Name: _____ UNI: _____

COMS W4187: Security Architecture and Engineering
October 2009

Rules

- Remember to write your name and UNI on the blue exam book.
- **Important: also write your name on this paper**
- You must turn in *both* the exam sheet and the blue book
- Books and notes are allowed during this examination; computers are not permitted.
- This is a time-limited test. All papers must be turned in 75 minutes after the beginning of the test.
- The total points add up to 80 .
- Good luck, and may the Force be with you.

1		15
2		15
3		20
4		10
5		10
6		10
Total		80

Questions

1. (15 points) I commute to campus using NJ Transit and the New York City subways. For the subway, I of course use a Metrocard with a mag stripe, which I swipe at the turnstile. An ordinary NJ Transit ticket costs me about $7; it's just a piece of paper I hand to the conductor. A monthly NJ Transit ticket, which I show to the conductor but retain, costs about $180, and has a fancy hologram on it.

a. (5 points) Metrocards don't have holograms. Why are they unnecessary?

b. (10 points) An ordinary NJ Transit ticket also does not have a hologram. Should it? Why or why not?

2. (15 points) As explained in class, databases typically have their own access control mechanisms. Someone asserts that OS access controls, if properly enhanced, suffice. The enhancement suggested is to permit ACLs for arbitrary byte ranges of the file. Bytes 10017-10032 might have one set of permissions for some user and group, 207178-208333 might have another, etc. This is a thoroughly bad idea. Explain why I say that.

3. (20 points) Some day in the future, there may be a centralized database of medical records, for use by all medical personnel everywhere. You are charged with designing the authentication system for access by emergency room staff. What sort of scheme would you use? Justify your answer.

4. (10 points) Assume there was an operating system where setUID programs inherited some of the invoker's environment. (Obviously, that's not a very difficult assumption.) Suppose that all possible

inherited attributes could be enumerated, and that some OS required that every setUID program have attached to it a description of permissible values for every attribute. Thus, the maximum file size might be constrained to be at least 10MB for some given program. Is this a good idea? Explain some advantages and disadvantages of this scheme.

5. (10 points) Buffer overflows are a major source of security problems. Suppose, instead of allocating local storage for each procedure on a normal stack, we instead used a link list of areas allocated on the heap. That is, when a procedure is entered, it does a malloc() or equivalent to allocate as much memory as it needs, and links it back to the calling procedure's area. On exit, it picks up that pointer and frees its area before returning. Does this solve the problem posed by buffer overflows? Explain.

6. (10 points) A privileged program takes input from three sources: command-line parameters, user input, and input from system files. Which of these input sources need sanitization? Explain.