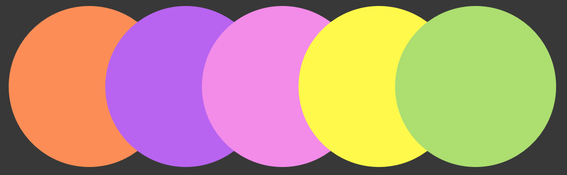
Ånund Kielland Jore

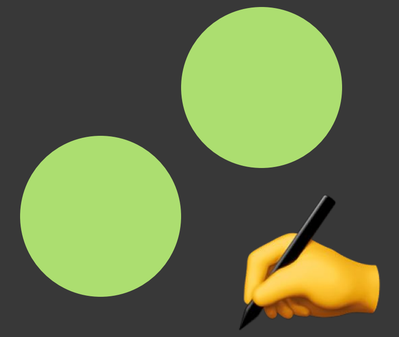
Onsdag 16 Oktober

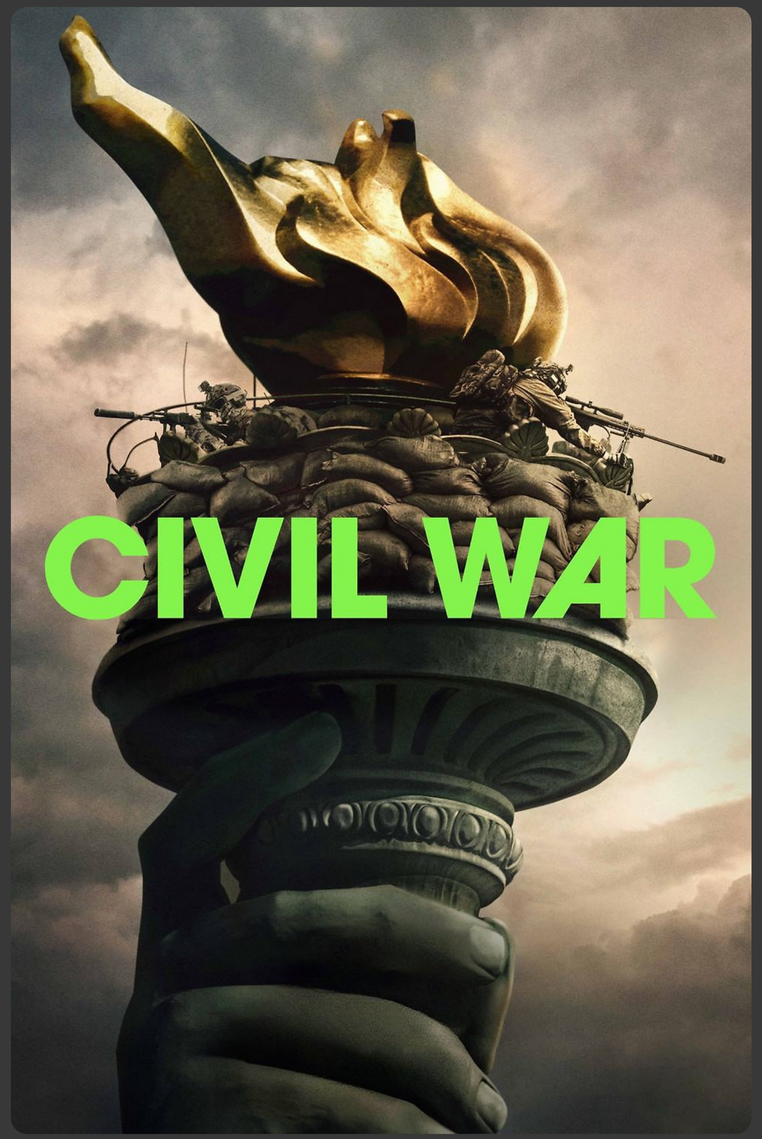
Tjenester på internet

IN1020



1. Diskutere noen oppgaver
2. Pause
3. Diskutere noen eksamensoppgaver
4. Selvstendig arbeid





Ukens Filmtips - Civil War

“ In the near future, a group of war journalists attempt to survive while reporting the truth as the United States stands on the brink of civil war. “

