IN1020 – nettverkskommunikasjon og kryptografi

Øvingsoppgaver gruppetime 8 (uke 42)

Oppgave 1: Lagdeling i datakommunikasjon

1) Hvilke av lagene i TCP/IP-modellen kommuniserer kun ende-til-ende?
2) Hva er en MAC-adresse, og på hvilket lag brukes den?
3) Hvilke lag i nettverksstakken kan vi gjøre kryptering på, og hva er fordelen og ulempene med dette?

Oppgave 2: Nettverkslaget

1) IP'en til en maskin er gitt i CIDR-notasjon ved: 192.168.0.165/28
    a) Hva er IP-adressen med hver oktett notert binært?
    b) Hva blir nettverksmasken med hver oktett notert binært?
2) For å finne subnettadressen til maskinen må du gjøre en bitvis AND operasjon mellom IP-adressen og nettverksmasken.
    a) Hva blir subnettet til maskinen over i CIDR-notasjon?
    b) Hvor mange adresser er det i vertsdelen av dette subnettet?
3) For å finne kringkastingsadressen til et subnett, må du gjøre en bitvis OR-operasjon mellom maskinens IP-adresse og bit komplement (bitvis invers) av nettverksmasken.
    a) Hva er kringkastingsadressen til subnettet i oppgave 2 a)?

Oppgave 3: NAT og IPv6

1) Hva er NAT, og hvordan fungerer det?
2) Hva er hovedgrunnen til at man forøker å gå over til IPv6?
3) Hvorfor er det vanskelig å bytte IP-protokollen?

Oppgave 4: DHCP

1) Hva er DHCP, og hvorfor bruker man denne protokollen?
2) Hvorfor er det vanlig å «frigi» en IP-adresse utdelt med DHCP etter en viss tid?

Oppgave 5: Transportlaget

1) Hvilke tjenester tilbyr UDP?
2) Hvilke tjenester tilbyr TCP?
3) Hvorfor ønsker man noen ganger å bruke UDP til tross for at TCP tilbyr flere tjenester?

Oppgave 6: Praktisk anvendelse av kryptografi

a) I hvilke situasjoner og til hvilke formål kan kryptografi benyttes til å ivareta konfidensialitet til informasjon/data?
b) Hvilke andre sikkerhetsmål kan understøttes ved bruk av kryptografi? Forklar kort.
c) Bruker du kryptografi i hverdagen? Eller bruker du digitale tjenester der data eller kommunikasjon ikke er kryptert, som kanskje burde vært det? Identifiser og diskuter 😊

Oppgave 7: Nøkler og nøkkeldistribusjon

a) Hva er en kryptografisk nøkkel?
b) Nevn de tre hovedtypene av kryptografiske nøkler, og for hver av dem forklar kort hvilke *sikkerhetsmål* som er viktig å ivareta for å beskytte de ulike typene nøkler.
c) Beskriv kort hovedformålet med *offentlig-nøkkel sertifikater* og *offentlig-nøkkel infrastruktur* (*PKI)*, og hvilke utfordringer disse løser.

Oppgave 8: Symmetrisk kryptering

Som vi vet fungerer symmetrisk kryptering litt som en dagbok med en lås. Du bruker en nøkkel til å låse ned innholdet i dagboken og den samme nøkkelen brukes til å få tilgang til innholdet igjen.

Det finnes en myriade av forskjellige måter for hvordan utveksle data i dag. Noen er «fysiske» mens andre foregår trådløst. Tenk deg at du skal sende data som er kryptert symmetrisk via disse ulike kanalene. Diskuter hver av dem. Hvilke utfordringer byr de på og hvordan kan vi sørge for at ikke uvedkommende får tilgang til informasjonen?

a) Radio
b) CD/DVD
c) USB
d) E-post

Oppgave 9: Asymmetrisk kryptering

I asymmetrisk kryptering har man et nøkkelpar, der én nøkkel brukes til å kryptere og én brukes til å dekryptere melding. Som regel er en av disse hemmelige, mens den andre er offentlig. Hvem har den offentlige nøkkelen og hvem har den hemmelige nøkkelen i disse scenarioene?

