

i Informasjon om eksamen



UiO : Institutt for informatikk

Det matematisk-naturvitenskapelige fakultet

Avsluttende eksamen i IN2120 Informasjonssikkerhet (Høst 2022).

Dato og tidspunkt: 9. desember 2022, kl.15:00 - 19:00 (4 timer).

Ingen hjelpemidler er tillatt.

Merk følgende:

- Oppgavene i denne eksamen er gruppert under 10 deler som tilsvarer omtrent 10 av forelesningene i dette emnet.
- Det er mulig å oppnå 10 poeng for hver del, totalt 100 poeng (= 100%).
- Man kan navigere frem og tilbake mellom oppgavene.
- Skåring for hver oppgave angis eksplisitt. Det kan gis negative poeng for feil svar/valg, men total poengsum for hele oppgaven er minimum 0 (selv om summen over alle svarene er negativ).
- Vær kortfattet når du skriver tekst som svar på en tekstoppgave. Svaret kan skrives på norsk eller engelsk.
- I navigasjonslinjen nederst på skjermen indikeres fullførte oppgaver med blå søyler.

Lykke til!

i Del 1: Generelt

1.1 1.1 Sikkerhetsmålsettinger

Indiker hvilken sikkerhetsmålsetting som typisk brytes som resultat av hvert angrep.

Poeng: 0,5 for hver riktig, -0,5 for for hver feil, 0 for ubesvart, 3 for alle riktig, minimum 0.

Finn de som passer sammen:

	Tilgjengelighet	Integritet	Konfidensialitet
Keylogger/tastaturlogger	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Løsepenge/krypto-virus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Passordcracking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vandalisering av nettside	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
DDoS-angrep	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kryptoanalyse	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 3

1.2 1.2 Begreper

For hver beskrivelse, angi hvilket begrep som representerer beskrivelsen, ved å velge blant begrepene Hendelse, Konsekvens, Risiko, Sårbarhet, Trussel, Verdi, og Risiko,. Poeng: 0,5 for hver riktig, -0,5 for for hver feil, 0 for ubesvart, 3 for alle riktig, minimum 0.

Angi riktig sikkerhetsbegrep:

	Trussel	Verdi	Hendelse	Sårbarhet	Konsekvens	Risiko
Brudd på konfidensialitet, integritet og/eller tilgjengelighet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tapt omsetning som følge av et cyberangrep	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Har krav om konfidensialitet, integritet, og/eller tilgjengelighet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
At en type angrep ikke kan forhindres	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kombinasjon av trussel, sårbarheter og verdier	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Skadelig aktivitet som kan utnytte sårbarheter og forårsake en sikkerhetshendelse	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 3

1.3 1.3 Identitets- og tilgangshåndtering

Identitets- og tilgangshåndtering (IAM: Identity and Access Management) består av trinn.

For hvert begrep nedenfor, indiker alle IAM-trinn begrepet består av.

Poeng: 0,2 poeng for hver riktig, -0,2 for hver feil, 0 for ubesvart, 4 for alle riktig, minimum 0.

Skåring for hvert begrep er minst 0 poeng.

Brukerautentisering: Velg ett eller flere trinn

Registrer

Klargjør

Autoriser

Gi bruker-ID

Gi autentikator

Tilgangskontroll

Identitetshåndtering: Velg ett eller flere trinn

Registrer

Klargjør

Autoriser

Gi bruker-ID

Gi autentikator

Tilgangskontroll

Tilgangshåndtering: Velg ett eller flere trinn

Registrer

Klargjør

Autoriser

Gi bruker-ID

Gi autentikator

Tilgangskontroll

Konfigureringsfasen: Velg ett eller flere trinn

Registrer

Klargjør

Autoriser

Gi bruker-ID

Gi autentikator

Tilgangskontroll

Bruksfasen: Velg ett eller flere trinn

Registrer

Klargjør

Autoriser

Gi bruker-ID

Gi autentikator

Tilgangskontroll

IAM: Velg ett eller flere trinn

Registrer

Klargjør

Autoriser

Gi bruker-ID

Gi autentikator

Tilgangskontroll

Maks poeng: 4**i Del 2: Systemsikkerhet****2.1 2.1 Filer, prosess , CPU og minnet**

Velg riktig ord i hvert utsagn nedenfor.

Poeng 0,5 for hver riktig, -0,5 for hver feil, 0 for ubesvart, 2 for alle riktig, minimum 0.

En (prosess, minneadresse, kjørbare fil, CPU) inneholder instruksjoner som vil bli utført av CPU når filen kjøres.

Når den startes opprettes en (prosess, CPU, kjørbare fil).

Da vil en del av (prosess, minnet, CPU, kjørbare fil) allokeres, relevante deler vil lastes inn i det, og instruksjoner den inneholder vil kjøres i (minnet, prosess, CPU, kjørbare fil).

Maks poeng: 2

2.2 2.2 Prosesser og minnet

Indiker om utsagnene nedenfor er sanne eller usanne.

Poen 0,5 for hver riktig, -0,5 for hver feil, 0 for ubesvart, 1 for begge riktig, minimum 0.

To prosesser kan **ikke** ha samme virtuelle minneadresse.

Velg ett alternativ:

Usant

Sant

Virtuelle minneområder fjerner buffer-overflow sårbarheten

Velg et alternativ

Usant

Sant

Maks poeng: 1

2.3 Buffer overflow

I en prosess som kjører har følgende skjedd:

