University of Oslo
INF3510 Information Security
Spring 2012
Workshop Questions and Answers

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.

Answer

a. Social engineering exploits vulnerabilities in humans, such as human ignorance, gullibility and lack of awareness.
b. Possible controls to prevent phishing attacks could be awareness training so people are better able to identify e.g. attackers who pretend to be legitimate persons, or fake email messages, and by using practical security mechanisms to detect social engineering attacks e.g. by filtering email, making email authentication practical, and by clearly indicating when a website server certificate is fake.

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?

Answer

a. 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.
b. The definitions of authorization are inconsistent with the definitions of confidentiality and integrity. The definition of authorization assumes that the system can authorize. In reality a system can only approve access based on authorizations previously defined by an authority (a human) or his delegate within the domain.

Question 3

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

Answer

E.g.: *"Only I can use my laptop"*, or "*My partner can go online, but only I can access files".*

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)

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 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.

Answer

i. Message confidentiality implies message integrity. If it is assumed that the message is encrypted with a secret key known only to the sender and recipient, then it also implies message authentication.
ii. Message integrity implies message authentication if it is assumed that the cryptographic checksum is generated by a key known only to the sender and recipient. Under that assumption, message integrity and message authentication are equivalent.
iii. Message authentication implies message integrity.
iv. Non-repudiation of message origin implies message authentication and 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 are authentic as a result of the user authentication.

Answer

User authentication provides relatively low assurance of 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 which sends data to the server without the user's knowledge, even if the user physically sits in front of the computer.

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.

Answer

i. The likelihood of threat occurrence is an increasing function of the attacker's motivation.

ii. The potential attacker gain of a successful attack is often related to the potential impact of threat occurrence (e.g. theft of money from an online bank is a gain for the attacker and a cost for the bank). Then the attacker's motivation could be influenced by the cost of threat occurrence.

iii. As a consequence of i) and ii), the likelihood of threat occurrence can be influenced by the potential impact of threat occurrence. On other words, the more money there is in the bank, the more likely it is that criminal hackers will try to steal it.

iv.