

Assignment 2

Submit your write-up as a pdf document on blackboard. Include your full name at the writeup. Name the writeup as x-assignment2.pdf, where x is your first and last name.

- I. Exercise 1, Chapter 2. Describe each of the following three(3) kinds of access control mechanism in terms of:
- i. ease of determining authorized access during execution
 - ii. ease of adding access for a new user
 - iii. ease of deleting access by a user
 - iv. ease of creating a new object (file, program, database, etc.) which all users have, by default, access.

Access control mechanisms:

- per-user access control lists - one list for each user determinizes all the objects the user has access to.
- per-object access control list - each object has a list of users who have access.
- access control matrix.

- II. Exercise 11, Chapter 2. Outline the design of an authentication scheme that "learns". The scheme would initially have some information about a user - e.g. the username and password. As the use of the computing system continued, the authentication system would "gather" additional information, e.g. programming languages used, dates and times of use, etc. The authentication requirements would become more personalized with time.
- A. List the types of information the system could gather. Assume that the authentication scheme is for a laptop or a phone.
 - B. Consider how the authentication information would be presented and validated. Does the user answer true/false or multiple-choice questions? Does the system need to interpret natural language prose?
- III. Research the Advanced Encryption Standard on-line.
- A. What key lengths are used today for TOP SECRET government usage?
 - B. When did the National Security Agency decide that AES could be used to encrypt classified documents?
 - C. Describe one-type of attack against AES.