CPE5021 Semester 2, 2007 – Individual and group assignments – 80%

The assignments consist of three parts that are assessed separately and are due on different times. All the works will be assessed with interviews.

While you have not had lectures covering the topics related to your practical works and assignments. It is wise to prepare yourselves from week 1. You may need to search for materials about Linux firewalls (SQUID), Intrusion Detection System (SNORT) about how to find vulnerabilities in your system and possible attacks, RSA and ECC source codes, etc. It is actually the nature of learning security!

Part I - 40% - 2 Individual assignments (20% each) – Due by 5:00 PM, Friday of week 7

You are required to design and implement simple RSA and ECC public key systems using C or Java.
You can find some sample codes on the Internet. However, the work you have to do is much simpler. Full description of the assignment will be handed to you in week 3.

Part II– 10% - Group work: IDS using SNORT (Group Size: Min 2 – Max 3) – due during the lab of week 12.

Your group is required to install, configure and experiment the Intrusion Detection System Snort with the help of your tutor.

Part III– 30% - Group work (Min 2 – Max 3 persons) – due during the lab of week 12.

Your group is required to find possible vulnerabilities in **your system (on your removable hard drive ONLY)** using any possible tools that you can get from the Internet.
When you have identified the vulnerabilities in your system, you need to work out how to attack your system successfully. **Remember that we MUST not break the law. You can only attack your own system and you are NOT allowed to attack any other system by law**. *The purpose of this work is educational ONLY.*

Every successful attack will count, no matter how simple it is. You need to provide at least three successful attacks to get to HD level. You are required to demonstrate your work

You also have to write a concise report to explain how you find the vulnerabilities in your systems and step-by-step how your successful attacks have been done.

If you cannot make any successful attack, you can do research about the vulnerabilities of your system and produce a report. You will get up to 60% of the full mark of part III.

- **If you do not specify the contribution of each member in your group, we will assume that all members contribute 100% and you all will have equal marks. Your tutor can interview any member of your group for assessment.**
- **It is a good idea, if you can install a similar system at home to do your work.**
- **You have to write a report for each part as specified in the handout for each part.**

Requirements of submission of report:

- **Follow standard report format for a Master Course.**
- **Include all references with details and**
- **Cite references in the text or diagrams.**
- **Submit the hard copy with cover and a soft copy of the report on a floppy or CD (the tutor will run a scanner to check your work). Please do not email it to me. I will remove it from my mail box.**
- **Do not extract line-by-line from any sources in your report.**