Lecture 9: 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 and management".

Answer

a. The meaning of the concepts:
   (i) Entity: A person, organisation, agent, system, etc.
   (ii) Identity': A set of attributes of an entity in a domain
   (iii) Name: An attribute that points to a (specific) entity within a domain
   (iv) Digital identity: Identity resulting from digital codification of attributes in a way that is suitable for processing by computer systems
b. **Identity and access management (IAM)** is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons.

QUESTION 2

a. Name the phases of IAM
b. Is *identification* something that the user does, or something that the SP does?
c. Explain the correct as well as the incorrect but common interpretation of authorization.

Answer

a. Configuration phase, operation phase (and termination phase)
b. Identification by the user means "to claim an identity", which the SP can verify by checking user credentials such as a password. Identification by the SP means that the SP somehow can select a specific identity in the list of users based on some attributes, which e.g. can be biometrics, and the SP does not necessarily need to verify the identity any further.
c. The correct interpretations of authorization:
   i)   The correct interpretation of authorization is "to specify access policy" which happens during configuration phase.
   ii)   The incorrect but unfortunately common interpretation of authorization is "to grant access" which happens during operation phase.

QUESTION 3

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

Answer

a. In the silo model SP = IdP, where SP defines name space and provides credentials and names to each user.
b. i) Advantages: Simple to deploy, low cost for SPs
   ii) Disadvantages: Identity overload for users, poor usability

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. Find real examples of different federated Id systems, and see where they fit in the table below. 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		

Answer

Fill in table, see p.13 in lecture presentation L09 2018.

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 ?

Answer

a. Browser Post (Token via Front-channel) and Browser Artifact (Token via Back-channel).
   In the Browser Post profile the IdP passes the cryptographic token via the user's browser which forwards it to the SP. In the Browser Artifact profile the IdP passes an artifact (reference) via the user's browser to the SP. Then the SP requests the cryptographic token by sending the artifact directly to the IdP which returns the token via back channel.
b. Browser Artifact profile, because the security token passes directly from the IdP to the SP. Possible security advantage is that token can not be intercepted in client domain.

QUESTION 6

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

Answer

a. With DAC the access authorization policy is specified with names of subjects (users) and objects (files etc.). DAC is therefore often called name-based access control. The term 'discretionary' refers to the property that an individual owner of a object can authorize access at his/her 'discretion'. DAC is normally implemented with ACL (access control list) associated with each object/domain.
b. With MAC the access authorization policy is defined with labels associated with subjects and objects. A subject label is typically called 'security clearance' and an object label is typically called a 'classification level'. MAC is therefore often called label-based access control. The logic for comparing the labels and making an access approval decision is typically based on the Bell-LaPadula model. MAC is called 'mandatory' because the owner of an object can not at his discretion authorize other users access to the object. It is the authority who assigns security clearance and classification levels who then 'mandates' the access control policy.
c. i) DAC
   ii) MAC and DAC

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 (*)

Answer

a. Confidentiality
b. Military
c. The BLP properties are
- ss-property: Suppose a subject has read access to an object. The ss-property is satisfied if the current subject label is equal to, or higher than the object label.
- *-property: Suppose a subject has write access to an object. The *-property is satisfied if the current subject label is equal to, or lower than the object label.

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.

Answer

a. i) Subject attributes, ii) Object attributes, iii) Context attributes, iv) Action attributes
b. Define ACL as object attribute for each object, where authorized subject name(s) and authorized action(s) are defined. Then use the subject name as subject attribute and the requested access mode(s) as action attributes. It is straightforward to define a policy for making access decisions based on these attributes, i.e.: approve access when subject name and requested action are specified in the ACL of the requested object.
c. Define security clearance as subject attribute, and classification level as object attribute. Then use the requested access mode as action attribute. The policy can e.g. be based on the Bell-LaPadula model.
d. Define ACL as object attribute for each object, where authorized subject roles(s) and authorized action(s) are defined. Then define available roles as subject attribute for each subject. During user authentication the user must activate a specific role so that the this role becomes an active attribute. It is straightforward to define a policy for making access decisions based on these attributes, i.e.: approve access when subject role and requested action are specified in the ACL of the requested object.

QUESTION 9

What is the role of XACML when implementing ABAC systems ?

Answer

The attributes for subjects, objects, context and action need to be communicated between the various parties in a distributed access control domain. To make this practical a common language for expressing attributes is needed, and this is precisely what XACML does.