University of Oslo
INF3510 Information Security
Spring 2012
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

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.
c. AAA means "Authentication, Authorization and Accounting. The use of "authorization" is a misnomer because the intended meaning is "access approval".

QUESTION 2

a. Name the 3 phases of identity and access management
b. Name the functional steps related to identity and access management that are required before an authorized party can access a resource during operations.
c. Explain the two interpretations of authorization.

Answer

a. Registration phase, operation phase and termination phase
b. Identification, authentication, and access approval.
c. i) Authorization as definition of access rights policy during registration phase, and ii) autorizaiton as granting of access 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

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. Identifier (and credential) issuance as for the silo model Mapping between a user's different unique identifiers Authentication by one SP/IdP (identity provider), communicated as security assertions to other SPs. Provides SSO in open environments
b. i) Advantages: Improved usability (theoretically) Compatible with silo user identity domains Allows SPs to bundle services Allows SPs to collect user information
   ii) Disadvantages High technical and legal complexity. High trust requirements, e.g. SP1 is technically able to access SP2 on user's behalf. Privacy issues. Unimaginable for all SPs to federate, multiple federated SSOs not much better than the silo model

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 could be considered more secure and why?

Answer

a. Browser Post (Token via Front-End) and Browser Artifact (Token via Back-End).
   The Browser Post profile is via the user's browser only. The Browser Artifact profile is using an artifact with an additional back channel communication.
b. Browser Artifact, because the security token never passes through the user's browser and can not be intercepted there

QUESTION 6

a. What is required, technically and legally, to become an Identity Provider) for OpenId?
b. What is the format of a name (identity) in OpenId?
c. How can a service provider make sure that a user with an identity for OpenId has registered the identity with a serious OpenId IdP?

Answer

a. You need a domain name with IP address and a web server. Then install OpenId server software and start offering registration of identities for OpenId. No legal requirements.
b. The format is <name within domain>.<domain name>
c. The SP can define a list of accept OpenId IdPs (identity providers) so that only users from accepted IdPs are accepted.

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) according to TCSEC.
c. Which form(s) of access control is/are typically implemented in
    i) Commercial systems
    ii) Military systems

Answer

a. A system operating under Discretionary Access Control allows an individual user of the system to define access control rights to an object of the system for all subjects of the system. It is normally implemented with ACL (access control list).
b. A system operating under Mandatory Access Control requires the system to enforce a set of rules to control access to an object by all subjects and subjects may not by-pass these rules. It is normally implemented with security labels.
c. i) DAC
   ii) MAC and DAC

QUESTION 8

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 (*), and
   (iii) Discretionary security property (ds).

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.
    - The ds-property of BLP demands that the current access by the subject to any object is permitted by the DAC access permission matrix (or ACL).

QUESTION 9

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 10

What is the role of OAuth in the Web 2.0 environment?

Answer

OAuth provides a way to grant access to your user data on a website to a third party website, without needing to provide this third party website with your authentication information for the first website."