**201390 ITC 593**

**Assessment Item 3**

**Value:** 25%

**Due date:** 31-Jan-2014

**Return date:** 14-Feb-2014

**Task 1. Online Discussions (24 marks)**

Below are listed a set of topics. You are required to conduct research and participate in online/forum discussions on a topic from the set (total of seven topics). In your discussion postings, you should try and address the following points:

* Provide information about the topic (discuss the topic, describe the relevant technologies, applications of the technologies, clarify vague areas of other students postings, etc.)
* Raise questions about the information provided by other students (this must be done in an adequately professional manner)
* Respond to questions raised about your own information and other student's
* Contribute to discussions in general

Note that the aim of this task is:

* To build an understanding and perspective of current hot topics in Network Security; and
* To build generic skills including, but not limited to
  + A capacity for teamwork and collaboration
  + An ability for critical thinking, analysis and problem solving
  + Gaining or improving information technological literacy
  + A capacity for lifelong learning and an appreciation of its necessity

As such, the more you contribute the development of these topics and related discussion the more likely you will score well in this task.

**Topic Set**

1. The security advantages of using two-factor authentication, such as the integrated fingerprint reader in the more recent iPhone models, particularly to support internet services (such as online banking)
2. The future of internet anonymity services, [such as Tor](http://en.wikipedia.org/wiki/Tor_(anonymity_network)), given the recent revelations of NSA hacking on a global scale
3. Encrypting more and more internet services with SSL (HTTPS) by default
4. The security risks around BYOD (Bring Your Own Device) in the workplace
5. The security risks around using Cloud Computing
6. The security risks to critical infrastructure (such as power, communication, water) from malicious cyber attacks
7. Offering financial rewards for finding security vulnerabilities in software

**Your submission**

You are required to prepare and submit a report on your topic to address the following questions:

1. Summarize the topic and the issues discussed. Discuss how your own posts contributed to this knowledge.
2. Based on your own research, discuss whether or not the summary presented in (1) is accurate.
3. Identify any important issue/s that you believe were not addressed, or not addressed adequately in the discussions. Explain why you view this issue/these issues as important.
4. Discuss what you believe to be the most important lesson you have learnt as a result of these discussions. Explain the impact of this and its application/impact in real life.

**Task 2: Security Infrastructure and Protocols (16 marks)**

1. PKI and PGP are two methods for generating and managing public keys for use in protocols such as secure email. Compare and contrast the trust models for public keys used in PKI and PGP, and assess the statement that a PKI is a “top-down” approach to trust and PGP is a “bottom-up” approach to trust. (8 marks)
2. The SSL protocol uses (X.509) certificates to create a secure session between a server and a client in a web session. Discuss the browser-based trust model assumed in SSL, and compare it with the trust model used in Kerberos. Kerberos is designed to operate is a relatively small domain, such as a single company. Discuss the practical issues around extending the Kerberos trust model to a global scale, say to provide secure services between Amazon and its customer base (8 marks).

**Task 3: Security Primitives (20 marks)**

1. Explain the different roles between hashing and message authentication codes (MAC). Can a good hash function serve as a good MAC, and vice versa?

(4 marks)

1. What is the relationship between hashing and digital signatures? Which fields of an X.509 certificate are related to hashing and/or digital signatures?

(8 marks)

1. Explain how hashing, MACs and digital signatures are used in SSL. Explain how the cipher\_suites parameters are used to specify or change a given collection of algorithms for hashing, MACs and digital signatures. (8 marks)

**Marking Scales**

**Task 1 Marking Scale (24 Marks)**

* Correct and concise summary of the issues discussed in forum (6 Marks)
* Analysis of the summary (4 Marks)
* Discussion of the important issues not addressed in the forum (6 Marks)
* Discussion of the learning and exploring the impacts in real life (8 Marks)

**Task 2 Marking Scale (16 marks)**

1. PKI and PGP (8 marks)

* + A thorough (about a page) comparison between the PKI and PGP trust models (5 marks)
  + A coherent explanation while PKI is top down and PGP is bottom up (3 marks)

1. SSL and Kerberos (8 marks)
   * A thorough (about a page) comparison between the browser-based and Kerberos trust models (5 marks)
   * A coherent review on the issues involved in attempting to scale Kerberos and how these issues are avoided by SSL (3 marks)

**Task 3 Marking Scale (20 marks)**

1. Hashing and MACs (4 marks)

* Listing the key differences between Hashing and message authentication codes (MAC) (4 marks)

1. Hashing and digital signatures (8 marks)

* Correctly identifying the relationship between hashing and digital signatures (3 marks)
* Correctly identifying fields of an X.509 certificate related to hashing and digital signatures (5 marks)

1. SSL primitives (8 marks)

* Correct explanation of how hashing, MACs and digital signatures are used in SSL (5 marks)
* Correct explanation of how cipher\_suite parameters are used to specify or change a given collection of algorithms for hashing, MACs and digital signatures (3 marks)