University of Oslo
INF3510 Information Security
Spring 2014
Workshop Questions

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 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 management consists of representing and recognising entities as digital identities, for managing name spaces, for assigning unique names to entities, for assigning access credentials/tokens to entities, and provides a basis for Authorization, Authentication, Access Control and Accounting.

QUESTION 2

Look at lecture 1, page 51.
a. Name the 3 phases of identity and access management
b. Name the functional steps during the operations phase that are required before an authorized party can access a requested resource.
c. Explain the two common but inconsistent interpretations of authorization.

Answer

a. Configuration phase, operation phase and termination phase
b. Identification, authentication, and access control.
c. Two common interpretations of authorization:
   i) authorization as defining access policy during configuration phase (OK)
   ii) authorization as granting access (access control) during operation phase (not OK)

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

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

Answer

a. Identity Federation: A set of agreements, standards and technologies that enable a group of SPs (service providers) to recognise user identities and entitlements from other SPs and IdPs (Identity Providers). Identifier (and credential) provisioning can be as for the silo model, or it can be managed by a centralized IdP. Authentication by one IdP/SP is communicated in the form of a cryptographic token (security assertion) to other SPs. Provides SSO in open environments.
b. i) Advantages: Improved usability by allowing single Id & credential in federated domain, and by allowing SSO, Can be compatible with silo user identity domains, Can allow SPs to bundle services. Can allow SPs to collect user information
   ii) Disadvantages: High technical and legal complexity. High trust requirements and need for legal agreements. Privacy issues because IdP receives info about every service accessed. Unimaginable for all SPs to federate, multiple federated SSOs, so Fed-IdMan does not eliminate the need to manage multiple sets of Id/Cred.

QUESTION 5

SAML specifies two different protocol profiles for browser SSO (Single Sign-On)
a. Name and briefly explain the two profiles.
b. Which profile does **not** relay the security assertion (crypto token) via the client browser ? Is this an advantage ?

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.
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 '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

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?

Answer

a. Separation of duties means that the same person should not fill multiple roles where there can be a conflict of interest, or where it can be required to take extra precautions in the form of involving multiple entities to perform an action.
b. Item, separation of duties can be implemented by assigning specific roles to different persons. It can formally be enforced by specifying that two roles are mutually exclusive, in the form of SSD (Static Separation of Duties).
c. Least privilege means that a user or role should not have more privileges than is necessary to fulfill required tasks. This is useful to avoid abuse of power, and to avoid excessive consequences of error.
d. Least privilege can be implemented by conservative assignment of permissions to roles, and by specifying constraints on simultaneous role invocation in the form of DSD (Dynamic Separation of Duties)

QUESTION 9

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 10

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.