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.

Assets	Threats	Threat agents	CIA
Patient's documents/information	Malicious modification, deletion. Reveal.	Private investigators Hackers	Integrity – due to modification Availability if deleted. Confidentiality if revealed
Computer & OSes	Compromise of the OS, computer is not working when needed.	Virus, Virus writer, Uneducated personnel who disables updates or configured them incorrectly	Integrity – since the integrity of the OS is compromised Availability – Computers were not available when there was a need for them.
Patient's health/life when in the operating room	Damage/loss	Virus, Virus creator, improperly configured updates	No information is exposed More a physical loss of health
Reputation of the hospital	Damage	Competitors, Virus, Virus creator, Uneducated personnel	No information is exposed

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. **Accept – Accept the risk (i.e., live with it) and continue to use the computer systems.**

2. **Avoid – avoid the risk by not using computers at all, go back to paper based management.**

3. **Transfer – transfer the risk to someone else, e.g., buy insurance.**

4. **Reduce – reduce the risk by properly configure the updates and use modern and up to date anti-virus software.**

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	X	X						X					X		
Fail-Safe Defaults		X	X	X	X										
Economy of Mechanism															
Complete Mediation			X					X							
Open Design														X	
Separation of Privilege	X					X	X		X	X	X	X	X		X
Least Common Mechanism						X	X					X			X
Psychological Acceptability	X	X		X											
Defense in depth	X		X		X	X	X	X	X	X	X		X		
Question assumptions															

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

An example of an answer that was credited as 10 points:

1. User permission model – least privilege because users are given the minimum privilege they to complete the job. Separation of privilege because by default users are not granted all permissions they have, thus, users will need to do additional authentication for some tasks.
2. Firewalls – default safe because by default all connections on the computer are prohibited (except from the apps that come with the OS X).
3. Mandatory Access Control – default safe because the execution of a recently downloaded binary is prohibited and users' explicit confirmation is required.
4. Execute Disabled – Defense in depth, because it is an additional layer of protection between the apps and the OS.
5. SLR – least common mechanism, because applications that are using the same library will never share the same address of the entry points to the functions in the library. Such entry points if persistent and known can be abused by calls to private objects members.
6. Sandboxing – defense in depth, because it serves as another layer between the apps running on the OS and between the apps and the OS itself. Least common mechanism, because apps do not share the same environment, thus it is hard for an app to influence execution of another app.
7. Open Source Software – open design, where the source code is available for investigation and analysis by anyone.
8. Guest Account – Least privilege, because the account has the fewest permission required for executing the basic tasks.