# T-00
# INTRODUKSJON

## 1) Hva er informasjonssikkerhet?

- Informasjonsikkerhet handler om å sikre informasjon og sørge for at den ikke kommer ut til uvedkommende og at informasjonen ikke blir endret utilsiktet eller av uvedkommende samt at informasjonen er tilgjengelig i forhold til behovet.

## 2) I forhold til informasjonsikkerhet hva står «C.I.A» for?

- Confidentiality(konfidendsialitet)
- Integrity(integritet)
- Availability(tilgjengelighet)

## 3) Forklar begrepene nedenfor (gi gjerne eksempler på begrepene også):

- **Kryptering**
  - En måte der man kan la to parter utfører konfidensiell kommunikasjon over en usikker kanal som foreksempel kan overvåkes. Informasjonen skal dermed være sikker fordi den er kryptert
- **Adgangskontroll**
  - Regler og retningslinjer som begrenser adgangen til konfidensiell informasjon til de personene/systemene som «trenger å vite»(«need to know»). Dette gjelder både personer og datasystemer.
- **Autentisering**
  - Å avgjøre identiteten eller rollen en person har, eksempler kan være passord, bilnøkkel, fingeravtrykk o.l.
- **Autorisering**
  - Å bestemme hvilke ressurser en person/system skal ha tilgang til. Eksempler på autorisering kan være låser på dører der bare personen med nøkkel har tilgang.

**4) Hva betyr Integritet? Hvordan kan man bevare integriteten til noe?**

- Integritet handler om at informasjonen ikke har blitt endret på en uautorisert måte. Ulike måter man kan bevare integritet på kan være for eksempel backup og sjekksummer

**5) Hva betyr Tilgjengelighet?**

- Tilgjengelighet handler om at informasjonen er tilgjengelig og mulig å endre innenfor en rimelig tid av de som er autorisert til dette.

**6) Hva står begrepet «A.A.A» for? forklar kort hva hver enkelt «A» står for.**

- Assuranse(forsikring/tillit)
  - Forventet atferd, hva som er tillat og hvilke mekanismer som benyttes for å håndheve retningslinjer.
- Autentisitet
  - Måten man kan bestemme om utsagn, retningslinjer og tillatelser som blir gitt av en person eller et system er ekte.
- Anonymitet
  - Anonymitet handler om at transaksjoner eller lagrede data ikke skal kunne føres tilbake til et bestemt individ.

**7) Er Cæsar Chiper en «sikker» måte å kryptere informasjon på?**

- Ja
- Nei

**8) Hva slags kryptografiske funksjoner er: «SHA-1» og «SHA-256» eksempler på?**

- Dette er ikke kryptografiske funksjoner
- Dette er Hash funksjoner
- Dette kan man ikke svare på uten å vite hvilken algoritme klokkesyklusen på en datamaskin kjører.

**9) Hva står «MAC» for?**

- Message Autorization Certificate
- Message Authentication Codes
- Message Anonymity Controll
- Ingen av alternativene

**10) Hva vil et «DOS» angrep bety?**

- Denial-of-service angrep betyr å avbryte eller forhindre en datatjeneste eller ødelege tilgang.

**11) Nevn de 10 prinsippene for sikker design av datasystemer og en kort beskrivelse av hver av de.**

- Economy of mechanism
  - Enkelt mulig design og implementering av sikkerhets-tiltak sånn at andre lettere kan forstå og videre utvikling og verifisering effektiviseres.
- Fail-safe defaults
  - Standard konfigureringer som følger konservative beskyttelses-skjema(er). «Bedre å gi for lite tilgang enn tilgang til for mye»
- Complete mediation
  - Sjekke all tilgang til en ressurs og passe på at det er i tråd med beskyttelses-skjema. For eksempel automatisk utlogging etter en viss periode
- Open design
  - Burde dele arkitektur og design for at andre parter kan undersøke og analysere systemet. Eneste som ikke burde deles er de kryptografiske nøklene.
- Separation of privilege
  - Man må kunne få tilgang til en del av systemet uten at man får tilgang til hele systemet. Systemet må også kunne kreve at flere ulike betingelser er innfrid for å få tilgang til ressurser eller at et program skal utføre en bestemt handling.
- Least privilege
  - Hvert program bør operere med kun det minimum av rettigheter det trenger for å fungere skikkelig. Opperere med «need to know» prinsippet for deling av informasjon.
- Least common mechanism
  - I systemer med flere brukere bør mekanismer som tillater deling av en ressurs mellom flere brukere minimeres.
- Psychological acceptability
  - Bruker-grensesnitt og tilbakemeldinger bør være godt designet og «intuitive» samt alle sikkerhets-innstillinger bør være i tråd med hva en «vanlig bruker» forventer.
- Work factor
  - Kostnadene ved å måtte omgå/bryte en sikkerhets-mekanisme bør sammenlignes med de ressursene en forventet angriper vil disponere. Dette vil dermed si at et system som skal beskytte for eksempel karrakterene til studenter der ofte studentene er angripere ikke trenger å være like

