University of Oslo
IN2120 Information Security
Autumn 2018
Workshop Questions

Lecture 9: User Authentication

Question 1

Assume that a user has authenticated to an online bank, and that the session is protected/encrypted with TLS. Describe possible threat scenarios where false transaction data get sent from the client to the server, despite correct user authentication.

Question 2

a. What are challenge-response authentication protocols, and what is special about these?
b. Explain the steps of the HTTP Digest Access Authentication protocol.
c. Is it required to encrypt the HTTP-connection to make it secure to use HTTP Digest Access Authentication? Explain why / why not.
d. Can the password database at the server-end be hashed/salted when using HTTP Digest Access Authentication? Explain why / why not.

Question 3

a. A password is normally considered to be a credential based on something you know. Discuss whether this is still the case when the password is written down.
b. Briefly explain the typical security policy requirement for password selection. You can look at the sample Password Policy document from SANS Institute at:
https://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines
or at UiO's requirement for password complexity:
http://www.uio.no/tjenester/it/brukernavn-passord/passordtjenester/hjelp/kompleksitet.html
or the guidelines from NIST SP800-63B Section 5.1.1.2 Memorized Secret Verifiers
https://pages.nist.gov/800-63-3/sp800-63b.html
   - What do the password policies say regarding length and complexity of passwords?

c. To what degree does the UiO password policy follow the NIST guidelines?
d. Give an example of the shortest possible password according to the UiO password policy.
e. Why is it often recommended to memorize passwords, and not to write down passwords?
f. Assume that you don't agree with (e), suggest and discuss alternative methods.

Question 4

a. Briefly define the concept of a biometric system.
b. A biometric system may operate in either verification mode or identification mode. Briefly explain the operation in both of these modes. State which of these modes is the most efficient to operate and the easiest to implement, and explain why.
c. A biometric system consists of four main components. Briefly describe these components.

Question 5

a. Any human physiological or behavioural characteristic can be used as a biometric characteristic as long as it satisfies four basic requirements. Briefly describe these four basic requirements.

b. For the practical implementation of a biometric system some additional requirements should also be considered. Briefly describe relevant additional requirements.

c. Briefly describe the extent to which each of the following biometric types satisfies the characteristics and additional requirements you described under questions (a) and (b).
   - Fingerprints
   - Facial recognition

   For background information, look at the article: "*An Introduction to Biometric Recognition"*
   http://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf

Question 6

a. The score ***s*** quantifies the similarity between the collected biometric sample and the stored biometric sample. Explain how the score ***s*** and the threshold ***T*** are used to determine *mate pairs* and *non-mate pairs* between samples, which lead to *accept* and *reject* respectively.

b. The threshold ***T*** can be tuned to provide the optimal balance between FMR (False Match Rate) and FNMR (False Non-Match Rate). Explain how threshold ***T*** should be adjusted as a function of the costs associated with cases of *false accept* and *false reject*.

Question 7

Several governments have national authentication frameworks. The Norwegian framework "*Rammeverk for Autentisering og Uavviselighet*" (RAU) can be accessed at
http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf
The ISO29115 **Entity authentication assurance framework** can be accessed at the INF3510 wiki: https://wiki.uio.no/mn/ifi/INF3510-2018/

a. To what degree are authentication assurance levels of RAU and ISO29115 compatible?

b. RAU does not explicitly focus in identity registration, whereas ISO29115 does. Give a possible explanation for why RAU does not focus on identity registration.

c. Discuss whether RAU covers user authentication for e.g. EU citizens to access Norwegian e-Government services.

d. The eIDAS regulation to be implemented in the EU in 2018 only provides three different LoA (Levels of Assurance) for authentication, see EU Regulation 2015/1502
   http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002
   Why did the EU decide to specify only three levels of authentication assurance in eIDAS?

e. What are the terms used to denote each LoA in eIDAS?