EECE 412, Fall 2012

Quiz #1

Your Family name: _____

Your Given name: _____

Your student ID: _____

_____

Notes:
- Make sure your handwriting is legible. If the teaching staff does not understand what your wrote, they mark your answer as if the unreadable text is missing.

- Aim to be precise and to the point. The experience of teaching this course since 2004 suggests that excessively long answers tend to correlate with lower marks.

- As in real world, stated questions and/or accompanied descriptions in this quiz are often open-ended and one has to make assumptions in order to answer them. If you do make assumptions, state them clearly and explicitly.

- The mark for this quiz will be pro-rated. That is, the best answer receiving 100% and the marks for all other answers being pro-rated accordingly. So, don't panic if you feel like you are severely short on time. Everybody is. ☺

1. (4 points) Based on the article from The Register about Conficker Worm, reproduced in handout #1, analyze (1) the value of the assets at risk, (2) threats to these assets, and (3) threat agents, for the hospitals across Sheffield due to the described attack. If necessary, make reasonable assumptions and state them clearly. Explain which of the CIA properties of the valuable assets were reduced as a result of the incident.

2. (4 points) Consider the risks due to Conficker Worm explained for the previous problem. For each of the four ways of managing this risk, give one example of what the hospitals can do. Be specific.

1.

2.

3.

4.

3. The handout contains a reproduction of the Mac OS X v10.6 security features.

    a. **(7 points) For each principle for designing secure systems, put a checkmark in the following table for those aspects of Mac OS X v10.6 that enable or follow this principle.**

        Attention: The total number of points for this question will be determine using the following formula: $R - W$, where R is the number of right checkmarks and W is the number of wrong checkmarks.

	User permission model	Mandatory Access Controls	Firewalls	Protection against Trojan horse downloads	Execute disable	System library randomization	Sandboxing	Application Signing	FileVault	Encrypted Disk Images	Encrypted Virtual Memory	Private Browsing	Guest Account	Open Source Software	Sharing and Collaboration Configuration
Least Privilege															
Fail-Safe Defaults															
Economy of Mechanism															
Complete Mediation															
Open Design															
Separation of Privilege															
Least Common Mechanism															
Psychological Acceptability															
Defense in depth															
Question assumptions															

b. (10 points) Write justification for the checkmarks in the above table.
(use the next page, if you need to)