sofistikert/avanser som et system som skal beskytte atomvåpen, statshemmeligheter eller industrihemmeligheter.

- Compromise recording
  - Noen ganger er det bedre å få oversikt(loggføre) konsekvensene av et inngrep enn å sette inn mer sofistikerte tilgang for å forhindre det. Eksempler kan være overvåkningskamerea i stedet for å sikre alle dører of vinduer bedre.

# T-01
# KRYPTERING

**1) Hva er kryptering**

Kryptering er den viktigste teknikken for å gjennomføre retningslinjene for å sikre systemet. Kryptering kan forklares som en matematisk metode som sørger for konfidensialitet ved at informasjon ikke kan leses/forstås av uvedkommende

**2) Hva er substitusjonschiffer**

Å bytte ut tegn med ett annet. For eksempel så kan man forskyve hele alfabete slik at bokstaven «A» blir bokstaven «N», «B» blir «O» osv...

**3) Kan man bruke subsitusjon på binærtall?**

- Ja
- Nei

**4) Hva er «One-Time pads» og er dette sikkert?**

One-time pads er en type kryptering der man benytter en tabell med shift-nøkler. One-time pads skal i prinsippet være umulig å knekke, men svakheten for denne typen er at nøkkelen må være like lang som klarteksten det vil si at skal du kryptere en bok så må nøkkelen være like lang som boken. En annen ting som også er viktig er at nøkkelen **ALDRI må gjenbrukes!** Brukes nøkklene omigjen så er dette ikke sikkert!

**5) Hva står «AES» for?**

- Advanced Encryption Standard
- Advanced Encryption Substitusjon
- Artifact Encounter Selection

**6) Hvilke av disse er «AES» versjoner?**

- AES-128
- AES-156
- AES-192
- AES-124
- AES-256
- AES-520

**7) Er «AES» 100% sikkert?**

Vi kan si at selve krypteringen er sikker, men vi kan ikke si at AES er 100% sikker uten å vite hvordan nøkkelen er delt. Så for å kunne snakke med hverandre sikkert må man bruke en nøkkel som er sikker, den nøkkelen er som oftest sendt med RSA som er «sikker» men krevere flere ressurser enn AES. Poenget ender med at AES ikke er sikkert så lenge man ikke vet om nøkkelen er delt på en sikker måte.

På dette spørsmålet kan man både argumentere for ja og nei og hva som blir riktig vil være avhangig av hvordan du begrunner svaret dit.

**8) Hva er asymetrisk kryptering (public key kryptering)**

Bob har to nøkler en privat nøkkel som må holdes hemmelig og en offentlig nøkkel som gis ut til «alle». Så når for eksempel Alice skal sende en meling til Bob så trenger hun Bob sin offentlige nøkkel som hun krypterer meldingen med og sender den til Bob dermed er det bare Bob sin private nøkkel som kan dekryptere meldingen og lese hva som står.

**9) Hva er Symetrisk kryptering?**

Alice og Bob deler en hemmelig nøkkel som brukes både til kryptering og dekryptering. Altså her må begge vite/ha nøkkelen for å lese meldingene

**10) Er «RSA» Symetrisk eller asymetrisk?**

- Symetrisk
- Asymetrisk

**11) Er «AES» Symetrisk eller asymetrisk?**

- Symetrisk
- Asymetrisk

**12) Forklar hvordan en person ville startet en samtale med «RSA», men senere byttet til «AES» like etter. Hvorfor ikke bruke «AES» hele tiden? Eller hvorfor ikke bare bruke «RSA»?**

For at samtalen skal være sikker så må den krypteres og vi vet at for å kunne kommunisere over AES så må man dele en nøkkel, nøkkelen må deles på en sikker måte som nevnt i spm 7. Så for at nøkkelen skal deles sikkert brukes RSA. RSA algoritmen er ressurs tung i forhold til AES og vi ønsker dermed ikke å bruke denne mer enn nødvendig, dermed byttes det over til AES når den hemmelige nøkkelen er delt og resten av kommunikasjonen fortsetter med AES.