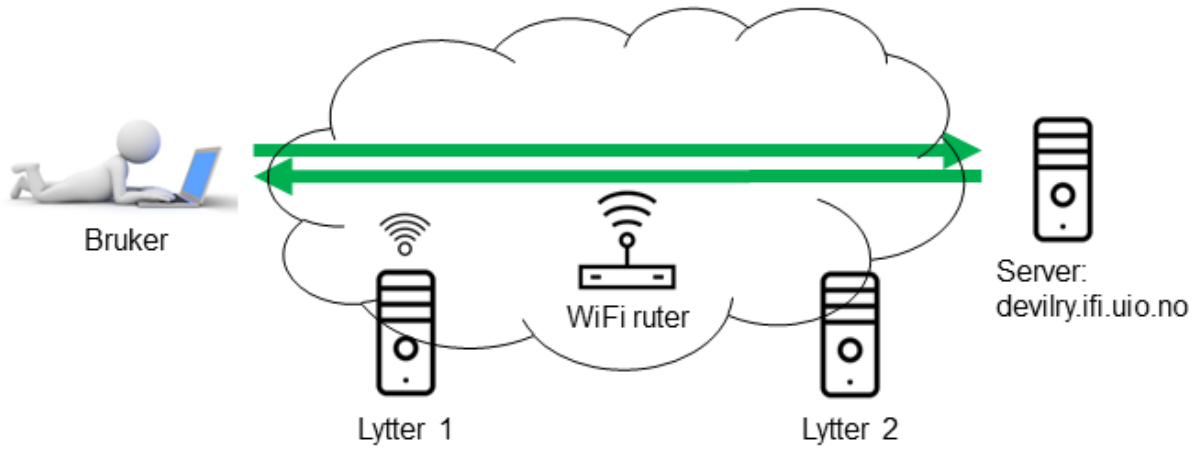
a) Du vil sende et hemmelig dokument til en kollega.
b) Du vil digitalt signere et dokument som skal oversendes kollegaen din.

Hvilke sikkerhetsmål blir ivaretatt i oppgave a og b?

Oppgave 10: Hash-algoritmer (sjekksumalgoritmer)

Hash-algoritmer (også omtalt som hash-funksjoner og sjekksumalgoritmer) gjør kryptering uten nøkler. Hva er de tre viktigste egenskapene til en god hash-algoritme?

Oppgave 11: Kommunikasjon i datanettverk



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?

Oppgave 12: Case-oppgave (Hash-kryptering/sjekksumalgoritme)

a) Du jobber som utvikler og teamet ditt er i ferd med å bygge en nettside. Besøkende på nettsiden kan registrere seg med e-post og lage et passord for å opprette en brukerprofil på siden. Teamet ditt har forstått at det er en dårlig idé å lagre passordene til brukerne i klartekst, så dere vil i stedet benytte en hash-algoritme for å kryptere passordene. Er dette en god idé? Hvilke svakheter kan dere identifisere med denne strategien?
b) Hvilke sikkerhetsmål er hash-algoritmer med på å ivareta når passord hashes som omtalt her?
c) For den interesserte: I forbindelse med hash-kryptering nevnes ofte «message-digest» eller «hash-digest». Hvorfor brukes dette som uttrykk?

Praktiske oppgaver:

Oppgave 13: Test av sjekksumalgoritmer – praktisk oppgave

Gjennomføres på Ifis linux-maskiner.

a) Programmet sha256sum genererer en sjekksum av en fil basert på algoritmen SHA256. Lag en liten tekstfil med innhold, kall den f.eks. abc.txt. Kjør så programmet sha256sum:
[kritisk@vestur]>sha256sum abc.txt
[6ee0c32c675ce6d3bd3f6e326c81e45b3d6675c29c0c9ced1398684a667804e9 abc.txt
Gjør endringer i fila abc.txt, og kjør programmet en gang til. Er nøkkelen den samme?
b) Hvordan kan sjekksumalgoritmer bidra til å sikre dataintegritet?
c) Finn og diskuter situasjoner/eksempler hvor bruk av sjekksumalgoritme kan være nyttig for deg.

Oppgave 14: Å bruke SSL Labs – praktisk oppgave

SSL Labs er et forskningssamarbeid som jobber for økt bevissthet rundt bruk av SSL. De tilbyr også en online-tjeneste for å teste nettlesere og web-tjenere med tanke på hvor godt (sikkert) SSL er implementert og konfigurert i den enkelte nettleser/tjener.

a) Bruk https://www.ssllabs.com/ for å sjekke nettleseren din. Nettleser på Ifi, bærbar PC, mobil, nettbrett, etc. Er den sårbar? Hvilke protokoller støtter den?
b) Bruk https://www.ssllabs.com/ for å sjekke kjente web-tjeneres sertifikat og konfigurasjon. Finner du sårbarheter? Kan du si noe om sertifikat, nøkkel samt protokoll(er) den enkelte tjener støtter?
c) Ta også en kikk på https://www.ssllabs.com/ssl-pulse/