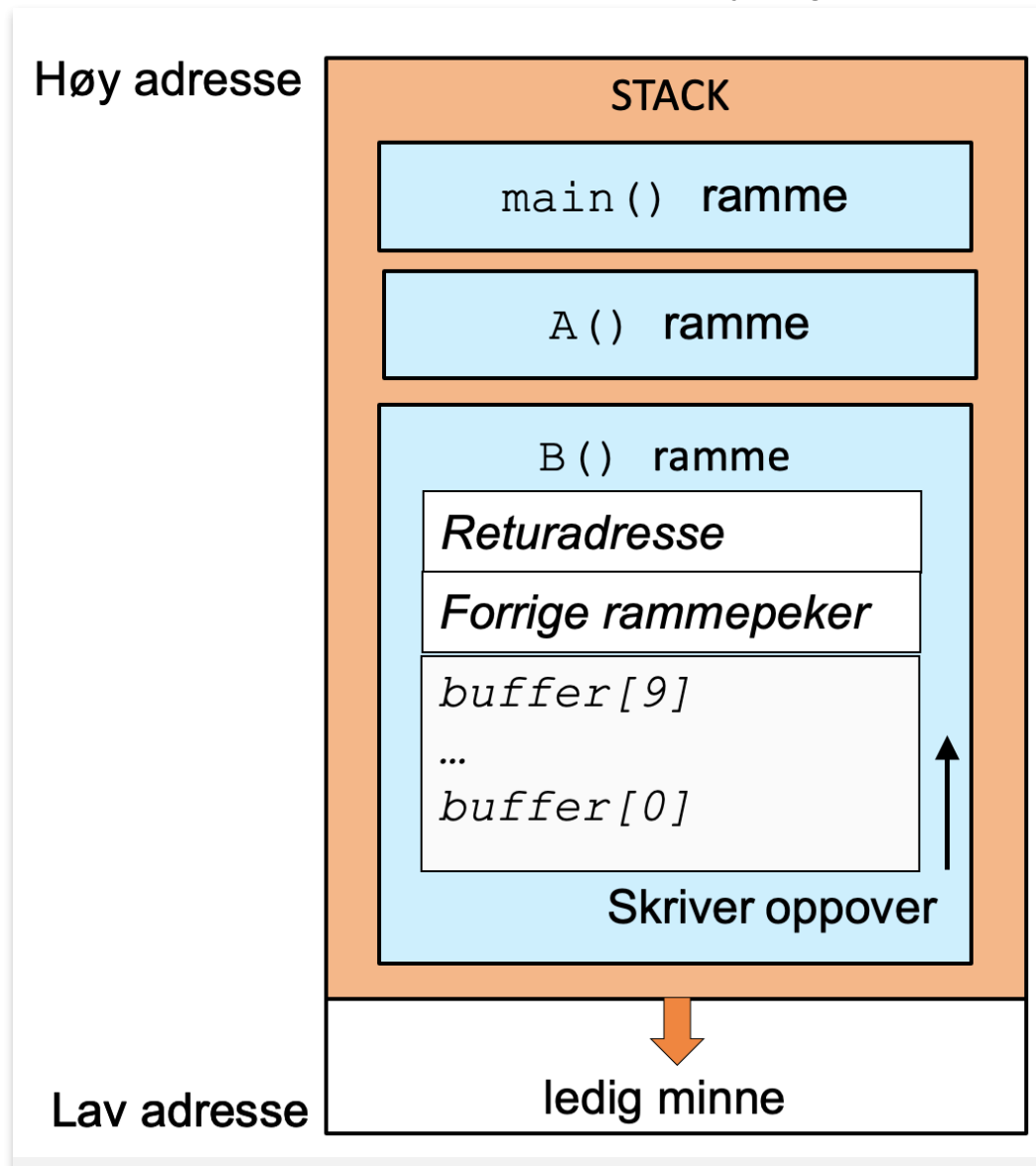
- Prosessen starter med å kjøre **main()** metoden, og det opprettes en ramme på stakken i minnet for den.
- I **main()**-metoden gjøres det et kall til en metode kalt **A()** som starter og det opprettes en ny ramme for **A()** på toppen av stakken.
- I **A()**-metoden gjøres det et kall til en metode **B()** og det opprettes en ny ramme for **B()** på toppen av stakken.

B() metoden inneholder et array kalt **buffer** som har plass til 10 elementer.

Diagrammet nedenfor viser hvordan stakken ser ut når metode **B()** kjører. Programmet har en bufferoverflow-sårbarhet som kan utnyttes gjennom å overskrive **buffer**, og angrepskoden som angriperen ønsker å kjøre ligger et annet sted i minnet. Klikk på den delen av minnet i figuren som angriper må overskrive for å få kjørt angrepskoden.

Poeng: 1 for riktig, 0 for feil.

Klikk på delen av bildet som man ønsker å overskrive for å få kjørt angrepskoden.



Maks poeng: 1

2.4 2.4 Virtualisering

Her brukes type 1 (native) virtualisering. Vis arkitekturen ved å dra de rette elementene til rett plass.

Poeng: 0,5 for hver riktig, -0,5 for hver feil, 2 for alle riktig, minimum 0.

 [Hjelp](#)

Docker Engine

Gjeste-OS

Hypervisor

Maskinvare

App

Kontainer



Four empty rectangular boxes are stacked vertically, each with a colored border. From top to bottom, the borders are cyan, yellow, purple, and red. Each box contains a light gray rectangular area in the center, intended for a drag-and-drop interaction.

Maks poeng: 2

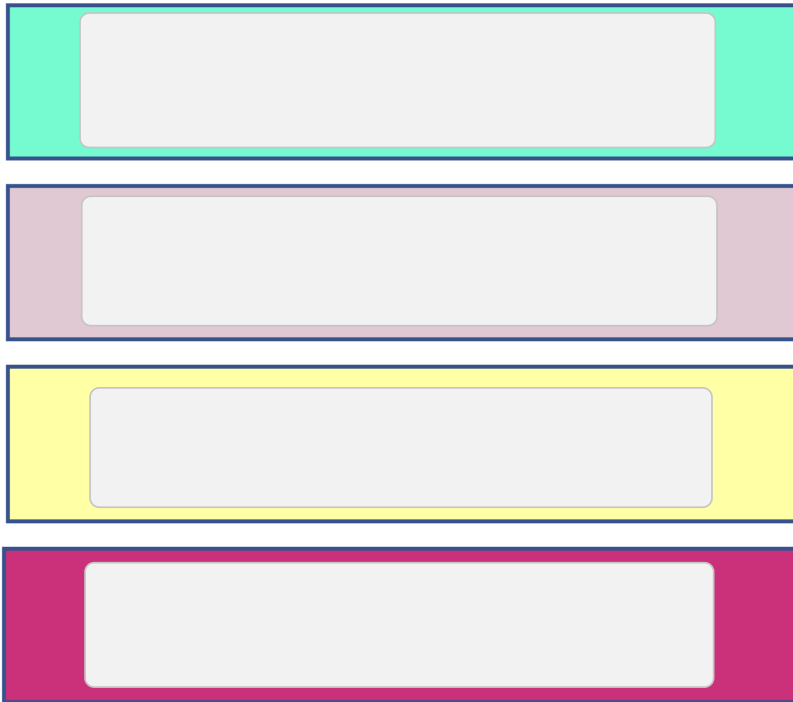
2.5 2.5 Kontainer

Her brukes kontainer (Docker Engine). Vis arkitekturen ved å dra de rette elementene til rett plass.

Poeng: 0,5 poeng for hver riktig, -0,5 for hver feil, 2 for alle riktig, minimum 0.

 [Hjelp](#)

Vert-OS	Docker Engine	Kontainer
Maskinvare		



Four horizontal bars are provided for drag-and-drop. Each bar consists of a colored outer layer and a central grey box. From top to bottom, the colors are: light blue, light purple, light yellow, and light red.

Maks poeng: 2

2.6 2.6 Sikker oppstart

Tema i denne oppgaven er sikker oppstart. Velg riktig svar for hvert utsagn.

Poeng: 0,5 for hver riktig, -0,5 for hver feil, 0 for ubesvart, 2 for alle riktig, minimum 0.

Finn de som passer sammen. "Bare TPM" betyr at det er sant for TPM men ikke UEFI. "Bare UEFI" betyr at det er sant for UEFI men ikke TPM. "Begge" betyr at det er sant for både TPM og UEFI, mens "Ingen" betyr at det hverken er sant for TPM eller UEFI.

