Kommentarer til eksamen i IN1020

Dag Langmyhr Omid Mirmotahari Kristin Skar
Håkon Kvale Stensland

Eksamen 9. desember 2019

Generelt

- Ingen oppgave vil gi mindre enn 0 poeng.
- Strykgrensen var **44** poeng.
- 7,1 % av de som leverte, strøk.

1.1) Sikkerhetsmål

Poengberegning: 0,5 for rett, –0,5 for feil

Alternativene er:

- Tilgjengelighet: Korrekt
- Sporbarhet: Korrekt
- Uavviselighet: Korrekt
- Integritet: Korrekt
- Brannmur: Feil; sikkerhetstiltak
- Sikkerhetskopiering; Feil; sikkerhetstiltak
- Tofaktor-autentisering: Feil; autentiseringsfaktor/sikkerhetstiltak
- Kryptering: Feil; sikkerhetstiltak

1.2) Sikkerhetstiltak – konfidensialitet

Poengberegning: 0,5 for rett, –0,5 for feil

Alternativene er:

- Benytte sjekksumalgoritmer for data som skal overføres i nettverk: Feil; sjekksumalgoritmer bidrar ikke til konfidensialitet, kun til å f.eks. sjekke integritet (at data ikke er endret).
- Benytte diskkryptering ved lagring av data: Korrekt; kryptering av data lagret på disk vil gjøre det vanskeligere for uvedkommende å forstå/lese dataene hvis de skulle få tilgang til dem.
- Bruk av tofaktor-autentisering for systemer som behandler konfidensielle data: Korrekt; bruk av tofaktor-autentisering kan gjøre det mer komplisert å tilegne seg uautorisert tilgang til et system.
- Benytte HTTPS framfor HTTP som protokoll i nettverkskommunikasjon: Korrekt; HTTPS som protokoll bidrar til kryptert nettverkskommunikasjon, som igjen gjør det vanskeligere for den som evt avlytter nettverkstrafikk å forstå informasjonen og dermed få tilgang til data.
- Bevissthetstrening for alle som behandler data: Korrekt; Opplæring av f.eks. ansatte i konfidensialitet og hvordan data skal behandles konfidensielt er et vesentlig sikkerhetstiltak.

1.3) Sikkerhetstiltak – fysisk sikring

Poengberegning: 2 for rett, –1 for feil

Alternativene er:

- Fordi en inntrenger kan stjele biometriske identiteter: Feil.
- Fordi kritiske systemer ikke har kryptering: Feil.
- Fordi fysisk tilgang til et system gjør det enklere å autentisere seg: Feil.
- Fordi en inntrenger kan omgå så og si alle sikkerhetstiltak ved å ha fysisk tilgang til et system: Korrekt; ved å ha fysisk tilgang til et system kan du f.eks. installere fysiske tasteloggere, eller du kan i verste fall stjele datamaskinen inkludert disker, minnebrikker og annet som du i fred og ro kan hente informasjon fra.

1.4) Autentisering

Poengberegning: 2 for rett, –1 for feil

Alternativene er:

- Ved å benytte biometri kan ikke uvedkommende autentisere seg ved å utgi seg for å være en annen: Feil; også biometri som autentiseringsfaktor kan forfalskes ved f.eks. «presentation attacks». Eks. bilde for ansiktsgjenkjenning, kopi av fingeravtrykk, osv.
- Flerfaktor-autentisering gjør det enkelt å begrense gjentagende forsøk på å tilegne seg ulegitimert tilgang: Feil; flesfaktor-autentisering gjør det ikke nødvendigvis enkelt å begrense gjentagende forsøk, men det vil være vanskeligere for uvedkommende å finne/gjette riktig kombinasjon for å tilegne seg tilgang.
- Flerfaktor-autentisering vil begrense hva brukerne har lov til å gjøre i et system: Feil.
- Ved å benytte en kombinasjon av autentikatorer vil det være vanskeligere for uvedkommende å tilegne seg ulegitimert tilgang til et system: Korrekt; det vil være vanskeligere for uvedkommende å finne/gjette riktig kombinasjon av autentikatorer.

