University of Oslo
IN2120 Information Security
Autumn 2018
Workshop Questions

Lecture 10: 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 of IAM (Identity and Access Management).

Question 2

a. Name the phases of IAM
b. What does *identification* mean from the user side, and from the SP side?
c. Explain the correct as well as the incorrect but common interpretation of authorization.

Question 3

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

Question 4

Federated Id management models can have centralised or distributed authentication, and can have centralised or distributed name spaces, and sometimes use a centralised broker. Identify prominent examples of different federated Id systems in use on the Internet, see where they fit in the table below, and explain in what way they are centralised or distributed. Consider e,g, Aadhaar (Indian Unique Identity), Eduroam, Facebook Connect, FEIDE, Google+, Id-porten, HelseId, and others that you can think of.

	Centralised namespace	Distributed namespace
Centralised authentication		
Distributed authentication		

Question 5

SAML specifies two different authentication protocol profiles for identity federation.

a. Briefly explain the two profiles.
b. Which profile does **not** relay the security assertion (crypto token) via the client browser ? Is this an advantage ? Why / Why not ?

Question 6

a. Briefly define the concept of discretionary access control (DAC) (identity-based access control) according to TCSEC.
b. Briefly define the concept of mandatory access control (MAC) (label-based access control) according to TCSEC.
c. Which form(s) of access control is/are typically implemented in
    i) Commercial systems
    ii) Military systems

Question 7

The Bell-LaPadula model (BLP) 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. Briefly describe the security properties of the Bell-LaPadula security model:
    (i) Simple security property (ss),
    (ii) Star property (*)

Question 8

ABAC (Attribute-Based Access Control) is a flexible model for access control.

a. Mention the 4 sources of attributes used in ABAC.
b. Explain how DAC can be implemented with ABAC.
c. Explain how MAC can be implemented with ABAC.
d. Explain how RBAC can be implemented with ABAC.

Question 9

What is the role of XACML when implementing ABAC systems ?