

UiO : Institutt for informatikk

Datateknologi og sikkerhet

IN1020 – Introduksjon til datateknologi

Temavideo 1 uke 2: Autentisitet og autentisering

Kristin Skar
kritisk@ifi.uio.no

Nødvendighet av autentisitet

- Hvor stor tillitt har du til at
  - en *bruker (person)* er autentisk?
  - en *organisasjon* er autentisk?
  - et *(data)system er* autentisk?
  - *opprinnelsen til data* (ofte kalt en melding) er autentisk?

Identifisering

Å gi seg til kjenne, etablere identitet for hvem/hva noen/noe er.

- **Identitet**: Den eller det noen eller noe er.
- **Identifikator**:
  - Svært ofte kjent, dvs. ikke hemmelig. Navn, brukernavn, fødselsnummer, epost-adresse, IP-adresse, IMEI, registreringsskilt for bil, osv.
  - Ønsker som regel entydig idenifikator.
  - Utfordring: Hvordan vet man at en identifikator er ekte?

Autentisering

Å bekrefte en hevdet identitet.

Former for autentisering:

- Organisasjonsautentisering (*organization authentication*)
- Systemautentisering (*system authentication*)
- Autentisering av dataopprinnelse (*data-origin authentication/ message authentication*)
- Brukerautentisering (*user authentication*)

Organisasjonsautentisering

Å verifisere at en *virksomhet/organisasjon* er ekte, altså den den utgir seg for å være, i en online interaksjon.

- Hvordan oppnås *organisasjonsautentisitet*?
  Svar: Bruk av kryptografi



Systemautentisering

Å verifisere at et *datasystem* er det det utgir seg for å være.

- Hvordan oppnås *systemautentisitet*?
  Svar: Bruk av kryptografi



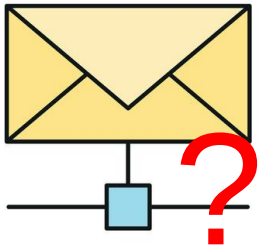
Autentisering av dataopprinnelse

Å verifisere at meldingen/data man mottar kommer fra en hevdet sender

og

at innholdet er ikke endret underveis i forsendelsen.

- Hvordan oppnå *dataautentisitet*?
  Svar: Bruk av kryptografi



Brukerautentisering

Å verifiserer en hevdet identitet for en bruker som ber om å aksessere et system eller et program.

- Hvordan oppnå *brukerautentisitet* (også kalt *personautentisitet*)?
  Svar: Bruk av autentiseringsfaktorer



Brukerautentisering: Autentiseringsfaktorer

- Tre hovedkategorier *bevismateriale* (autentiseringsfaktor) for identitet:
  - Noe du vet, noe du har og/eller noe du er
- I tillegg:
  - Andre mekanismer, som SMS eller e-post til en *kanal* du har kontroll over
  - Kombinasjon av flere

"Always remember the three main authentication factors: what can be easily guessed, what can be left in a cab, and what can be chopped off"

Autentiseringsfaktor: Noe du vet

Cons and pros:

Fordel:

- Du har det alltid med deg

Ulempe:

- Lett å glemme
- Lett å gjette for uvedkommende
- Lagres på datamaskin? Nedskrevet?
- Lagres hos tjenesteleverandør

Noe du vet:

- Passord til IT-system
- Kode til elektronisk dørlås

Autentiseringsfaktor: Noe du har

Cons and pros:

Fordel:

- Du slipper å huske

Ulempe:

- Lett å miste
- Kan stjeles/«lånes»

Noe du har:

- Nøkkel til lås
- Engangspassord fra *kodegenerator*
- SIM-kort
- Kontaktløse brikker (RFID-kort)

Autentiseringsfaktor: Noe du er

Cons and pros:

Fordel:

- Du slipper å huske
- Du har det alltid med deg

Ulempe:

- Unikt nok?
- Permanent nok?
- Sikkert nok?
- Krever ekstrautstyr (sensorer, lesere, ol)
- Ressurskrevende å sammenligne

Noe du er:

- Ansiktsgjenkjenning
- Fingeravtrykk
- Scanning av øyet
- Signatur
- Ganglag

Flerfaktor-autentisering

Utfordring: Passord kan gjettes, objekter kan mistes/stjeles.

Løsning: Autentisering med flere faktorer

- Kombinasjon av to eller flere ulike faktorer
- Øker sikkerheten betydelig, men autentisering blir mer tungvint for den som skal autentisere seg.
- Økende antall tjenester tilbyr to-faktor-autentisering, mens svært kritiske systemer også benytter seg av kombinasjoner med ennå flere.

Oppfordring: Bruk to-faktor-autentisering der det er tilgjengelig.

Autentiseringsløsning som tjeneste

Aktører tilbyr elektronisk identitet og autentisering som en tjeneste.

- Eksempler:
  - Feide, Google, Facebook, BankID, MinID
- Fordeler
  - God kompetanse, ekspertise og dermed økt sikkerhet i tjenesten som tilbys
  - Brukerne må forholde seg til færre brukeridentiteter/passord
- Ulemper
  - Knekkes autentiseringsfaktoren(e) vil hackere ha tilgang til flere tjenester som deg.
  - Vane å logge inn gjør oss til et enkelt mål for svindel.

Takk for i dag!

mn.uio.no/ifi

