SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1 2014

Tutorial Questions for L5: Access Control Principles

*Attempt these questions **before** you attend your workshop/tutorial session, and bring your prepared answers with you. Come prepared to discuss your answers and/or any problems you encountered in trying to answer these questions.*

QUESTION 1

Read through Clause 7 Asset Management of *AS27002:2006 Code of practice for information security management* to answer the following questions:

a) Why is it important to create an inventory of assets as a first step in determining an access control policy?

b) Why is it important to determine the sensitivity of assets when determining an access control policy?

c) What is an access control policy? What should access decisions be based on? (Also need to check AS27002:2006 Clause 11.1.1. for this)

d) Read the 2011 story '*Season of TV shows blown out of cloud... for good*' available at: http://www.theregister.co.uk/2011/04/04/cyberlynk_zodiac_island/. To avoid this sort of incident, which aspects of Clause 7 do you think would be useful for the production company WeR1 to consider?

a) Inventories help to ensure that effective asset protection takes place. Need to identify all assets, and document the importance, the business value and the security classification of each.

b) Determining the sensitivity of assets is important, so that appropriate protection can be applied.

c) A statement that includes the access control rules and rights for each user or group of users. Based on business and security requirements for access.

d) Lost TV show: most of Clause 7 would be useful.

   a. From Clause 7.1, WeR1 should have identified the TV show files as important assets, and known where the asset was located, the business value of the files, and backup details in the event of a disaster.

   b. From Clause 7.2, WeR1 should have classified the files and known how critical they were to the organisation. If WeR1 had defined appropriate

procedures for secure processing, storage etc for files classified as critical, and then applied these procedures it is possible the situation may have been avoided.

c. **Note: Clause 6.2.3 could have been useful in forming the agreement with CyberLynk regarding WeR1's security requirements for their resources.**

QUESTION 2

Access controls can be physical or logical. Physical access control is discussed in Section 9.1 of *AS27002:2006 Code of practice for information security management*, and logical access control is discussed in a number of sections, including Section 11.

a) Give three examples of control mechanisms for each access control category.

b) Which factors might influence the decision taken by an organisation to use a particular control mechanism?

a) Examples:

   a. Physical access control mechanisms include walls, gates, locks, guards, etc

   b. Logical access control mechanisms include passwords, PINs, challenge-response

b) Decisions are influenced by type of asset being protected, location of asset, environment, cost of protection, sensitivity of asset (cost of failure to protect), etc.

QUESTION 3

When discussing access control, what is meant by each of the following terms or phrases?

a) Subjects

b) Objects

c) Resource owners

a) Subjects are active entities in the system (for example users, processes, other computers), that cause information to flow among objects or change the system state.

b) Objects are passive entities in the system that contain or receive information. Objects are repositories of information such as disks, files and datasets. Objects are the resources being accessed.

c) Resource owners are those who have responsibility for the resource objects, control them, may give access privileges and implement the access control mechanisms.

QUESTION 4

Briefly define the concepts of:

a) Discretionary access control (DAC).

b) Mandatory access control (MAC).

c) Role-based access control (RBAC).

a) 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.

b) 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.

c) In role-based access control access rights are based on the role of the subject, rather than the subject's identity. A role is a collection of procedures or jobs that the subject performs.

QUESTION 5

Two commonly applied guidelines in access control are the *need to know principle* and *separation of duties*.

a) Describe what is meant by each of these two principles.

b) To what extent can mandatory access control (MAC) be used to implement the *need to know principle*?

c) Explain how role-based access control (RBAC) can be used to implement *separation of duties*.

a) Descriptions:

a. The <u>need to know principle</u> says that access should be granted to users only when they have a need for that access to complete their job functions.

b. <u>Separation of duties</u> involves breaking tasks into multiple components, with each component performed by different entities, so that cooperation is required to complete the task.

b) Mandatory access control provides only limited ability to implement the need to know principle. For example, typical MAC rules make use of user clearances and object classification based on hierarchical levels. A user who fits such a rule will have access regardless of whether that user has a current need to access the data or not.

c) In RBAC a user can only take on one role at any one time. Therefore separation of duties can be implemented by ensuring that users in two different roles are required to complete a task.

QUESTION 6

Access control can be considered as occurring in two phases: *policy definition* and *policy enforcement*. In the *policy enforcement* phase several steps are required before an authorised party is permitted access to a resource. Explain these steps in the order they must occur.

Before an authorised party is permitted access to a resource, the system must check that the requested access is authorised. The required steps are (see slides 41 and 42):

a) **Identification (requester claims an identity),**
b) **Authentication (the process of verifying the requester is the identity they claim to be)**
c) **Verification of authorisation (checking that the authenticated identity is authorised for the type of access requested).**

QUESTION 7

Authentication of system users can be grouped into four general categories:

1. Knowledge based
2. Object based
3. ID based
4. Location based

a) For each of these categories,
   a. Describe the major characteristic.
   b. Give an example.
   c. Describe one advantage and one disadvantage.
b) What is two-factor authentication?
   a. Give an example, and explain the advantage of this approach.

Knowledge based:

a) **Secret or obscure - something only the user would know**
b) **PIN, password, etc**
c) **Advantage: Easy to implement, readily accepted**

Disadvantage: Can be shared by user, user may be unaware of compromise

Object based:

a) **Something that the user can provide - User has physical possession of a token**
b) **Key, ID badge, Swipe card, token to generate access codes**
c) **Advantage: Difficult to share, if taken, user should be aware token is missing**

Disadvantage: May be difficult to recover without user cooperation. If lost, finder

can make use of token.