**13) Hva er en kryptografisk nøkkel?**

En kryptografisk nøkkel er en nøkkel/parameter som avgjør hvilke resultat den kryptere informasjonen vil vise. Har man korrekt nøkkel så vil man kunne se den rette informasjonen, er nøkkelen feil så vil man mest sannsynelig ikke forstå noe av informasjonen.

**14) Forklar hva SHA-256 er?**

SHA-256 står for Secure Hash Algorithm – 256 bit og er en type hash funksjon som regnes som sikker.

# T-02
# OPERATIVSYSTEM

**1) Hva er Multitasking?**
Gir hver kjørende program tids-luker på CPU. Sørger for at det kan se ut til at flere programmer kjører «samtidig», Men i realiteten bytter veldig fort mellom hvert program.

**2) Hva er forskjellen på User- vs Kernel-modus?**
Vanlige applikasjoner og mange andre av tjenester OS-et tilbyr kjører i «user mode» altså (ring 3), mens OS-kjernen kjører i kjernemodus(ring 0). I user mode kan man ikke aksessere hardware(HW) og utstyrsdrivere direkte og har kun tilgang til minne som OS-et har tildelt samt at man har et begrenset instruksjonssett. I kjernemodus kjører man i såkalt protected mode og har tilgang til hele minnet samt at alle instruksjoner kan kjøres. I kjernemodus har man også ingen sikring fra hardware(HW)

**3) Hva er forskjellen på prosess og tråd?**
Når et program kjøres på en datamaskin kalles det en prosess. En prosess er allokerings-enhet og OS oppretter en prosess samt tideler den rettigheter og ressurser. En prosess kan innholde flere tråder som kan utføre instruksjoner delvis uavhengig av hverande. En tråd er en utførings-enhet og utfører instruksjoner.

**4) Hva tilbyr som oftest et filsystem?**
Et filsystem tilbyr som oftest en abstraksjon av hvordan eksternt, ikkeflyktig minne er organisert. De fleste filsystemene organiserer filer hierarkisk i kataloger.

**5) Hva er en virtuell maskin(VM)?**
En programmvare som simulerer hardware ved å «hijacke» alle systemkall og ellers kjøre instruksjoner som vanlig.

## 6) Nevn noen basic NTFS tillatelser

| NTFS Permission | Folders | Files |
|---|---|---|
| Read | Open files and subfolders | Open files |
| List Folder Contents | List contents of folder, traverse folder to open subfolders | Not applicable |
| Read and Execute | Not applicable | Open files, execute programs |
| Write | Create subfolders and add files | Modify files |
| Modify | All the above + delete | All the above |
| Full Control | All the above + change permissions and take ownership, delete subfolders | All the above + change permissions and take ownership |

## 7) Nevn minst ett viktig tiltak for å sikre OS mot angrep

- Laste ned patcher/opdateringer med en gang disse blir tilgjengelige
- Ingen brukere med høyere tilgangsnivå enn absolutt nødvendig
- Konservativ installasjonspolicy generelt

## 8) Hva er Rootkits?

Rootkits er en samling av software som brukes til å få tilgang til områder personen ikke er autorisert til. Rootkits kan manipulere data på root-nivå og dermed endre/fjerne filer. Siden rootkit kan endre filer så kan den også skjule seg for antivirus programmer.

- Ved å hooke NtQueryDirectoryFile kan man velge å fjerne oppføringer av enkelte filer (som man ønsker å skjule).
- Dette vil da medføre at FindNextFile ikke viser filen du ønsker å skjule.
- Anti-Virus applikasjoner som skanner filer ved å enumerere ut filer på harddisken vil da ikke finne filen du har skjult.
- På denne måten har ”rootkittet” klart å skjule seg selv på systemet.

## 9) Hva er stack-buffer overflow? Hvordan kan dette være en svakhet?

Stack-buffer overflow handler om at man kan sende in mer data enn stacken forventer og dermed overskriver retur-adressen. Dette kan være en svakhet ved at man kan gi en returadresse som viser til “farlig” kode. Dette skjer fordi språk som for eksempel “C” ikke sjekker grensene for arrays når de deklareres og de leser stort sett user-input inn I arrays.

