University of Oslo
INF3510 Information Security
Spring 2011
Workshop Questions

Lecture 8: Identity and Access Management

QUESTION 1

a. Briefly explain the following concepts related to identity management.
   (i) Entity.
   (ii) Identity.
   (iii) Name (identifier).
   (iv) Digital identity
b. Briefly explain what is meant by the concept "identity management".
c. Explain what is meant by AAA services, and why this name partially is a misnomer

QUESTION 2

a. Briefly describe the silo identity model for management of user identities.
b. Describe advantages of the silo model.
c. Describe disadvantages of the silo model.

QUESTION 3

a. Briefly describe the federated model for management of user identities.
b. Describe advantages of the federated model.
c. Describe disadvantages of the federated model.
d. Briefly explain what is meant by user-centric identity management.

QUESTION 4

SAML specifies two (2) different protocol profiles for browser SSO (single sign-on)
a. Name of each of these two (2) profiles.
b. Briefly explain the two (2) profiles.
c. Which profile could be considered more secure and why?

QUESTION 5

A new identity and access model promoted by Microsoft is called U-Prove, see
http://blogs.msdn.com/b/card/archive/2011/02/15/beyond-windows-cardspace.aspx
a. Will U-Prove be added to, or will it replace the existing CardSpace model that has been promoted by Microsoft in the last few years?
b. What is the main service(s) provided by U-Prove, and what type of cryptographic mechanism/token is used to support the service(s)?

QUESTION 6

a. Name the functional steps related to identity and access management that are required before an authorized party can access a resource during operations.
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 7

a. Briefly define the concept of discretionary access control (DAC) according to TCSEC.
b. Briefly define the concept of mandatory access control (MAC) acording to TCSEC.
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 8

The Bell-LaPadula model 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 Bell-LaPadula 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).

QUESTION 9

A large advertising company handles campaigns for a number of different clients, including two competing detergent manufacturers Whizzo and Oh-Mo, 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:

Whizzo: Object 1, Object 2, Object 3
Oh-Mo; 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, corresponding to subject *i*'s previous accesses, 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 10

RBAC 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?