SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1, 2014

Workshop for Lecture 9: Network Security

QUESTION 1

TLS is a cryptographic services protocol based upon PKI and commonly used on the Internet.
(a) What port is reserved for HTTP over TLS? What is the prefix for a URL that describes a resource accessible by HTTP over TLS?
(b) TLS is designed to secure reliable end-to-end services over TCP. Briefly describe where the TLS operates in the OSI and TCP/IP protocol stacks.
(c) Briefly explain the purpose of the TLS Handshake protocol.
(d) Identify the security services provided to TLS connections by the TLS Record Protocol.
(e) How are the TLS Handshake Protocol and the TLS Record protocol connected?
(f) As part of the Handshake Protocol the client and server negotiate which 'cipher suite' to use. In what circumstances is this negotiation useful? Why can this negotiation lead to potential security weaknesses?

QUESTION 2

Internet Protocol security (IPSec) is a framework of open standards for Internet Protocol (IP) networks.
(a) Briefly describe three major benefits of using IPSec.
(b) Three security services that can be provided by IPSec are: message confidentiality, message integrity and traffic analysis protection. Briefly explain the mechanism used to provide each of these services.
(c) Briefly describe the three major VPN architectures supported by IPSec. Describe typical application scenarios for each of these architectures.

QUESTION 3

Suppose that you are responsible for designing a secure Internet banking application. You have been asked to consider basing security on one of three security protocols:

- HTTP Application level authentication
- TLS
- IPSec

Consider each of these protocols in turn to answer the following questions:
(a) Is HTTP Application level Authentication a suitable choice? Explain your answer.
(b) Does TLS provide the required security services? What assumptions would you need to make about the client's computing environment?
(c) Does IPSec provide the required security services? What IPSec architecture would be suitable? Why is this choice not widely used in practice?

QUESTION 4

A firewall is a component or set of components that restricts access between a protected

network and other sets of networks, and is often used to protect an organization's networks from the Internet.
(a) Briefly describe the operational characteristics of:

- A simple packet filter;
- A stateful packet filter;
- An application proxy gateway.

(b) Briefly discuss the strengths and weaknesses of deploying:

- A packet filter;
- An application proxy gateway.

QUESTION 5

The type of firewall that is most appropriate for protecting a network depends on the organization itself and the size of the network. Some factors to consider are the cost, the ease of use and the level of security available if the product is used correctly. Use your web browser to find information on commercial firewall products, and see if you can find products that you think are suitable in the following cases:
(a) A home user with a single PC.
(b) A small organization such as a local accounting business with less than 10 employees.

QUESTION 6

Malicious software is one of the major threats to modern computer system security.
(a) Briefly describe the following types of malware:

a. Spyware
b. Botnets
c. Phishing
d. Rootkits

(b) What is the difference between Resident and Non-Resident viruses?
(c) The Melissa virus was one of the first macro viruses that became very wide spread at the time of its inception. Read the following historical description of this virus at the following link https://www.cert.org/historical/advisories/CA-1999-04.cfm. Briefly describe how this virus worked and why it was so successful in its aims.