	Begge	Ingen	Bare TPM	Bare UEFI
Kan brukes for å bedre sikkerhet ved oppstart	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tillitskjede basert på sertifikat i firmware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kan brukes til å støtte autentisering	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Erstatter BIOS	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 2

i Del 3: Angrepsvektorer og skadevare

3.1 3.1 Tilgang for skadevare

Du kjører uheldigvis skadevare på maskinen din med din administratorbruger. Du har slått av UAC (User Account Control) på maskinen din – Hvilke rettigheter får skadevaren da?

Poeng: 1 for riktig, 0 for feil eller ubesvart.

Velg ett alternativ:

- Bruker
- Gjest
- Administrator
- Power user

Maks poeng: 1

3.2 3.2 Phishing

Hva slags phishing-angrep er dette? Se bildet under (zoom inn og ut ved å trykke Ctrl + (pluss) og Ctrl – (minus). Bruk + og – tastene på det numeriske tastaturet). PS: Jeg verken har, eller har noensinne hatt Netflix.

Poeng: 1 for riktig, 0 for feil eller ubesvart.

Velg ett alternativ:

- Spyd-phishing
- Klone-phishing
- Direktørsvindel (whaling)
- Masse-phishing

Kjære kunde,

Noe av kontoinformasjonen din kan mangle eller være feil. Oppdater kontoinformasjonen din umiddelbart slik at du kan fortsette å nyte alle fordelene med Netflix-kontoen din.

Hvis du ikke oppdaterer informasjonen din innen 24 timer, begrenser vi hva du kan gjøre med Netflix-kontoen din.

Bare klikk på URL-en nedenfor:

Takk for din interesse.

Hilsen,

Netflix-tjenester

[Klikk her](#)

Har du noen spørsmål? Ring 800 050 [701](#)

International BV

Netflix sendte denne meldingen til et medlems e-post.
SRC: 15973_cs_NO

Maks poeng: 1

3.3 Strafferamme ulovlig datainnbrudd

I henhold til straffelovens § 204 – hva er strafferammen for gjennomføring av ulovlig datainnbrudd? (I denne oppgaven må svaret være helt korrekt - hvis korrekt svar er "bøter og fengsel" og du svarer "bøter" - så er svaret altså feil.)

Poeng: 1 for riktig, 0 for feil eller ubesvart.

Velg ett alternativ:

- Fengsel i inntil fem år
- Bøter eller fengsel i inntil ti år
- Bøter
- Bøter eller fengsel i inntil to år

Maks poeng: 1

3.4 Skadevare

Velg den kolonnen som passer best med hver rad. Det gis ett poeng for hvert svar, 0 for blanke og minus ett for hvert gale.

Poeng: 1 for hver riktig, -1 for hver feil, 0 for ubesvart, 4 for alle riktig, minimum 0.

Finn de som passer sammen:

	Bakdør	Dataorm	Virus	Løsepengevirus	Trojaner
En skjult metode for å omgå normal autentisering og tilgangskontroll	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Maskerer seg som legitime programmer som faktisk (eller tilsynelatende) har nyttige funksjoner.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Infiserer andre programmer ved at skadelig kode legges til og flettes inn i andre programmer.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
SQL-slammer er en	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 4

3.5 3.5 Løsepengevirus

I denne oppgaven kommer to utsagn, velg om de sanne eller usanne.

Poeng: 0,5 for riktig, -0,5 for feil, 0 for ubesvart, maks 1, minimum 0.

Mange løsepengevirus krypterer offerets systemer ved hjelp av av SHA-256

Velg ett alternativ:

- Usant
- Sant

Et viktig sikkerhetstiltak mot løsepengevirus i virksomheter er å ikke gi brukerne administratorrettigheter

Velg et alternativ

- Usant
- Sant

Maks poeng: 1

3.6 Angrepsvektorer

I første kolonne står enkelte former for angrep, velg den angrepsvektoren som beskriver angriperen best.

Poeng: 0,5 for hver riktig, -0,5 for hver feil, 0 for ubesvart, 2 for alle riktig, minimum 0.

Finn de som passer sammen:

	Drive-by-angrep	Phishing	Automatisk spredning av skadevare	Falske nettsider	Leveransekjedeangrep
XSS-angrep	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Nettside som sender skadevare automatisk til klienten uten brukerinteraksjon	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dataorm	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Overbevise noen til å installere en keylogger	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 2

i Del 4: Innebygd informasjonssikkerhet og pentesting

4.1 4.1 Innebygd informasjonssikkerhet

Vi har beskrevet livssyklusen for innebygd informasjonssikkerhet som en prosess av 7 faser. Velg riktig fase for hver av aktivitetene under.

Poeng: 0,5 for hver riktig, -0,5 for hver feil, 0 for ubesvart, 2 for alle riktig, minimum 0.

Mål med (Test, Design, Krav, Koding, Forvaltning, Produksjonssetting, Opplæring) å avdekke sårbarheter som ikke har blitt oppdaget i design- eller kodefasene.

Statisk analyse og kode gjennomgang brukes i (Opplæring, Koding, Produksjonssetting, Forvaltning, Test, Design, Krav) .

Prosedyrer for patching og hendelseshåndtering utvikles i (Produksjonssetting, Krav, Forvaltning, Opplæring, Koding, Design, Test).

Fasen (Test, Design, Koding, Forvaltning, Opplæring, Krav, Produksjonssetting) er ikke med i DevSecOps.

Maks poeng: 2

4.2 4.2 Trusselmodellering og applikasjonssikkerhet

Tema for denne oppgaven er trusselmodellering gjennom bruk av STRIDE og OWASP top 10. Poeng: 0,5 for hver riktig, -0,5 for hver feil, 0 for ubesvart, 2 for alle riktig, minimum 0.

Vi har diskutert bruk av STRIDE for trusselmodellering. En angriper som gjør endringer i minnet til en prosess den ikke skal ha rettigheter til er i STRIDE en del av trusselkategori

Velg alternativ (Repudiation, Elevation of privilege, Denial of service, Informasjon

disclosure, Spoofing, Tampering) og er et brudd på Velg alternativ (Tilgjengelighet, Konfidensialitet, Integritet).

OWASP top 10 kan være en god kilde for trusselmodellering for applikasjonssikkerhet. Her rangeres de 10 mest kritiske sikkerhetsrisikoene Siste versjon kom ut i 2021 som vi tar utgangspunkt i her.

En angriper får tjener-applikasjon til å gjøre forespørsel til et domene spesifisert av angriper.

