Name: _____ **USC ID:** _____

CSci 530 Final Exam

Fall 2008

Instructions:

Show all work. No electronic devices are allowed. 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**	**Letter**

Name: _____ **USC ID:** _____

1. **(25 points) Privacy.** Explain in no more than 5 sentences how information from each of the following sources may be used today to track the movements of individuals.
   a) RFID Tags

   b) Cell phone records

   c) Web (HTTP) server logs

d) Access (Proximity) cards for access to buildings/doors/garages

e) Credit card transaction records

Name: _____ **USC ID:** _____

2. **(25 points) Intrusion Detection -** Explain the limitations of each of the classes of intrusion detection listed below. In your explanation of the limitations, for each limitation give an example of a kind of attack or a situation under which the particular kind of intrusion detection will not be effective.
(5 points each part)

a) Signature based intrusion detection

b) Anomaly based intrusion detection

c) Host based intrusion detection

d) Network based intrusion detection

e) Application based intrusion detection

Name: _____ **USC ID:** _____

3. **(20 points) Persistence of Protection –** Explain the persistency of the confidentiality protection provided in each of the following systems. In particular, explain where the data is protected, and where it is visible in its plaintext form. Discuss the implications of this for security of the data, and also the implication for the complexity of the system needed to manage the data (i.e. the key management problem).

   a) Data protected by SSL or TLS

   b) Encrypted messages in PGP or S/MIME

c) Information retrieved over a Virtual private network connection

d) Data protect by WEP or WPA (i.e. 802.11 encryption)

Name: _____ **USC ID:** _____

4. **(30 points) Design Question –** You have been hired by the state of California to improve the security of the computer systems at the department of motor vehicles. Much if the information in the system is sensitive and it will be important to limit access to this data, not just by the general public, but also to maintain strict accountability for access by DMV and law enforcement employees themselves. Given the large number of terminals throughout the state (including those in patrol cars) from which such data is accessible, you have been asked to consider approaches that will prevent data from being downloaded and then transferred to other computer systems outside of the states network.

   a) Describe the data to be protected in such a system and suggest the policy that should be applied for each class of data – i.e. who can view it and who can modify it. (10 points)

   b) Suggest techniques that can be applied to prevent mis-use of the data by insiders, i.e. those that might have authorization to access the data according to the policies implemented by the computer systems, but who might not have legitimate need to access the data. (5 points)

c) Suggest techniques that could prevent the data from being accessed by malicious code that might end up installed on, and having infected, terminals in the system. (10 points)

d) Suggest techniques that would prevent data from being downloaded from the system and then transferred to other external systems over which the access controls to the data might not be enforced. (10 points)