Så over til pensum

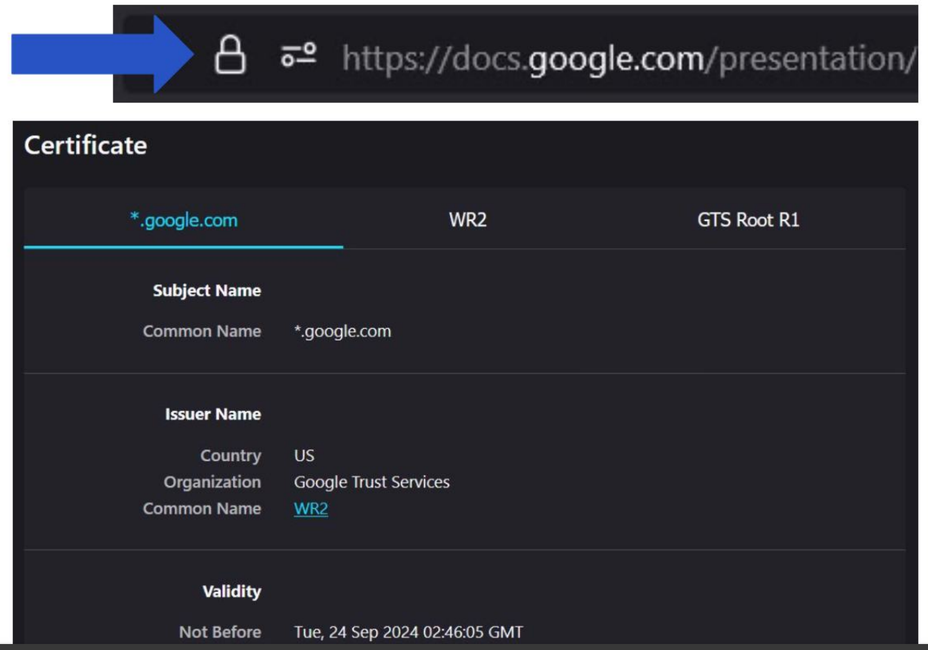
PKI (Public key infrastructure)

Offentlige nøkler er et potensielt svakt punkt i kryptering, derfor brukes PKI for å ha **rammeverk rundt distribuering av offentlige nøkler**, fra tiltrodde tjenere.

Offentlige nøkler kommer med et **sertifikat** som inneholder nøkkelen samt info, slik som f.eks. når nøkkelen går ut på dato og hvilken autoritet som utstedet sertifikatet.

Det **bygger på tillit til autoriteter**. Tjenesten er bedømt som autentisk av en autoritet. Denne autoriteten er bedømt autentisk av En enda høyere autoritet.

Husk! Et sertifikat betyr IKKE nødvendigvis at tjenesten ikke er ondsinnet. Kun at den er autentisk.



Aksessmodeller

Klient-tjener:

- Sentralisert arkitektur
- Forbindelsesstrategier:
  - Pull
  - Push
  - Publish-subscribe
- Data lagres ofte sentralisert på serveren
- Enklere styring og sikkerhetssjekk da kontroll er sentralisert
- Kan kreve kraftige servere for å håndtere høy belastning
- Servere kan bli en enkelt feilpunkt; redundans kan bygges inn
- Eksempler: Web-servere, filservere, e-postservere

Peer-to-Peer:

- Desentralisert arkitektur
- Alle noder kan både initiere og motta tjenester
- Data kan være spredt over flere noder
- Alle noder kan endre og dele data, sikkerhet er vanskeligere å administrere
- Hver node bidrar med ressurser, kan skaleres ved å legge til flere noder
- Pålitelighet: Mer robust mot enkeltfeil siden data er distribuert; dog kan enkelte noder være mindre pålitelige
- Eksempler: Fildelingsnettverk (f.eks. BitTorrent), kryptovalutaer (f.eks. Bitcoin)

Aksessmodeller - Oppgave

4.1 Klient-tjener

Hva kjennetegner aksessmodellen klient-tjener?
Velg ett eller flere alternativer

En tjener lytter etter henvendelser og leverer tjenester på forespørsel.

En klient initierer utvekslingen ved å koble til en tjener og spørre om å få utført en tjeneste.

Nodene kan være både klint og tjener samtidig.

Mange uavhengige noder samarbeider om å tilby en tjeneste.

