

Information and Communications Security SS 11 Assignment 2

Fachbereich
Wirtschaftswissenschaften

Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security
www.m-chair.net

Prof. Dr. Kai Rannenberg
M.Sc. Ahmad Sabouri
Dipl.-Ing. (FH) Christian Weber MBA

Telefon +49 (0)69-798 34705
Telefax +49 (0)69-798 35004
E-Mail sec@m-chair.net

Study the following questions and return your answers by email to ahmad.sabouri@m-chair.net, before **2nd of May 2011, 18:00 pm**.

Exercise 1:

Alice can read and write to the file x, can read the file y, and can execute the file z. Bob can read x, can read and write to y, and cannot access z.

- Write a set of access control lists for this situation. Which list is associated with which file?
- Write a set of capability lists for this situation. With what is each list associated?

Exercise 2:

- Name a fundamental difference between the security model of Bell-LaPadula and the Chinese Wall Model. What are the additional security assets that the Chinese Wall Model is supposed to refer to?
- The concept of roles has been introduced to you during the last lectures. Please describe this concept briefly.
- Please assume that you are working for the University of Frankfurt as a research assistant after having received your diploma. Please identify four different roles that you might be authorised to assume. Please note for each identified role one or two problems that might be encountered by a role-based access control model.

Exercise 3:

Revocation of an individual's access to a particular file is easy when an access control list is used. How hard is it to revoke a user's access to a particular set of files, but not all files? Compare and contrast this with the problem of revocation using capabilities (capability lists, c-lists).

Exercise 4:

Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.

- a) Paul, cleared for (TOP SECRET, {A, C}), wants to access a document classified (SECRET, {B, C}).
- b) Anna, cleared for (CONFIDENTIAL, {C}), wants to access a document classified (CONFIDENTIAL, {B}).
- c) Jesse, cleared for (SECRET, {C}), wants to access a document classified (CONFIDENTIAL, {C}).
- d) Sammi, cleared for (TOP SECRET, {A, C}), wants to access a document classified (CONFIDENTIAL, {A}).
- e) Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, {B}).

Exercise 5:

Consider an access control method that wants to allow an object to have more than one owner. Explain how you would implement this with both ACLs and capabilities.