Midterm #2
Fall 2001 15-712

Please write your name on the following line:

____

This midterm is open book and open notes.

You should write brief, precise, and legible answers. Rambling brain-dump answers may be punished twice — you run out of time writing them and we run out of patience reading them. :–)

There are eight questions but we will only grade six. (We will also look at the bonus question, but that question does not count towards the six you need to complete.) List the six questions we should grade:

____

Name: ________________________________

1. Hive tries to partition OSes into failure-independent "cells", which is similar to one major benefit (i.e., fault isolation) of processes. Give a concrete example of when Hive cannot fully isolate problems that occur within one cell from affecting other cells.

There are multiple answers.

   (a) *When one cell "borrows" physical memory from a second, the failure of the second cell can corrupt the borrowed physical memory.*

   (b) *When two cells explicitly share memory, the failure of one can affect the other.*

Name: ______________________________

2. The "pump" form of thread usage appears in many systems, offering a convenient programming model (simple pipeline elements). It also offers a convenient mechanism for exploiting multiple machines. Explain briefly.

"Pump" elements of a pipeline can be placed on distinct machines, communiting via a remote version of their original interface (e.g., sockets or procedure calls). This is reminiscent, for example, of the Abacus programming model.

Name: ________________________________

3. Consider these two approaches to delegating your access privileges to a server. (1) give it your account name and password, so that it can authenticate to a third party as you, (2) give it a capability (e.g., your Kerberos ticket) to act as you. Explain briefly why the second approach is superior. Also, indicate a situation in which it may not work.

Both approaches allow the server to act as you, but the second approach allows you to limit the time period and rights of what can be done as you. With your password, the server can become you whenever it wants. With a capability, the server can do only what you specified and only for as long as the capability is valid.

The second approach will not work for services that do not include support for capabilities delivered by you. For example, the services you wish to use may not have Kerberos support or may reside in a realm that does not know about you.

Name: ______________________________

4. Many consider anonymity to be a critical component of censorship-resistent publication systems. Identify two roles for anonymity in such systems and what value each each provides.

Three possibilities:

(a) Anonymity of content creator. One way to censor publications is to threaten writers so as to dissuade them from sharing unpopular thoughts. This is particularly effective when the publication system includes a delete function. Allowing the originator to remain anonymous makes this "impossible".

(b) Anonymity of content distributor. Another way to censor publications is to forcibly remove all copies from servers that distribute them. Keeping the server identities anonymous makes this "impossible".

(c) Anonymity of content reader. Another way to censor publications is to threaten readers in some way (embarassment, physical harm, etc.). Allowing anonymous retrieval makes this "impossible".

Name: ____________________________________

5. A "Lamport clock" can be used to sort a set of distributed system events into a partial order. Describe a simple way to create a total order from a single Lamport clock and per-machine identifiers.

Assume each event is labelled with a tuple consisting of the Lamport clock value and a machine ID. One correct total order can be constructed by sorting first by clock value and then by machine ID (i.e., all events with equal clock value are sorted by machine ID). [Note: clearly, this total order may bear little resemblance to the actual order in time.]

Name: ______________________________

6. Consider a storage system of N servers, each containing a replica of the same read-only data. For each scenario below, how many servers (N=?) must there be for client reads to complete successfully in the face of one Byzantine failure? Justify each answer (briefly!).

   - if each server sends its response directly to the client.

     With N=3 and one Byzantine failure, the client will always see at least two correct responses. With simple voting, it can determine the correct value.

   - if the servers must agree on an answer before responding to the client.

     To come to agreement, the servers must solve the Byzantine generals problem, requiring N=4 servers.

Name: ____________________________________

7. To increase security at CMU, some have proposed using fingerprint readers at each building entrace. But, we know that fingerprint checks sometimes fail. To ameliorate this, they are thinking of also using 4-digit PINs. What problem, if any, exists with each of these designs:

   - access will be allowed if either the fingerprint matches or the PIN is known

     It is unclear that this provides any security beyond just using the PIN in the first place, since the PIN is sufficient. The fingerprint readers may be an unnecessary cost.

   - access will be allowed if both the fingerprint matches and the PIN is known

     In this case, the PIN may provide some additional verification of identity, but it does nothing to ameliorate the problem of falsely rejected people.

   - access will be allowed if the fingerprint is close and the PIN is known

     This seems like a good design, given the components available.

Name: ______________________________

8. Consider a transaction processing system in which each ongoing transaction consumes some amount of main memory. If the system begins to experience heavy paging, what could it do to mitigate the problem??

The system could abort some ongoing transactions, queue them up, and then restart them after earlier transactions complete. [Note: think of excessive paging as a non-deadly form of deadlock.]

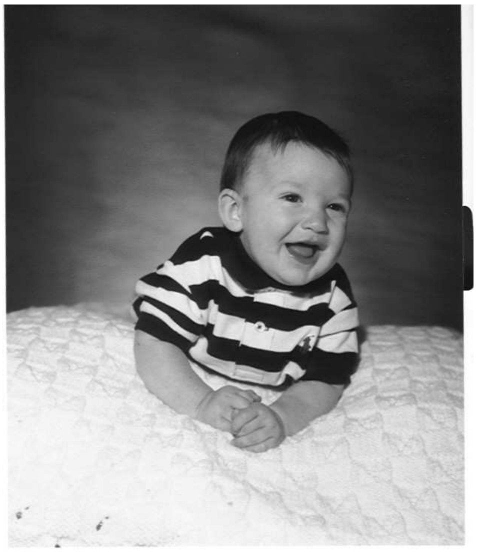
Name: ___________________________________

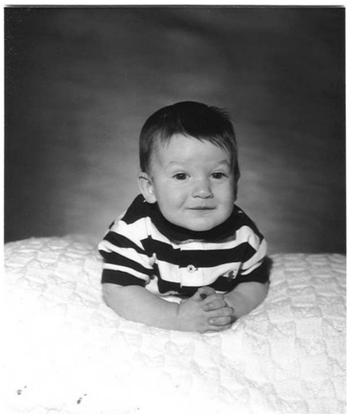
- (Bonus, 1 point) What super-hero did Timmy dress up as for Halloween??

  Superman.

Name: ______________________________

- (Bonus, 1 point) What is this cute baby's name?





Timmy.