Information Security (CP3404)
Chapter 6 practical

- This practical consists of some quick quiz questions, tutorial type questions, and hands-on projects relevant to (chosen from) Chapter 6 of the textbook (i.e., Mark Ciampa, *CompTIA® Security + Guide to Network Security Fundamentals, Fifth Edition*, USA, 2015).
- You may not be able to complete this practical within the scheduled one-hour practical session for this subject. You are strongly recommended to complete it in your own time (note that you are expected to work 10 hours per week on this subject, including 3 hours of contact time).

Section A – Quick-Quiz/Multiple-Choice Questions:

- Each week, complete the test on LearnJCU within the time allocated, which is before the next practical session.
- These on-line tests are worth 20% of the total marks for this subject.

Section B – Short Answer (Tutorial-Type) Questions:

- Answers to this set of questions are available at the end of this document (Section D).
- Effective learning implies you answer the questions before seeing the answer.

1. Explain how digital certificates are managed.
2. List three general duties of a CA (Certificate Authority).
3. Identify the general duties of an RA (Registration Authority).
4. List the three PKI (Public Key Infrastructure) trust models that use a CA (Certificate Authority).
5. List the four stages of a certificate life cycle.
6. Explain the difference between key revocation versus key suspension. Give an example for each.
7. Discuss the three areas of protection that are provided by IPsec (Internet Protocol Security).

Section C – Hands-On Projects:

Due to security issues, you may not be allowed to practise hands-on projects with university's computers. Interested students are encouraged to do these projects on their own computers (if available). You will not be assessed for utilities/commands that cannot be practised on university computers. Note that you may still be assessed for descriptions/definitions that are provided in this section.

Viewing Digital Certificates[1]

In this project, you will view digital certificate information using Microsoft Internet explorer.

1. Use your web browser to go to **www.google.com**
2. Note that although you did not enter *http://*, nevertheless Google created a secure HTTP connection. Why would it do that?
3. Click the padlock icon in the browser address bar.
4. Click **View certificates**
5. Note the general information displayed under the **General** tab.
6. Now click the **Details** tab. The fields are displayed for this for this X.509 digital certificate.
7. Click **Valid to** to view the expiration date of this certificate.
8. Click **Public key** to view the public key associated with this digital certificate. Why is this site not concerned with distributing this key? how does embedding the public key in a digital certificate protect it from impersonators?
9. Click the **Certification Path** tab. Because web certificates are based on the distributed trust model, there is a ''path" to the root certificate. Click the root certificate and click the **View Certificate** button. Click the **Details tab** and then click **Valid to**. Why is the expiration date of this root certificate longer than that of the website certificate? Click **OK** and the click **OK** again to close the certificate window.
10. Now view all the certificates in this web browser. Click the **Tools** icon and then **Internet options**.
11. Click the **Content** tab.
12. Click the **Certificates** button.
13. Click **Trusted Root Certification Authorities** to view the root certificates in this web browser. Why are there so many?
14. Click the **Advanced** button.
15. Under **Export format**, what is the default format? Click the **down arrow**. Which PKCS format can this information be downloaded to? Why this format only?
16. Close all windows.

Section D – Answers to Short Answer (Tutorial-Type) Questions:

1. Explain how digital certificates are managed.

   Answer:
   Several entities and technologies are used for the management of digital certificates, such as applying, registering, and revoking. These include the Certificate Authority (CA) and Registration Authority (RA), along with a Certificate Revocation List (CRL) and a Certificate Repository (CR). In addition, digital certificates can be managed through a Web browser.

[1] If you are concern about installing any of the software in this project on your regular computer, you can instead install the software in the Windows virtual machine created in practical-1. Software installed within the virtual machine will not impact the host computer.

2. List three general duties of a CA (Certificate Authority).

   Answer:
   Any three of the followings:

   - Generate, issue, and distribute public key certificates.
   - Distribute CA certificates.
   - Generate and publish certificate status information.
   - Provide a means for subscribers to request revocation.
   - Revoke public-key certificates.
   - Maintain the security, availability, and continuity of the certificate issuance signing functions.

3. Identify the general duties of an RA (Registration Authority).

   Answer:

   - Receive, authenticate, and process certificate revocation requests.
   - Identify and authenticate subscribers.
   - Obtain a public key from the subscriber.
   - Verify that the subscriber possesses the asymmetric private key corresponding to the public key submitted for certification.

4. List the three PKI (Public Key Infrastructure) trust models that use a CA (Certificate Authority).

   Answer:
   The models are:

   (i) The hierarchical trust model
   (ii) The distributed trust model
   (iii) The bridge trust model

5. List the four stages of a certificate life cycle.

   Answer:

   (i) Creation
   (ii) Suspension
   (iii) Revocation
   (iv) Expiration

6. Explain the difference between key revocation versus key suspension. Give an example for each.

   Answer:
   The revocation of a key is permanent; key suspension is for a set period of time. For example, if an employee is on an extended medical leave, it may be necessary to suspend the use of her key for security reasons. But if an employee is fired then key revocation should apply. A suspended key can be later reinstated.

7. Discuss the three areas of protection that are provided by IPsec (Internet Protocol Security).

   Answer:

   (i) *Authentication* – IPsec authenticates that packets received were sent from the source that is identified in the header of the packet, and that no man-in-the-middle attacks or replay attacks took place to alter the contents of the packet. This is accomplished by the Authentication Header (AH) protocol.

(ii) *Confidentiality* – By encrypting the packets, IPsec ensures that no other parties were able to view the contents. Confidentiality is achieved through the Encapsulating Security Payload (ESP) protocol. ESP supports authentication of the sender and encryption of data.

(iii) *Key management* – IPsec manages the keys to ensure that they are not intercepted or used by unauthorized parties. For IPsec to work, the sending and receiving devices must share a key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which generates the key and authenticates the user using techniques such as digital certificates.