**Answers and grading comments for Assignment 1 – Week 1**

**DO NOT COPY, SHARE OR REPRODUCE THIS MATERIAL AS IT CAN GET YOU EXPELLED FROM M.U.M.**

**(1)** **A threat happens when the security of the system is violated.**

a) true  
b) false

**ANS: b**

A threat is a potential violation of security, not an actual violation. See section 1.2 (p.4)

**(2) Select all factors that directly affect the integrity of data**

a) its origin  
b) its size  
c) how well the data is protected before it arrived at its destination  
d) how well it is protected at its destination machine  
e) whether it is encrypted or not  
f) none of the above

**ANS: a,c,d**

Some students said size affected integrity because a size field will indicate that something is missing. Since that increases your trust that you received all data, I will accept that answer as an optional choice. Encryption does not directly affect the integrity of the data because the encrypted data can be tampered with.

**(3) A security policy is a statement of what is, and what is not allowed, and recommends procedures to enforce its requirements.**

a) true  
b) false

**ANS: b**

See definitions 1-1 and 1-2 of section 1.3 (p.7)

**(4) Origin integrity is a**

a) prevention mechanism  
b) detection mechanism  
c) none of the above

**ANS: a**

Origin integrity is not a detection mechanism. It's purpose is to prevent unauthorized users access to the system so that detection mechanisms don't have to be used to clean up the mess.

**(5) Cryptography can be used to assure which of the following?**

a) confidentiality  
b) integrity  
c) availability  
d) none of the above

**ANS: a, b**

Cryptography can also be used for digital signatures which are a way of assuring origin integrity. Since this was not mentioned in the first chapter, you did not lose points if you didn't select integrity. Availability really doesn't apply. The only way you could argue for it is to say that encrypting/decrypting slows the server down so that it can process as many clients, but that is a stretch.

**(6) Which of these threats affect disclosure (the unauthorized access to information)?**

a) snooping  
b) modification or alteration  
c) masquerading or spoofing  
d) repudiation of origin  
e) denial of receipt  
f) delay  
g) denial of service  
h) none of the above

**ANS: a**

These terms are defined in section 1.2 (p.4-6) of the textbook. I also accepted masquerading or spoofing since if somebody can pretend to be someone else, they might be able to see data that they shouldn't see.

**(7) A denial of service attack is an attack on**

a) confidentiality  
b) integrity  
c) availability  
d) none of the above

**ANS: c**

See section 1.1.3 (p. 4) of the textbook.

**(8) What is the weakest link in the security mechanisms of any computer system?**

a) the network  
b) the operating system  
c) the application programs  
d) the human beings using the system

**ANS: d**

If somebody gives their password to an attacker, the security mechanisms won't be able to stop him/her.

**(9) Assurance is an attempt to quantify trust.**

a) true  
b) false

**ANS: a**

See section 1.5 (p.10) of the textbook. If you said in a comment that assurance is an attempt to quantify "trustworthiness" I would have to agree with you. I think the author is using the word "trust" loosely here.

**(10) There is no technical solution to the problem of social engineering**

a) true  
b) false

**ANS: a**

If you can trick somebody into telling you their password all technical measures are worthless.

**(11) Cost-benefit analysis and risk analysis are techniques used to increase assurance.**

a) true  
b) false

**ANS: b**

Cost-benefit analysis and risk analysis let you determine how much you want to spend on security. Once you pay for it, then you are interested in assurance, namely that the security system you have purchased does what it is supposed to do.

**(12) A mail server that drops all messages that mention a URL, have an attachment, contain non-ASCII characters or are longer than 2KB is an example of what kind of security mechanism?**

a) secure  
b) precise  
c) broad

**ANS: a**

It is not precise because it drops messages that are not a threat to security. It is not broad because its criteria are so strict that a threat to security cannot arise. Therefore it is secure. See Definition 1-3 of p.10 of the textbook.

**(13) Performing regular backups is a means to realize the security goal of**

a) prevention  
b) detection  
c) redundancy  
d) none of the above

**ANS: d**

Backups allow for recovery once prevention has failed and detection has detected the problem. To say that a backup "prevents" loss of data is not using the word "prevents" in the sense it is used in security. In security "prevention" means that nothing happens to the data in the first place. Several students said that comparing a backup to the current state of the system might detect illegal modifications. I gave them credit for this, but this is not the main use of a backup.

**DO NOT COPY, SHARE OR REPRODUCE THIS MATERIAL AS IT CAN GET YOU EXPELLED FROM M.U.M.**