**10) Hva er et “0-day”-attack?**

0-day attack er ett angrep/svakhet som ennå ikke er kjent/funnet. Dette gjør svakheten farlig fordi selskapet selv ikke vet om svakheten og brukerne er dermed ikke beskyttet mot denne svakheten.

# T-02
# MALWARE

**1) Hva står «malware» for? Hva betyr «malware»?**
Malware står for «Malicious Software».
Malware er en fellesbetegnelse på «ondsinnet programmvare» som utfører uautoriserte og (oftest) skadelige handlinger.

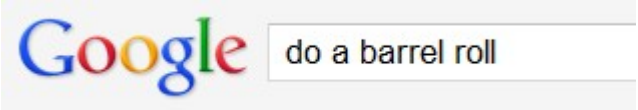
**2) Hvilke ulike klassifikasjoner av malware har vi?**
Vi kan dele malware opp i ulike typer etter hvordan den spres og skjules.

- Spredning
  - Virus
    - Menneskeassistert spredning (Spres ikke automatisk). Denne typer krever for eksempel at en bruker åpner et vedleg i epost.
  - Orm
    - Spres automatisk og krever dermed ikke at noen menneskeassistering. Denne typen kan spres mellom maskiner over nett.
- Skjuler seg
  - Rootkit
    - Endrer OS for å skjuler sitt nærvær.
  - Trojaner
    - Nytteprogram som skjuler ondsinnede operasjoner. Dette vil si at det er et program som en bruker ser på som «vanlig» og ikke farlig, men inneholder onsinnede operasjoner. Eksempler her er keylogger
- «Nyttelast» (Payload)
  - Alt fra humor/irritasjon til ran av maskinkraft og identitetstyveri

**3) Hva menes med «innside-angrep»?**
Insider-angrep betyr at det er noen som er en del av orginisasjonen som er med å kontrollere eller bygge tjenesten som legger inn for eksempel «backdoor» (sikkerhetshull som er lagt inn med vilje av en programmerer)

**4) Hva menes med «backdoor»?**
En skjult metode/kommando i et program som tilater en bruker å utføre handlinger man normalt ikke har tillatelse til.

**5) Hva er «Easter Egg» i forhold til Malware?**
Easter egg er en type backdoor som ofte er lagt inn med vilje, men ikke er skadelig.
Eksempel på dette kan være å gå på «www.google.com» og søke på «do a barel roll»



**6) Hva menes med Logikkbomber**
Logikkbomber utfører en handling først når en bestemt betingelse inntreffer

Eksempel på Logikkbombe kan være at en person er med å lage software til mini-bank. Enten legger personen inn en «bug» i koden med vilje eller ikke og i dette eksempelet kan dette føre til at visst man utfører en kommando klokken 15:02 så vil maskinen «spytte» ut penger.

**7) Hva er et virus?**
Ett virus er et program som kan replisere seg selv ved å enten endre andre filer/program, infisere dem med kode eller formere seg viere. Virus krever vanligvis brukerassistering for å formere seg.

**8) Hvordan spredde «Brain»-viruset seg?**
Viruset spredde seg rundt i verden via diskett

**9) Hva er en orm («Worm»)?**
Dette er malware som sprer kopier av seg selv uten å infisere andre program, og vanligvis kreves det ingen menneskelig medvirkning(brukerassistering). I de fleste tilfeller vil ormen ha en ondsinnet nyttelast (payload) der den for eksempel kan installerere en bakdør(backdoor) eller slette filer

**10) Skriv en kort sammendrag av hva «ILOVEYOU»-ormen var**
ILOVEYOU-ormen var den aller første ormen som spredde seg gjennom epost og kom 4. mars 2000. Brukeren måtte manuelt åpne en fil i eposten. Den gjorde egentlig ikke noen skade, men bare spredde seg. I løpet av 9 dager så hadde 50 millioner Pcer blitt infisert

**11) Hva er en «Trojaner»**
Dette er malware som ser ut til å utføre en nyttig jobb, men i tillegg gjør noe ondsinnet. Eksempler på dette kan være at man laster ned en musikkspiller, men uten at du vet det så eksekverer dette programmet kode som logger alle tastetrykk og sender det til en «ond» person.

**12) Hva er et Rootkit?**
Rootkits er en samling av software som brukes til å få tilgang til områder personen ikke er autorisert til. Rootkits kan manipulere data på root-nivå og dermed endre/fjerne filer. Siden rootkit kan endre filer så kan den også skjule seg for antivirus programmer.

