SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1 2014

Outline solutions for Tutorial 2

(relates to L1: Introduction material)

Note that many of the questions this week do not have exact answers and are mainly intended to promote discussion. Some questions introduce you to Australian organisations with a role in providing information security advice to Australian businesses and industries (CERT and AusCERT).

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

The definitions of all of these terms are in the Lecture 1 outline. You can check them there.

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?

This question is intended to increase your awareness of information security events related to computer security.

a) According to the report section “Key Findings”:

i. Over 20% of organisations know that they experiences a cyber incident in 2012.

ii. Of those who experienced cyber incidents, 44% reported it to law enforcement.

iii. Of those who experienced cyber incidents, 20% chose not to report it to law enforcement because of fear of bad publicity.

b) From the “Cyber Incidents” section:

i. 9% of organisations surveyed did not know whether they had experienced a cyber incident.

ii. Of those who had experienced an incident, 5% did not know how many.

c) “Case Study - Ransomware” attacks are performed by:

i. Compromising the information system of a particular organisation.

ii. Encrypting the files on the compromised system (and also the

backups) and/or locking out the user.

iii. **Notifying the victim that if they paid a ransom, they would be given the codes to decrypt the data and/or the computer would be unlocked.**

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 18-24, 2013)
   ii. one month (February, 2013)
   iii. this year to date (January and February of 2013)
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?

a) AusCERT – Australian Computer Emergency Response Team.
b) Located at The University of Queensland.
c) This question is intended to alert you to the frequency and range of security vulnerability and other information security events. There are multiple security bulletins from AusCERT every day.

d) These cover all mainstream operating systems, so many of them are likely to relate to platforms that you use. It's worthwhile having a look here from time to time to see what's happening.

e) Stuxnet virus:

- **a. Modify the behaviour of an industrial control system by modifying programmable logic controllers**
- **b. Mainly relates to integrity: the virus was able to modify instructions given to control processes.**
- **c. Suspect the target was an Iranian nuclear power plant.**
- **d. Potential to cause a lot of damage to critical infrastructure.**

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:
   a. confidentiality
   b. integrity
   c. 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.

a) There are many possible answers. A threat concerning:

- **a. Confidentiality could be disclosure of personal banking accounts and balances;**
- **b. Integrity could be alteration of the same personal information; and**

c. **Availability could be the inability to connect to the bank to transfer funds or make payments.**

b) **The confidentiality and integrity threats above apply to data in storage (on home PC) and in transmission (on the Internet or LAN). The threat against availability concerns the (lack of) processing of data.**

c) **All three types of security measure may prove useful to address the threats. For example, technology such as SSL can be used to protect confidentiality and integrity of data in communication; a policy to avoid home banking from Internet Cafes can limit disclosure of information stored on the PC; education can help ensure that users do not download untrusted software onto machines used for home banking.**

d) **Threat examples:**

a. **An accidental threat is one caused by mistake or by a random event. For example, you could accidentally key in the wrong recipient account in a bank transfer.**

b. **An intentional threat is one caused deliberately. For example a malicious program (trojan horse) could alter the recipient account name.**

c. **An active attack involves a deliberate unauthorized change to the state of the system. This could be an attacker changing the balance in a bank account.**

d. **A passive attack involves unauthorized disclosure of information without changing the state of the system. This could be observing the value of a bank account by looking at somebody else's monitor in an Internet cafe.**

QUESTION 5

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

There are lots of possibilities here. Think about the technology you use, policy and procedures you follow, etc.