Det finnes ingen sentralisert kontroll over tjenesten.

Aksessmodeller - Oppgave

4.1 Klient-tjener

Hva kjennetegner aksessmodellen klient-tjener?
Velg ett eller flere alternativer

- [x] En tjener lytter etter henvendelser og leverer tjenester på forespørsel.
- [x] En klient initierer utvekslingen ved å koble til en tjener og spørre om å få utført en tjeneste.
- [ ] Nodene kan være både klint og tjener samtidig.
- [ ] Mange uavhengige noder samarbeider om å tilby en tjeneste.
- [ ] Det finnes ingen sentralisert kontroll over tjenesten.

CDN - Content Delivery Network (Bare for klient-tjener)

- Hvor skal vi lagre data? Bare på kjerneservere?
  - Spørs på popularitet
- Proxy-cache
  - Forward Proxy
    - Server > Internet > Proxy > Klient
    - Nærme klient
  - Reverse Proxy
    - Server > Proxy > Internet > Klient
    - Nærme tjeneren

CDN - Oppgave

17 CDN

Hvilke av disse påstandene er riktige for et Content Delivery Network (CDN)?
Velg ett eller flere alternativer

Den kan redusere forsinkelsen for brukeren ved å flytte data nærmere brukeren.

Den kan avlaste tjeneren som har originaldataene dersom det er mange samtidige brukere.

Den øker sikkerheten siden den virker som en brannmur mot tjeneren som har originaldata.

Den sparer maskinvare og energi ved å virtualisere nettverkstjenestene.

CDN - Oppgave

17 **CDN**

Hvilke av disse påstandene er riktige for et Content Delivery Network (CDN)?
Velg ett eller flere alternativer

- [x] Den kan redusere forsinkelsen for brukeren ved å flytte data nærmere brukeren.
- [x] Den kan avlaste tjeneren som har originaldataene dersom det er mange samtidige brukere.
- [ ] Den øker sikkerheten siden den virker som en brannmur mot tjeneren som har originaldata.
- [ ] Den sparer maskinvare og energi ved å virtualisere nettverkstjenestene.

DNS - Domain Name System

- Hvordan koble seg til en annen maskin?
  - Bruke IP-adresse?
- Nei! DNS er en løsning på dette
- Oversetter fra domenenavn til IP-adresser for oss
- Trestruktur med lokale skop for hver sone
- Spør om IP-adressen, klient-tjener, bruker UDP og TCP
- Gjøres sikrere ved å kombineres med f.eks digital signatur og PKI (DNSSEC)

DNS - Oppgave

2.12 DNS

Hva er DNS-prefetching?

Velg et eller flere alternativer

En tjeneste mellomlagrer MAC-adressen til webtjenere for raskt oppslag.

En tjener mellomlagrer hjemmesider, slik at forespørselen ikke trenger å gå helt til kilden.

En nettleser slår opp IP-adressen på alle domenenavn (URLer) den finner i et webdokument for å spare tid i tilfelle brukeren trykker på linken.

En hjemmerouter lagrer DNS-oppslag slik at brukeren ikke behøver å kontakte en rottjener.

DNS - Oppgave

2.12 DNS

Hva er DNS-prefetching?

Velg et eller flere alternativer

- [ ] En tjeneste mellomlagrer MAC-adressen til webtjenere for raskt oppslag.
- [ ] En tjener mellomlagrer hjemmesider, slik at forespørselen ikke trenger å gå helt til kilden.
- [x] En nettleser slår opp IP-adressen på alle domenenavn (URLer) den finner i et webdokument for å spare tid i tilfelle brukeren trykker på linken.
- [ ] En hjemmerouter lagrer DNS-oppslag slik at brukeren ikke behøver å kontakte en rottjener.

