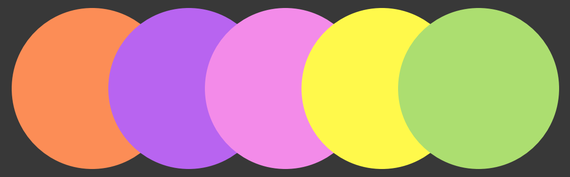
Ånund Kielland Jore

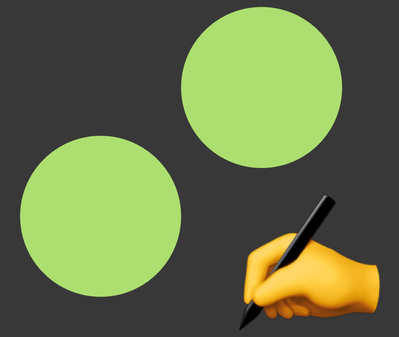
Onsdag 25 September

Datasikkerhet og Nettverk



IN1020

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





Ukens filmtips

Coco - tett bra

Identifikator og autentifikator

Identifikator

- Noe som identifiserer noe(n)
- Kan være et navn, brukernavn, e-post, telefonnummer

Autentifikator

- Noe som brukes for å sjekke om identiteten er autentisk
- F.eks et passord, biometri, fyisk kort eller nøkkel

Ukesoppgave

Du skal kjøpe (rådyre) pensumbøker på Akademika, og bruker et bankkort i kassa for betaling. Hva er egentlig identifikator og autentifikator for et bankkort? Hva identifiserer det? Og brukes 2FA

5 min

Fasit

Både identifikator og autentifikator er i kortet.

Førstnevnte er kontonummer og autentisering skjer via elektronikk som er i kortet. 2FA skjer de gangene du taster inn kode. 2FA her er altså en blanding av noe du har (kortet) og noe du vet (kode)

Autentisering og Autorisering

Autorisering

- Er ikke et sikkerhetsmål
- Det er basert på policy
- Handler om å fordele privilegier, slik som hvem som har lov til å gjøre hva.
- Autentisering er ofte grunnlag for å kunne kontrollere at autorisasjon oppholdes.
- Autorisasjon er ikke teknisk i seg selv, men inngår i tilgangskontroll.

Autentisering

- **Er et sikkerhetsmål**
- **Betyr at personen/enheten/ prosessen det er snakk om er den den gir seg ut for å være**
- **Tenk på begrepet “autentisk”**
- **Autentisitet kan oppnåes via en autentifikator, slik som noe du har (adgangskort, en nøkkel), noe du er (fingeravtrykk, irisscan, ansiktsgjenkjenning) eller noe du vet (passord, pinkode)**

Ukesoppgave

Du er med i utvikling av en webapplikasjon, og tilgangskontroll til denne. Dere vil implementere brukerautentisering der brukere logger seg inn med e-mail og et selvvalgt passord. Du er bekymret for at brukerne deres ikke kommer til å utøve nettvett og vil velge svake passord. Hvordan kan dere gå frem for å hindre dette? Kan bruk av andre autentiseringsfaktorer eller -løsninger være nyttig?

6 min

Sikker tilgangskontroll

- **Tvinge bruker til å lage lange passord med spesialtegn, tall og store bokstaver. -**
  - **Pros: Passordene blir fryktelig vanskelig å gjette eller hacke**
  - **Cons: Folk har en tendens til å lage passord på en forutsigbar måte. Med tall først eller sist, første bokstav er stor og spesialtegn til sist. Mange folk gidder ikke å ha mange kompliserte passord, så de gjenbruker sterke passord mange steder, som betyr at passordet kun er så sterkt som det minst sikre stedet det brukes.**

- **Oppfordre bruker til å ta i bruk tredjeparts passord tjenere**
  - **Pros: du kan ha så mange unike passord du vil uten å måtte huske dem**
  - **Cons: Dersom du trenger å logge inn på en tjeneste på en annen enhet kan dette svekke tilgjengeligheten din til tjenesten.**

- **Innføre 2FA med en tredjepart slik som Google, Microsoft eller ID-porten**
  - **Pros: Øker sikkerheten betydelig, siden angripere ikke kan logge inn selvom passord er lekket.**
  - **Cons: Noen brukere synes det er irriterende å måtte logge inn to ganger**

Ukesoppgave

En kjent sportsbutikk har sin egen nettside som inneholder nettbutikk og en kundeklubb. Brukere kan ta del i kundeklubben ved å lage en profil. Brukerprofilene inneholder data slik som e-mail, navn, adresse og telefonnummer for rask betaling via vipps. I tillegg kan brukere få oversikt over tidligere kjøp de har gjort og samle poeng som kan gi dem rabatter på fremtidige kjøp.

a) Hvilke verdier kan dere identifisere i dette scenarioet?

b) Hvem/hva er mulige trusselaktører?

c) Hvilke sikkerhetsmål vil dere prioritere å gjøre tiltak for å ivareta, og hvorfor?

d) Kan dere tenke ut noen sikkerhetstiltak som vil ivareta disse målene?

10 min

Beskriv kort forskjellene mellom linjesvitsjing (circuit switched) og beskjedsvitsjing (message switched) nett. Hva ligner mest på Internett i dag?

Circuit switching og message switching

Circuit switching

- Linjesvitsjing er ofte forbundet med telefonlinjer
- Det settes opp en dedikert, statisk tilkobling som må opprettes før kommunikasjon kan starte og lukkes når kommunikasjon er ferdig.

Message switching

- Beskjedsvitsjing er mest likt internettkommunikasjon i dag. (I dag brukes noe som heter pakkesvitsjing.)
- Den er tilkoblingsløs, som betyr at data kan ta ulike veier og ikke må følge en etablert kobling hver gang.

Ukesoppgave

Hvilke nettverkstopologier er mest vanlige i dag?

Hvilke sikkerhetsutfordringer har de mest brukte nettverkstopologiene, og hvordan kan vi løse disse utfordringene?

Ukesoppgave

- **En nettverkstopologi er strukturen på hvordan noder i et nettverk er koblet sammen. En node er alle enheter i et nettverk som oppretter, sender, lagrer eller mottar data.**
- **Topologier kan være fysiske, der de er koblet med ledninger eller logiske.**
- **Stjerne- eller tre-topologi med kablet nettverk (Ethernet) og Broadcast-nettverk (WiFi, 4G, 5G) er de mest vanlige topologiene.**
- **Begge disse har svakheter sikkerhetsmessig. Broadcast-nettverk har ikke kontroll på hvilke enheter som lytter til trafikken, så derfor dataen eller nettverket ikke er kryptert kan hvem som helst overvåke det. Med ethernet er dette litt vanskeligere, siden man må ha fysisk tilgang på nettverket for å lytte til trafikken, men i en organisasjon kan dette også forekomme.**

15 Minutter pause

Selvstendig arbeid

Spør om hjelp hvis dere lurer på noe :-)

Takk for i dag!

- aanundj@uio.no

Sees neste uke