Homework 2

Due Date: May 9, 2000 **Points**: 200

1. (*20 points*) A noted computer security expert has said that without integrity, no system can provide confidentiality.
   a. Do you agree? Please justify your answer.
   b. Can a system provide integrity without confidentiality? Again, please justify your answer.
2. (*25 points*) Given the security levels TOPSECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, say what type of access (read, write, or both) is allowed in the following situations. Assume discretionary access controls allow anyone access unless otherwise specified.
   a. Paul, cleared for (TOPSECRET, { A, C }), wants to access a document classified (SECRET, { B, C }).
   b. Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, { B }).
   c. Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }).
   d. Sammi, cleared for (TOPSECRET, { A, C }), wants to access a document classified (CONFIDENTIAL, { A }).
   e. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, { B }).
3. (*25 points*) Declassification effectively violates the *-property of the Bell-LaPadula Model. Would raising the classification of an object violate any properties of the model? Why or why not?
4. (*30 points*) Please show how separation of duty is incorporated into Lipner's model.
5. (*100 points*) The host *pacific-hts.cs.ucdavis.edu* is a Windows 2000 system on the network. We will be conducting a penetration test as a class experiment throughout this term. The goal is to acquire access to the system as a user (*administrator* or otherwise). The first step in a penetration test is to hypothesize flaws, or potential vulnerabilities. For this exercise, you must assume you are analyzing the system as though you have no access to it other than from the network. You will hypothesize potential flaws, but ***not*** test them yet.
   a. Determine what network servers *pacific-hts* is running. (***Hint***: find the program *nmap*, download it and use it.)
   b. Please devise three possible network-based vulnerabilities on the system using your knowledge of the servers and of potential vulnerabilities in them. You must justify why you think the system may have that vulnerability. Please post your description to the newsgroup *ucd.class.ecs253.d*. As part of the requirement for this answer, *each student must submit 3 different potential vulnerabilities*; the first poster of each potential vulnerability gets credit for it. So be sure your vulnerabilities are different than your classmates'!

   For credit for this problem, please turn in the following:
   a. The output of a port scanner run against *pacific-hts*. Please be sure to put the date in the output (you can do this by hand if you like) because the configuration will be changing.
   b. Three possible vulnerabilities using the template below. Fill in what you can; put "to be determined" where you don't know. Please don't submit things that others have posted to the newsgroup. However, if you have an idea for a different vulnerability inspired by something that was posted, go ahead and submit that. Grading will *not* be based on whether the hypothesized flaw exists; it will be based upon your creativity, ideas, and justifications. On the form, incidentally, your justification should go in the section for the long description. Your description here should explain the vulnerability on an existing system, and why you think *pacific-hts* may suffer from it; or, explain what you think the vulnerability would be, and (again) why *pacific-hts* may have it.

