Velkommen!

Datasikkerhet: kryptering som sikkerhetstiltak og systematisk datasikkerhet

Gruppetime 12: 16. november 2021

(Hanne-)Kristin Schrøder Leiros

hkleiros@uio.no

Plan for dagen

- Repetisjon av ukas pensum
- Ukesoppgaver
  - 3 om kryptering
  - 2 case-oppgaver
  - 1 enkel trusselmodellering
  - 2 praktiske oppgaver
- Eksamensoppgaver
  - H2018 – datasikkerhet
- Ønsker til neste ukes repetisjonstime

Prøveeksamen publisert

Eksamen fra Høsten 2019 som vi hovedsakelig har jobbet med oppgaver fra

Tilgjengelig fram til 8. desember

https://uio.inspera.no/

Dagens læringsmål

Kryptering som sikkerhetstiltak:

- Symmetrisk kryptering og bruksområder
  - Hva kjennetegner symmetrisk kryptering
  - Hvordan kryptere data og melding(er)
- Asymmetrisk kryptering og oversikt over bruksområder og utfordringer:
  - Hva kjennetegner asymmetrisk kryptering
  - Bruksområder, hvordan:
    - Kryptering av data og melding(er)
    - Digital signatur
  - Hvorfor vi trenger sertifikater og Offentlig nøkkel-infrastruktur (PKI)

Dagens læringsmål

- Kjenne til hovedprinsipper i EUs personvernforordning gjennomgått på forelesning.
- Forstå sammenhengen mellom personvernregelverk og krav til informasjonssikkerhet.
- Kjenne til sikkerhetsutfordringer knyttet til tjenesteutsetting.
- Vite hva trusselmodellering og risikoanalyse innebærer, samt nytten av gjennomføring
- Forstå viktigheten av at datasikkerhet er en integrert del av en virksomhets styring.
- Forstå at datasikkerhet og sikring av verdier og ressurser er en kontinuerlig prosess.

Kryptering som sikkerhetstiltak

Kryptering

- Sikre konfidensialitet og/eller integritet
- Brukes også til autentisering av dataopprinnelse og for å oppnå uavviselighet

- Hash-algoritmer – enveiskryptering (sjekksum algoritmer)
- Symmetrisk kryptering – én hemmelig delt nøkkel
- Asymmetrisk kryptering – nøkkelpar: offentlig og privat nøkkel

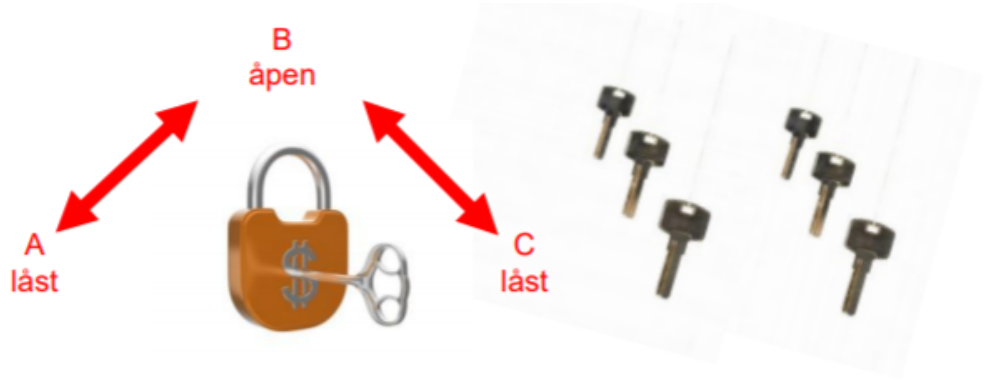
Symmetrisk kryptering

- To kopier av samme nøkkel
  - Nøkkelen kan både «låse» og «låse opp» meldingen
- Anvendes til kryptering av data, kryptering av meldinger

- **Hvilke sikkerhetsmål kan ivaretas?**
  - Konfidensialitet? **JA**
  - Integritet? I praksis **JA**
  - Autentisering av dataopprinnelse? **JA**
  - Uavviselighet? **NEI**

