**Answers and grading comments for Assignment 2 – Week 2**

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

**(1) You should have a high degree of trust in applets which are Java programs that are downloaded from the Internet by the browser and run on your machine. The browser runs them in what is called a sandbox, which restricts what the applet can do on your machine.**  
a) yes  
b) no  
c) depends whether I have the latest Java Runtime Environment (JRE) installed.  
  
**ANS:  c**  
This question really cries out for a clarification on your part. The issue here is not how reliable the applet is, but rather how reliable the JVM (sandbox) is. If you argued that even the latest version of the JRE might have vulnerabilities in it, I gave you full credit for the question if you answered "no". If you answered "no" then you really should turn off applets in your browser. You could also question what does "high" means.

**(2) Create an XML document that represents the following information**  
The role named "student" has read access to file1, append access to file2 and read/write access to file4. The role named "intern" has write access to file1 and read/write/execute access to file3.   
Here is how the roles are distributed   
  1. joe is both a student and an intern  
  2. jack is a student  
  3. pat is a student  
  4. kathy is an intern  
   
ANS:

<os>  
 <roles>  
   <role name='student'>  
     <operation object='file1' rights='r'/>  
     <operation object='file2' rights='a'/>  
     <operation object='file4' rights='rw'/>  
   </role>  
    
   <role name='intern'/>  
     <operation object='file1' rights='w'/>  
     <operation object='file3' rights='rwe'/>  
   </role>      
 </roles>  
   
 <users>  
   <user subject='joe'>  
     <role>student</role>  
     <role>intern</role>  
   </user>  
   <user subject='jack'>  
     <role>student</role>  
   </user>  
   <user subject='pat'>  
     <role>student</role>  
   </user>  
   <user subject='kathy'>  
     <role>intern</role>  
   </user>  
 </users>  
</os>

Your definition of role should not contain subjects.

**(3) In Windows, the owner of a file can control who can access the file. This is an example of**

a) mandatory access control  
b) discretionary access control  
c) originator access control  
d) password access control  
e) none of the above  
  
**ANS: b/c**

**(4) Represent the following access control matrix as an XML document. Your representation should be optimized for use as a capability list.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | file1 | file2 | file3 | file4 |
| bob | read,write,own |  | read | read,write,execute,own |
| jill | append | append | read | read,write,execute,own |

**ANS:**

<processList>  
 <subject name='bob'>  
   <capabilities>  
     <capability object='file1' rights='rwo'/>  
     <capability  object='file3' rights='r'/>  
     <capability object='file4' rights='rweo'/>  
   </capabilities>  
 </subject>  
   
 <subject name='jill'>  
   <capabilities>  
     <capability object='file1' rights='a'/>  
     <capability object='file2' rights='a'/>  
     <capability object='file3' rights='r'/>  
     <capability object='file4' rights='rweo'/>  
   </capabilities>  
 </subject>  
</processList>

**(5) Consider the following access control matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | file1 | file2 | file3 | file4 |
| bob | read,write,own | read | read,write,execute,own |  |
| jill | append | Read,own | execute | read,write,execute,own |

Which of the following statements are true about this access control matrix.

a) bob and jill can read file4  
b) bob can write file3  
c) some objects are owned by more than one subject  
d) file3 is a program  
e) all subjects can write to the objects they own.  
  
**ANS: b, d**  
The question was specifically about the given access control matrix. The first three choices are unambiguous. The last two might be interpreted differently than I had in mind when I wrote the question. So if you did not select "file3 is a program" and justified your answer by saying that "execute" could mean something else other than its normal meaning I did not take off a point. And if you selected the option that "all subjects can write to the objects they own" and justified it by saying that an owner of the object can modify the permissions of the object and hence can give themselves write permission, then I did not take off a point.  
  