1.5a) Digital signatur

Poengberegning: 1,5 for rett, –1,5 for feil

Alternativene er:

- Kan bekrefte avsenders identitet ovenfor en tredjepart (uavviselighet): Korrekt; kun entiteten (f.eks. personen) som kjenner den private nøkkelen brukt til signering kan ha signert meldingen.
- Baserer seg på symmetrisk kryptering: Feil; digital signatur baserer seg på asymmetrisk kryptering med bruk av privat/offentlig nøkkelpar.
- Sikrer konfidensialitet for meldingen som signeres: Feil; alle som kjenner den offentlige nøkkelen tilhørende den private nøkkelen brukt til signering kan lese innholdet i meldingen.
- Kan bekrefte avsenders identitet ovenfor mottager: Korrekt; kun entiteten (f.eks. personen) som har den private nøkkelen brukt til signering kan ha signerte meldingen.

1.5b) Digital signatur

Poengberegning: 1,5 for rett, –1,5 for feil

Alternativene er:

- Mottagers private nøkkel: Feil; mottagers nøkkel er ikke involvert ved digital signatur.
- Mottagers offentlige nøkkel: Feil; mottagers nøkkel er ikke involvert ved digital signatur.
- Senderens offentlige nøkkel: Korrekt; denne nøkkelen benyttes når mottager skal dekrypterer medlingen.
- Senderens private nøkkel: Korrekt; denne nøkkelen benyttes til kryptering ved signeringen.
- Symmetrisk nøkkel generert av mottager: Feil; det benyttes asymmetrisk kryptering.
- Symmetrisk nøkkel generert av sender: Feil; det benyttes asymmetrisk kryptering.

1.6) Behandling av personopplysninger

Poengberegning: 2 for rett, –2 for feil

Alternativene er:

- Navn eller fødselsnummer lagres ikke i systemet, og det er dermed ikke nødvendig å forholde seg til personvernregelverket: Feil; personvernregelverket omfatter alle identifiserbare personopplysninger, ikke kun navn og/eller fødselsnummer.
- Studentene har rett til å få vite hvilke opplysninger om dem som behandles i systemet: Korrekt; i følge perosnvernregelverket har man som registrert rett til innsyn i opplysninger om seg selv.
- Fordi tjenesten helt og holdent er levert av andre, er Institutt for informatikk er ikke juridisk ansvarlig for at informasjon om studentene og deres eksamensbesvarelse behandles i samsvar med personvernregelverket: Feil; virksomheten som samler/benytter persondata er fortsatt juridisk ansvarlig for at data behandles i samsvar med personvernregelverket selv om de overlater selve behandlingen (f.eks. lagring) til en annen virksomhet (3. part).
- Institutt for informatikk er juridisk ansvarlig for at informasjon om studentene og deres eksamensbesvarelse behandles i samsvar med personvernregelverket: Korrekt; virksomheten som samler/benytter persondata er fortsatt juridisk ansvarlig for at data behandles i samsvar med personvernregelverket selv om de overlater selve behandlingen (f.eks. lagring) til en annen virksomhet (3. part).

1.7) Trusselmodelering – tilgjengelighet

Poengberegning: 1,5 for rett, –1,5 for feil, 5 for alle rett

Alternativene er:

- Tastelogger plassert i overgangen mellom tastatur og datamaskin: Feil; tastelogger benyttes for å avlytte informasjon mellom datamaskin og tastatur for å få ulegitimert tilgang til data.

