



Lecture 1: Basic Information Security Concepts

Question 1

- a. Look at the definitions of confidentiality, integrity and authorization in X.800 (<http://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/docs/x800.pdf>) .
 - i) Are the definitions of confidentiality and integrity from X.800 meaningful with relation to how authorization is defined? Why or why not?
 - ii) Is the US Computer Fraud and Abuse Act meaningful from the same perspective? See e.g. the section 18 U.S. Code § 1030 - Fraud and related activity in connection with computers <http://www.law.cornell.edu/uscode/text/18/1030>
 - iii) Explain how authorization should be defined to make meaningful the definitions of confidentiality and integrity in X.800, and also the US Computer Fraud & Abuse Act.
 - iv) Is the text book (Shon Harris CISSP, 7th edition) clear on the interpretation of authorization ? See e.g. p.725 2nd and 3rd paragraphs (Ch.5, Section *Identification, Authentication, and Accountability*)

Question 2

Mention threats against the steps in the configuration phase of IAM (Identity and Access Management).

Question 3

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

Question 4

Articulate a simple security policy for your personal computer, stating who is authorized to access it.

Question 5

X.800 specifies security services 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 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 is authentic as a result of the user authentication.

Question 7

- a. Explain why data privacy can not be provided by information security (CIA properties) alone.
- b. Explain why data privacy depends on information security.