  
**(6) Wood mentions the following security policy item:**  
Power conditioning equipment required for all PCs Policy: All PCs must be outfitted with either uninterruptable power supply systems, electrical power filters, or surge supressor which have been approved by the information systems department. This is a means to assure:  
a) confidentiality  
b) integrity  
c) availability   
**ANS: c**

**(7) Here are six policies from Wood regarding computer usage. Choose the 3 that are most appropriate for the M.U.M. computer lab.**  
a) Games may not be used on any computers that use the M.U.M. LAN. Policy: Since games can introduce viruses, take up system resources and are generally a distraction from the main purpose of the M.U.M. LAN which is to promote Computer Science education, no games may be stored on or used by any computer hooked up to the M.U.M LAN.  
b)  No personal use of the Internet Policy: M.U.M. computers must be used for educational purposes only related to the courses and job search requirements of the students. Personal use (e.g., reading the news or downloading videos) is allowed only by special permission of the department manager.  
c) Personal use of computers only after class time. Policy: M.U.M. encourages students to explore the Internet, but if this exploration is for personal use, it must be done on personal time after daily homework has been been completed. Likewise, for news feeds, discussion groups, games and other activities which cannot be definitively linked to an individual's educational responsibilities must be performed on personal time.  
d) Granting user IDs to outsiders Policy: Individuals who are not M.U.M. faculty, staff or students must not be granted a user ID or otherwise to use the M.U.M computer lab unless written approval of a department head has first been obtained. This includes giving a non-M.U.M. person your user ID and password.  
e) Disclaimer of responsibility for damage to data and programs. Policy: M.U.M. uses access controls and other secruity measures to protect the confidentiality, integrity and availability of the information handled by computers and communication systems. In keeping with these objectives, management maintains the authority to: (1) restrict or revoke any user's privileges, (2) Inspect, copy, remove,or otherwise alter any data, program, or other system resource that may undermine these objectives. (3)take any other steps deemed necessary to manage and protect its information systems. This authority may be exercised with or without notice to the involved users. M.U.M. disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.  
f) Information ownership must be assigned Policy: Management must clearly specify in writing the assighment of ownership responsibilities for databases, master files, and other shared collections of information. These statements must also indicate the individuals who have been granted authority to originate, modify, or delete specific types of information found in these collections.  
**ANS:  a, c, d, e**  
No personal use of computers is too extreme. How would students check email? Information ownership might apply to interns but not to students. Other choices are more relevant.

**(8) The textbook has a reference to an earlier version of Charles Cresson Wood's book Information Security Policies made Easy . The latest version of this book costs $795.00. Why so much? Because it contains 842 items that a company or university could include in their security policy. All you have to do is copy his words. This will definitely save a company who wants to be sure that they don't overlook anything a lot of money.  
The following questions lists 8 login related security policy items from that book. Your job is to select the 3 ones that would most appropriate for a security policy for the M.U.M. computer lab. Hint: students will probably choose different items but some items are just too strict for an academic computer lab and you will lose points if you choose them.**

a)Pronounceable system-generated passwords Policy: So that users may more easily remember them, and so that users will not need to write them down, all system-generated passwords for end-users must be pronounceable (e.g., brom\_howser)  
b)  Periodic forced password changes Policy: All users must be automatically forced to change their passwords at least once every ninety(90) days.  
c) Assignment of expired passwords Policy: The initial passwords issued by a security administrator must be valid only for the involved user's first on-line session. At that time, the user must be forced to choose another password before any other work can be done.  
d) Use of duress passwords Policy: Whenever system access to a particularily valuable or sensitive data is given to a user, the user must be given two passwords: a regular password and a duress password. The duress password is used to covertly signal the system that this user is being pressured to log on. Duress passwords are special passwords used only in those circumstances where an alarm should be triggered, but where the user's safety may be jeopardized if the bad guys forcing the user to log on know that an alarm has been triggered.  
e)  Requirement for different passwords on different systems. Policy: To prevent the compromise of multiple systems, computer users must employ different passwords on each of the systems to which they have been granted access. For example, the NT login and the password used to connect to the SMTP server or POP server for email.  
f) Prohibition of multiple simulaneous login sessions Policy: Unless special permission has been granted by the system manager (e.g. Payman), computer systems must not allow any user to conduct multiple simultaneous on-line sessions.  
g) Automatic log off process Policy: If there has been no activity on a PC for more than 10 minutes, the system must automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided the proper password.  
h) Must log off if leaving computer Policy: If the computer system to which they are connected contains sensitive or valuable information, users must not leave their PC unattended without first logging out.