Hvilket av OWASP top 10 er dette et eksempel på? Velg alternativ

(1. Brudd på tilgangskontroll, 2. Kryptografiske feil, 3. Injeksjon, 4. Usikkert design, 5. Feilkonfigurert sikkerhet, 6. Sårbare og utdaterte komponenter, 7. Feil i identifisering og autentisering, 8. Feil i (data og programvare) integritet, 9. Utilstrekkelig logging og overvåking, 10. Server side request forgery (SSRF))

Manipulert input-data sendes til en applikasjon som en del av en forespørsel/kommando som lurer applikasjonen til å utføre utilsiktede eller uautoriserte handlinger. Hvilke av OWAPS top 10

er dette et eksempel på? Velg alternativ (1. Brudd på tilgangskontroll, 2. Kryptografiske feil, 3. Injeksjon, 4. Usikkert design, 5. Feilkonfigurert sikkerhet, 6. Sårbare og utdaterte komponenter, 7. Feil i identifisering og autentisering, 8. Feil i (data og programvare) integritet, 9. Utilstrekkelig logging og overvåking, 10. Server-side request forgery (SSRF))

Maks poeng: 2

4.3 4.3 Bokser

I planleggingen av en pentest får du utlevert all systemdokumentasjon om et system. Dette inkluderer fulle nettverkstegninger. Hva kalles denne typen testing?

Poeng: 1 for riktig, 0 for feil eller ubesvart.

Velg ett alternativ:

- Svartboks-testing (Blackbox)
- Gulboks-testing (yellow box)
- Hvitboks-testing (white box)
- Gråboks-testing (grey box)

Maks poeng: 1

4.4 Misbruk av sudo

I løpet av en pentest har du funnet passordet til en bruker som kan logge inn på en maskin gjennom ssh. Du logger inn og sjekker rettigheter – se bildet under.

Nevn to måter å misbruke sudo-rettighetene du ser på bildet til å oppnå et root-shell.

Du trenger ikke å gi uttømmende svar her, skriv en - eller maks to setninger for hver måte du nevner. Hver måte (tekst) gir 2 poeng, men det er mulig å oppnå totalt 5 poeng hvis du skriver en tilnærmet fungerende kode (pseudokode) for å gjennomføre ett av angrepene.

```

silje@in: ~
PS C:\Users\nilsp> ssh silje@192.168.211.129
silje@192.168.211.129's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

11 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Tue Sep 13 12:52:01 2022 from 192.168.211.1
silje@in:~$ sudo -l
[sudo] password for silje:
Matching Defaults entries for silje on in:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
use_pty

User silje may run the following commands on in:
(root) /usr/bin/python3
silje@in:~$

```

Skriv ditt svar her

Format | **B** | *I* | U | x_2 | x^2 | I_x | | | | | | | | |

Σ |

Words: 0

Maks poeng: 5

i Del 5: Kryptografi

5.1 5.1 Digital signatur

Alice ønsker å sende en digitalt signert melding til Bob slik at en tredjepart (f.eks. en dommer) kan verifisere signaturen. Velg riktig eier og type nøkkel for signering og verifisering.

Poeng: 0,5 for hvert riktig, -0,5 for hver feil, 0 for ubesvart, 2 for alle riktig, minimum 0.

For å signere meldingen må Alice bruke (dommerens, sin egen, Bobs)

(symmetriske, offentlige, private) nøkkel.

For å verifisere den digitale signaturen må Bob bruke (Alices, sin egen, dommerens)

(private, symmetriske, offentlige) nøkkel.

Maks poeng: 2

5.2 Hashfunksjoner

Her er fire utsagn om hashfunksjoner - velg om de er sanne eller usanne?

Poeng: 0.5 for hver riktig, -0,5 for hver feil, 0 for ubesvart, 2 for alle riktig, minimum 0.

Når man har hashsverdien av en streng er det enkelt å finne tilbake til strengen.

Velg ett alternativ:

- Usant
- Sant

Hashfunksjoner kan brukes til å kryptere og dekryptere tekst

Velg et alternativ

- Sant
- Usant

MD5 er en sikrere hashfunksjon enn SHA-1

Velg et alternativ

- Sant
- Usant

SHA-512 er sikrere enn SHA-256

Velg et alternativ

- Sant
- Usant

Maks poeng: 2

5.3 5.3 MAC og Digital Signatur

For hver egenskap, angi hvilken mekanisme som har egenskapen, ved å velge blant mekanismene MAC (Message Authentication Code), DigSig (Digital Signatur), Begge (både MAC og DigSig) eller Ingen (hverken MAC eller DigSig).

Poeng: 0,5 for hver riktig, -0,5 for for hver feil, 0 for ubesvart, 3 for alle riktig, minimum 0.

Angi mekanismen som passer til hver egenskap

	MAC	DigSig	Begge	Ingen
Mottager kan autentisere meldingen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tredjeparter kan autentisere meldingen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mekanismen beskytter konfidensialitet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mekanismen beskytter integritet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mekanismen benytter en symmetrisk kryptoalgoritme	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mekanismen benytter an asymmetrisk kryptoalgoritme	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 3

5.4 5.4 Asymmetrisk kryptering

Hvilke nøkler benyttes i forbindelse med **asymmetrisk kryptering og dekryptering** av en hemmelig melding som skal sendes fra en avsender til en mottager?

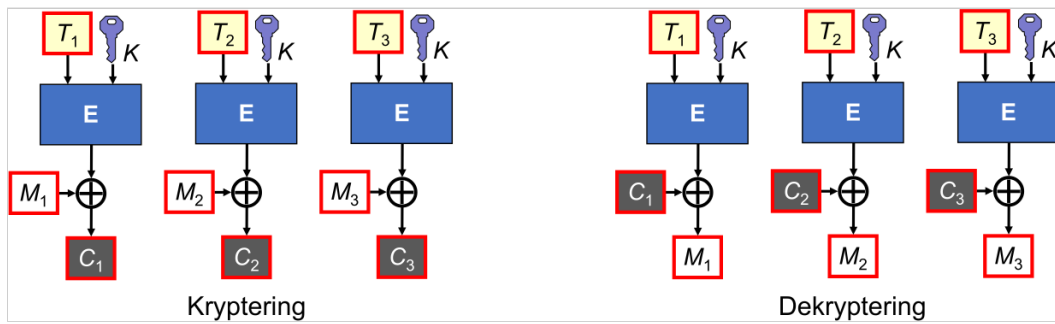
Poeng: 0,5 for hver riktig, -0,5 for hver feil, 0 for ubesvart, 1 for alle riktig, minimum 0.

Velg ett eller flere alternativer

- Privat nøkkel til mottager
- Private nøkkel til avsender
- Offentlig nøkkel til avsender
- Offentlig nøkkel til mottager

Maks poeng: 1

5.5 5.5 Tellermodus



Anta et blokkchiffer som benyttes i tellermodus, slik som vist på figuren, der blokkstørrelsen og nøkkellengden er 4 bits (som et lekeeksempel). Anta følgende parametre:

a) Kryptering

Hemmelig nøkkel $K = 0111$

Telleverdi $T_1 = 0001$

Kryptert telleverdi $E(T_1, K) = 1101$

Klartekstblokk $M_1 = 0101$

Skriv chifferblokk C_1 : .

b) Dekryptering

Hemmelig nøkkel $K = 0111$

Telleverdi $T_2 = 0002$

Kryptert telleverdi $E(T_2, K) = 0011$

Chiffertekstblokk $C_2 = 1100$

Skriv klartekstblokk M_2 :

1 poeng for hvert riktige svar, 0 for feil svar, maks 2, minimum 0 poeng.

