

UiO : Institutt for informatikk

Datateknologi og sikkerhet

IN1020 – Introduksjon til datateknologi

02.09.2021

Kristin Skar
kritisk@ifi.uio.no

Obligatorisk oppgave nr. 1 IN1020

Oppgavetekst finner dere her:
https://www.uio.no/studier/emner/matnat/ifi/IN1020/h21/obligatoriske-innleveringer/

Leveres i Devilry: https://devilry.ifi.uio.no/ innen **Onsdag 15. september kl. 23:59.**

Oppgaven skal gjøres og leveres individuelt.

Har du oppgaven godkjent fra 2020 eller 2019 er det ikke nødvendig å levere den på nytt.

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
- Innleveringen bør ikke være på mer enn ca. 1000 ord
- Filformatet **skal** være pdf

Læringsmål etter 02.09.21

- 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 sikkerhetstrusler og sikkerhetstiltak i datanettverk, knyttet til:
  - *Nettverkskommunikasjon*, både trådløs og over kablede nett
  - *Skallforsvar*
- Ha god forståelse for hvordan sikkerhetstiltak direkte påvirker oppnåelse av de ulike sikkerhetsmålene.

Eksamensoppgave 1! ☺

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	Nei, *bare* identifisering er ikke til hjelp. Hvem som helst kan jo identifiseres.
☐ Sikkerhetskopiere alle data	Nei, sikkerhetskopiering bidrar til gjenoppretting, men ikke konfidensialitet.
☒ Innføre tilgangskontroll til IT-systemet	
☐ Ha gode rutiner for gjenoppretting av data	Nei, dette bidrar til gjenoppretting, men ikke konfidensialitet.

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

«Epost-kontoen er navet i ditt digitale liv»

Å planlegge for katastrofe

- Sikkerhetskopier
- Redundante systemer





Refleksjon:

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

Tilgang, logging og sporbarhet



LOGGING AV HENDELSER SOM BIDRAG TIL SPORBARHET



KAN LOGGING AV HENDELSER HA FLERE FUNKSJONER?



Refleksjon:

Har all informasjon samme beskyttelsesbehov?

Eksamensoppgave 2! ☺

Sikkerhetsmål

Sikkerhetsmål er et sentralt begrep innen informasjonssikkerhet. Hvilke av følgende defineres som sikkerhetsmål:
Velg ett eller flere alternativer

☒ Integritet	
☒ Data-autentisitet	
☐ Orm	Nei, *en orm* er en form for skadelig programvare (undervises senere i IN1020).
☐ Autorisering	Nei, autorisering er en policy for hvem eller hvilke roller som skal ha tilgang til hvilke ressurser.
☐ Brannmur	Nei, en brannmur er en komponent i et nettverk som fungerer som en *tilgangskontroll* for nettverket.

Lenkesamling (ikke pensum)

- UiOs veiledning for dataklassifisering:
  https://www.uio.no/tjenester/it/sikkerhet/lsis/tillegg/infoklasser.html
- UiOs lagringsguide for informasjon:
  https://www.uio.no/tjenester/it/sikkerhet/lsis/tillegg/lagringsguide.html

- Alt kan hackes, anbefalt TED-talk:
  https://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked



Bitt av basillen?

- Institutt for informatikk:
  - IN1030: Systemer, krav og konsekvenser (vår)
  - IN2100: Logikk for systemanalyse (vår)
  - IN2120: Informasjonssikkerhet (høst)
  - IN3210: Network and Communications Security (høst)
  - IN5130: Uangripelige IT-systemer (høst)
  - IN5280: Security by Design (vår)
  - IN5290: Ethical Hacking (høst)

- Institutt for teknologisystemer (Kjeller):
  - TEK4500: Innføring i kryptografi (høst)
  - TEK5510: Sikkerhet i operativsystemer og programvare (høst)
  - TEK5520 – Cybersikkerhet i industrielle systemer (høst)
  - TEK5530 – Målbar sikkerhet for tingenes internet (høst)

Takk for i dag!

mn.uio.no/ifi