HTTP - HyperText Transfer Protocol

- Protokoll i applikasjonslaget
- Klient spør om webobjekter, tjener sender disse tilbake
- Krever TCP-forbindelse
  - Ikke-persistent (HTTP/1.0)
    - Ny TCP-forbindelse for hver forespørsel
  - Persistent (HTTP/1.1)
    - Flere forespørsler og svar i en forbindelse

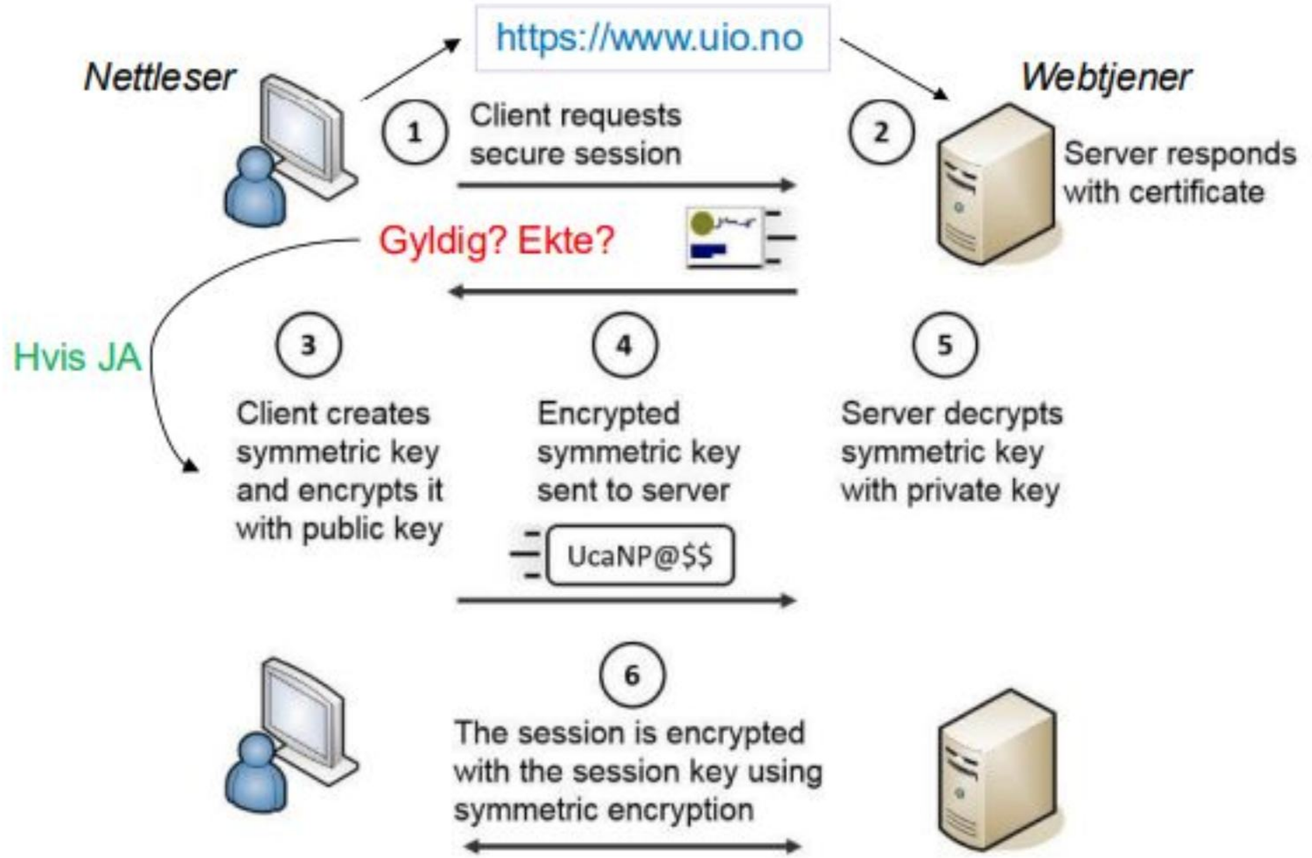
HTTP (part 2)

- Request/response
  - 200 OK
  - 301 Moved permanently
  - 400 Bad Request
  - 404 Not Found
  - 505 HTTP Version Not Supported
- Tjener bruker Cookies for å cache informasjon fra klient
  - Slipper å spørre om det samme senere

HTTPS - HyperText Transfer Protocol Secure

For å:

- Bruke kryptert kommunikasjon mellom klient og tjener
- Sikre autentisitet til tjeneren



Strømming av video

- Ikke det samme som nedlastning av video
- Strøm av data
- Mindre lagring kreves
- Mindre nettverksbruk
- Klient velger kvalitet
- Videoen deles opp i korte segmenter som sendes avgårde
  - Kvalitet på videoen og tilgjengelig nettverk avgjør opplevelsen for klient
- Som regel UDP

HTTP Streaming - Oppgave

4.9 HTTP-streaming

Hvilke utsagn stemmer om streaming av video over HTTP?
Velg ett eller flere alternativer

Video deles opp i små segmenter og forskjellige kvaliteter.