Maks poeng: 2

i Del 6: Nøkkelhåndtering og PKI

6.1 6.1 PKI

Våre venner Alice og Bob kommuniserer begge med Charlie, og kommunikasjonen krypteres ved hjelp av offentlig/private nøkkelpar. Anta at alle meldinger kan ses, mottas og sendes på tvers av alle parter (som i en lokal wifi - alle parter kan altså se all kommunikasjon som går mellom alle parter) uavhengig av hvem kommunikasjonen faktisk er ment for. **Anta at Alice har stjålet Bobs private nøkkel** - hvilke utsagn er da korrekte?

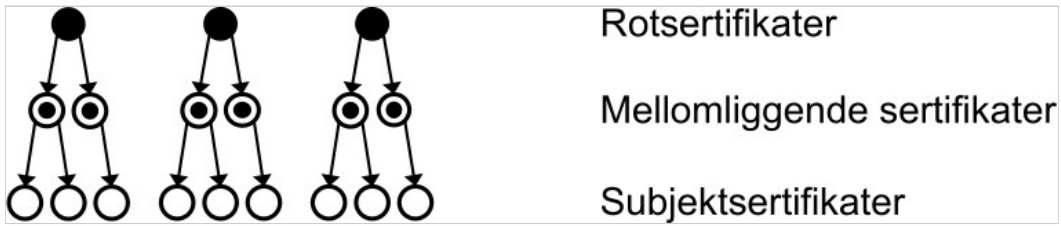
Poeng: 1 for hver riktig, -1 for hver feil, 0 for ubesvart, 3 for alle riktig, minimum 0.

Velg ett eller flere alternativer

- Alice kan lese (dekryptere) meldinger sendt fra Bob til Charlie.
- Alice kan signere forfalskede meldinger fra Charlie til Bob.
- Alice kan signere forfalskede meldinger fra Bob til Charlie.
- Alice kan lese (dekryptere) meldinger sendt fra Charlie til Bob.
- Alice kan signere meldinger fra Alice til Charlie.
- Bob kan lese (dekryptere) meldinger sendt fra Charlie til Alice.

Maks poeng: 3

6.2 6.2 Sertifikater



For hver beskrivelse, angi riktig sertifikat (der Ingen også er et alternativ).

Poeng: 0,5 for hver riktig, -0.5 for for hver feil, 0 for ubesvart, 3 for alle eriktig, minimum 0.

Velg riktig sertifikat

	Rotsertifikater	Mellomliggende sertifikater	Subjektcertifikater	Ingen
Inneholder webtjeners offentlige nøkkel	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Inneholder webtjeners private nøkkel	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Er signert av webtjener	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Er selvsignert	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Er signert av rot-CA (ikke selvsignert)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Brukes til signering av subjektcertifikater	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 3

6.3 6.3 PKI og tillit

Angi 4 korrekte utsagn om PKI og tillit.

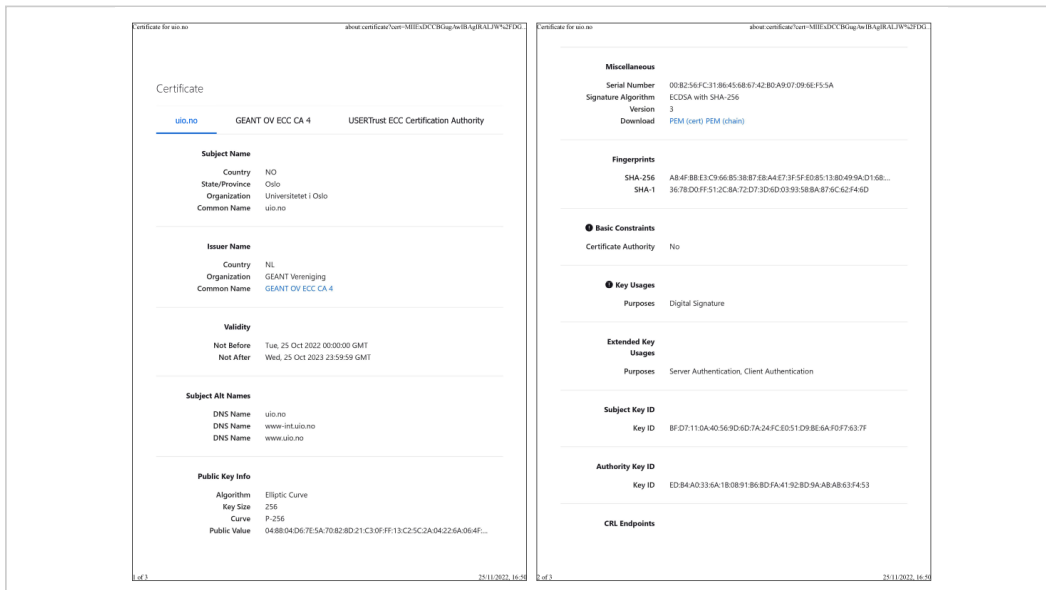
Poeng: 0,5 for hver riktig, -0,5 for hver feil, 0 for ubesvart, 2 for alle riktig, minimum 0.

Velg ett eller flere alternativer

- PKI gjør det mulig å utveksle private nøkler mellom klient og server.
- Tillitsmodellen for internett-PKI har flere enn bare én rot-CA.
- Et server-sertifikat gir en garanti for at nettsidens domenenavn er autentisk.
- En CA sjekker identiteten til eieren av et domene før det utstedes serversertifikat for domenet.
- Korrekt validering av et server-sertifikat gir en garanti for at nettsiden er pålitelig.
- Server-sertifikater gjør det mulig for klient å autentisere tjener ved opprettelse av en øktnøkkel.
- Server-sertifikater gjør det umulig å spoofe nettsider.
- Selv-signering av rot-sertifikater gir en garanti for at rot-sertifikatet er autentisk.

Maks poeng: 2

6.4 6.4 Sertifikat for uio.no.



Bildet viser utdrag av tjener-sertifikatet for uio.no. Forstørr bildet for å gjøre det leselig (zoom inn og ut ved å trykke Ctrl + (pluss) og Ctrl – (minus). Bruk + og – tastene på det numeriske tastaturet).

Angi hvilke utsagn nedenfor som er korrekt vedrørende sertifikatet.

Poeng: 1 for hver riktig, -1 for hver feil, 0 for ubesvart, 2 for alle riktig, minimum 0.

Velg opp til 2 alternativer

- Sertifikatet inneholder tjenerens offentlige nøkkel.
- Sertifikatet kan brukes til å lage digital signatur.
- Sertifikatet kan brukes til å validere digital signatur.
- Sertifikatet kan brukes til å dekryptere.
- Sertifikatet kan brukes til å kryptere.
- Sertifikatet inneholder tjenerens private nøkkel.

Maks poeng: 2

i Del 7: Nettverkssikkerhet

7.1 7.1 Internettstakken

Her skal du matche protokoll/utsagn mot riktig lag i internett-stakken (0,5 poeng for riktig svar, -0,5 for feil svar, 0 poeng for å ikke svare).

