University of Oslo
INF3510 Information Security
Spring 2018
Workshop Questions and Answers

Lecture 10: Communications Security

Question 1

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

Question 2

TLS is an Internet security protocol which actually consists of multiple sub-protocols.

a. Which port is reserved for HTTP over TLS? Which URL prefix denotes resources using HTTP over TLS?
b. 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. In the Handshake Protocol the client and server negotiate which 'cipher suite' to use. Why is this negotiation useful? Why is the negotiation a potential security weakness?

Question 3

TLS (previously called SSL) is potentially vulnerable to TLS stripping.

a. What makes websites vulnerable to TLS stripping?
b. Briefly explain how TLS stripping works.
c. What does the acronym HSTS mean?
d. How does HSTS protect against TLS stripping?
e. How do browsers get HSTS policies for websites?
f. How can HSTS policies be removed from a browser?
g. Use a tool for checking the TLS configuration of servers, e.g. https://www.ssllabs.com/ssltest/
   Test your online bank(s) and other secure sites to see of their TLS configuration is secure.

Question 4

Internet Protocol Security (IPSec) is an open standard 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 5

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 6

Suppose that you are responsible for designing a secure Internet banking application. You are tasked with selecting one of three security protocols to provide communication confidentiality. Assess the suitability of each protocol below.

- **HTTP Digest Authentication**. Can it support confidentiality? Explain your answer.
- **TLS**. Does this provide confidentiality? What assumptions would you need to make about the client computing environment? Is key management practical?
- **IPSec**. Does this provide confidentiality? What IPSec architecture would be suitable?

Question 7

a. Explain why people can be tricked to believe that a criminal website is their own online bank, despite the connection being secured with TLS and even HSTS which provides strong sever authentication.
b. What is the difference between syntactic and semantic/cognitive server authentication?
c. Mention disadvantages of using a petname system.

Question 8

a. When using a cloud VPN, what type of information is hidden from the user's ISP ?
b. When using a cloud VPN, what type of information can the VPN provider see?
c. When using Tor, what type of information is hidden from the user's ISP ?
d. When using Tor, what type of information can the Tor access server see?
e. How can you prevent that your ISP knows that you're accessing Tor?