**13) Hva er «botnet»?**
Malware kan gjøre maskinen om til en «zombie», som er en eksternt kontrollert maskin som benyttes i ondsinnede angrep, vanligvis som en del av et botnet

**14) Hvordan bruker antivirusprogrammer signaturen til å flagge programmer?**
Signaturen til et malware er selve «fingeravtrykket» og antivirusprogrammer har en malware database med alle kjente signaturer. Så fort antivirusprogrammer klarer å finne en kjent signatur så vil den flagges.

**15) Hva er en Heuristisk analyse?**
Dette er en analyse som brukes  til å identifisere nye og «zero-day-malware». Basert på instruksjonene forsøker antiviruset å bestemme om det er malware ut fra om det for eksempel forsøker å ende/slette system-filer. Også Emulering av eksekvering hvor man kan kjøre koden i et isolert miljø og overvåke atferden, dersom det finnes mistenkelig atferd så markeres det som malware.

TK2100

# T-04
## Nettleser- og www-sikkerhet

**1) Hvilke metoder finnes under HTTP/1.1**

- GET
- POST
- HEAD
- PUT
- DELETE
- OPTION
- TRACE

**2) Nevn noen grunner til å bruke «cookies»**

HTTP er "stateless" tilstandsløs og cookies kan dermed bevare tilstand. Cookies kan også "huske» autorisasjoner.

**3) Hva er «session hijacking» (sniffing)?**

Session hijacking er hvor en angriper gjetter seg fram til riktig session id og «later» som om han er den originale brukeren.

**4) Hva er et serfikat?**

Et serfikat er identifikator som er gitt av sertifiseringsautoriteter. Sertifikater viser også til «ekteheten» av siden.

**5) Hva er «Cross Site Scripting» (XSS)?**

XSS er å Injisere script på webserver i andres web-applikasjoner. Dette kan for eksempel være å legge inn ondsinnet kode i inputfelt.

**6) Hva er «Cross Site Request Forgery» (CSRF)**
CSRF er det motsatte av XSS og utnytter en sides tillit til en bruker, ikke brukerens tillit til siden. Eksempel på dette kan være at brukeren er logget på i banken samtidig som brukeren også besøker en øndsinnet side.

```
<script>
  document.location="http://www.naivebank.com/
  transferFunds.php?amount=10000&fromID=1234&toID=5678";
</script>
```

**7) Hva er «SQL-injection»?**
SQL-injection handler om å prøve å manipulere siden sine egne spørringer. Eksempel på dette kan være et inputfelt der man kan søke etter varer. Her kan man legge inn en annen spørring som spør etter alle brukere og passord. Dette eksempelet er ganske naivt, ved at man vanligvis ville sikret innputfelt, men har man ikke gjort dette så kan en angriper skrive hva han vil og spørringen vil bli kjørt.

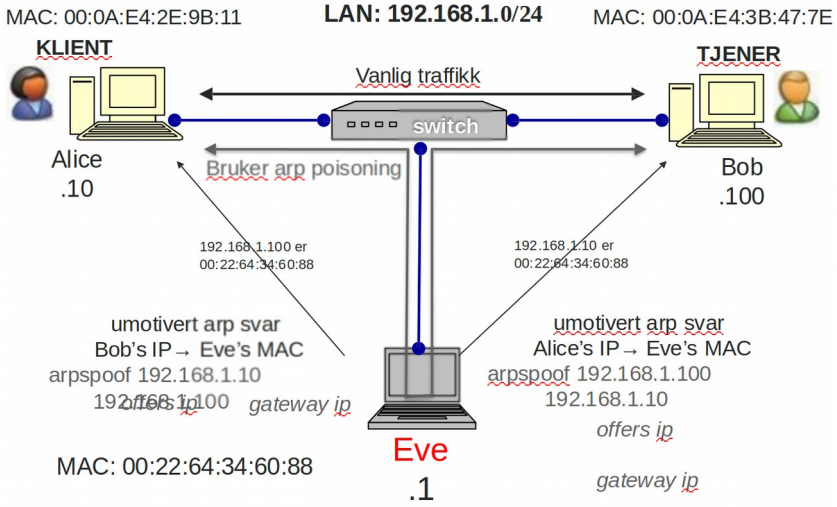
**8) Hva er “phishing”?**
Phishing er en angrepsmetode som handler om at noe/noen fremstår å være en annen person eller virksomhet. Her ingår foreksempel det å lage en falsk facebook-side som ser helt lik ut som den originale men når man logger inn så vil passord og brukernavn bli sendt til en angriper.

