SCIENCE AND ENGINEERING FACULTY

# INB255/INN255 Security

Semester 1, 2014

## Workshop for Lecture 8: Access Control Mechanisms

### QUESTION 1

Reusable passwords are the authenticator most commonly used for computer systems. However, there are some problems associated with their use.

a) Briefly describe the problems associated with reusable passwords.
b) Which of these problems are specific to user selected passwords?
c) Which problems are more commonly associated with computer generated passwords?
d) Information security expert Bruce Schneier's blog "Schneier on Security" (available at http://www.schneier.com/blog/ ) has an April 24, 2013 blog posting on password protection mechanisms. The post includes a link to an Ellen de Generes video where a password protection device is discussed. Which of the problems you identified above are discussed in the video? What does Ellen suggest is a security issue with the proposed password protection device?

### QUESTION 2

Where passwords are user selected, the application of a password checking process should be considered, as a means to ensure quality passwords are used.

a) Read through Section 11.3 *User responsibilities* of AS27002 *Code of practice for information security management* to find the advice to users on selecting quality passwords. Record this advice.
b) Password checking can be *proactive* or *reactive*. Explain the process involved in each case. What sort of checking is performed for QUT Access passwords?
c) What are the advantages and disadvantages associated with each of the methods discussed in part b)?

### QUESTION 3

An alternative to reusable passwords is to use one-time passwords. The one-time password system S/KEY makes use of a hash function to produce a series of one-time passwords. Read the article on Wikipedia about S/KEY: `http://en.wikipedia.org/wiki/S/key`, and use the information to answer the following questions:

a) Give an example of a situation in which S/KEY could be used.
b) Explain the basic operation of S/KEY in terms of what is computed and stored
   i. *on the client side* and
   ii. *on the server side* and
   iii. *what is sent* each time the protocol is run.
c) Which property of cryptographic hash functions is required in order for S/KEY to be secure?

**QUESTION 4**

Hardware tokens are an example of object-based authentication – authentication based on *something you have*.

a) The synchronised one-time password generator is one method to provide user authentication. Describe the operation of the synchronised password generator method using clock-based tokens.

b) Watch the video 'How do RSA SecureID tokens work' available at: http://www.youtube.com/watch?v=k_zpbJF9pmc.

   i. Look carefully at the 6-digit display showing on the device. How often does it change?

   ii. From the explanation given in the video, explain how the system manages a small loss of synchronisation (say, clock drift of one minute) between the device and the authentication server (about 3 minutes into the explanation).

   iii. What is the probability that an attacker could guess the correct passcode (6-digit number) and gain access?

c) Read the section of the Wikipedia entry on SecureID http://en.wikipedia.org/wiki/SecurID that relates to the RSA security breach in March 2011. What are the hackers alleged to have obtained from RSA, and how would this information be of use to them?

d) Briefly explain the operation of a token-based challenge-response system.

e) Describe one major advantage and one major disadvantage for hardware tokens, when compared to standard user-selected passwords.

f) Compare the two token-based methods (clock based or counter based). What is a possible advantage of each compared with the other?

**QUESTION 5**

An alternative means for user identification and authentication makes use of biometrics.

a) Briefly define the concept of a biometric.

b) A basic biometric system consists of four main modules. Briefly describe these four modules.

c) A biometric system may operate in either *verification* mode or *identification* mode.

   i. Briefly explain the operation of both of these modes.

   ii. When the system is in use, which of these modes is likely to return a result faster? Explain your answer.

**QUESTION 6**

Any human physiological or behavioural characteristic can be used as a biometric characteristic as long as it satisfies four basic requirements.

a) Briefly describe each of these four requirements.

b) For a proposed biometric system (a system that employs biometrics for personal recognition) there are three practical aspects that require consideration. These are Performance, Acceptability and Circumvention. Briefly describe what each of these three aspects considers.

c) An article in 2008 noted the publication of the fingerprint of a high ranking German public official: http://www.theregister.co.uk/2008/03/30/german_interior_minister_fingerprint_appropriated/. Relatively inexpensive methods for making use of publically available fingerprints have also been widely reported (example: the news article relating to Tsutomu Matsumoto's 'gummi bear' fingerprint research: http://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/). How could the published fingerprint be used? How does the publication of this fingerprint relate to your answers to parts (a) and (b)?

d) Briefly describe the extent to which each of the following biometric types satisfies the characteristics and issues you described for parts a) and b).
   i. Fingerprints
   ii. Facial recognition

**QUESTION 7**

a) The matcher module in a biometric system computes a matching score ***s*** that quantifies the similarity between the user input and the template representation stored in the database. Briefly explain how the matching score ***s*** and the threshold ***t*** are used to determine mate pairs.

b) For the terms *false match rate* (FMR) and *false non-match rate* (FNMR)
   i. Clearly explain what each term means.
   ii. Give an example related to facial recognition to illustrate your explanations.

c) Explain how the FMR can be reduced.

d) Explain how the FNMR can be reduced.

e) Explain how the trade-off between security (low FMR) and practicality (low FNMR) is related to the threshold *t*.

f) Can you think of an example where it is more important that the false match rate must be very low?

g) Can you think of an example where it is more important that the false non-match rate is low?