



Del 7: Brukerautentisering

Oppgave 1: Passord

- Hvorfor bør passord ikke lagres i klartekst på autentiseringstjeneren?
- Hva menes med passordsalting, og hva er hensikten med det?
- Hvilken kjent tjeneste på internett brukes for å sjekke om en bruker-ID (og passord) kan være stjålet. Sjekk om en av dine egne bruker-ID-er kan være stjålet, og endre passordet hvis den er det.
- Nevn en grunn til at passord aldri bør gjenbrukes..

Oppgave 2: Biometri

- Forklar hvordan kvaliteten på et system for biometrisk autentisering kan uttrykkes med EER (Equal Error Rate).
- Hvis et biometrisk system konfigureres med svært lav FMR (False Match Rate), hva er konsekvensen for FNMR (False Non-Match Rate)?
- Se for deg et system som er konfigurert med svært lav FMR. I hvilken grad gjør det at systemet er robust mot tilsiktet forfalskning (eng. presentation attack)?

Oppgave 3: Veileder for autentisering

- Hva er formålet med å ha en veileder/forordning for e-autentisering?
- Hvilken veileder/forordning for e-autentisering gjelder for Norge?
- Nevn norske autentiseringstjenester som tilfredsstillt krav til høyeste autentiseringsnivå.

Oppgave 4: Passordpolicy

- Et passord regnes vanligvis som en autentikator basert på noe du vet. Diskuter om dette fortsatt er tilfelle når passordet er skrevet ned på papir eller et annet sted.
- Sjekk typiske retningslinjer for passord, f.eks. UiOs beregning av kompleksitet i passord: <https://www.uio.no/tjenester/it/brukernavn-passord/passordtjenester/hjelp/kompleksitet.html> eller passordveileder fra NIST SP800-63B (*Section 5.1.1.2 Memorized Secret Verifiers* og *Section 10.2.1 Usability of Memorized Secrets*) <https://pages.nist.gov/800-63-3/sp800-63b.html>
 - Hva sier retningslinjene om lengde og kompleksitet av passord?
 - Hva sier retningslinjene om krav til bytte av passord?
- I hvilken grad følger UiOs passordpolicy NIST sin veileder?
- Gi et eksempel på kortest mulig passord i henhold til passordpolicyen for UiO.
- Hvorfor er det ofte anbefalt å huske passord, og ikke å skrive ned passord?
- Anta at du ikke er enig med (e), foreslå og diskutere alternative metoder.

Oppgave 5: Biometrisk autentisering og identifisering

- Gi en kort og konsis beskrivelse av hva et biometrisystem er.
- Et biometrisystem kan virke i enten autentiseringsmodus eller identifiseringsmodus. Forklar kort prinsippene for begge moduser.
- Si hvilken av disse modusene er minst/mest effektive, dvs. som krever minst/mest prosessering, og forklare hvorfor.
- Beskriv kort hvilken modus (autentisering eller identifisering) som brukes i) for pass og ii) for kriminalteknisk etterforskning.

Oppgave 6: Optimalisering av biometrisk autentisering

- Skåring s kvantifiserer likheten mellom innhentede biometriprøve og lagret mal av biometriprøve. Forklar hvordan skåring s og terskel T brukes til å bestemme om prøvene er *like par* eller *ulike par*, som fører til henholdsvis *aksept* eller *avvisning*.
- Terskelen T kan justeres for å gi den optimale balansen mellom FMR (False Match Rate) (raten av feil aksept) og FNMR (False Non-Match Rate) (raten av feil avvisning). Forklar hvordan terskelen T bør justeres som funksjon av kostnadene forbundet med henholdsvis tilfeller av feil aksept og feil avvisning.

Oppgave 7: Biometriske modaliteter

- Enhver menneskelig fysiologisk eller atferdsmessige karakteristikk kan brukes som en biometrisk karakteristikk så lenge det tilfredsstiller syv grunnleggende krav. Beskriv kort disse syv grunnleggende kravene.
- I hvilke situasjoner kan det være aktuelt å stille krav til trygghet ved bruk av biometri? Se f.eks. artiklene:
<http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm>
<https://www.nytimes.com/2023/03/29/nyregion/indictments-nyc-gay-bars-homicide.html>
- Beskriv kort i hvilken grad hver av de følgende biometrimodaliteter oppfyller karakteristikkene og tilleggskrav du beskrev under spørsmål (a).
 - Fingeravtrykk
 - AnsiktsgjenkjenningFor bakgrunnsinformasjon, se på artikkelen: "*An Introduction to Biometric Recognition*"
http://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf

Oppgave 8: Passnøkler

- Hvordan utføres phishingangrep mot tradisjonell brukerautentisering?
- Hva betyr det at en autentiseringsmetode er phishingresistent?
- Hvorfor er passnøkler (FIDO/WebAuthn) phishingresistent? Se f.eks. <https://m.youtube.com/watch?v=qMIAqdxNGpc&t=1258>
- Anta at passnøkler blir svært utbredt, slik at klassisk phishing ikke lenger kan benyttes for å stjele identiteter. Foreslå angrep mot phishingresistent brukerautentisering. Se f.eks. <https://blog.talosintelligence.com/what-might-authentication-attacks-look-like-in-a-phishing-resistant-future/>