TK2100

# T-05
# Nettverk og internett 1

**1) Hva er «MAC-spoofing»?**
Mac-spoofing handler om å utgi seg for å ha en annen adresse en det man har. Her kan man sniffe/søke etter en mac-adresse man ønsker og deretter sette denne på sin egen masin. Vanskelig å beskytte seg mot dette.

**2) Hva er «ARP-spoofing»?**
ARP cache oppdateres på grunnlag av alle ARP-responsene og Mangelen på autentisering gjør derfor disse sårbare for spoofing. Eksempel på arp-spoofing med arp-poisoning. Flere eksempler i slidene fra forelesning




**3) Hvorfor er "ip-spoofing" ofte brukt I "DoS-angrep"?**
Når man utfører DoS angrep så er ikke angriperen interessert i å få noen respons/svar. Angriperen ønsker derimot bare å overbelaste mottakeren.

**4) Hva er ett «Smurf-attack» Smurfe-angrep?**
Smurfe angrep benytter seg av ICMP-protokolen og handler om at angriperen broadcaster ICMP-echo pakker på netverket med offerets spoofede ip-adresse som avsender. Dette vil da si at angriperen later som om han er offeret og sender denne ICMP-echo meldingen som trigger automatisk svar hos alle som motar den. Siden det er offeret som står som sender vil offeret da få alle de automatiske responsene.

**5) Hva er «SYN-flod attack»?**
Dette handler om at en angriper lager en stor mengde pakker med «falske» avsender-adresser og setter SYN-flagger i disse. Tjeneren vil da svare med SYN/ACK og åpne en socket. Her vil tjeneren aldri få noe flere svar og angriperen vil bare sende nye SYN-meldinger som til slutt vil overbelaste serveren.

**6) Hva er «(D)DoS»**
(D)DoS betyr (Distrubuted) Denial of Service og handler om å forhindre andre (legitime) brukere fra å få tilgang til en tjeneste. Dette kan være å enten kræsje tjenesten eller overbelaste den.

**7) Hva mener Kripos er de typiske formene for datakriminalitet?**
- Datainnbrudd
- Databedrageri
- Informasjonsheleri
- Skadeverk
- Dokumentforfalskning
- Piratkopiering
- Beskyttelsesbrudd(TV- og radiosignaler)

**8) Kan man bruke Wireshark, nmap eller andre sikkerhets-verktøy utenfor sitt egen «eiendom/område» så lenge man ikke planlegger å gjøre skade?**
Nei, man kan ikke bruke disse uten å få eksplisitt tillatelse til det.

TK2100

# T-07
# Nettverk og internett 2

**1) Hva står «DNS» for?**
DNS – står for Domain Name System

**2) Hva er forskjellen på Pharming og Phishing?**
Pharming vil si at man kan for eksempel legge inn falske IP-adresser forbundet med ekte DNS-navn for å lede offeret til å laste den malware eller legge inn brukernavn/passord e.l.

Phising betyr å lage en webside e.l. som ser ekte ut, og får offeret til å oppgi informasjon(passord, kredittkortnummer, osv...)

**3) Hva er DNS cache-forgiftning?**
Dette er å gi DNS tjenere falske svar og få dem cachet. Først vil man sende en vanlig forespørsel om et domene til en navnetjener. Deretter vil vi selv sende et falsk svar til navnetjeneren, ID'en til svaret vil vi bare tippe og dermed så vil det svaret vi sendte bli cachet og alle som benytter denne tjeneren få den «falske» ip'en vi nettop sendte inn.

**4) Hvorfor kan vi bare gjette oss til DNS id?**
Fordi vi kan basere oss på bursdags-paradoxet som vil si at visst du har 23 personer i et som er sannsynligheten for at to personer har samme fødselsdag hele 50,7%. Dette beslekter også til å gjette DNS-id. Visst vi sender n responser på n ulike forespørsler så vil vi i teorien etter 213 forsøk ha 50% sannsynelighet for å ha truffet riktig og etter 400 forsøk ha 92,4%.

