IN1020: Øvingsoppgaver gruppetime 10 (uke 44)

Oppgave 1: Kryptografi

a) I hvilke situasjoner og til hvilke formål kan kryptografi benyttes til å beskytte informasjon?
b) Hvorfor er riktig administrasjon av kryptografiske nøkler så viktig?
c) Beskriv kort hovedformålet med PKI

Oppgave 2: Symmetrisk kryptering

Som vi vet fungerer symmetrisk kryptering litt som en dagbok med en lås. Du bruker en nøkkel til å låse bort 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 de byr på og hvordan dere vil sørget for at ikke uvedkommende får tilgang til informasjonen?

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

Oppgave 3: Asymmetrisk kryptering

I asymmetrisk kryptering har man et nøkkelpar, der én nøkkel brukes til å kryptere og én brukes til å dekryptere. 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 benytter digital signatur i et dokument du sender til en kollega.

Hvilke sikkerhetsmål blir ivaretatt i oppgave a og b?

Oppgave 4: Hash-kryptering (sjekksumalgoritme)

Hash-kryptering er kryptering uten nøkler.

a) I forbindelse med hash-kryptering nevnes ofte «message-digest» eller «hash-digest». Hvorfor brukes dette som uttrykk?
b) 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?

c) Hvilke sikkerhetsmål er hash-algoritmer med på å ivareta?

Oppgave 5: Sjekksumalgoritme (hash-funksjon)

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 6: SSL

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/

Oppgave 7: Lagdeling i datakommunikasjon

Kommunikasjonsmodellen vi bruker i Internett i dag er kjent som TCP/IP-modellen, og er det vi kaller en protokollstack.

a) Hvilke lag finner vi i TCP/IP-modellen?
b) Hva er oppgaven til de forskjellige lagene?
c) Hvilke av lagene i TCP/IP-modellen kommuniserer kun ende-til-ende?
d) Hvilke lag i nettverksstakken kan vi gjøre kryptering på, og hva er fordelen og ulempene med dette?

Oppgave 8: Nettverksprotokoller

a) Hvorfor trenger protokoller en header?
b) Hvordan blir header lagt til av de forskjellige lagene i en stack, og hva skjer på mottakersiden?