SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1 2014

Week 2: Tutorial for L1 - Introduction

Attempt these questions **before** you attend your 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

Review the definitions given in the lectures slides for the following terms. You may be asked to define these terms in the quiz or final examination.

a) Confidentiality

b) Integrity

c) Availability

d) Entity Authentication

e) Data Origin Authentication

f) Non-repudiation

g) Asset

h) Vulnerability

i) Threat

QUESTION 2

This question requires you to browse through a security report. Locate the CERT Australia "Cyber Crime and Security Survey" online (available at https://www.cert.gov.au/newsroom).

a) Read the "Key Findings" on p 5. According to the report,

   i. What proportion of organisations know that they experienced a cyber incident in 2012?

   ii. What proportion of organisations reported the incident to a law enforcement agency?

   iii. Of the organisations experiencing a cyber incident, 20% chose not to report it to law enforcement. Why?

b) Read the “Cyber Incidents” section on p16 and 17. What information is contained in this report about:
    i. The proportion of organisations who did not know whether they had experienced a cyber security incident in the last 12 months?
    ii. Of the respondents who reported they had experienced a cyber security incident in the last 12 months, what proportion did not know how many incidents had been experienced?

c) Read the “Case Study - Ransomware” on p22-23. According to the report, how were the attacks conducted?

QUESTION 3

Visit the AusCERT website http://www.auscert.org.au/. Use the information from this site to answer the following questions:

a) What is the full name of the organization known as AusCERT?

b) Where is AusCERT located (physical location)?

c) Follow the Security Bulletins link (from the menu on the left). Select the security bulletins issued this year. How many security bulletins have been issued by AusCERT in:
    i. one week (0 Week, Semester 1: Feb 17-23, 2014)
    ii. one month (February, 2014)
    iii. this year to date (January and February of 2014)

d) From the Security Bulletins link, select those categorized by operating system/environment. How many recent bulletins are related to software platforms that you use regularly?

e) From the Publications link, select ‘Sabotage of a specific process, in a specific plant – the Stuxnet goal.’ Answer the following questions, based on the information contained in this publication:
    i. What was the main purpose of the Stuxnet Virus?
    ii. Which of the traditional security goals (Confidentiality, Integrity and Availability) does this relate to?
    iii. It is suspected that this was a targeted attack. Who or what is regarded as the most likely target?
    iv. Why would this type of organization be targeted?

QUESTION 4

Review the “cube” from the NSTISSI 4001 security model (slide 58). Consider a home banking application running on a mobile computing device connected to the Internet.

a) List three different threats in this context, with one threat concerning each of the security goals:

   i. confidentiality

   ii. integrity

   iii. availability

b) What data state do the threats you have identified apply to: data that is in transmission, in storage or during processing?

c) Can the threats that you identified be best addressed by using technology, by using policy and procedures, or through education/training/awareness?

d) Threats can be classed as *accidental* or *intentional*, and attacks can be classed as *passive* or *active*. Give one example of each in the context of the same home banking application.

QUESTION 5

List any information security measures that you currently use. What sorts of attacks are you trying to protect against? Consider whether they protect the confidentiality, integrity and/or availability of data.