University of Oslo
INF3510 Information Security
Spring 2010
Workshop Questions

Lecture 4: 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.hf.uio.no/it/student/eng_passordvedUiO.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

On Unix systems it is generally not recommended to store passwords in clear on the server side because attackers who get access to the password file will have immediate access to all the passwords. Instead the hash value of passwords should be stored on the server.

a. How can a Unix system verify user passwords when only their hash values are stored on the server?
b. Read the Wikipedia entry on password salting at: http://en.wikipedia.org/wiki/Salt_%28cryptography%29 What is the purpose of password salting?

Question 4

a. Briefly define the concept of a biometric.
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 four modules.

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 requirements.
b. In a practical biometric system (a system that employs biometrics for personal recognition) there are three other issues that should be considered. Briefly describe the purpose and operation of these three 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 6

a. The response of a biometric matching system is the matching score s that quantifies the similarity between the input and the stored template representation. Briefly explain how the matching score and the threshold t are used to determine mate pairs.
b. Briefly define the terms false match rate (FMR) and false non-match rate (FNMR).
c. There is a trade-off between false match rate (FMR) and false non-match rate (FNMR) in every biometric system.
   (i) Briefly explain how the FMR and FNMR are related to the threshold t.
   (ii) Briefly explain the equivalent trade-off when using passwords.

Question 7

Hardware tokens are an example of object-based authentication – something you have.

a. The synchronised password generator is one method to provide user authentication. Describe the operation of the synchronised password generator method using clock-based tokens.
b. Briefly explain the operation of a token-based challenge-response system.
c. Describe one major advantage and one major disadvantage of the above two methods compared to standard user-selected passwords.
d. Compare the above two token-based methods with each other. What is a possible advantage of each compared with the other?

Question 8

a. What is the difference between a digital signature and an electronic signature?
b. Mention the 3 main parties involved in electronic/digital signatures
c. Explain the property of WYSIWYS (What You See Is What You Sign). You can e.g. look at the Wikipedia article on Digital Signature.
d. Describe some of the challenges for making digital/electronic signatures acceptable as legal evidence.