- Farer: Nøkkel på avveie, nøkkel tapt

Asymmetrisk kryptering

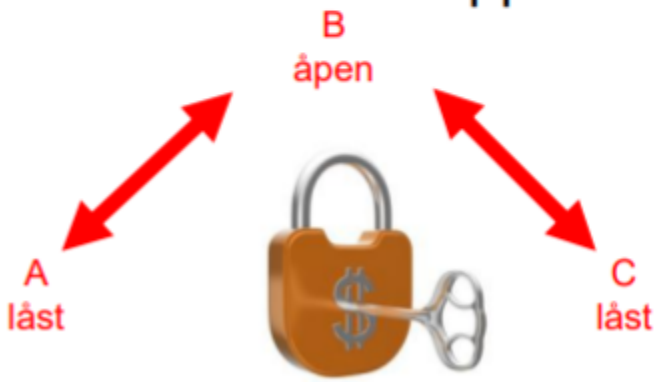


- Håkon har nok en boks med lås, men denne låsen er spesiell.
- Den har to ulike nøkler:
  - Én som kun kan vris **med** klokken (fra A til B til C)
  - Én som kun kan vris **mot** klokken (fra C til B til A)
- Den første nøkkelen holder Håkon for seg selv. Vi kaller denne Håkons «private nøkkel»
- Den andre nøkkelen kopierer Håkon i mange eksemplarer og deler ut til alle som vil ha. Dette er Håkons «offentlige nøkkel».

Asymmetrisk kryptering, scenario 1

Du vil overrekke Håkon et privat, «hemmelig», dokument:

1. Du putter brevet i boksen til Håkon (som er åpen).
2. Du låser boksen med din versjon av nøkkelen, dvs. en kopi av den *offentlige nøkkelen*, som du har fått av Håkon. Din nøkkel kan kun brukes *mot klokken*, så du låser til posisjon A.
3. Boksen er nå låst, og sendes Håkon!
4. Den eneste som kan låse opp boksen er nå Håkon, innehaveren av det vi kalte den *private nøkkelen*. Dette er den eneste nøkkelen som kan låse opp boksen *med klokken* til B.
5. Voilá!



Oppsummering asymetrisk kryptering for meldingsutveksling:

- Sender benytter mottagers offentlige nøkkel for å kryptere en melding. Mottager benytter sin private nøkkel til å dekryptere meldingen.
- Anvendes til trygg overføring av data/meldinger

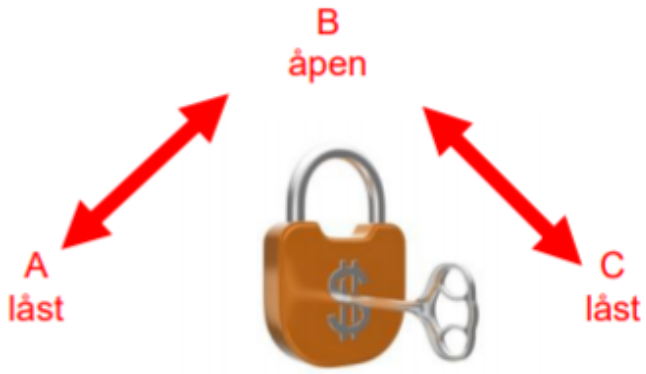
- **Hvilke sikkerhetsmål kan ivaretas?**
  - Konfidensialitet? **JA**
  - Integritet? I praksis **JA**
  - Autentisering av dataopprinnelse? **NEI**
  - Uavviselighet? **NEI**

Asymmetrisk kryptering, scenario 2

Noen overleverer deg med boksen og sier den er fra Håkon

1. Javel?
2. Ok, jeg har jo en kopi av Håkons offentlige nøkkel, så jeg finner den fram og forsøker å låse opp.
3. Vet at nøkkelen skal brukes mot klokken, forsøker dette.
4. Boksen går opp!
5. Hm, det kan jo bare betyr én ting: Boksen må være låst med Håkons private nøkkel, og innholdet må komme fra ham…

Dette kalles *digital signatur.*



Asymmetrisk kryptering for digital signering:

- Sender krypterer (og dermed signerer) en melding med sin private nøkkel. Mottager dekrypterer meldingen med senders offentlige nøkkel.
- Anvendes for å ivareta tillitt til at data/meldinger kommer fra en hevdet mottager.

- **Hvilke sikkerhetsmål kan ivaretas?**
  - Konfidensialitet? **NEI**
  - Integritet? I praksis **JA**
  - Autentisering av dataopprinnelse? **JA**
  - Uavviselighet? **JA**

- Farer: Nøkkel på avveie, falske nøkler

Krypteringsnøkler



- **Styrken i kryptografisk sikkerhet** avhenger av
  - Størrelsen/lengden på nøkkelen.
  - Håndtering og beskyttelse av nøklene.
  - Styrken i den kryptografiske algoritmen.

- **God nøkkelhåndtering** er basisen for trygg generering, lagring, distribusjon og destruksjon av nøkler.

Nøkkelutveksling og sertifikater

- Utfordring: Hvordan stole på at en offentlig nøkkel er ekte?
  Løsning: *Et sertifikat* som følger den offentlige nøkkelen knytter sammen nøkkel og en identitet.
- Neste utfordring: Hvordan stole på at sertifikatet er ekte?
  Løsning: *Sertifikatet* utstedes av en betrodd virksomhet (sertifikat-myndighet - CA), som går god for at nøklene er autentiske – altså *tilhører identiteten den utgir seg for å tilhøre*.

