Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2018
Workshop-spørsmål

Forelesning 3: Nøkkelhåndtering og PKI

Spørsmål 1

a. Hvorfor er god håndtering av kryptografiske nøkler essensiell for styrken på kryptografi?
b. Tre viktige kategorier er: i) symmetriske hemmelige nøkler, II) asymmetriske offentlige nøkler og III) asymmetriske privatnøkler. Forklar hvilken type sikkerhet tjenester/beskyttelse (dvs. konfidensialitet, integritet og autentisitet) som kreves for hver nøkkelkategori.
c. Beskriv sikkerhetsmekanismer/metoder som kan brukes til å implementere den nødvendige sikkerhetstjenesten/beskyttelse for nøkler.
d. Gi en kort liste over de viktigste prosesser/trinn i nøkkelhåndtering.

Spørsmål 2

a. Forklar diagrammet for nøkkeltilstander og overganger mellom nøkkeltilstander, som illustrert i NIST SP800-57, figur 5, s. 85. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
b. Når en nøkkel er aktiv, kan den være angitt til bare å beskytte, bare prosessere eller begge deler. Ved å henvise til de 19 nøkkeltypene som er beskrevet i NIST SP800-57, oppgi to eksempler på nøkkeltyper som bare beskytter, to eksempler på nøkkeltyper bare prosesserer, og to eksempler på nøkkeltyper som både beskytter og prosesserer.
c. Forklar hvorfor nøkkeltypene 17, 18 og 19 er feilbetegnelser. Foreslå bedre navn for disse nøkkeltypene.

Spørsmål 3

a. Hvorfor er det viktig å ha en begrenset kryptoperiode for nøkler? Nevn minst fire grunner.
b. Hva er forskjellen mellom beskyttelse og prosessering ved bruk av nøkler?
c. Sammenlign anbefalt kryptoperiod for private og offentlige signaturnøkler ifølge NIST SP800-57? Vil du si at gyldighetsperioden av rotsertifikater i nettlesere følger anbefalingene fra NIST SP800-57?
d. Hvis man antar at kraftige kvantekomputere vil være praktisk tilgjengelig innen 2030, er gyldighetsperioden av rotsertifikater fornuftig?

Spørsmål 4

a. Hva er spoofing-problemet med hensyn til offentlige nøkler?
b. Forklar hvordan digitale sertifikater kan gi en løsning på spoofing-problemet.
c. Hvilke betingelser bør man sette for å ha tillit til et digitalt sertifikat? Begrunn ditt svar.
d. Er en digital signatur det samme som et offentlig-nøkkelsertifikat? Begrunn ditt svar.

Spørsmål 5

a. Beskriv tillitsmodellen for PKI'en som brukes av nettlesere.
b. Nevn fordeler og ulemper ved denne modellen.

Spørsmål 6

Tilgang til lagrede rotsertifikater i nettleseren din(e) er via nettlesermenyene. Se gjennom rotsertifikater som er installert i webleseren for å se deres utløpsdatoer.

a. Hvor mange rotsertifikater er installert? Variere for eksempel mellom Firefox og Chrome?
b. Hvilke sertifikater har kort levetid?
c. Kan du finne sertifikater med utløpsdato i overkant av ti år fra nå?
d. Kan du finne sertifikater som allerede har utløpt? Hva skjer når du inspiserer dem?

Spørsmål 7

Hva er forskjellen mellom et standard serversertifikat og EV-serversertifikat?

Spørsmål 8

a. Hvorfor er det nødvendig med revokering / tilbakekallelse av sertifikater?
b. Hvilke problem er løste med «must-staple protokollen»?

Spørsmål 9

a. Hvilket problem er løst med CA-autorisering og sertifikat-transparens?
b. Hvor lagres CA'ens autoriseringspolicy?
c. Hva må domene-eieren gjøre for å være viss på at på at sertifiseringspolicyen følges?
d. Hva må domene-eieren gjøre hvis det oppdages at sertifiseringspolicyen er brutt?