CSci 530 Final Examination

Fall 2004

Instructions:

Show all work. **If a question asks for a numerical or algebraical result, indicate your answer clearly (for example, by drawing a box around it)**. No laptop computers are allowed; handheld calculators are permitted. This exam is open book, open notes. You have 120 minutes to complete the exam.

Please prepare your answers on separate sheets of paper.� You may write your answers on the sheet of paper with the question (front and back).� If you need more space, please attach a separate sheet of paper to the page with the particular question.� **Do NOT extend your answer on the back of the sheet for a different question, and do NOT use the same extra sheet of paper to answer more than one question**.

In particular, **each numbered questions must appear on separate pieces of paper so that the exam can be split for grading**.

Be sure to include your **name** and **USC ID** number **on each page**.

There are 100 points in all and 4 questions

	Q1	**Q2**	**Q3**	**Q4**	**Total Score**
Score					

1. **(20 points) Intrusion Detection Systems**
   Intrusion detection systems are usually classified along two dimensions: the source of the input data (2 or 3 values traditionally), and how that data is analyzed (two approaches).�� For each of these, give a name that describes the source of input or the method of analysis (hint: these are usually two word phrases and the second word is �based�), describe the source or approach, and give the advantages and disadvantages with respect to the other values in the same dimension.

a. Source of input data:

________________________� based is �

________________________� based is �

_________________________ based is �

b. Method of analysis

_________________________ based

_________________________ based

2. (30 points) Authorization and Policy

a. (10 points) List 10 places where policies are enforced within a network of computers (including points on the systems within the network itself) including at least two of which are specified by the current end user (as opposed to the owner of a resource).

________________________________��� ________________________________

________________________________��� ________________________________

________________________________��� ________________________________

________________________________��� ________________________________

________________________________��� ________________________________

b. (10 points) Authorization policies are often (but not always) based on the identity of some entity in the system.� Sometimes the identity has been authenticated, sometimes not.� Consider the policies typically enforced by the following devices.� For each, list the entity whose identity is a factor in the authorization decision, and whether that identity is authenticated in the common case.

Firewall���������� identity of the __________________________� Authenticated: yes/no

Web server���� identity of ____________________________��� Authenticated: yes/no

����� Or������������� identity of ____________________________��� Authenticated: yes/no

File System��� identity of� ____________________________�� Authenticated: yes/no

VPN Server��� identity of _____________________________� Authenticated: yes/no

���� c.�� (10 points) Describe the policies enforced by a digital rights management system.� In a well designed DRM system, what entities would be authenticated and what is the reason for doing so (i.e. what could happen if these entities were not authenticated).

3. (20 points) Wireless Security

(a) (points) What assurances are provided by wireless security protocols like WEP or WPA (when such protocols have not been broken).� Why are these protections useful?�

(b) (points) At what layer in the protocol stack are these protections provided, and why is this of concern?� In particular, what vulnerabilities remain if one depends on these protocols to secure wireless communications?

Q3. Wireless Security <continues>

(c) (points) What additional steps should one take to protect wireless communications?� If you take these additional steps, does it matter if you are running on an open wireless network, as compared with one running WEP or WPA?

(d) (points)� As an application developer, what steps can you take to ensure the security of your application, regardless of the location of your users?

4. (30 points) Design question:

You have been asked to design a system to support the collection and counting of votes for the next election.� In particular, you have been asked to design a system that will accurately tabulate votes entered by voters at poling places throughout the state and to transmit those votes to the county clerk of each county where the totals will be tabulated.
(*This is not the same problem as in the fall 2003 mid-term exam*).

(a) Threats (5 points). �What are the threats in such a system?�� What can go wrong?

(b) Requirements (10 points). What are the requirements for authentication, authorization, assurance, audit, and privacy?� Explain who and what must be authenticated, what authorizations are required, what assurance is needed for the software, and what kind of records must be maintained (as well as what kinds of records should not be maintained).

Q3. Design question <continues>

(c) (10 points) Considering the requirements listed above, and how they relate to the assurance problem, i.e. how can steps taken for authentication, authorization and audit be used to ensure that the software has not been modified to improperly record or transmit votes?

(d) (5 points) What technologies proposed for digital rights management be used to provide stronger assurance that the system�s integrity has not been compromised.�� What is similar about the two problems, and how would such technologies be applied to the voting problem.