**Answers and grading comments for Assignment 12 – Week 14**

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

**(1) Using fail-safe defaults lessens the psychological acceptability of a system.**

a) true  
b) false

**ANS: a**  
If access is the default, i.e., there are no fail-safe defaults, it means that users don't have to figure out how to grant access to resources. This is easy on the users, everything is accessible. Windows used to ship with everything accessible, you had to specifically deny access to resources. This was convenient for users (i.e., Microsoft wanted Windows to be easy to use), but it was paradise for attackers. Microsoft has since changed its policy.

**(2) Which of the following is a more serious attack on the DMZ web server?**

a) one coming from the internal network  
b) one coming from the Internet

**ANS: a**  
Which is worse? Having an enemy working in the state department or having an enemy in some faraway country? Internal attacks are very serious indeed because they come from inside the firewalls and Drib should be able to trust its employees not to do such a thing.

**(3) Each process running on a machine is a potential vulnerability.**

a) true  
b) false

**ANS: a**  
In general, you should only start the services that you actually need. So, for example, if you aren't using IIS, don't start it. The 19 deadly sins of computer security make every process a potential vulnerability!

**(4) The effects of** [**Murphy's Law**](http://www.google.com/url?q=http%3A%2F%2Fen.wikipedia.org%2Fwiki%2FMurphy%2527s_Law&sa=D&sntz=1&usg=AFQjCNF3SbaG1Uf2Mf4ap0bsCSCSrymQKg) **can be lessened by following which one of these principles?**

a) principle of least priviledge  
b) principle of fail-safe defaults  
c) principle of economy of mechanism  
d) principle of complete mediation  
e) principle of open design  
f) principle of separation of privilege  
g) principle of least common mechanism  
h) principle of psychological acceptability  
i) any principle, if followed correctly, will decrease the chance that something will go wrong.

**ANS: i**

**(5) M.U.M. uses different stickers on badges to give access to various things such as the dining room, meditation hall, or bookstore discounts. Which two of the following principles are most applicable to this situation?**

**Please list the two principles first followed by an optional brief justification of your choices.**

a) principle of least privilege  
b) principle of fail-safe defaults  
c) principle of economy of mechanism  
d) principle of complete mediation  
e) principle of open design  
f) principle of separation of privilege  
g) principle of least common mechanism  
h) principle of psychological acceptability

**ANS: b, f**  
Some possibilities:

1. Principle of least privilege - students only have stickers they have paid for the privilege to use.
2. Principle of fail-safe defaults - each activity student is qualified for is explicitly represented by a sticker. A badge is initially blank.
3. Principle of economy of mechanism - this is a very low tech, simple method. There is little that can go wrong here.
4. Principle of least common mechanism - it is hard to share a badge.
5. Principle of separation of privilege - in order to get into the dining hall you need both a badge and a sticker and perhaps they are issued by different people.
6. Principle of psychological acceptability. Badges are really, really easy to use.

The best ones are clearly separation of privilege and fail-safe defaults. However, I gave you  points for this question if you chose any of the answers that I gave above.  
And then subtracted a point for each of the following:

1. Principle of complete mediation - The mediator is the person who checks the badge. There is no mention of such a person in the question.
2. Principle of open design - I am sure that it is public knowledge how M.U.M. uses badges, but this is such an inferior choice compared to the other possibilities.

**(6) A** [**baby monitor**](http://www.google.com/url?q=http%3A%2F%2Fabout.pricegrabber.com%2Fsearch_getprod.php%2Fmasterid%3D1319407%2Fskd%3D1%2Fsearch%3DAngelcare%2520Baby%2520Monitor&sa=D&sntz=1&usg=AFQjCNFHKGfvaKy-YtJpPJ-Q5SDI6xY61g) **is an application of which one of the following principles?**

a) principle of least privilege  
b) principle of fail-safe defaults  
c) principle of economy of mechanism  
d) principle of complete mediation  
e) principle of open design  
f) principle of separation of privilege  
g) principle of least common mechanism  
h) principle of psychological acceptability

**ANS: d**  
This monitors baby's every action. This is so clearly a case of complete mediation that I am not inclined to give credit for any other answer. I expended all my generosity on the badge and sticker question. Psychological acceptability is not a good choice. Please reread the definition of psychological acceptability. It has to do with security not making the system more difficult to use. Nobody is worrying about security making the system easier to use! I did give some credit to those students who gave a somewhat plausible justification of their choice.

**(7) Please write down a main point for this week other than what was listed in the mainpoints16.htm file.**

**ANS:**

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