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

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*)

Answer

a. Authorization
   i) The definitions of confidentiality and integrity in X.800 become meaningless when authorization is defined in the sense that the system grants access to anyone who types the right password. Then an attacker with a stolen password is authorized, and would not breach confidentiality, which is meaningless.
   ii) The US Computer Fraud and Abuse Act would become meaningless if anybody with the correct password were authorized simply by logging on.
   iii) It is only meaningful to say that a system approves access based on authorizations previously defined by an authority (a human) or by his delegate within the domain. To authorize access is a policy process that takes place during the configuration phase of IAM prior to the user accessing the system. The authorization process defines the access privileges that the user should have according to job role when accessing the system.
   iv) The text book is totally confused on the interpretation of authorization. See e.g. p.725 2nd and 3rd paragraphs where authorization is described in two different ways that are contradicting.

Question 2

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

Answer

Potential threats are e.g.:

i. A person registers with the wrong name
ii. The person is correctly registered, but the credentials (e.g. password or token) are sent to the wrong person
iii. Correct registration and provisioning, but too powerful access permissions, inconsistent with the authorization policy, are implemented on the system.

Question 3

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

Answer

a. Social engineering attacks exploit vulnerabilities in humans, such as human ignorance, gullibility and lack of awareness.
b. Possible controls to prevent phishing attacks could be awareness training to make people able to detect when the sender is an attacker who pretends to be a legitimate person, or be able to spot fake email messages by their content. Technical controls must be in the form of practical security mechanisms to detect phishing attacks e.g. by filtering email by content or other characteristics, or by sender authentication (SPF: Sender Policy Framework and DKIM: DomainKeys Identified Mail).

Question 4

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

Answer

E.g.: *"Through the legal ownership of this laptop, only I am authorized to use it in general. On explicit consent by me, I can authorize a specific other person to use my laptop – when I unlock it and under my supervision - to access the web through a web browser on the laptop. At any time I can revoke the authorization by telling the other person to stop whereby the other person's usage of my laptop must cease immediately".*

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)

Answer

i. (Connection-less) confidentiality can be provided by encipherment and routing control. Encipherment means that the data is encrypted and therefore unreadable for attackers who can not decrypt. Routing control means that the data packets are routed through protected networks where non-authorized parties do not have access.

ii. (Connection-less) integrity can be provided by encipherment, digital signature, and data integrity. Encipherment means that the message is encrypted which makes it impossible for attackers to change or fabricate messages without detection because any change would make the message impossible to decrypt, but an attacker could possibly interrupt (delete) encrypted messages without detection, which would destroy integrity. Digital signature and Data integrity (aka. Message Authentication Code) means that a cryptographic checksum is sent with the original message, which can be verified by the recipient, so attackers can not modify or fabricate messages without detection because the verification by the recipient would fail, but an attacker could possibly interrupt (delete) a message without detection.

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.

Answer

User authentication provides relatively low assurance of data/message authentication. It is e.g. plausible that the user has left the client computer to get a coffee or go to the toilet, and that another person uses the client computer to send data to the server. Another possibility is that the client computer is infected with a Trojan that generates and sends data to the server without the user's knowledge, even if the user physically sits in front of the computer and actively executes transactions, e.g. to an online bank.

If the session between client and server is **not** protected with TLS (Transport Layer Security) or some other VPN (Virtual Private Network) technology, then it is plausible that a man-in-the-middle attack can insert, change or delete data exchanged between the client and server.

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.

Answer

a) Data privacy requires e.g. prevention of unauthorized collection and storage of personal information, which is not covered by the CIA properties.

b) Data privacy depends on information security because there must be adequate protection around the storage and processing of personal data.