Men hva er et sertifikat?



- 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 = vi har et sertifikat

(En standard for sertifikater er såkalt X.509)

PKI – publick key infrastructure

- Rammeverk for utstedelse, administrasjon og bruk av digitale sertifikater med offentlige nøkler
- Skal sikre ekteheten av offentlige nøkler, samt forenkle nøkkel-distribusjon
- PKI må inneholde
  - En policy for sertifikathåndtering
  - Teknologi for å implementere policyen
  - Prosedyrer for hvordan håndtere og forvalte nøklene
  - Tillittsmodell for sertifikatene med offentlige nøkler

Hvordan fungerer en PKI?

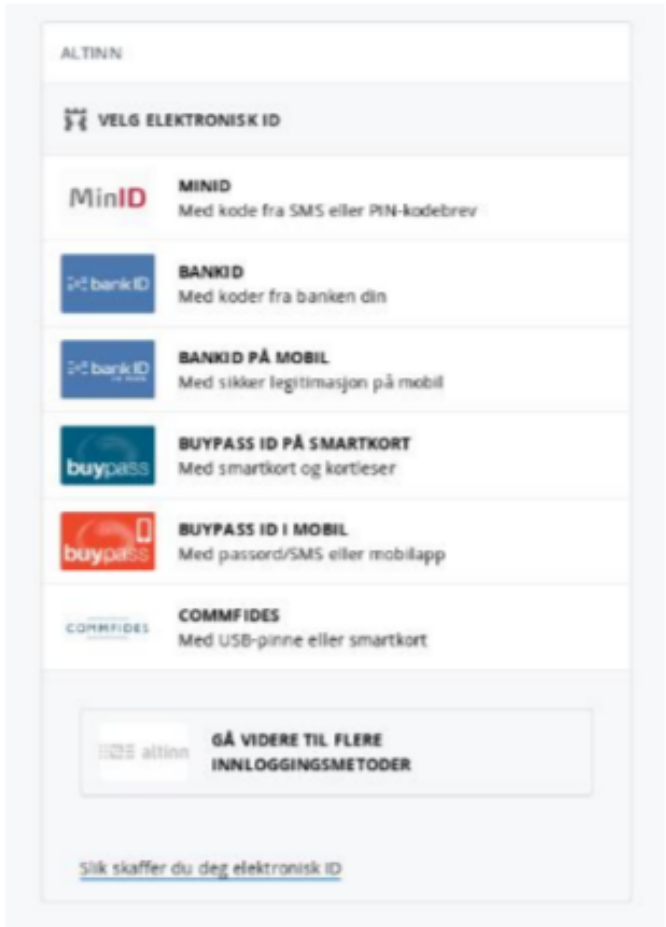
- Hver eneste offentlige nøkkel bakes inn i hvert sitt elektroniske sertifikat som knytter nøkkel og identitet sammen
- Et sertifikat utstedes av en Certificate Authority som går god for den offentlige nøkkelens ekthet
- Den tilhørende private nøkkelen kan oppbevares på en datamaskin, på SIM-kort, på et smartkort, i banken etc.
- Sertifikatene med de offentlige nøklene gjøres tilgjengelig for alle mottagere som skal kryptere og dekryptere meldinger.

Eksempler på PKI-er i bruk

- Sikker kommunikasjon i helsevesenet:
  - eResept, elektronisk sykemelding, etc
  - Knytter melding til individ (signatur med personlig sertifikat for lege) og sikre konfidensialitet (kryptering av forsendelse).

- Publikumsrettede PKIer i Norge:
  - MinID (offentlig), BankID, Buypass, Commfides (private)
  - Difi tilbyr ID-porten, en felles infrastruktur for innlogging til offentlige tjenester, basert på ovenfornevnte.

- Web PKI eller Browser PKI
  - Nettlesere kjenner den offentlige nøkkelen til alle betrodde sertifikatutstedere (CA), og bruker denne til å forsikre seg om at sertifikatet er gyldig.



EUs personvernforordning

- Alminnelige personopplysninger og særskilte personopplysninger
- Virkeområde: EØS samt virksomheter som tilbyr varer og tjenester til EØS-borgere
- Prinsipper:
  - Lovlighet, rettferdighet og åpenhet
  - Formålsbegrensning
  - Dataminimering
  - Riktighet
  - Lagringsbegrensning
  - Integritet og konfidensialitet
- Definerte roller
  - Behandlingsansvarlig
  - Databehandler
- Krav til innebygd personvern

Innebygd personvern

- Sørge for at programvaresystemene vi bruker oppfyllerpersonvernsprinsippene
- Ta hensyns til personvern i alle utviklingsfaser av et system eller en løsning
- Det minst personverninngripende alternativet skal være standarden i alle systemer og løsninger
  - Mengden personopplysninger
  - Omfang av behandling
  - Lagringstid
  - Tilgjengelighet

