Name: _____ **USC ID:** _____

CSci 530 Final Exam

Fall 2007

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 **3 questions.**

	Q1	Q2	Q3	Total Score	Letter
Score					

Name: _____ **USC ID:** _____

1. **(30 points) Defense Methods.** For each of the following defense mechanisms, indicate whether it is most effective or partially effective or not effective against viruses, worms, bot-nets/zombies, root kits, spyware, impersonation (including theft of passwords/credentials), denial of service attacks, network eavesdroppers, insider abuse (includes misuse of data to which one is allowed limited access), or penetration attempts by outside attackers. Briefly explain why. Your justification will likely apply to groups of attacks, e.g. this is ineffective against worms and viruses because …, and effective against insider and penetration attempts because …, and partially effective against eavesdropping because… List only those threats that are most relevant in each category (the categories are: most effective, least effective and partially effective against.) (5 points each part)

   a) Embedded Firewalls

   b) TLS or SSL

Name: _____ **USC ID:** _____

c) PGP or S/MIME

d) Trusted computing using a TPM

Name: _____ **USC ID:** _____

e) Biometric authentication

f) Signature based intrusion detection

Name: _____ **USC ID:** _____

2. (45 points) Trusted Computing – Design Question

If a system/platform is designed to provide support for trusted computing it is still possible for the system to run untrusted or uncertified programs. In contrast, if a program is designed to run with trusted computing support, such a program is **not** trusted if it runs on an untrusted platform. (while you may have seen this explanation before, but the rest of this question is different).

Consider a program designed to allow a user limited and controlled access to multi-media content downloaded from a server (a classic DRM application). The program runs on an operating system that supports trusted computing, on a computer with a trusted platform module. Consider a policy that allows (for example), that once a user has paid for a program, to download content for display from up to 5 machines over a period of 6 months. Viewing of the program is only authorized for the user that paid for the content.

a) If the application is expected to enforce such a policy, it is acceptable for the program to write the retrieved content to disk, or must it download the content from the server each time it is to be viewed? If it can not write the content to disk, explain why. If it is acceptable to write the content to disk, to save bandwidth for subsequent views, explain what measures must be taken by the application, or the OS in conjunction with such writes. (15 points)

Name: _____ **USC ID:** _____

b) Consider the authorization requirement that allows the data to be viewed from no more than 5 machines per purchase and only by the original purchaser. What security services are required to enforce such a constraint, and which software components (media server, tpm, operating system, client media application) must participate in that required service and for what purpose? (10 points)

c) Will it be possible for the authorized user to view his or her content when they are not connected to the network? If so, explain how the assurances validated in (b) will work when disconnected? (10 points).

Name: _____ **USC ID:** _____

d) Explain the precise meaning of the assurance that only the original purchase can view the content. The limitation that is implemented is only an approximation of the policy and I want to know the more precise policy that is implemented. (5 points)

e) For your design, explain the limitations, i.e. how extra copies of the data might be made (there will be ways to do this given the equipment description I have provided). (5 points)

Name: _____ **USC ID:** _____

3. (35 points) Authentication and Integrity

a) Explain the difference between the authentication provided by a system like Kerberos and a digital signature used to authenticate the sender of a message using PGP or S/MIME. Consider the issue of what assurances are provided, for how long, to whom, and what can be done with such assurances (10 points).

b) When a user's private key changes or is revoked, how long must we keep the old public key if we are to validate signatures generated by the user before the change? If the private key was compromised, what do we know about signatures generated with the old key and why are they still useful? What steps can we take before the key was compromised that will help us maintain non-reputability of the signature if the key is subsequently compromised? (15 points)

c) How does the use of a trusted platform module (TPM) or smartcard affect the confidence in the integrity and authentication provided using public key cryptography? (10 points)