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?

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?

QUESTION 3

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

a) Subjects

b) Objects

c) Resource owners

QUESTION 4

Briefly define the concepts of:

a) Discretionary access control (DAC).
b) Mandatory access control (MAC).
c) Role-based access control (RBAC).

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*.

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.

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.

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?