**5) Hva er en brannmur?**
En brannmur («firewall») er en samling av sikkerhetstiltak som skal forhindre uautorisert tilgang til et nettverk (av computere)

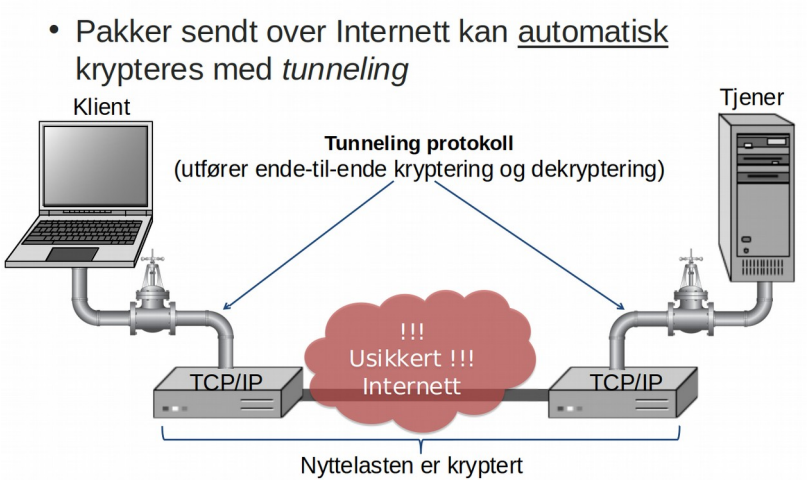
**6) Hva er white-og-white-listing? Hva er best?**
Dette er to forskjellige strategier for å gi tilganger.

Blacklisting vil si at **ALLE** pakker slipper gjennom bortsett fra de som er definert i reglene. Denne er veldig fleksibel, men naiv da den forutsette at man kan forutse alle trusler som kan oppstå.

Whitelistning vil si at **INGEN** pakker slipper gjennom, bortsett fra de som er definert i reglene.

Hva som er best kan argumenteres, men ved blacklisting så kan men glemme å forby noe og dermed få en trussel mens har man whitelisting så vil alt være forbudt og dermed vil man i verste fall bare miste funksjonalitet.

**7) Hva er «Tunneling»?**
Innholdet i TCP segmenter er vanligvis ikke kryptert og tunneling er en måte å forhindre avlytting uten å endre annen software. Her krypteres kommunikasjonen automatisk og gjør avlytting vanskelig/umulig.




**8) Hva står «VPN» for?**
Virtual Private Networking (VPN)

**9) Hva betyr «portscanning»? Hva brukes det til?**
Dette vil si å scanne computerens porter og se hvilke porter som er aktive/i bruk. Dette brukes ofte av angripere for å finne servere og brannmurers svakheter. Brukes også av oss for å avdekke våre egne svakheter og fikse dem

TK2100

# T-08
# Modeller, standarder, lover og penetrasjonstesting

**1) Hva er en sikkerhetsmodell?**
En sikkerhetsmodell er en abstraksjon som bidrar med begrepsapparatet som administratorer trenger for å spesifisere sikkerhetspolicy'er.

**2) Hva er «DAC» (Discretionary Access Control)?**
DAC («skjønnsmessig») er adgangskontroll der brukerene selv gis mulighet til å bestemme hvilke tillatelser/begrensinger som skal gjelde for egne filer.

- Typisk basert på kategoriene enkeltbrukere og grupper
- Gir brukere typisk mulighet til å gi tilgang til ressurser til andre brukere innenfor samme system

**3) Hva er «MAC» (Mandatory Access Control)?**
MAC («tvungen») er mer restriktiv enn DAC og tillater ikke brukere å selv bestemme rettigheter på filer og ressurser. Alle sikkerhetsavgjørelser foretas av en sentral policy administrator

- Hver sikkerhetsregel består av subjekt som vil ha adgang til et objekt og en liste som bestemmer hvem som har hvilke tilganger
- Eksempel:
  - Security Enhanced Linux (SELinux)
  - OSX tilbyr og bruker default
  - Windows nettverk med Domene Controller (Active Directory)

**4) Nevn og beskriv minst to ulike adgangskontroll-modeller**

- Bell-La Padula (BLP)
- Biba
- Low-Watermark
- Clark-Wilson model
- Chinese Wall model (Brewer & Nash)
- M.fl.

Beskrivelse finnes i slidene.

