

CS140 Operating Systems and Systems Programming Final Exam

December 12, 2005

Name: (please print) _____

In recognition of and in the spirit of the Stanford University Honor Code, I certify that I will neither give nor receive unpermitted aid on this exam.

Signature: _____

This examination is closed notes and closed book. You may not collaborate in any manner on this exam. You have 180 minutes (3 hours) to complete the exam. Before starting, please check to make sure that you have all 15 pages.

1		12	
2		13	
3		14	
4			
5			
6			
7			
8			
9			
10			
11		Total	

Name: _____

(1) (12 points) – Answer the following two questions about message digests.

- (a) Someone gives you a file along with an encrypted message digest of the file. The message digest has been encrypted with your public key. What use, if any, would there be for including such an encrypted message digest? If not useful, would there be any harm in it?

- (b) Someone gives you a file along with a message digest computed on the contents of the file concatenated with his or her private key. In other words, the message digest function was run on data that included the contents of the file appended to the private key. What use, if any, would there be for including such a message digest? If not useful, would there be any harm in it?

(2) (12 points) – Answer the following two security questions.

(a) Describe the relationship between complexity and security.

(b) What benefit could someone get from publishing the details of how their security system works?

- (3) (12 points) For each of the following attacks lists below, describe if a good public key cryptosystem would help solve the problem. If it does, say how. If it doesn't explain why.
- (a) Abuse of privileges
 - (c) Listener (eavesdropper) attack.
 - (d) Spoiler (denied of service) attack.

- (4) (14 points) Your Pintos partner asks you to add a capability-based protection system to your Pintos file system. Describe how you would go about doing this. Be sure to include data structure and algorithm additions and changes as well as any interface changes you will need.

- (5) (8 points) We use a set of techniques to synthesize reliability over unreliable network links when implementing protocols like TCP/IP. Explain why these techniques do not solve the distributed consensus problem (i.e. two army problem).

- (6) (10 points) Explain why the Internet kept working even after a successful denial of service (i.e. spoiler) attack against the root domain name service (DNS) servers.

(7) (18 points) Answer the following three networking questions.

- (a) What does the reverse address resolution protocol (RARP) do on an Ethernet network?
- (b) Explain the mechanism an Ethernet uses so a single machine cannot monopolize the network when other machines need to use it.
- (c) Describe the major features of the Internet protocol design that made it highly portable.

(8) (12 points) – Answer the following two file system questions.

- (a) Describe the techniques used by the BSD Fast File System (FFS) to improve the performance of small files.
- (b) Explain why the BSD Fast File System might spread a large file over the entire disk even though the file system is not run near capacity.

- (9) (12 points) What would be the implications of setting the log size of a write-ahead logging file system to a very small size (say just a few blocks). Consider both reliability and performance issues.

(10) (14 points) RAID

(a) For RAID4 storage devices the lecture notes say a single block write might take 2 reads and 2 writes. Explain why this is the case.

(b) Does RAID5 suffer this same problem? Justify your answer.

- (11) (12 points) What is an idempotent operation and why are they useful when dealing with a system with failures. Include an example of an idempotent operation in your answer.

- (12) (18 points) Describe what you would need to do to make your Pintos file system support keyed file access. Be explicit about the data structures and algorithms you will need to add. Also, describe what additional arguments you would need to add to system calls, etc.

- (13) (12 points) Metadata is used to describe the file system data associated with each file. The size of metadata usually scales with the size of the file. Describe a file index mechanism that does not scale with the size of the file.

- (14) (12 points) Explain how caching can improve both latency and bandwidth of a system. Give an example.