Poeng: 0,5 for riktig, -0,5 for feil, 0 for ubesvart, 4 for alle riktig, minimum 0.

Finn riktig lag i internettstakken

	Transportlaget	Ingen av gitt lag	Applikasjonslaget	Internettlaget
HTTP protokollen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
UDP protokollen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Laget du finner IP- sec	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
TLS-handshake protokollen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
TLS-record protokollen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
QUIC protokollen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
FTP protokollen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
TCP protokollen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 4

7.2 7.2 TOR og VPN

Ola og Kari kommuniserer over TOR-nettverket, hvor 3 VPN forbindelser som ligger oppå hverandre brukes. Det er satt opp en forbindelse mellom Ola og Kari som bruker TOR-nodene A, B og C som vist under:



Ola skal sende en (internett)-pakke til Kari. Hvis hvordan TOR-pakken er bygd opp gjennom hvilken nøkkel som brukes for kryptering av hvert av de 3 VPN-lagene.

Poeng: 1 for hver riktig, -1 for hver feil, 0 for ubesvart, 3 for alle riktig, minimum 0.

 [Hjelp](#)

Nøkkel delt med Kari

Nøkkel delt med B

Nøkkel delt med A

Nøkkel delt med C



Maks poeng: 3

7.3 7.3 Brannmurer og inntrengningsdeteksjon

Velg hvilke alternativer som er riktig (hvert utsagn kan ha flere riktige svar).

Poeng: 0,5 for riktig, -0,5 for feil, 0 for ubesvart, 3 for alle riktig, minimum 0.

Kan brukes til å filtrere ut uønskede nettverkspakker

Velg ett eller flere alternativer

- Brannmur
- Inntrengningsdeteksjon (IDS)

Vi ønsker å akseptere (bare) pakker som er en del av en eksisterende TCP-sesjon i en viss retning. Hvilke løsninger kan brukes?

Velg ett eller flere alternativer

- Tilstandsløs brannmur
- Signatur-basert deteksjon
- Tilstandsbasert brannmur
- Applikasjonsbrannmur

Maks poeng: 3

i Del 8: Brukerautentisering

8.1 8.1 Passordsikkerhet

Velg riktig sikkerhetstiltak i en kolonne til høyre for å dekke hvert sikkerhetskrav i venstre kolonne.

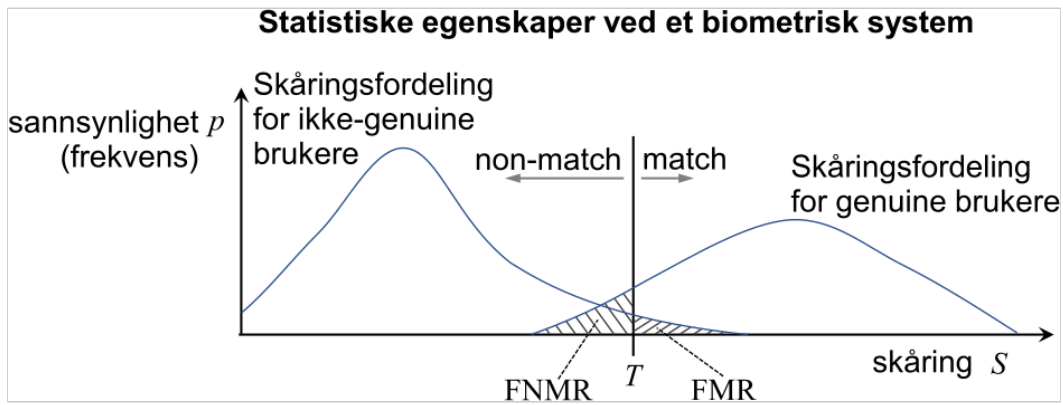
Poeng: 0,5 for hver riktig, -0.5 for for hver feil, 0 for ubesvart, 2 for alle riktig, minimum 0.

Angi riktig sikkerhetstiltak for hvert krav

	Komplekse passord	Salting	Hashing	Tilgangskontroll
Det skal ikke være mulig å benytte forhåndsgenererte hash-tabeller for å cracke passord i databasen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kun autoriserte skal kunne lese passorddatabasen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Det skal være svært vanskelig å cracke et saltet passord fra databasen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Passord skal ikke ligge i klartekst i passorddatabasen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 2

8.2 8.2 Biometris system



Statistiske egenskaper ved et biometrisk system reflekterer systemets kvalitet, som illustrert i figuren over.

Et biometrisk system blir testet med 100 genuine brukere som forsøker å logge inn på egen konto, og 100 ikke-genuine brukere som forsøker å logge inn på en annen konto enn sin egen. Anta at 96 genuine brukere og 6 ikke-genuine brukere blir godtatt.

Oppgi følgende rater som et desimaltall (bruk punktum som skille mellom heltall og desimaltall).

Merk at ratene ikke har noen sammenheng med størrelsen på feltene i figuren over.

TMR (True Match Rate):

TNMR (True Non-Match Rate):

FMR (False Match Rate):

FNMR (False Non-Match Rate):

Poeng: 0.5 for riktig, 0 for feil eller ubesvart, 2 for alle riktig, minimum 0.

Maks poeng: 2

8.3 FIDO-autentisering

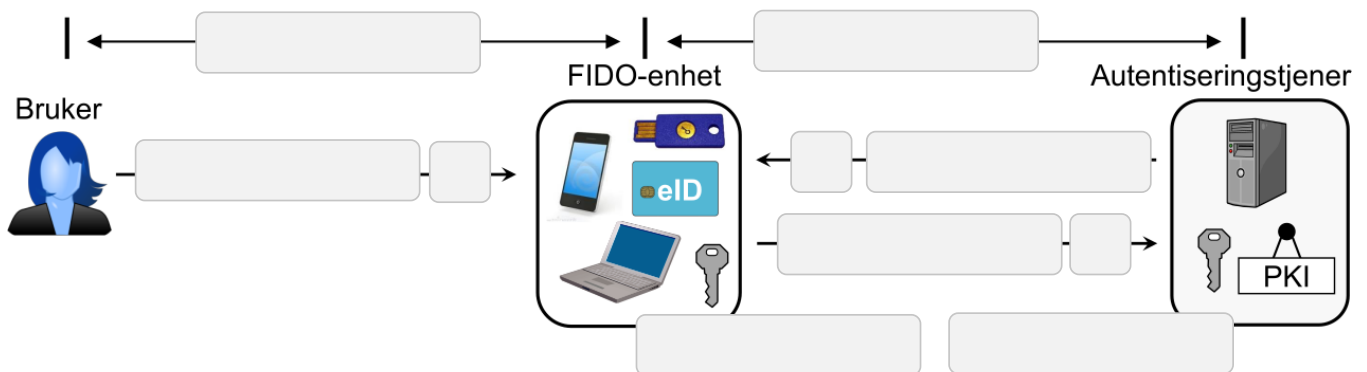
Figuren nedenfor viser scenario for brukerautentisering med FIDO 2.0-protokollen. Sett inn elementene i riktig felt, samt tallene 1,2,3 (i de små feltene) for å indikere rekkefølgen på meldingene.