Innebygd informasjonssikkerhet

- Betyr at det tas ekspilisitt hensyn til informasjonssikkerhet i hele livssyklusen til programvare og applikasjoner
- 7 faser:
  - Opplæring
  - Krav
  - Design
  - Koding
  - Test
  - Produksjonssetting
  - Forvaltning

Tjenesteutsetting

- Data lagret i «skyen» er faktisk lagret på et datamaskin som andre eier
- Tjenesteustetting: å sette ut en eller flere funksjoner til andre leverandører:
  - På eget datautstyr, hos leverandør, kombinasjon
- Skytjenester innebærer å få tilgang til et sett med dataressurser
  - Blir levert etter behov
  - Rask anskaffelse og tilgjengelighet
  - Betaler kyn for ressursene man bruker
  - Vet vi **hvor** «skyen» befinner seg
- Fordeler:
  - Redusere driftskostnader
  - Tilgang uavhengig av okalsituasjon
- Dersom en viksomhet ønsker å benytte skytjenester til bhenading av personopplysninger, er virksomheten juridisk ansvarlig for at personopplysningene prosesseres og lagres i samsvar med personvernregelverket

Sikkerhetsutfordringer knyttet til tjenesteutsetting

Trusselmodellering

- Trusselmodellering er en prosess der man systematisk gjennomgår sikkerheten for et IT-system og:
  - Identifiserer potensiell trusler
  - Evaluerer konsekvensen assosiert med hvert område
- Mål:
  - Tidlig håndtering av sikkerhetsproblemer
  - Gjøre bedre sikkerhetsvurderinger
  - Mer effektiv sikkerhetstesting
- Ulike innfallsvinkler:
  - Fokus på trusselaktør
  - Fokus på system
  - Fokus på verdi

Risikoanalyse

- Risiko involverer konsekvens, gjerne målt i kroner og øre
- Flere definisjoner av risiko, men:
  - «Risiko er et produkt av sannsynlighet for hendelse og kostnad/tap knyttet til hendelsen»
- Hvor skal innsatsen legges?
  - Usannsynlig hendelse som medfører store tap?
  - Sannsynlige hendelser som har lavere kostnad?

Administrative sikkerhetstiltak

Hvorfor går det galt?

- Sikkerhet nedprioriteres
- Ingen lang fagtradisjon
- Komplekse systemer
- Evig kappløp
- Lite åpenhet om feil

Hvilke tiltak kan gjøres?

- Internkontroll / LSIS
- Policyer / Standarder
- Prosedyrer og praksis
- Bevissthetstrening
- Sikkerhetsøvelser
- Håndtere hendelser

Styringssystem for sikkerhet

*«**Sikkerhetsstyring** er systematiske aktiviteter for å oppnå og opprettholde et sikkerhetsnivå i overensstemmelse med de mål og krav en organisasjon har satt seg»*

- Informasjonssikkerhet må inkluderes i virksomhetsstyringen
- Eksempel: NSMs styringshjul for informasjonssikkerhet



God informasjonsjonssikkerhet koster men er på sikt lønnsomt

- Kompetanse og bevissthet
- Styring og kontroll
- Drift og vedlikehold
- Tjenesteutsetting
- Sikkerhetstiltak

- Sikkerhet må prioriteres av ledelse og styret i en virksomhet

- Beskytte ressurser = skape verdi:
  - Tillitt
  - Rykte, merkevare
  - Konkurransefortrinn
  - Forebygge og redusere tap
  - Skape robusthet og sikre kontinuitet
  - Øker selskapets verdi

Tidligere eksamensoppgaver

IN1020 eksamen høst 2018

4(f) Trusselmodellering

For enkelhets skyld benytter en liten gruppe ansatte i en underavdeling i Forsvarsdepartementet en og samme brukeridentitet og passord for å autentisere seg i et saksbehandlingssystem.

Denne gruppen ansatte har en superbrukerrolle i saksbehendlingssystemet, som medfører utvidede privilegier sammenlignet med en ordinær ansatt i departementet. Blant annet har de privilegier til å både endre og slette *alle* lagrede dokumenter og saker.

IN1020 eksamen høst 2018

4(e) Asymmetrisk kryptering og nøkkelutveksling

Erna og Siv er midt i budsjettforhandlingene, og samarbeider om en rekke digitale dokumenter. De har nylig vært på kurs i informasjonssikkerhet, og har lært om blant annet asymmetrisk kryptering (offentlig-nøkkel-kryptering). De er enige om å benytte dette for sikker dokumentutveksling, og de har fått hvert sitt nøkkelsett bestående av privat og offentlig nøkkel.

Ønsker til repetisjonstimen?