ID based:

a) Physical characteristic unique to a person

b) Fingerprint, Iris or retinal scan, voiceprint, physical signature

c) Advantage: Can't be lost or forgotten, should require presence of user at point of authentication

Disadvantage: Complex system to implement, characteristic may not be 'secret', hard to replace a compromised biometric authenticator

Location based:

a) Based on location of user:

b) IP address, phone number (fixed line), GPS location marker

c) Advantage: could be useful if relatively local

Disadvantage: Potential privacy issues, location could be spoofed

b) Two factor authentication: using authenticators from two different categories together. Examples:

- **Something you know and something you have:**
  - **Swipe card and PIN (to access financial services at ATM)**
- **Something you know and something you are:**
  - **Password and fingerprint**
- **Somewhere you are and something you are:**
  - **Phone number and voiceprint**

QUESTION 8

The most commonly used authenticators are passwords. The following questions explore issues associated with passwords.

a) Browse through the article by Richard Smith on the Strong Password Dilemma http://www.cryptosmith.com/password-sanity/dilemma. (Four parts: Strong password policies, Passwords and usability, Dictionary attacks and password strength, Forcing functions and mouse pads).

(i) In 'Strong password policies' five rules for password selection are discussed. Do you agree with these rules? All of them?

(ii) 'Passwords and Usability' explores the mismatch between the requirements of password systems based on the five password selection rules and the suggested 'Golden Rules' for user interface design. Which aspects of the password systems make them hard to use?

(iii) 'Dictionary attacks and Password strength' uses the expected number of trial and error attempts an attacker must make to recover a secret as a measure of the strength of the authentication mechanism. Consider a four digit PIN:

   i. How many possible combinations are there?
   ii. If people are free to choose their PIN, which ones are most likely to be chosen?
   iii. How does this reduce the work required for an attacker to be successful?
   iv. Is the situation similar for people given the freedom to choose their own password?

(iv) 'Forcing functions and mouse pads' explains how placing restrictions on user selected passwords in an effort to make users choose harder to guess passwords shifts the security problem associated with passwords and may actually make it easier for an attacker to find a user's password. What does the article suggest as an attack strategy?

b) In *AS27002:2006* Clauses 11.2.3 and 11.3.1 deal specifically with user passwords (11.2.3 *User password management* and 11.3.1. *Password use*). Refer to these sections to outline typical security policy requirements for:

(i) Temporary passwords (given to users before they access system).

(ii) Regular user passwords

(iii) Password use, in the case of a user having multiple accounts each requiring a password for access. Is it OK to use the same password across multiple accounts?

c) Look at the advice and rules on selecting passwords provided by QUT's IT Services: http://www.itservices.qut.edu.au/generalservices/itsecurity/passwords.jsp

(i) What must be avoided?

(ii) What is required for QUT passwords?

(iii) Try out the password tester and see how some of your old passwords rate. Which ones are rated weak? Do you have any strong passwords?

a) Strong Password dilemma' by Dr Richard Smith.

(i) The five rules are:

   i. Each password should be new and different,
   ii. Passwords should be memorized,
   iii. They should be at least six characters long,
   iv. They should be replaced periodically, and
   v. Should contain a mix of upper and lower case letters, digits and punctuation characters.

(ii) The aspects of password systems that make them difficult for users to interact with are:

i. that you can't take shortcuts,
ii. you don't get informative feedback on errors,
iii. there are no strategies for error prevention,
iv. the user cannot easily reverse a wrong entry,
v. the user is not in control, and
vi. the system places a burden on the user to remember things.

However, making things easier for users of password systems may also make them easier for attackers.

(iii) 4 digit pin:

i. 10 x 10 x 10 x 10 = 10,000 possibilities.

ii. Most people choose dates, so that reduces the number of likely PINs to the number of days in the year: 366 in a leap year.

iii. Similarly people choose words rather than random strings of letters, since they are easier to remember. That makes dictionary attacks much more successful than just guessing random character strings.

(iv) Writing down a password may help the user in confidently choosing a good quality one, and may be necessary in order for the user to be able to reproduce the password (too hard to remember). Written down passwords should be kept in a safe place (locked up or in a wallet), but often they are not. They can be stuck to the computer monitor or 'hidden' under the mouse mat. So an attacker with physical access to an area can be very successful in locating a password to gain access to a system.

b) Refer to appropriate sections of Clause 11 in AS27002:2006

c) QUT IT Security and passwords:

http://www.itservices.qut.edu.au/generalservices/itsecurity/passwords.jsp

1. Users should avoid:

- Using predictable sequences or repeated characters
- Using only look alike substitutions of numbers or symbols, for example using @ to represent a, or $ for an s.
- Using user ID or log in name, any part of user's name or birthday, or dictionary words in any language as passwords.
- Using the same password for all your accounts.
- Writing down your password, especially if left on post-it notes near the computer.
- Sharing their password.

2. Passwords should:

- Not consist entirely of numbers.
- Contain upper and lower case characters.
- Be at least 8 characters in length.
- Have a mixture of upper and lower case letters, or at least 1 number.
- Not have a single character repeated more than 3 times.
- Not be an exact match of you username, forwards or backwards.

There is also some other advice on practical IT security from the menu on the left of this password page.