SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1 2014

Outline solutions for Week 3 Tutorial

Relates to L2: Threats, Vulnerabilities and Attacks

*Attempt these questions **before** you attend your 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

Clearly explain:

a) The difference between vulnerabilities and threats. Give an example to illustrate your answer.
b) The relationship between threats, vulnerabilities and attacks.
c) Is it possible for a threat and a vulnerability to coincide without an attack occurring? Explain your answer.
d) The difference between passive and active attacks. Give an example to illustrate your answer.

a) Vulnerabilities are weaknesses, flaws or holes in the system protecting information assets. A threat is anything that has the potential to harm information assets, intentionally or by accident. For example, storing sensitive information in an unsecured physical location is a vulnerability. Threats to the information asset include theft and destruction.

b) The relationship between these is that when vulnerabilities are deliberately exploited by threats, it results in an attack on the information asset.

c) If a threat and vulnerability coincide and the threat is <u>not</u> the result of deliberate human action then the result is a security incident (which may cause extensive damage to information assets) but this is <u>not</u> described as an attack. For example, the recent floods in Brisbane resulted in a loss of

availability for many services. As this was due to an act of nature, it is considered a security incident rather than a DoS attack.

d) Passive attacks do not require the attacker to interact with the system and alter it in any way. This makes them very difficult to detect. For active attacks, the attacker must take some action and interact with the information assets in some way. If you are monitoring your information system, you may be able to detect the attacker's actions. There are plenty of examples of both types of attacks in the lecture outline.

QUESTION 2

Your current position as a QUT student requires you to access and use information assets, and to develop your own information assets. This question concerns the information security of your personal information system with respect to your PC or mobile device.

a) Identify threats to the information assets you have developed and stored. Make **two** lists of possible threats: one for those related to natural events, and one for those related to human actions. Include at least four threats on each list.
b) For each identified threat, determine which security goal is affected.
c) Identify vulnerabilities associated with the scenario above. Try to list at least **five** vulnerabilities.
d) Considering the threats you listed and the vulnerabilities you have identified, are there any plausible attacks on your information assets?

a) Lots of possibilities, some more plausible than others.

<u>Natural events:</u> cannot access your PC because you are cut off from that location by floodwaters, thunderstorm results in power loss to your suburb and are unable to switch on PC, building collapses in earthquake and your PC is squashed, lightning strike and power surge kills your PC.

<u>Human action: Accidental</u>: Spill coffee on your laptop and damage it. Drop your laptop when getting off the bus. Save your important file to USB, but leave USB in your pocket and put it through the wash. Left your laptop in a café or taxi or ….

<u>Human action: Deliberate</u>: Your PC is stolen. Your computer is infected with a virus that deletes some of your (important) files. Your ex smashes your PC because…you spent too much time on it. A keystroke logger is installed on your computer. Your flat mate copies your assignment and submits it as if it were his/her own work.

b) For many threats, the security breach is availability. Could be some for confidentiality or integrity.

c) Vulnerabilities include location (prone to flooding?), lack of physical security mechanisms, use of mobile or portable devices, lack of offsite backups, AVS, etc.

d) Malicious code and theft of mobile device may be most plausible. Depending on your living arrangements, it may be a flatmate that copies your assignments. Especially if you share computing devices.

QUESTION 3

Visit the AusCERT website http://www.auscert.org.au/. Follow the links to the Security Bulletins page, and use the information from this site to answer the following questions:

a) What sort of information is included in the security bulletin titles (Look for AusCERT Bulletin Format)?

b) What information is conveyed in the security bulletin *title* for the security bulletin numbered ESB-2014.0230?

c) Read the bulletin. Describe:

   i. the vulnerabilities.

   ii. what could happen if these vulnerabilities are exploited.

d) Does an attacker need the user to take any particular action in order to exploit these vulnerabilities?

e) How can this problem be prevented?

a) The bulletin titles:

- **begin with ASB or ESB, to indicate AUSCERT material, or material from external sources being re-released by AUSCERT, respectively.**

- **have an ID number (and revision number if applicable)**
- **have a [tag] to indicate affected systems,**
- **include the product name, and**
- **(usually) the most severe impact if this vulnerability is exploited**

b) ***From the title*, we know that ESB-2014.0230 is an alert related to vulnerabilities in Apple iOS affecting iOS and Apple TV that, if exploited could allow remote unathenticated access to privileged data.**

c) **The vulnerabilities relate to the validation process for the connection. Some steps were missed. If a user has an iPhone, iPod touch iPad or Apple TV (certain versions) an attacker can capture or modify data in sessions in protected by SSL/TLS.**

