne typen angrep?

4. Eksamensoppgaver 3.5 og 3.6 fra eksamenssettet H22.

5. Eksamensoppgaver 12 og 13 fra eksamenssettet H20.

6. Case-oppgave:

   Til tross for at en webtjeneste for en nettbank er svært sikkert konfigurert, kan ting gå galt f.eks. når en bruker skal bruke (logge seg inn til) banken for å betale en regning. Diskuter mulige feil som kan oppstå (hint: brukerfeil, trådløst nett, etc).

7. Case-oppgave:

   I oppkobling mot en online webtjeneste autentiseres brukeren i starten av sesjonen. Data utveksles så med webtjeneren til og fra vedkommendes lokale maskin (endenode). Kan tjenestetilbyder på bakgrunn av brukerautentiseringen anta at data som mottas gjennom den etablerte forbindelsen er autentiske?