**5) Hvordan ser sikkerhetsprosessen ut?**

1. Vurdere risiko: Verdier, trusler, tap
2. Utforme policy: Informasjon, systemer, bruk, backup, tilgang, hendelser, avbruddsplan
3. Innføre: Raportering, autentisering, inbrudds-deteksjon, krypering, fysisk sikkerhet
4. Opplæring: Ansatte, ledere, utviklere, sikkerhets-ansatte
5. Revisjon: Etterlevelse, periodisk vurdering, innbrudds-tesing

**6) Beskriv «Standard: ISO 27000»**
ISO 17799: 2005 (= 27001) fokuserer på  sikring av tilgjengelighet, integritet og konfidensialitet av informasjon

Sikringen foretas gjennom et sett kontroller, som angir konkrete krav. Kontrollene beskrives og vedlikeholdes i organisasjonen.

Standarden kan opprettholdes og dokumenteres gjennom en sertifiseringsordning, og kontrolleres via intern og ekstern revisjon.

**7) Hva er «PCI DSS»?**
Payment Card Industry Data Security Standard
Standarden som f.eks. Visa, Mastercard og andre (kort-)leverandører av betalingstjenester bruker

- Stiller krav til sikring av kunde, leverandør og transaksjon.
- Må sertifiseres og revideres etter denne standarden dersom du f.eks. skal drive en server-farm for en bank, nettbutikk e.l.

TK2100

# T-09
# Opphavsrett og spam

**1) Hva er patent? Hva er patent godt for?**
En patent er en eneret til kommersiell utnyttelse av en oppfinnelse for et begrenset tidsrom (20 år) innenfor et juridisk område (stat). Dette er godt fordi den skal sikre alle tilgang til oppfinnelsen og kunnskapen bak, ved at virkemåten offentliggjøres.

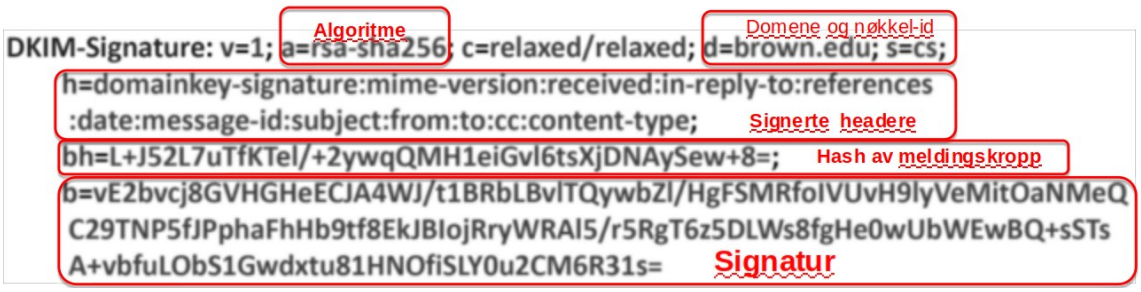
**2) Hva skal «DRM» (Digital Rights Management) beskytte mot?**
DRM skal (ofte) beskytte mot lovstidig endring, deling, kopiering, utskrift og fremvisning av digitale media.

**3) Hvilke  metoder kan brukes til kopibeskyttelse?**

- Dongle
  - HW-utstyr som må plugges
  - inn og inneholder nøkkel/
  - kryptoprosessor (jf TPM) som kreves for å kjøre programvaren
- Produkt-nøkkel
  - Legges inn under installasjon
  - Testes online for duplikat
  - Lisensen knyttes til maskinen v.hj.a. OS- eller HW- signatur
- Telefon-aktivering
  - Må ringe opp og snakke med noen («avskrekking»)

**4) Hva står «DKIM» for? (i forhold til email)**
**D**omain**K**eys **I**dentified **M**ail (DKIM)

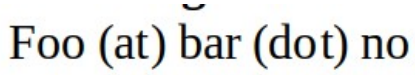
**5) Hva er «DKIM»? (i forhold til email)**
Dette er en måte å signere/verifisere eposter. Vanligvis er det serveren som signerer og verifiserer og den er basert på DNS (TXT RR). Den signerer også header-feltene (FROM: osv). For eksempel Gmal godtar ikke epost fra paypal.com og ebay uten gyldig DKIM signatur.



**6) Gi et eksempel på hvordan man kan legge ut en epostadresse med en format som er vanskelig å identifisere. Altså ikke skrive emailen som «foo@bar.com».**

Tekst:
Foo (at) bar (dot) no

bilde:




**7) Hva kan «Captcha» være godt for i forhold til email?**

For å vanskeliggjøre automatisk opprettelse av webmail-kontoer o.l.

- Ikke vanskelig å komme forbi, men øker kostandene for spammer'ne

Google's nyeste reCAPTCHA sjekker også adferd på brukeren…