- Manglende sikkerhetsoppdateringer av programvaren og operativsystemet systemet benytter: Korrekt; manglende sikkerhetsoppdateringer kan føre til at et system rammes av f.eks. løsepengevirus eller andre typer ondsinnet programvare som gjør systemer/informasjon/data utilgjengelig for de som trenger det.
- Svikt i lagringsrutinene som fører til at studenter kan se hverandres eksamensbesvarelser: Feil; dette fører til brudd på konfidensialitet, ikke tilgjengelighet.
- Feil i systemet som utfører tilgangskontroll i datasystemet: Korrekt; feil i systemet som utfører tilgangskontroll kan føre til at de som skal ha tilgang til et system ikke gis tilgang.
- Utilgjengelighetsangrep (DDoS) fra utenforstående med ondsinnede hensikter: Korrekt; ved å overbelaste tjenester kan utenforstående ramme virksomheter.

1.8) Trusselmodelering

Poengberegning: 1 for rett, –1 for feil

Alternativene er:

- De kan stjeles: Korrekt; en USB-minnepinne er en liten, ekstern enhet som kan fort stjeles (eller mistes). Hvis data på minnepinnen ikke er krytert, kan uvedkommende på den måten enkelt få tilgang til dataene.
- De kan utilsiktet bli kryptert av for eksempel løsepengevirus: Feil; utilsiktet kryptering fører til brudd på tilgjengelighet, ikke konfidensialitet.
- De kan bringe med seg skadevare som omgår andre sikkerhetsmekanismer: Korrekt; en USB-minnepinne kan overføre skadevare fra en datamaskin til en annen.
- De kan bruke for mye strøm og på den måten påvirke en datamaskin negativt: Feil.

2.9) Protokoller

Poengberegning: 1 for rett, –0,5 for feil

Løsningen på «legg på rett plass»-oppgaver vises ikke i den automatisk genererte fasiten. Her er den:

TCP:	HTTP, SMTP, DASH
TCP og/eller UDP:	DNS, DHCP

3.1) Tall på ulik form

Poengberegning: 1 for rett, –0,5 for feil

Løsningen på «legg på rett plass»-oppgaver vises ikke i den automatisk genererte fasiten. Her er den:

For å sammenligne tallene må vi omforme dem til samme form, for eksempel desimalt:

$$\begin{aligned} 2013 \quad (\text{oktalt}) &= 1035_{10} \\ 40E \quad (\text{hex}) &= 1038_{10} \\ 1031 \quad (\text{desimalt}) &= 1031_{10} \\ 10000001001 \quad (\text{binært}) &= 1033_{10} \end{aligned}$$

Da er det lett å sortere dem.

3.3) Assemblerkode 1

Poengberegning: 4 for rett, -1 for feil

Følgende skjer:

1. Programmet leser verdien 7 som lagres i x.
2. Verdien 11 lagres i y.
3. Programmet beregner $x - y$ som blir -4; dette tallet skrives ut.

3.4) Assemblerkode 2

Poengberegning: 4 for rett, -1 for feil

Programmet går i løkke og leser verdier brukeren oppgir. Variabelen x teller antall verdier, og innlest verdi 0 angir avslutning (og skal ikke telles). Til slutt skrives svaret 4 ut.

3.5) Assemblerkode 3

Poengberegning: 4 for rett, -1 for feil

Programmet skriver ut en bokstav som angir ukedagen.[1] Det skjer ved å modifisere instruksjonen b som henter bokstaven. Husk at instruksjonene lagres som tall i minnet, og da kan vi regne med dem.

3.6) Maskinkode

Poengberegning: 5 for rett, -1 for feil

Programmet ganger brukerens oppgitte verdi med 7 ved å doble verdien tre ganger og så trekke fra det opprinnelige tallet. Her er tallkodene vist som instruksjoner:

```
start   INP             // A <- 8
        STA     x       // x <- 8
        ADD     x       // A <- A+x = A+8 = 16
        STA     y       // y <- 16
        ADD     y       // A <- A+y = A+16 = 32
        STA     y       // y <- 32
        ADD     y       // A <- A+y = A+32 = 64
        SUB     x       // A <- A-x = A-8 = 56
        OUT             // Skriv ut 56.
        HLT

x       DAT     0
y       DAT     0
```

[1] Programmet skriver T for både tirsdag og torsdag, men vi tar ikke det så nøye.