**Answers and grading comments for Assignment 3 – Week 3**

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

**(1) The Chinese Wall model always prevents two different subjects from reading the same CD in a COI.**

a) true  
b) false

**ANS: b**

There is no conflict of interest if two different subjects can read the same CD.

**(2) Auditting is required in which of the following models?**

a) Access Control Matrix  
b) Bell-La Padula  
c) Biba  
d) Clark-Wilson  
e) Chinese Wall  
f) Clinical Information Systems  
g) Originator Controlled  
h) Role-Based  
  
**ANS: d,** e**, f**  
  
ACM, Bell-LaPadula, Biba, ORCON, and Role-Based do not mention auditting. Clark-Wilson and Clinical Information systems specifically mention it. If you consider keeping track of who has accessed which CDs as a form of auditting then Chinese Wall also has auditting. So if selected or didn't select Chinese Wall you got it correct. Auditting requires keeping a log file!!

**(3) If a TP is not associated with a CDI x in the certified relation (see question 4), then the system will not allow the TP to modify x.**  
This policy is called white-listing, namely, only the permitted operations are listed. The opposite of white-listing is black-listing in which the operations that are **not** permitted are given.  
White-listing is an example of which principle of computer security?

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**

**(4) Enforcement rule 1 which says that "The system must maintain the certified relation, and must ensure that only TPs certified to run on a CDI manipulate that CDI" is an example of which principle of computer security?**  
Hint: The answer to this question should be different than the answer to the previous question.

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,** a  
  
The key phrase here is "must ... ensure that only TPs certified to run on a CDI manipulate that CDI". I gave partial credit if you chose least privilege and justified it by saying that TPs only have privileges need to execute certain CDIs.

**(5)** **Consider an XML database that contains accounts:**

 <accounts>  
   <account name='savings' owner='bob' amount='100'/>  
   <account name='checking' owner='bob' amount='200'/>  
...  
 </accounts>  
   
There is a TP named "transfer" that transfers money from one account to another. Note that this is a transaction, it is all or none. For example, after transferring $20 dollars from bob's savings account to his checking account, the database would look like this:  
   
 <accounts>  
   <account name='savings' owner='bob' amount='80'/>  
   <account name='checking' owner='bob' amount='220'/>  
...  
 </accounts>

Create an XML document that contains information that should be added to the log when the transfer TP is used to transfer $20 from bob's checking account to his savings account.

Your log must at least contain the date of the transaction, i.e., the XML document must represent the date somehow. Use good element and attribute names, so I can easily understand what you are saving in the log.

**ANS:**

<logTransfer>  
<transactionTime>10PM</transactionTime>  
<loginID>acct1</loginID>  
<status>successful</status>  
<transferAmount>20</transferAmount>  
<details>IP: 10.10.10.242</details>  
<from>  
 <owner>bob</owner>  
 <account>savings</account>  
 <newAmount>80</newAmount>  
</from>  
<to>  
 <owner>bob</owner>  
 <account>checking</account>  
 <newAmount>220</newAmount>  
</to>  
</logTransfer>

**(6) One encryption option for DRM is to download an encrypted key with the media and store the key in a hidden file. This violates which computer security 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**

It was in the lecture notes. It is naive to think that a hacker cannot find a hidden file.

**(7) The role-based access model is primarily concerned with protecting the integrity of information, "who can perform what acts on what information".**

a) true  
b) false

**ANS: a**

It was straight from the lecture notes.

**(8) Which model has the following principle: "Information derived from record A may be appended to record B if and only if B's access control list is contained in A's".**

a) Chinese Wall  
b) Clinical Information Systems  
c) ORCON  
d) Role-Based Access Control  
e) none of the above

**ANS: b**

It was straight from the lecture notes.

**(9) Consider the following Biba integrity levels.**

Highly trusted = 3  
trusted = 2  
not trusted = 1

Let's say that program P1 is highly trusted, P2 is trusted and document D1 is highly trusted and D2 is not trusted. Which of the following are true?

a) P1 can read D1  
b) P1 can read D2  
c) P2 can read D1  
d) P2 can read D2  
e) P1 can write D1  
f) P1 can write D2  
g) P2 can write D1  
h) P2 can write D2

**ANS: a, c, e, f, h**

**(10) Do you promise to never build a SQL query from user input using string concatentation or a format statement?**  
  
a) Yes  
b) No  
c) I want to talk to my lawyer before answering this question. **ANS: a**

**(11) Lipner's second point requires that developers do not develop programs on the production system. One way to achieve this is to not give the developer account on the production machine privileges to execute a compiler. Another way of doing it is to not give the developer an account on the production machine at all. And a third way is to not have a compiler on the production machine. This is an example of which principle of computer security:**

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**

**(12) Microsoft's SQL Server has two authentication modes:  
  1. Windows Authentication: The windows login is also used to log onto the SQL database  
  2. SQL Server Authentication: You must also log onto the SQL server database, the windows login will not get you into the database.  
SQL Server Authentication is an example of which computer security 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: f**

If you justified you answer with a comment, I gave you partial credit for complete mediation. There is no default behavior here, you have to select which type of authentication you want.

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