**Name:** _____ **USC ID:** _____

# CSci 530 Final Exam

# Fall 2006

**Instructions:**

Show all work. No electronic devices are allowed. This exam is open book, open notes. You have **115 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 **3 questions.**

| | Q1 | Q2 | Q3 | Total Score |
|---|---|---|---|---|
| **Score** | | | | |

**Name:** _____ **USC ID:** _____

1. (40 points) Overview of Countermeasures

   Consider the security technologies and methods listed below. For each, list the kinds of threats against which the countermeasure is most effective and the kinds of threats against which it least or not effective (you may list as many as you want, but wrong answers will lose points – you can get no more than 4 or less than 0 points per sub-part).

   a) Dedicated perimeter firewalls.

   b) Host based firewalls.

   c) Network Based intrusion detection

**Name:** _____ **USC ID:** _____

d) Anomaly Based intrusion detection systems.

e) Virtual Private Networks

f) IPSec or IPV6 Security

g) Anti-virus software

h) Encryption based authentication (e.g. Kerberos or Certificate based)

i) Smartcards

j) Trusted Computing

**Name:** _____ **USC ID:** _____

2. (25 points) Malware

a) **Detection avoidance -** List 3 substantially different techniques used by malware to avoid detection and explain how each is accomplished. (10 points – note that the more different the techniques are, the more likely you are to get full credit ).

**Name:** _____ **USC ID:** _____

b) **Separation of phases –** Explain why you think the steps taken for propagation of malware (e.g. insertion phase of a virus) are often described separately from the malicious action (e.g. the payload)? How will the effectiveness or timing of one phase affect the success of the other phase? (10 points)

**Name:** _____ **USC ID:** _____

c) **Detecting Malware –** What is the most important characteristic of a detection mechanism that will enable it to effectively detect malicious code that has infected a system? Explain your answer. (5 points) [hint – think about this question philosophically]

**Name:** _____ **USC ID:** _____

3. (35 points) Designing Secure Systems

You have been hired by NASA to develop the network and system architecture for the computers that will be installed on the first manned base on the moon. As part of the requirements for the system, each crew member's quarters will have a computer device that must be usable to access the mission critical systems to which they are assigned, but which can also be used for personal purposes at other times, including communication through the general internet email system on earth (let's not debate whether this is a good idea – it isn't, but it is in the requirements you were given).

Your mission, should you decide not to resign in protest, is to develop the high level design for the system and network that will provide the strongest security, and greatest isolation for the critical functions that run on the systems. (Please read all parts – a b c – of this question before you begin to answer)

a) Discuss the security requirements for such a system. What is the data and what are the functions to be protected? What are the threats and vulnerabilities that might be present and how might the vulnerabilities be exploited? (10 points)

b) Discuss approaches that can be used to improve the security of such a system. What hardware features would you advise including in the computers on the network? How would these features help to improve the security of the system? What kinds of authentication methods would you deploy? What operating system features would improve the security of the system? (15 points)

c) Discuss the security requirements for the network in such a system. What network based defenses will you deploy? How will you protect availability of network communication for critical functions from denial of service attacks that might be targeted at or carried by non-critical functions (e.g. spam, viruses or worms)? (10 points)