University of Oslo
INF3510 Information Security, Spring 2012
Workshop Questions

Lecture 1: Background and Basic Concepts

Question 1

a. Which vulnerability(ies) is/are mainly exploited by phishing attacks?
b. Propose security controls (methods) to prevent phishing attacks.

Question 2

a. Mention threats against the registration phase of access control.
b. Are the definitions of authorization in X.800 (http://www.uio.no/studier/emner/matnat/ifi/INF3510/v10/learningdocs/X0800E.pdf) and in RFC2196 (http://tools.ietf.org/html/rfc2196) meaningful in relation to the definitions of e.g. confidentiality and integrity in X.800? Why or why not?

Question 3

Articulate a simple security policy for your personal computer, stating who has authorized access.

Question 4

X.800 specifies security for computer networks, such as OSI and TCP/IP based computer networks. Check Table 1 (p.15) in X.800 to see which security mechanisms (controls) can be used to support the communication security services below, and explain how each mechanism provides the service.

i. Connection-less confidentiality (i.e. message confidentiality)
ii. Connection-less integrity (i.e. message integrity)

Question 5

The 4 services i) “message confidentiality”, ii) “message integrity”, iii) “message authentication” and iv) “non-repudiation of message origin” are related in the sense that one service often implies/provides another. Indicate for each service which of the 3 other services is/are also provided.

Question 6

A user is authenticated to an online web service at the start of a session, and sends data to the web server through his client computer. Explain to what degree the service provider can assume that the data received during the session are authentic as a result of the user authentication.

Question 7

The 3 concepts: “motivation of attacker (threat agent)”, “likelihood of threat occurrence”, and “cost of threat occurrence” are used in risk management. Describe possible dependencies between these 3 concepts.