Seminar 12 (litt mer om kryptering)

Pensum

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/402082a5-e4c5-4466-8ac8-209239e02f2d/uke-45-kryptering-som-sikkerhetstiltak.pdf

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/17aa9992-4181-4916-b629-b8a73f649331/uke-45-systematisk-datasikkerhet.pdf

Kryptering som sikkerhetstiltak

- En kort repetisjon av sikkerhetsmål og sikkerhetstiltak
  - 6 mål (flesh out)
  - uendelige mange tiltak (flesh out)
- Hovedmål:
  - Sikre konfidensialitet og/eller integritet
  - Brukes også til autentisering av dataopprinnelse og for å oppnå uavviselighet
- Krypteringsformer:
  - Hash-algoritmer (enveis-kryptering, ikke reversbar)
  - Symmetrisk (én hemmelig delt nøkkel)
    - repetisjon
  - Asymmetrisk (nøkkelpar: offentlig + privat nøkkel)
    - repetisjon

    - husk at hvis det som krypteres er hemmelig, det må krypteres ved en offentlig nøkkel, sånn at kun eier av den private nøkkelen kan dekryptere den.
    - Det er vel ikke så smart å kryptere ting med sin private nøkkel - for alle kan se hva du skrev, siden den offentlige nøkkel er lett tilgjengelig på nettet.
      Du krypterer ting med sin privat nøkkel kun når du vil bruke den som digital signatur - et bevis for at det var du som sendte meldingen.
    - La oss si at Jehan og jeg har hver sin par av nøkkler - privat og offentlig.
      Hvis Jehan vil sende noe til meg sånn at kun jeg vet hva det er, hun skal ta min offentlige nøkkel og kryptere meldingen med den.
      Hvis jeg vil sende noe til Jehan som er også hemmelig, må jeg få tak i hennes offentlige nøkkel.
      En metafor med en ekte lås hjelper litt, fordi både privat og offentlig nøkkel kan brukes til å låse og åpne låsen - eller kryptere og dekryptere ting.
    - Du må aldri dele sin private nøkkel med noen. Dette er hele poenget med asymmetrisk kryptering.

Nøkkelutveksling og sertifikater

- Sertifikat brukes som bevis på at den offentlige nøkkel du fikk fra noen er ekte
- Et sertifikat består av den offentlige nøkkelen, samt en rekke attributer knyttet til nøkkelen:
  – Eier, gyldighetsperiode, utsteder, kryptoalgoritme brukt, nøkkelstørrelse, etc.
- Attributtene pakkes sammen og signeres av sertifikatutstederen

PKI - Public Key Infrastructure

- PKI er et rammeverk for utstedelse, administrasjon og bruk av digitale sertifikater med offentlige nøkler
- **Hovedformål**: Sikre ektheten av offentlige nøkler, samt forenkle nøkkeldistribusjonen.
- PKI må inneholde:
    - En policy for sertifikat-håndtering
    - Teknologi for å implementere policyen

    - Prosedyrer for hvordan håndtere og forvalte nøklene
    - Tillittsmodell for sertifikatene med offentlige nøkler
- Et god eksempel - BankID på mobil, der du har sin privat nøkkel lagret på sim-kortet
  (godt for både PKI og asymmetrisk kryptering)

Personopplysninger

- Personopplysninger er alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson.
- Den norske loven skiller mellom
    - Alminnelige personopplysninger
        - Navn, brukernavn, telefonnummer, studentnummer, adresse, IP-adresse, fingeravtrykk, adferdsmønster, …
        - Fødselsnummer (men kun når den er helt nødvendig)
    - Særlige kategorier personopplysninger
        - Helseopplysninger, seksuell legning, religion, straffedommer, etnisk opprinnelse,
          fagforeningsmedlemskap, …

Exam 2017

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/379155ee-af91-4494-96e4-1f3753b5906a/x2017-utenfasit.pdf

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/01144d5f-1fe4-48b2-bb80-5056088c8385/x2017.pdf

Ukeoppgaver

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/20c7d316-2bac-4fb2-b2e6-dd26738324f2/uke46-sikkerhet-oppgaver.pdf

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/eb1c0f53-91e1-4ab3-9a00-bc249aef643c/uke46-sikkerhet-losning.pdf