University of Oslo
INF3510 Information Security
Spring 2010
Workshop Questions

Lecture 5: Access Control and Security Models

QUESTION 1

In access control terminology, specific terms are being used to describe different roles.

a. What are subjects?
b. What are objects?
c. What are resource owners?
d. Who performs authorization and who is being authorized?

QUESTION 2

a. In the access control policy enforcement phase, several sequential steps are required before an authorized party is given access to a resource. Name these steps in the correct order.
b. In the WS-Security terminology, what are the respective names of the functional points where i) the access control policy is stored, ii) the access control decision is made, and iii) the access control decision is enforced?

QUESTION 3

a. Briefly define the concept of discretionary access control (DAC) and how it is usually implemented.
b. Briefly define the concept of mandatory access control (MAC) and how it is usually implemented.
c. Assume that an access control system uses labels defined as $L = (h, c)$ where $h \in H$ (a set of ordered hierarchical security levels) and $c \subseteq C$ (a set of categories). How many different labels can be defined in this system? You must consider the cardinalities of H and C.

QUESTION 4

The Bell-LaPadula model was first described in the 1970s and is a formal model of a computer security policy designed to provide access control based on information sensitivity and subject authorizations.

a. Identify the major security goal of the Bell-LaPadula security model.

b. Give an example of an environment where the use of the Bell-LaPadula security model is appropriate.

c. Give an example of a suitable set of hierarchical security levels.

d. Briefly explain the concept of partially-ordered security levels and why partially-ordered security levels are necessary.

e. Briefly define 'domination' with respect to security labels.

f. Briefly describe the security properties of the Bell-LaPadula security model:
(i) Simple security property (ss),
(ii) Star property (*), and
(iii) Discretionary security property (ds).

g. Specify simpler definitions of the ss-property and the *-property in terms of the subject current label L^{SC}. In fact, 30 years after the publication of the original Bell-LaPadula model David Elliott Bell wrote a paper entitled "Looking Back at the Bell-La Padula Model" where he admits that the definitions of the ss and * properties where more complicated than necessary, see: http://www.acsac.org/2005/papers/Bell.pdf.

QUESTION 5

A given access control system is based on the Bell-LaPadula model. The security levels, ordered from highest to lowest, are TOP SECRET, SECRET, CONFIDENTIAL and UNCLASSIFIED and the categories are A, B and C. Assume that discretionary access control allows all accesses unless otherwise specified. Determine whether the requested access is allowed in each of the following cases. Provide a clear justification in terms of the properties of the Bell-LaPadula model.

a. User has label L^{SM} = (TOP SECRET, {A, C}) and wants to view a document whose security label is L^{O} = (SECRET, {B, C}).

b. User has label L^{SM} = (SECRET, {C}) and wants to view a document whose security label is L^{O} = (CONFIDENTIAL, {C}).

c. User has L^{SM} = (TOP SECRET, {A, C}) and wants to view a document whose security label is L^{O} = (CONFIDENTIAL, {A}).

d. User has L^{SM} = (UNCLASSIFIED, {A, B, C}) and wants to view a document whose label is L^{O} = (CONFIDENTIAL, {B}).

e. User with L^{SM} = (SECRET, {A, B}) wants to view a document X which has the security label L^{O}_{X} = (SECRET, {A,B}), while simultaneously writing to a document Y with security label L^{O}_{Y} = (CONFIDENTIAL, {A}).

f. User with L^{SM} = (TOP SECRET, {A,B}) wishes to view a document X which has security label L^{O}_{X} = (SECRET, {A}), while simultaneously writing to a document Y with L^{O}_{Y} = (SECRET, {A,B}).

g. User has a label L^{SM} = (CONFIDENTIAL, {A, C}) and wants to write to a document whose label is L^{O} = (CONFIDENTIAL, {B}).

QUESTION 6

a. Give an example of an application environment for the Brewer-Nash Chinese Wall model.
b. Explain the term conflict of interest.
c. In terms of the Brewer-Nash Chinese Wall model, briefly describe what is meant by the terms: (i) Objects, (ii) Company datasets, and (iii) Conflict classes.
d. Briefly describe the access matrix N used in the Brewer-Nash Chinese Wall model.
e. Briefly explain how the Brewer-Nash Chinese Wall model achieves:
• Brewer-Nash Simple security (BNss) property, and
• Brewer Nash Star (BN*) property.

QUESTION 7

A large advertising company handles campaigns for a number of different clients, including two competing detergent manufacturers Suds-Oh and Bubbles, and two rival soft drink manufacturers Fizzo and So-Low. Information related to these companies is contained in a total of ten different objects, with the relationships as follows:

Suds-Oh:	Object 1, Object 2, Object 3
Bubbles;	Object 4, Object 5
Fizzo:	Object 6, Object 7, Object 8
So-Low:	Object 9, Object 10

A Brewer-Nash Chinese Wall security model has been implemented. The *i*-th row of the access permission matrix N is as follows:

Object nr.	1	2	3	4	5	6	7	8	9	10
Subject *i*	T	F	T	F	F	F	F	T	F	F

Which of the following access requests by Subject *i* would be granted? Provide a clear justification for your decision in terms of the properties of the Brewer-Nash security model.
a. Read only access to Object 9
b. Read only access to Object 2
c. Simultaneous read access to Object 8 and write access to Object 3
d. Simultaneous read access to Object 8 and write access to Object 7

QUESTION 8

RBAC (Role Based Access Control) is suitable for enforcing the separation of duties and least privilege principles.
a. What is separation of duties, and why is it useful?
b. How can the principle of separation of duties be implemented with RBAC?
c. What is least privilege, and why is it useful?
d. How can the principle of least privilege be implemented with RBAC?