



Datateknologi og sikkerhet

IN1020 – Introduksjon til datateknologi

19.10.2022

● *Kristin Skar*
● *kritisk@ifi.uio.no*

Obligatorisk oppgave nr. 3 IN1020



Opgavetekst finner dere her:

<https://www.uio.no/studier/emner/matnat/ifi/IN1020/h22/obligatoriske-innleveringer/>



Leveres i Devilry: <https://devilry.ifi.uio.no/> innen **torsdag 3. november kl. 23:59.**



Opgaven skal gjøres og leveres individuelt.



Sykdom og utsatt innlevering? Se IFIs oblig-reglement:

<https://www.uio.no/studier/eksamen/obligatoriske-aktiviteter/mn-ifi-obliger-retningslinjer.html>



Om innleveringen:

- Oppgaven leveres som én fil, med navn og brukernavn godt synlig
- Skriv kort og konsist, max 1500 ord pleier være nok
- Filformatet **skal** være pdf

Så langt, så vel

- ✓ Intro til sikkerhet
- ✓ Sikkerhetsmål
- ✓ Sikkerhetstiltak
- ✓ Autentisitet og autentisering
- ✓ Tilgangskontroll
- ✓ Trygg lagring
- ✓ Nettverkssikkerhet

Autentisering

- Autentisering bekrefter en hevdet identitet:
 - ✓ Autentisk bruker (person) - *brukerautentisering*
 - ✓ Autentisk organisasjon - *organisasjonsautentisering*
 - ✓ Autentisk (data)system - *systemautentisering*
 - ✓ Autentisk data-opprinnelse - *dataautentisering*

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

- Passord til IT-system
- Kode til elektronisk dørlås

Fordel:

- Du har det alltid med deg

Ulempe:

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

Autentiseringsfaktor: Noe du har

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

Fordel:

- Du slipper å huske

Ulempe:

- Lett å miste
- Kan stjeles/«lånes»

Autentiseringsfaktor: Noe du er

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

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

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 (2FA), mens svært kritiske systemer også benytter seg av kombinasjoner med ennå flere faktorer.

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
- 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.

123456
Password
12345678
qwerty
12345
123456789
letmein
1234567
football
Iloveyou
admin
monkey
welcome
login
abc123
starwars
123123
dragon
passw0rd
master

Hvordan knekkes koder/passord?

“1,4 milliarder passord lekket i søkbar database – en rekke profilerte nordmenn er rammet”

- Passord lagres kryptert
- Likevel kan de «knekkes»:
 - Intelligent søk. Kunnskap om deg?
 - Systematisk gjetting (*brute-force*) og «ordlisteangrep»
 - Utnytte svakheter i datasystemene
- <https://haveibeenpwned.com/>
- <http://lastbit.com/pswcalc.asp>

Elektronisk identitet

«E-postkontoen er navet i ditt digitale liv»



Refleksjon:

Betyr det at du *har tilgang til en ressurs* at du også er *autorisert* til ressursen?



Eksamensoppgave 1

Sikkerhetsmål

Sikkerhetsmål er et sentralt begrep innen informasjonssikkerhet. Hvilke av følgende definerer vi som sikkerhetsmål i IN1020:

Velg ett eller flere alternativer

- Integritet
- Data-autentisitet
- Orm
- Autorisering
- Brannmur

Eksamensoppgave 2

Konfidensialitet

Konfidensialitet er et sentralt krav i norsk personvernlovgivning. Hvilke av følgende sikkerhetstiltak kan sørge for konfidensialitet for persondata i et IT-system:

Velg ett eller flere alternativer

- Kryptere alle data som lagres
- Identifisere alle brukere av IT-systemet
- Sikkerhetskopiere alle data
- Innføre tilgangskontroll til IT-systemet
- Ha gode rutiner for gjenoppretting av data

Tilgang, logging og sporbarhet

- ✓ Loggføring av hendelser er bidrag til sporbarhet.
- ✓ Kan loggføring av hendelser ha flere funksjoner?





Refleksjon:

**Har all informasjon samme
beskyttelsesbehov?**



Å planlegge for katastrofe

- Sikkerhetskopier
- Redundante systemer



Lenkesamling (ikke pensum)

- UiOs veiledning for dataklassifisering:
<https://www.uio.no/tjenester/it/sikkerhet/isis/tillegg/infoklasser.html>
- UiOs lagringsguide for informasjon:
<https://www.uio.no/tjenester/it/sikkerhet/isis/tillegg/lagringsguide.html>
- Alt kan hackes, anbefalt TED-talk:
https://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked



Læringsmål etter 19.10.22

- Forstå sikkerhetsmålet *autentisitet*, kjenne til de ulike formene for *autentisering*, samt styrker og svakheter ved ulike *autentiseringsfaktorer*.
- *Tilgangskontroll*: Forstå hvordan tilgangskontroll fungerer, og hva som oppnås.
- Kjenne til sikkerhetstrusler og sikkerhetstiltak knyttet til *lagring av informasjon*.
- Kjenne til vanlige sikkerhetstrusler og sikkerhetstiltak i datanettverk, knyttet til:
 - *Nettverkskommunikasjon*, både trådløs og over kablede nett, og
 - *Skallforsvar*
- Ha god forståelse for hvordan sikkerhetstiltak nevnt så langt direkte påvirker oppnåelse av de ulike sikkerhetsmålene.



UiO • Institutt for informatikk

Takk for i dag!

mn.uio.no/ifi

