**Answers and grading comments for Assignment 11 – Week 13**

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

**(1) What is a DMZ (demilitarized zone)? Choose all that apply.**

a) it is another name for a firewall  
b) it is a portion of a network that separates a purely internal network from an external network  
c) it is a router that bypasses an internal network

**ANS: b**  
See Definition 23-1 in textbook. It implies there are more computers than just a firewall so the first choice is not correct.

**(2) The way that the Drib corporation moves data from one class to another is best described by 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 acceptibility  
  
**ANS: f**  
The key word in the question was "moves". Two people are involved in all moves of data from one class to another, i.e., a single person does not have the privilege to do so.

**(3) The firewalls are configured using configuration files. The only packets that are let through are those that are specifically allowed. E.G., there is an entry in the configuration file of the outer filewall that allows a packet coming from the Internet addressed to port 80 to be sent to the DMZ Web Server.**

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 acceptibility

**ANS: b**  
The key phrase here is "specifically allowed". The default is to not allow. This is a safe default. Students who justified their choice of "complete mediation" got partial credit.

**(4) The fact that developers are not allowed to telecommute, e.g., VPN into the internal network from home, is a violation of which of principle?**

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 acceptibility

**ANS: h**  
Imagine that a developer lives twenty miles from work and needs to make one small change to one of his programs. Not being able to VPN in means that he will have to drive 40 miles. He would probably think of this as psychologically unacceptable.

**(5)** **The policy and rules of the Drib security policy are available to all employees. In fact, the employees are encouraged to understand them. This is an example of which principle?**

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 acceptibility

**ANS: e**

**(6) The fact that every packet sent from the internal network must go through the inner firewall and every packet coming from the Internet must go through the outer firewall is an example of which one of these principles at work?**

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 acceptibility

**ANS: d**  
The key phrase here is "every packet". A description of complete mediation always has a word like "every" in it.

**(7) At one level, the security of the Drib system is based on how firewalls and access control lists are configured. But this security depends on the correct functioning of the firewall software and the operating system. What principle should the writers of the firewall software follow to minimize the chance that the firewall software will fail to work according to its specification?**

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 acceptibility

**ANS: c**  
This question was not about the configuration of the firewall or its function, but rather about the reliability of the firewall software. In general, the simpler the software, the more likely it will work according to specification. This is the principle of economy of mechanism.

**(8) Not allowing developers to view customer data is an example of**

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 acceptibility

**ANS: a**  
It is not separation of privilege because developers have no privilege whatsoever to view customer data.

**(9) What kind of access control policy is implemented in the internal Drib network?**

a) discretionary  
b) mandatory  
c) originator controlled  
d) none of the above

**ANS: b**  
Employees do not have the ability to let users in certain user group read their files. For example, a corporate employee does not have the ability to give a customer service employee access to files that contain financial data.

**(10) The fact that the internal network has to get through both inner and outer firewalls to get to the Internet is an example of which one of these 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 acceptibility

**ANS: f**  
The key word here is "both".

**(11) The four servers in the DMZ zone are all on separate computers. This is an example of which principle?**

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 acceptibility

**ANS: g**  
The key phrase here is "separate computers". By being on separate computers, they do not share a file system or a CPU and this limits the covert channels that are possible. It also means that if one computer goes down, Drib doesn't lose all its servers.

**(12) Preventing the Drib's employees from accessing the Internet is described in   
        the Bell-LaPadula model as:**

a) no reads up  
b) no writes down  
c) no reads down  
d) no writes up

**ANS: b**  
The Internet is unclassified, the internal network is classified (or higher). Drib's employee's can't read from the Internet but that is not disallowed by Bell-LaPadula (read downs are okay). But if a Drib employee were to write something to the Internet this would be a write down which is disallowed by Bell-LaPadula.

**(13) Preventing developers from writing to the web server machine in the DMZ is described in the Biba integrity model as:**

a) no reads up  
b) no writes down  
c) no reads down  
d) no writes up

**ANS: d**  
Only a trusted administrator can write to the DMZ web server. Developers aren't trusted to do so. This is a case of no write up. The integrity of the developer is less than the integrity of the DMZ web site.

**(14) Briefly argue that the customer service group does not have access to the Web-Clone machine because of confidentiality concerns. (Hint: use Bell-LaPadula)**

**ANS:** The Web-Clone machine will be ported to the DMZ web server, hence information on it should be unclassifed. However, the CSG has access to credit cards which are classified. Bell LaPadula prohibits write-down.

I wanted to know **why** the CSG should not be allowed to write to the WWW-Clone machine.

**(15) Now briefly argue that the customer service group does not have access to the Web-Clone machine because of integrity concerns. (Hint: use Biba)**

**ANS:** The Web-Clone machine much have high integrity because it will be copied to the DMZ web server and be seen by the whole world. Members of the customer service group probably have no web programming skills, i.e. their integrity is low and they might (inadvertently) make modifications to the Web-Clone machine that will break the web application. Biba does not allow write up from a lower integrity level to a higher one.

**(16) When is cryptography used in the Drib system?**

a) when a trusted administrator copies web pages from WWW-Clone to the DMZ web server  
b) When a developer copies web pages to the WWW-Clone machine  
c) when an Internet customer, using the web site, views a list of products that Drib provides  
d) when any employee sends an email

**ANS: a**  
Since web pages are public, they do not have to be encrypted when uploaded to the DMZ web server. The products of the company are not confidential so they don't need to be encrypted. Encrypting an email means the receiver has to be able to decrypt it. This would be too much of a restriction for the customer service group because customers would need to install something like PGP to receive email about their orders.

**(17) In the Drib system, how is malicious logic prevented from entering the internal network?**

a) mail server proxy in DMZ  
b) internal mail server  
c) educating of the Drib employees about the danger of malicious logic

**ANS: a**

**(18) Which three of the following principles are most relevant to the failing to store and protect data securely sin?**

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 acceptibility

**ANS: a, e, f**  
I suppose that violation of any of these principles could affect the security of data. I took off a point if you did not choose principle of open design because that is clearly relevant (always assume that an attacker can reverse engineer a program). I also took off a point if you did not choose principle of least privilege. Clearly you do not give everybody read/write access to secret data. Otherwise, I gave you credit if you chose any of the others, although I think that the principles of economy of mechanism and complete mediation are less relevant than the other three.

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