University of Oslo
INF3510 Information Security
Spring 2011
Workshop Questions

Lecture 7: Authentication

Question 1

a. What is the limitation of user authentication for protection of communication?
b. What is a challenge-response authentication protocol, and what is it's purpose?
c. Mention 3 cryptographic methods of achieving message authentication.

Question 2

Browse through the article by Richard Smith on the Strong Password Dilemma http://www.cryptosmith.com/password-sanity/dilemma and review the lecture notes on passwords.

a. Briefly describe the problems and limitations associated with reusable passwords.
b. Briefly explain the typical security policy requirement for password selection. You can look at the example Password Policy document at:
   http://www.sans.org/resources/policies/Password_Policy.doc
   or at UiO's requirements for acceptable and secure passwords at:
   http://www.uio.no/tjenester/it/brukernavn-passord/passord.html
c. In particular check what advice is given (if any) by the policy and requirements referred to under (b) regarding using the same or similar passwords for different services.
d. Why is it often recommended to memorize passwords, and not to write passwords down?
e. Assume that you don't agree with (d), suggest alternative methods for managing personal passwords, and discuss their security issues.

Question 3

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 of both of these modes. State which of these modes is easier to implement and explain why.
c. A basic biometric system consists of four main modules. Briefly describe these modules.

Question 4

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 three additional requirements should also be considered. Briefly describe these three additional requirements.
c. Briefly describe the extent to which each of the following biometric types satisfies the characteristics and issues you described for parts (a) and (b).
   • Fingerprints
   • Facial recognition
   For background information, look at the article: "*An Introduction to Biometric Recognition*"
   http://www2.citer.wvu.edu/members/publications/files/RossBioIntro_CSVT2004.pdf

Question 5

a. The response of a biometric matching system is the score s that quantifies the similarity between the input sample and the stored sample. Explain how the score s and the threshold T are used to determine mate pairs and non-mate pairs between the samples.
b. The threshold T should be tuned to provide the optimal balance between FMR (False Match Rate) and FNMR. Explain roughly the principle for adjusting threshold T as a function of the costs associated with false match and false non-match.

Question 6

a. SMS-based authentication schemes are often used to secure web transactions. Briefly describe a typical protocol used in an SMS-based authentication scheme?
b. What type(s) of authentication can SMS-based authenticaiton provide?
c. Assume that a criminal organisation wants to attack an online bank that uses an SMS-based authentication scheme. Which systems on the user side would need to be compromised, and what types of attacks against those systems would be necessary to make the attack possible. Read about recent attacks in e.g.: http://packetstormsecurity.org/news/view/18675/ZeuS-Trojan-Attacks-Banks-2-Factor-Authentication.html

Question 7

Several national governments have specified national authentication frameworks. The Norwegian FADS "*Framework for Authentication and Digital Signatures*" can be accessed at http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf
The Australian NeAF "*National e-Authentication Framework*" can be accessed at: http://www.finance.gov.au/e-government/security-and-authentication/docs/NeAF-framework.pdf

a. To what degree are the authentication assurance levels of FADS and NeAF compatible?
b. FADS does not explicitly focus in identity registration, whereas NeAF does. Give a possible explanation for why FADS does not focus on identity registration.
c. How many Authentication Assurance Levels (AAL) does NeAF specify and what are they called?
d. What does "Identity Registration Assurance Level 0" means in the NeAF terminology?
e. NeAF specifies the possibility of registering anonymous identities. Explain why it could be meaningful to have high authentication assurance level in a pseudonym identity?