Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2018
Workshop-spørsmål

Forelesning 9: Brukerautentisering

Spørsmål 1

En bruker er pålogget en nettbank, beskyttet med TLS. Beskriv mulige trusselscenarier der falske transaksjonsdata sendes fra klient til server, til tross for korrekt brukerautentisering.

Spørsmål 2

a. Hva er autentiseringsprotokoller basert på utfordring-svar, og hva er spesielt med slike?
b. Forklar trinnene i protokollen HTTP Digest Access Authentication.
c. Er det nødvendig å kryptere HTTP-forbindelsen for å kunne bruke HTTP Digest Access Authentication? Forklar hvorfor/hvorfor ikke.
d. Kanne passord lagres i hashet/saltet form på serveren når det benyttes HTTP Digest Access Authentication? Forklar hvorfor/hvorfor ikke.

Spørsmål 3

a. Et passord regnes vanligvis som et akkreditiv basert på noe du vet. Diskuter om dette fortsatt er tilfelle når passordet er skrevet ned på papir eller et annet sted.
b. Beskriv kort typiske krav og retningslinjer fra passordpolicyer. Se f.eks. på passordpolicyen fra SANS Institute: https://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines eller UiOs måte å beregne kompleksitet i passord: http://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 https://pages.nist.gov/800-63-3/sp800-63b.html
   - Hva sier passordpolicyene om lengde og kompleksitet av passord?
c. I hvilken grad følger UiOs passordpolicy NIST sin veileder?
d. Gi et eksempel på kortest mulig passord i henhold til passordpolicyen for UiO.
e. Hvorfor er det ofte anbefalt å huske passord, og ikke å skrive ned passord?
f. Anta at du ikke er enig med (e), foreslå og diskutere alternative metoder.

Spørsmål 4

a. Definere hva et biometrisystem er.
b. Et biometrisystem kan virke i enten verifiseringsmodus eller identifiseringsmodus. Forklar kort prinsippene for begge moduser. Si hvilken av disse modusene er den mest effektive og den enkleste å implementere, og forklare hvorfor.
c. Et biometrisystem består av fire hovedkomponenter. Beskriv kort disse komponentene.

Spørsmål 5

a. Enhver menneskelig fysiologisk eller atferdsmessige karakteristikk kan brukes som en biometrisk karakteristikk så lenge det tilfredsstiller fire grunnleggende krav. Beskriv kort disse fire grunnleggende kravene.
b. For praktiske implementering av et biometrisystem bør tilleggskrav også vurderes. Beskriv kort relevante tilleggskrav.
c. Beskriv kort i hvilken grad hver av de følgende biometrimodaliteter oppfyller karakteristikkene og tilleggskrav du beskrev under spørsmål (a) og (b).
   • Fingeravtrykk
   • Ansiktsgjenkjenning
   For bakgrunnsinformasjon, se på artikkelen: "*An Introduction to Biometric Recognition*" http://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf

Spørsmål 6

a. 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*.
b. 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.

Spørsmål 7

Flere stater har nasjonale autentiseringsrammeverk. Det norske rammeverket "*Rammeverk for Autentisering og Uavviselighet*" (RAU) fins online:
http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf
Atandarden ISO29115 **Entity authentication assurance framework** fins på wikien for IN2120:
https://wiki.uio.no/mn/ifi/IN2120-2018/

a. I hvilken grad er autentiseringsnivåene i RAU og ISO29115 kompatible?
b. RAU fokuserer ikke på registrering av identiteter, mens ISO29115 gjør det. Gi en mulig forklaring på hvorfor RAU ikke fokuserer på registrering av identiteter.
c. Diskuter om RAU dekker brukerautentisering av f.eks. EU-borgere for tilgang til norske e-Government tjenester (NAV, skatt etc.)
d. eIDAS-forordningen som innføres i EU i 2018 definerer bare tre autentiseringsnivåer (LoA - Levels of Assurance of authentication), se EUs forordning 2015/1502
   http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002
   Hvorfor besluttet EU å ha bare definere tre autentiseringsnivåer i eIDAS?
e. Hvilke termer betegne hvert autentiseringsnivå i eIDAS?