NOTE: The vulnerabilities have been reported previously (CVE-2014-1266). You can use these CVE numbers to check up on the details of a particular vulnerability. For example, at http://www.cvedetails.com/*. Just enter CVE-2014-1266 into the box (top right). For this vulnerability, the problem is the missed steps in certificate checking code, so that it does not actually check the signature in a TLS Server Key Exchange message (part of setting up the SSL connection). This allows man-in-the-middle attackers to spoof SSL servers. So you've got a secure connection, but not necessarily to the endpoint you think it is!*

d) **An attacker needs a user with a device (iPhone, iPod, iPad, etc) that has a vulnerable version of iOS, and access to the user's communications network. When the user tries to establish a secure connection to a site (https) the attacker is a MITM and can intercept the data.**

e) **The alert tells us that upgrading to the latest version of iOS resolves the problem.**

QUESTION 4

To protect information assets you need to know what your assets are, and where they are stored. However, many organizations overlook data storage in devices such as photocopiers and printers. Read the CBS News article "Digital Photocopiers loaded with secrets" available at:

http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml

With this in mind, answer the following questions:

a) Suppose an organization sells their used photocopier at auction without first removing the stored data from the hard drive. Which information security goal will potentially be breached if this data is exposed?

b) Is disposing of the used photocopier considered a threat, vulnerability or an attack? Explain your answer.

c) Many photocopiers are multifunctional and also operate as printers for other networked devices. Describe a threat to information assets that may arise through the use of these devices within the organization (that is, before they are decommissioned).

d) Visit the AusCERT website and look at Security Bulletins listed under the category 'Dedicated Device'. Some bulletins related to printers. View some of these to find out what attackers can do, and the type of access they need to enable these actions.

a) Most likely is a breach of confidentiality. The original assets are presumably retained by the company. The material on the hard drive is a copy of the originals, but if exposed the information is no longer confidential.

b) Disposing of the copier without sanitizing it first leaves the organization vulnerable. There is now a threat that an unauthorized person can gain access to the data. If they do, then the confidentiality is breached and there is a security incident. A lack of knowledge of the capability of the technology being used and possibly a failure in the policy regarding asset disposal are vulnerabilities.

c) Access to the copier over the network makes it possible for files sent to the printer to be viewed, copied or redirected by others, and possibly to be modified and then retransmitted. Thus the confidentiality breach may occur much sooner (no need to wait until the copier is decommissioned). And there is potential for breaches of integrity also. Depending on the access management, it may be possible to cancel or delete files before they are printed.

d) There are Security bulletins for various brands of printers. Some vulnerabilities could, if exploited, allow attackers to gain unauthorized access, execute arbitrary code, or perform denial of service (DoS) attacks. To exploit the vulnerabilities, mostly the attacker requires remote unauthenticated access. That is, the threats outlined in c) are realistic concerns.

QUESTION 5

The article '*Trojan program hijacks World of Warcraft accounts despite two-factor authentication*' available at:
http://news.techworld.com/security/3495965/trojan-program-hijacks-world-of-warcraft-accounts-despite-two-factor-authentication/
describes the situation where players' computers became infected with malicious code. Answer the following questions based on the information contained in the article.

a) Why is the malware described as a Trojan?
b) What is the legitimate function performed by the downloaded software?
c) What is the additional function performed by the software, without the user's consent?

a) The victims downloaded a 'Curse Client' [described in the article as fake but working] that (unknown to the victim) contained the malware code within it.

b) The legitimate function is the 'Curse Client' function: used to install add-ons and modifications for games including WoW.

c) The additional function that the software performs is to steal both user account information and the authenticators used for verification (used for two factor authentication). Since the attackers use the authenticator with the account before the user can, the legitimate user login is then blocked.

QUESTION 6

Consider the following scenario: An employee finds a portable storage device (a USB) in the foyer of the company office building. The employee thinks that the USB was most likely dropped by another employee, and decides to access the contents on the device in an attempt to discover the device owner and return the lost property.

a) Outline likely threats associate with this scenario.
b) What sort of vulnerabilities may exist within the organization?
c) Suppose the USB contains malicious code which infects the organization computer system. Given that the employee did not intentionally introduce the viral code, would this be considered an attack? Justify your answer.

a) The content of the USB is potentially malicious.

b) <u>Technology</u>: there may not be effective AVS.

<u>People</u>: lack of user education about introducing unknown items to the network, or process for handling items of this nature.

<u>Processes</u>: Is there a process for handling unknown items/lost property?

c) If the USB contains malicious code then someone wrote the code (intentional) which was transferred to the USB (could have been intentional, but possibly not). So this can be considered an attack even though the actions of our naïve employee were not intended to cause harm. It is possible that the USB was intentionally placed in the building foyer in the hope that it would be taken into the organization. Then the actions of the employee represent a vulnerability that is deliberately exploited by someone else in the attack.