Streaming over HTTP bruker kun UDP til overføring.

Med HTTP-streaming må man bufre hele videoen før avspilling kan starte.

Det er klienten som bestemmer kvaliteten som lastes ned, ikke tjeneren.

Internet of Things (IoT)

- Millioner av duppedingser koblet på internett
- Er det virkelig nødvendig
- Hvorfor?
  - Praktisk eller bare “kult”
- Kan lett angripes av hackere
  - Dårlige sikkerhetstiltak og flere bakdører

Ukeoppgave 10: Tjenestenektangrep

Tjenestenektangrep er en form for angrep som gjerne forbindes med herverk og sabotasje, eller økonimisk kriminalitet i form av utpressing

a. Hvilke sikkerhetsmål påvirkes av denne type angrep?
b. Hvilke ulike former for tjenestenektangrep benyttes ofte av hackere i dag?
c. Hva kan virksomheter gjøre for å sikre seg mot denne typen angrep?

Tjenestenektangrep

DoS-angrep

- Vanlig metode er en buffer overflow: Skriver mer til minnet enn det det er plass til, slik at man kan lure inn ekstra kommandoer som refererer til lokasjoner i minnet.
- Kilden til angrepet er én maskin.

DDoS-angrep

- Når angriper overbelaster tjenesten med forespørsler, slik at den crasher.
- Kilden til angrepet er flere maskiner: Benyttes ofte et botnett, men kan også gjøres manuelt.
- Både DoS og DDoS er vanskelige å sikre seg helt mot, men redundante systemer og blokkering av mistenkelig aktivitet kan hjelpe.

Ransomware

- Forveksles noen ganger med RDoS (ransom DoS)
- Krypterer innhold i systemet, slik at det ikke lenger er tilgjengelig.
- Kan unngås/rettes opp i med god sikkerhetskultur, sikkerhetskopier, brannmurer, VPN, end-to-end-protection

Hvordan brukere kan angripe webtjenester via browser

SQL-injisering

- Bruker gir SQL-kommandoer i innputt-felt
- Kan f.eks brukes som en bakvei som unngår autentisering eller manipulere databaseminnet.

XSS (Cross-Site Scripting)

- Kan skje i input-felt som ikke validerer eller encoder input som skal inkluderes i dynamiske side-elementer som sendes til andre sluttbrukere.
- Eks. mySpace som lot brukere legge inn egen javascript, som førte til Samy-ormen.

HTTP-Cookies

EUs “The cookie law”, eller ePrivacy Directive trådde for alvor i kraft i 2011, og regulerer bruk av informasjonskapsler (cookies) på nettsider. Dette har du nok lagt merke til ettersom nesten alle nettsiden i dag spør om lov til å bruke cookies.

Hvorfor ønsker/ønsker vi ikke at nettsider skal lage cookier for oss?

HTTP-cookies (fasit)

En HTTP-cookie hjelper nettsider med å holde på info om brukere, slik at preferanser ikke tilbakestilles og brukeren logges ut hver gang de går til en annen del av siden.

- Persistente cookies lagres i brukerens sekundærminne, som kan være slitsomt ettersom de tar plass.
- Nettsider bruker dem også å samle mye ekstra info om de besøkende. Hvilke knapper de trykket på, hvor lenge de var der.
- Third party cookies er ofte forbundet med reklame og cookies generelt. Disse er fra andre domener, som kan plante cookiene sine på andre nettsider, ved at sistnevnte brukes ressursene deres, slik som bilder, scripts, etc. Det er ofte disse som gjør at andre nettsider får nyss om hva du har sett på.
- Man har mulighet til å skru av third-party cookies i browseren sin.

15 Minutter pause

Selvstendig arbeid

Spør om hjelp hvis dere lurer på noe :-)

Takk for i dag!

- aanundj@uio.no

Sees neste uke