Poeng: 0,5 for riktig, -0.5 for feil, 0 for ubesvart, 5 for alle riktig, minimum 0.

 [Hjelp](#)

Privat FIDO-nøkkel	1
Autentikator(er)	Utfordring
Autentiseringsetappe 1	3
Respons	Autentiseringsetappe 2
2	Offentlig FIDO-nøkkel

Brukerautentisering med FIDO 2.0



Maks poeng: 5

8.4 Rammerk for e-Autentisering

Rammeverk for e-Autentisering og uavviselighet definerer autentiseringsnivåer for bruk i e-Forvaltning (online tjenester til innbyggere) i Norge. Ulike autentiseringsløsninger gir ulike autentiseringsnivåer.

Gi et eksempel på en løsning som gir nivå HØY: (Biometri, BankID, FIDO, MinID).

Gi et eksempel på en løsning som bare gir nivå MODERAT: (FIDO, Biometri, MinID, BankID)

Poeng: 0,5 for hver riktig, -0.5 for feil, 0 for ubesvart, 1 for begge riktig, minimum 0.

Maks poeng: 1

i Del 9: Identitets- og tilgangshåndtering

9.1 9.1 Identitetsføderering

I et domene for identitetsføderering kan forvaltning av identiteter være sentralisert eller distribusert, og forvaltning av autentisering kan være sentralisert eller distribuert. Angi alle mulige riktige alternativer for hvert tilfelle nedenfor. Merk at flere alternativer er mulig.

Poeng: 0,2 for hver riktig, -0,2 for hver feil, 0 for ubesvart 3 for alle riktig, minimum 0.

OpenID Connect-protokollen (OIDC) støtter:

sentr. ID	distr. ID	sentr. Aut	distr. Aut
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ID-porten har følgende karakteristikk:

sentr. ID	distr. ID	sentr. Aut	distr. Aut.
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ID-føderering på Internett med fb, google og twitter etc. har følgende karakteristikk:

sentr. ID	distr. ID	sentr. Aut	distr. Aut
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Silo-modellen for identitetshåndtering har følgende karakteristikk;

sentr. ID	distr. ID	sentr. Aut	distr. Aut
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

FIDO-autentisering kan brukes sammen med følgende:

sentr. ID	distr. ID	sentr. Aut	distr. Aut.
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Hvis myndighetene i et land bruker personnummer (social security number) for e-Autentisering, så kreves følgende:

sentr. ID	distr. ID	sentr. Aut	distr. Aut
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Maks poeng: 3

9.2 9.2 SP og IdP

Indiker hvilke(n) funksjon(er) som utføres henholdsvis av SP (Service Provider) og IdP (Identity Provider) som del av identitetsfødering.

Poeng: 1 for hver riktig, -1 for hver feil, 0 for ubesvart, 2 for alle riktig, minimum 0.

SP utfører:

Tilbyr tjenester

Autentiserer bruker

Genererer sikkerhetsbillett

Tar imot sikkerhetsbillett

IdP utfører:

Tilbyr tjenester

Autentiserer bruker

Genererer sikkerhetsbillett

Tar imot sikkerhetsbillett

Maks poeng: 2

9.3 9.3 MAC-modellen

MAC-modellen (Mandatory Access Control) for tilgangskontroll definerer tilgangsrettigheter basert på merker/labler, som kalles sikkerhetsklarering for brukere/subjekter og sikkerhetsgradering for data/objekter.

I MAC-modellen har brukere en fastsatt maks klarering, og velger en (lik eller lavere) aktuell klarering for hver økt. Angi for hvert tilfelle nedenfor hvilke(t) graderingsnivå(er) brukeren kan aksessere med enten LESE eller SKRIVE. Flere valg er mulig i hvert tilfelle.

Poeng: 0,2 for hver riktig, -0,2 for hver feil, 0 for ubesvart, 2 for alle riktig, minimum 0.

Hva kan en bruker LESE som har maks klarering HEMMELIG og aktuell klarering HEMMELIG?

BEGRENSET

KONFIDENSIELT

HEMMELIG

STRENGT HEMMELIG

Hva kan en bruker SKRIVE som har maks klarering HEMMELIG og aktuell klarering HEMMELIG?

BEGRENSET

KONFIDENSIELT

HEMMELIG

STRENGT HEMMELIG

Hva kan en bruker LESE som har maks klarering HEMMELIG, og aktuelt klarering KONFIDENSIELT?

BEGRENSET

KONFIDENSIELT

HEMMELIG

STRENGT HEMMELIG

Hva kan en bruker SKRIVE som har maks klarering HEMMELIG og aktuell klarering KONFIDENSIELT?

