Name: _____ UNI: _____

COMS W4187: Security Architecture and Engineering
October 2008

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 85 .
- Good luck, and may the Force be with you.

1		10
2		15
3		10
4		20
5		15
6		15
Total		85

Questions

1. (10 points) The web site I mentioned that describes how to build a Geiger counter-based random number generator contains the following text:

> If you don't know what you're doing, radioactive material of any kind is better left strictly alone. I am not encouraging you to fool around with hot stuff-especially when there's no need to, since you can get all the random bits you need from the Fourmilab generator.

Why do I disagree with this advice? (Note 1: you do not need any other material from that site to answer this question, so don't regret not printing it out. Note 2: if you think you need knowledge of physics to answer it, your answer is wrong.)

You don't know if the operator of that site is competent or honest. What if the numbers really aren't random? Maybe he's using a pseudo-random number generator. Maybe his hardware generator isn't working properly. Maybe he's making a copy of the random numbers he's handing out. Maybe someone has hacked his site and is making a copy.

2. (15 points) You are designing a computer security procedure for laptops for a top secret intelligence agency. Someone proposes the following scheme.

> The files on the laptop's disk drive are encrypted. The only copy of the key is on the employee's badge, encrypted with the employee's fingerprint. To log in, the employee must insert the badge into the computer and supply a fingerprint. Then and only then will the files be decrypted.

There are several things wrong with this idea. Name at least two.

If the badge is lost, so is the data. If the employee dies, the data is lost. It's hard toget a key from a fingerprint or other biometric. Badges tend to travel with people; there's no security redundancy against, say, an armed enemy — remember that we're talking about intelligence agencies.

3. (10 points) A user has a file containing the private key to a certificate. This file is stored encrypted with an 8-character password. What should the permissions on this file be? Why?

600 or 400 — it should not be readable by others. It may be useful to write-protect the file, since there are few reasons to overwrite it, but that's a matter of taste.

4. (20 points) Your task is to design an authentication and access control regimen for a large, distributed consulting company. Each site has its own, independently run computers. The consultants who do the work travel frequently from office to office; the support staff never knows who will show up the next day to work on some project.

a. (10 points) What sort of authentication system would you use for logins for these consultants? Explain.

To get full credit for this question, your answer had to say something showing that you realized it was a very distributed environment.

I prefer certificate-based authentication, since it doesn't rely on a centralized authentication database. All that's needed is a certificate signed by another site.

b. (10 points) What form of access control should the administrative support staff use for access to the consultants' email, expense reports, etc.? Explain.

There was an experience disconnect here. People at the level of these consultants are probably not doing their own expense reports; rather, the administrative support staff *would* do it. Many people assumed — incorrectly — that they should have no such access. I gave full credit for people who made that mistake, even though I think that the wording of the question implies that they do have access.

Role-based access control is best, since who has the role of a particular person's assistant will change from day to day.

5. (15 points) Web browser bugs, including buffer overflows, have been a persistent source of security problems. A security researcher makes the following proposal: make all web browsers on a system run setUID to, say, user `firefox`. That way, if there are any security problems, only files belonging to the `firefox` user are at risk. Is the researcher right or wrong? Justify your answer.

Wrong answer. First — if there's a penetration (perhaps a buffer overflow), the injected code can revert to the real UID, so there's no protection. Second, the web files of all other browser users on the system are at risk if a single user's browser is penetrated.

6. (15 points) Suppose a system administrator could insert filters — whatever programs he or she wished — in front of any or all vulnerable listeners in a message-passing system.

a. (5 points) What are the advantages of this from a security perspective?

These filters form a sort of firewall in front of the receiver. They can block unwanted or unauthorized messages.

b. (10 points) What are the very real practical difficulties?

You have to know the exact semantics of every receiver for this to be useful. Potentially, there are very many of them.