

CS110 - Principles of Computer Systems

Final Exam

(Total time = 180 minutes, Total Points = 180)

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 book and closed notes. You may not collaborate in any manner on this exam. You have 180 minutes to complete the exam. Please write your answers on the exam. Note there is one problem per page so the amount of space provided does not necessarily provide an indication of the expected length of the answer. In other words, do not feel compelled to fill every nanoacre of the exam with writing. Before starting, please check to make sure that you have all 16 pages.

Question	Points	Score
1	12	
2	12	
3	12	
4	12	
5	12	
6	12	
7	12	
8	12	
9	12	
10	12	
11	12	
12	12	
13	12	
14	12	
15	12	
Total	180	

1. (12 points) Prof. Al Dente published the following message in the Journal of Pasta Research, a printed journal syndicated to institutes of culinary science worldwide:

I have made an amazing discovery!

SHA-1: 2fd4e1c67a2d28fced849ee1bb76e7391b93eb12

This was the entire message! Recall that SHA-1 is a secure hash algorithm. The hash was of Prof. Dente's invention description. Why might Prof. Dente have published this message and what benefit could he get from it?

2. (12 points) Cryptography can be used for *authentication*, *integrity*, and *confidentiality*. For each attack type listed below state which of the three uses of cryptography would be most relevant or state “Not Helpful” if cryptography would not be helpful at all. Explain your answer.
- a) Trojan Horse attack
 - b) Eavesdropper attack
 - c) Timing attack
 - d) Denial of service attack

3. (12 points) The WiFi network on the Stanford campus that we use for wireless networking operates in a relatively crowded frequency range where other devices operate, including some cordless phones and microwave ovens. Interference from other sources can cause packets sent over a WiFi link to be lost.
- a) Describe the mechanism used by TCP/IP to detect and recover from when such a packet loss occurs on a WiFi connection.
 - b) When using TCP/IP to transfer a large file over a WiFi connection you notice that after recovering from packet loss the throughput of the file transfer is lower than before the packet loss. Explain the justification behind TCP/IP doing this.

4. (12 points) In building computer security systems we separate the implementation into *mechanisms* and *policies*. For each of the security-related terms below, state if it's a mechanism or a policy. If it is a mechanism describe a policy that can be used for it. If it is a policy describe what mechanism might be used.
- a) Access control lists
 - b) Capabilities
 - c) Biometrics

5. (12 points) Assume you have an Internet in which almost all of the 32-bit IP addresses have been allocated to machines. Explain how the forwarding tables in Internet routers are far smaller than the billions of entries that 32 bits would imply.

6. (12 points) Networking link layers have a maximum transfer unit (MTU) associated with them.
 - a) Describe the disadvantage of using TCP on link layer with a small MTU of 256 bytes.
 - b) Why would a link layer designer want to avoid having to implement a large (e.g. 32KB) MTU?

7. (12 points) We have all experienced variable delays when using a network even when the packets take exactly the same route through the network. Rank from lowest to highest the following sources of delay in a packet switched network in terms of the variance. **Note:** the ranking is on the variance, not the magnitude of the delay. Assume all packets take the same route. Explain your answer.
- Transmission delay
 - Propagation delay
 - Queuing delay

8. (12 points) Describe the problem with using shortest seek time first (SSTF) scheduling on a modern magnetic disk using a modern operating system.

9. (12 points) A 1GB process with no locality of memory references (e.g. random memory references) would perform poorly on a machine with virtual memory compared to a machine without virtual memory hardware (i.e. process ran in physical memory). This would be true even if all the process' pages were resident in physical memory. Explain why.

10. (12 points) Describe why a program that has much global data initialized to zero would start up faster than a program that has its global data initialized to 1.

11. (12 points) Can a caching optimization ever hurt performance? Explain your answer.

12. (12 points) Enforced modularity of processes running on a CPU depends on complete mediation of the accesses done by the process. Modularity violation such as a user-mode process trying to access a privileged resource (e.g. the memory management unit) is considered an error and will result in a modern operating system terminating the process. Explain why, when running a virtual machine monitor, this kind of modularity violating detection mechanism is used as part of normal operation.

13. (12 points) Early Unix operating systems supported only one thread per address space. A typical layout of the address space of a process was to have the stack start at the top of the address space and grow down, while everything else was in the bottom of the address space and grew upwards. The maximum size of a stack was only limited by the size of the address space. When multiple threads per address space were added (as in pthreads), stacks were given a fixed maximum size that wasn't nearly as large.
- a) Explain why the maximum size of stacks is so much smaller when multiple threads are used.
 - b) Many thread systems use the virtual memory system to detect if a thread runs off the end of its stack. Describe how the virtual memory could be used to detect stack overflow condition.

14. (12 points) Below is a list of the security principles covered in CS 110. Select the two most directly related to the concept of microkernel operating systems and the two least relevant to microkernel operating system. Explain your answer. Be sure to identify which two you choose for “most directly related” and which two you choose for “least directly related.”

Minimize secrets

Economy of mechanism

Minimize common mechanism

Complete mediation

Fail-safe defaults

Least privilege principle

15. (12 points) Security researcher H. Ackerman has developed a new web browser called Securefox, based on the open-source browser Firefox. Ackerman claims that Securefox is safer than Firefox because it runs each tab in a separate thread. He claims that if a tab visiting <http://evil.com> is compromised, a separate tab visiting, say, <http://bank.com>, won't be. To protect his intellectual property, Ackerman has not published the changes he made to Firefox; instead, he distributes Securefox only in binary form.

Give two reasons not to believe Ackerman's claims.