The Template For the Holes

This may be found on the web as http://seclab.cs.ucdavis.edu/projects/vulnerabilities/doves/template.html.

```
<!-- This is an SGML comment.
     The next line identifies the dtd and document type and must be
     included in every vulnnerability description.                    -->
<!DOCTYPE vdbentry SYSTEM "vulner.dtd">
     <!-- The next line begins the document type and identifies it as
          a vulnerability database entry. The "refer" attribute is the
          number of the vulnerability in the database; the DOVES
          registry (for now, at UC Davis) will assign it.              -->
<vdbentry refer="V-nnnnn">
     <!-- the title of the vulnerability                               -->
<title>
</title>
     <!-- the descriptive components of the vulnerability              -->
<desc>
     <!-- a short description; one or two sentences                   -->
  <short>
  </short>
     <!-- a long description; what causes the vulnerability, in
          detail (if you have code, put it here!)                      -->
  <long>
  </long>
     <!-- components involved in causing the vulnerability; these
          can be program names, files, and anything necessary for
          the vulnerability to occur; if there is a version
          associated with any component, give it (and label it
          verified, trusted, or unverified)                            -->
  <comp>
  </comp>
     <!-- on what operating system or windowing system has it been
          seen? the os need NOT be involved in the vulnerability!
          again, if there is a version associated with the os
          involved, give it (and label it verified if you yourself
          have seen it or found it; trusted if you've not seen it
          but someone or some source you trust has announced it --
          be sure you identify the source in the history section;
          or unverified if this is a rumor or something you've heard
          but are not too confident of                                 -->
  <os>
  </os>
     <!-- the effect of the vulnerability being exploited; this is
          to be a description of what happens; the access field
          gives a short, one-word desription of the effect (choose
          one of the words below)                                     -->
  <veffect access="root|user|read|write|execute|deny">
  </veffect>
     <!-- how do you detect this vulnerability? list these as
          multiple techniques; an implicit one is to use the attack.
          don't list that one here; list techniques to find the
          vulnerability that don't involve attacking                  -->
  <vdetect>
```

```
          <!-- you can have numerous techniques to locate a
               vulnerability                                          -->
    <tech>
               <!-- the technique may have 0 or more steps; put
                    these around each step                            -->
      <step>
      </step>
    </tech>
  </vdetect>
     <!-- how do you fix this vulnerability? list these as multiple
          techniques                                                  -->
  <vfix>
          <!-- you can have numerous techniques to fix a
               vulnerability                                          -->
    <tech>
               <!-- the technique may have 0 or more steps; put
                    these around each step                            -->
      <step>
      </step>
    </tech>
  </vfix>
     <!-- put anything else into this category; if you want to add
          fields, put them in here for now and they can be moved out
          later                                                       -->
  <vother>
  </vother>
</desc>
     <!-- list meaningful keywords; check the keyword catalogue
          first to see if any there apply (the registry will add
          new ones as you list them)                                  -->
<keyword>
</keyword>
     <!-- this section contains cataloguing information for other
          catalogues                                                  -->
<cat>
          <!-- if you have a classification scheme, make up an
               SGML tag for it; you will maintain all
               classifications for it. Current tags follow.
               pa = program analysis project category                 -->
     <pa>
     </pa>
          <!-- risos = research into secure operating systems
               category                                               -->
     <risos>
     </risos>
          <!-- dcs = decomposition classification scheme category  -->
     <dcs>
     </dcs>
          <!-- mitre = CVE classification; refer is number, field
               is CVE cluster                                         -->
     <mitre refer="#####" field="#####">
     </mitre>
</cat>
     <!-- this section contains pointers to attacks; they refer
```

```
          to the exploits section of the database                  -->
<exploit>
          <!-- this is where you put the pointer to the attack;
               you can list several attacks, one per field         -->
  <attack>
  </attack>
</exploit>
     <!-- this section contains related information such as
          pointers to advisories, other vulnerabilities, and
          papers, and so forth; feel free to explain the
          relevance of anything you put in here                    -->
<relinfo>
          <!-- advisories and other references; put URLs if
               you have them (we will try to fill them in if
               you don't want to)                                  -->
  <adv>
  </adv>
          <!-- put DOVES references in here; again, we will
               try to fill out cross-references of other
               vulnerabilities, attacks, and signatures unless
               you don't want to                                   -->
  <ovn>
  </ovn>
</relinfo>
     <!-- this section contains bibliographic information for
          the vulnerability; please be as precise as you can,
          since we want to give credit where credit is due         -->
<history>
          <!-- this says who reported the problem,and where;
               you can have multiple of these sections             -->
  <report>
       <!-- who; give email address if you've got it (or other
            contact info, such as a web page)                      -->
    <reporter>
    </reporter>
               <!-- where was it reported; please be as precise
                    as possible (message IDs are nice if the
                    messages are publicly available)               -->
    <where>
    </where>
               <!-- when was it posted/announced/etc.             -->
    <when>
    </when>
  </report>
</history>
     <!-- this section contains bibliographic information for
          the ENTRY; say what you changed in the entry (or
          say that you created the entry) and when; please put
          enough information in there so we can contact you!
          We will pull that out, add you to our database of
          contributors, and put your name or ID into the "who"
          field when we distribute it, again unless you tell
          us otherwise                                             -->
<revision>
```

```
          <!-- here's where you put your info; you can have
               multiple of these, one per alteration (or user)     -->
  <changes date="" who = "">
  </changes>
</revision>
    <!-- ALL DONE! (PHEW!)                                        -->
</vdbentry>
```