BEGRENSET

KONFIDENSIELT

HEMMELIG

STRENGT HEMMELIG

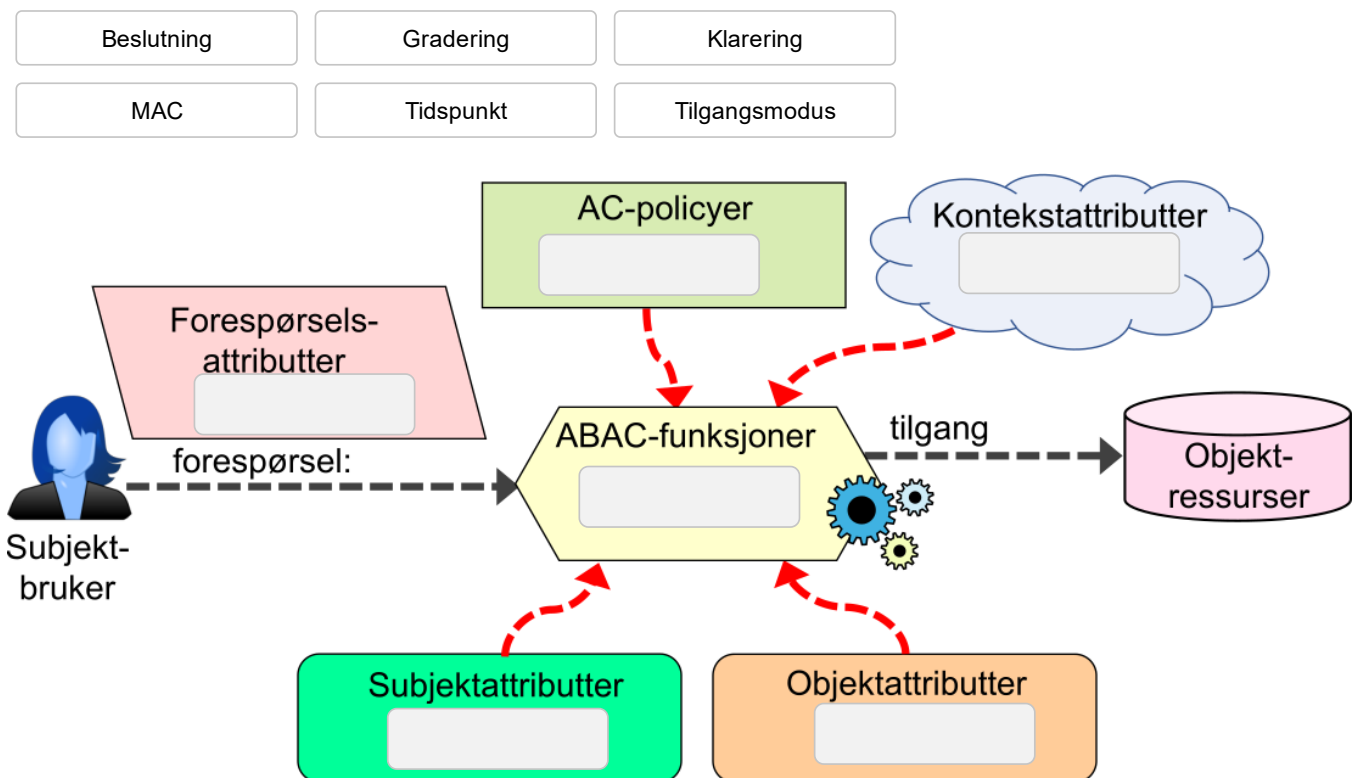
Maks poeng: 2

9.4 9.4 Attributtbasert tilgangskontroll

ABAC (Attribute Based Access Control) er en generell modell for tilgangskontroll som kan være basert på ulike kategorier med policyer/regler, funksjoner og attributter, som vist i figuren nedenfor. Tilordne hver policy/funksjon/attributt til riktig kategori i figuren.

Poeng: 0,5 for riktig, -0,5 for feil, 0 for ingen tilordning, 3 for alle riktig, minimum 0.

 Hjelp



Maks poeng: 3

i Del 10: Risikostyring

10.1 10.1 Prosess for risikostyring

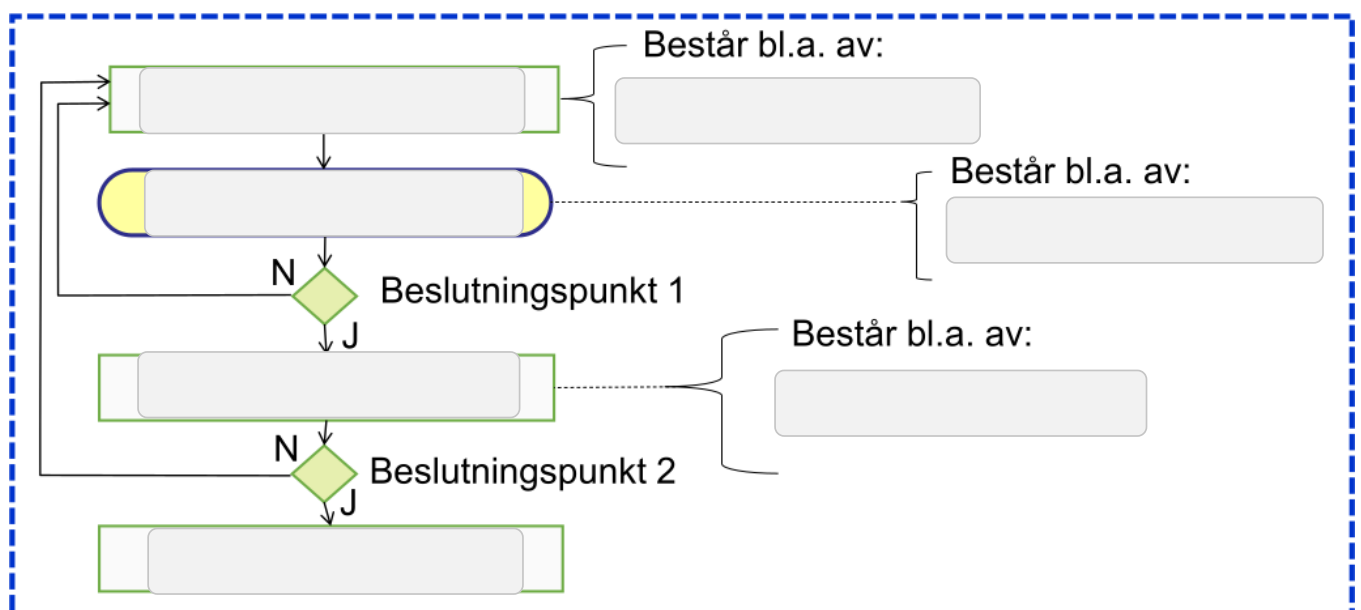
Figuren nedenfor viser prosess for risikostyring der trinnene mangler beskrivelse. Sett inn elementene i riktig felt for å beskrive trinnene.

Poeng: 0,5 for riktig, -0.5 for feil, 0 for ubesvart, 4 for alle riktig, minimum 0.

 Hjelp

Risikovurdering	Implementer sikkerhetstiltak
Planlegging	Risikokriterier
Håndteringsplan	Risikoreduksjon
Risikoanalyse	

Risikostyring for informasjonssikkerhet



Maks poeng: 4

10.2 10.2 Beslutningspunkter

Til venstre beskrives noen utsagn vedrørende risikostyring som er relevante enten for beslutningspunkt 1 eller for beslutningspunkt 2 i henhold til figuren for risikostyring i forrige oppgave. Velg hvilket beslutningspunkt som er relevant for hvert utsagn.

Poeng: 0,5 for hver riktig, -0,5 for hver feil, 0 for ubesvart, 2 for alle riktig, minimum 0.

Velg riktig beslutningspunkt

	Punkt 2	Punkt 1
For høy restrisiko i henhold til kriterier	<input type="radio"/>	<input type="radio"/>
For stor uvisshet rundt risikoer	<input type="radio"/>	<input type="radio"/>
Passe restrisiko, men utilstrekkelig budsjett for sikkerhetstiltak	<input type="radio"/>	<input type="radio"/>
Dårlig spredning av risikoer	<input type="radio"/>	<input type="radio"/>

Maks poeng: 2

10.3 10.3 Kvantitativ risikovurdering

Denne oppgaven ser på kvantitativ risikovurdering. En risiko er vurdert slik at hendelsen vil inntreffe gjennomsnittlig en gang hvert andre år. Som følge av hendelsen forventes tapt fortjeneste på NOK 1 000 000 og utgifter til gjenoppretting på NOK 500 000.

Oppgi hendelsens sannsynlighet som desimaltall (med punktum) mellom 0 og 1:

Oppgi kvantitativ konsekvens i NOK: .

Oppgi kvantitativ risiko som tap per år i NOK: .

Et sikkerhetstiltak som koster NOK 100 000 forventes å redusere den kvantitativ risikoen med NOK 500 000.

Oppgi ROI (Return on Investment) for sikkerhetstiltaket:

Poeng: 1 for riktig. 0 for feil eller ubesvart, 4 for alle riktig, minimum 0.

Maks poeng: 4

i Slutt på eksamen