**ANS:  a, b, c, f, g, h**  
You lost points if you chose either "use duress passwords" or "different password on different systems" since there are clearly more appropriate choices for M.U.M. (it would be too much trouble to force students to have different passwords for NT and for the CoopDB page.)

**(9) Create access control lists from the following role information**.

<os>  
 <roles>  
   <role name='student'>  
     <operation object='file1' rights='r'/>  
     <operation object='file2' rights='a'/>  
     <operation object='file4' rights='rw'/>  
   </role>     
   <role name='intern'/>  
     <operation object='file1' rights='w'/>  
     <operation object='file3' rights='rwe'/>  
   </role>      
 </roles>   
 <users>  
   <user subject='joe'>  
     <role>student</role>  
     <role>intern</role>  
   </user>  
   <user subject='jack'>  
     <role>student</role>  
   </user>  
   <user subject='pat'>  
     <role>student</role>  
   </user>  
   <user subject='kathy'>  
     <role>intern</role>  
   </user>  
 </users>  
</os>  
   
ANS:

<?xml version="1.0" encoding="utf-8"?>  
<filesystem>  
 <object name="file1">  
   <acl>  
     <ace subject="joe" rights="rw"/>  
     <ace subject="jack" rights="r"/>  
     <ace subject="pat" rights="r"/>  
     <ace subject="kathy" rights="w"/>  
   </acl>  
 </object>

 <object name="file2">  
   <acl>  
     <ace subject="joe" rights="a"/>  
     <ace subject="jack" rights="a"/>  
     <ace subject="pat" rights="a"/>  
   </acl>  
 </object>

 <object name="file3">  
   <acl>  
     <ace subject="kathy" rights="rwe"/>  
     <ace subject="joe" rights="rwe"/>  
   </acl>  
 </object>

 <object name="file4">  
   <acl>  
     <ace subject="joe" rights="rw"/>  
     <ace subject="jack" rights="rw"/>  
     <ace subject="pat" rights="rw"/>  
   </acl>  
 </object>  
</filesystem>

**(10) The next five questions test your knowledge of the Bell-LaPadula model. They are based on the following information:**  
The security levels are TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest)  
The categories are A, B and C.  
Discretionary access controls allow anyone access unless otherwise specified.  
Paul, cleared for (TOP SECRET, {A, C}), wants to access a document classified (SECRET, {B, C}). What type of access does he have?  
a) read  
b) write  
c) both  
d) neither  
**ANS: d**

**(11) Sammi, cleared for (TOP SECRET, {A, C}), wants to access a document classified (CONFIDENTIAL, {A}). What types of access does he have?**  
a) read  
b) write  
c) both  
d) neither  
**ANS: a**

**(12) Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, {B}). What types of access does she have?**  
a) read  
b) write  
c) both  
d) neither  
**ANS: b**  
CONFIDENTIAL is greater than UNCLASSIFIED and the empty set (the categories of Robin) is a subset of {B} so the object dominates the subject and hence Robin can write.  
  
**(13) Anna, cleared for (CONFIDENTIAL, {C}), wants to access a document classified (CONFIDENTIAL, {B}). What types of access does she have:**  
a) read  
b) write  
c) both  
d) neither  
**ANS: d**   
  
**(14) Jesse, cleared for (SECRET, {C}), wants to access a document classified (CONFIDENTIAL, {C}). What types of access does he have?**  
a) read  
b) write  
c) both  
d) neither  
**ANS: a**  
Remember, no writes down.

**(15) Wood mentions the following two policies:**  
No read up permissions to access sensitive information Policy: Workers who have been authorized to view information classified at a certain level must be permitted to access only the information at this level and at less sensitive levels.  
No write down permissions to access sensitive information Policy: Workers must never be authorized to move information classified at a certain sensitivity level to a less sensitive level unless this action is a formal part of an approved declassification process.  
Which access control model would cover the above two policy items?  
a) Bell-LaPadua  
b) Role-Based Access Control Model  
c) Access Control Model  
d) None of the above  
**ANS: a**

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