**University of Oslo**
**INF3510 Information Security**
**Spring 2012**
**Workshop Questions**


# *Lecture 9: Communication Security*

## QUESTION 1

a. What is a security protocol, and what is its purpose?
b. Give examples of services that can be provided by security protocols.

## QUESTION 2

TLS is a cryptographic services protocol based upon public-key certificates, and is 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 3

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 type of 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 architecture.

## QUESTION 4

Encapsulating Security Payload (ESP) is an IPSec protocol that can be run in two modes: transport mode and tunnel mode.

a. Explain the main difference in packet processing between these two modes.
b. Briefly describe the most typical application scenario for ESP in tunnel mode.
c. Briefly describe an application scenario for ESP in transport mode.
d. Briefly explain the additional security services provided by using ESP in tunnel mode as opposed to using ESP in transport mode.

## QUESTION 5

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

- **HTTP Digest Authentication**. Would this be a suitable choice? Explain your answer.

- **TLS**. Does this provide the required security services? What assumptions would you need to make about the client computing environment?

- **IPSec**. Does this provide the required security services? What IPSec architecture would be suitable? Why is this choice not widely used in practice?