

CS 491/591 Spring '09 Test 2 Key

Name: _____

This is a take-home test, **due Friday March 27th at the beginning of class**, turned in to either myself directly or to the ITV proctor (students registered through UNM/Sandia can submit their answers via email, but the timestamp in my gmail account must say that it was received before the beginning of class on Friday). This is open Google, open book, open notes, open test 1 key, open everything *except each other*. You may not communicate with any of your classmates about this test in any way, or let anybody else handle your test (*e.g.*, to turn it in for you). **This test will not be curved.** The lowest score you can possibly receive will be your adjusted test 1 score, but since test 3 will be very hard you should take this opportunity to ace what should be an easy test 2.

You can email questions directly to me (jedcrandall@gmail.com), if I can answer them I'll answer and cc: secpriv-chat. Send your questions directly to me, though, not to secpriv-chat so I can filter anything that gives the answers away. Questions need not be about the test logistics, they can be about the material, but I'll have to decide how to answer each without giving the answer away, though.

You can type your answers, or print this and write them, or anything you like as long as it's clear which answers correspond to which questions.

#1. (6 points) What is the difference between an access control list and a capability?

An access control list is stored with the object and specifies what subjects can access that object, capabilities are stored with the subject and specify which objects that capability allows the subject to access.

#2. (10 points) What was the main contribution of Rivest, Shamir, and Adleman in publishing the RSA algorithm? In other words, Diffie and Hellman proposed public key cryptography in 1976, what properties/"things you can do" did RSA accomplish in 1977 that the Diffie-Hellman key exchange did not accomplish in 1976?

Diffie and Hellman proposed the idea of doing public key cryptography and proposed

an assymmetric algorithm for exchanging keys to be used in symmetric crypto, but they did not present an algorithm that could do assymmetric encryption and signatures. Using ring theory, Rivest, Shamir, and Adleman gave an algorithm that could do both encryption (rather than just exchanging keys for then doing symmetric crypto) and signatures (based on the property of non-repudiation).

For questions, 3, 4, 5, and 6, consider the following polices: Bell-LaPadula, Biba's low-water-mark policy, Clark-Wilson, Chinese Wall policy. There is a one-to-one correspondence between these four policies and the answers to the next four questions. Of those four policies, which would an organization be most likely to use if...

#3 (10 points) ...they maintain a source code repository, and want to make sure any source code that is modified by untrusted subjects is itself marked as untrusted:

Biba's low-water-mark integrity policy

#4 (10 points) ...they're a company that performs security audits of major corporations, and are worried about conflicts of interest when individual auditors they employ audit multiple corporations:

Chinese Wall policy

#5 (10 points) ...they're a major retailer that wants to ensure the integrity of their data regarding stock, payments, customer credit, *etc.*, and are particularly concerned about separation of duty and maintaining specific integrity properties such as “Customer account balance at the close of the business day is equal to the balance at the beginning of the day minus any payments and plus any interest”:

Clark-Wilson

#6 (10 points) ...they're a government contractor and deal with classified data that must be kept secret:

Bell-LaPadula

#7 (10 points) If I use the command “chmod o+w GradeBook.ods” to make my grade book on a Fedora Core 10 machine (with SELinux enabled) writable by anybody with an account on that machine, which have I changed: the permissions of a discretionary access control, or of a mandatory access control?

DAC. The access control is at the discretion of the user.

(Your answer can just be either MAC or DAC, it need not be a long answer.)

#8 (5 points) What is roll-based access control (RBAC)?

Roll-based access control associates access controls with job functions rather than with identities, so that people's access controls depend on the job function they're carrying out at the time. This lends itself naturally to environments where people have multiple rolls or there are personnel shifts, promotions, etc. to consider.

#9 (10 points) Give an example of the Principle of Complete Mediation (don't just say “Windows,” be specific.). You can choose either an example of good application of this principle or bad application, and it can be an example you found on Google or one we talked about in class (but not one from the book), but explain why your example is good or bad in terms of the Principle of Complete Mediation (in your own writing, you'll get a 0 on this question if I enter your answer into Google and find out you cut-and-pasted it off of some web page).

Many good possible answers, see the book for specific examples.

#10 (5 points) Why do we salt passwords in authentication schemes? In other words, how exactly does this force the attacker to invest more effort in a dictionary attack?

*Salting adds a random bit string to the end of the password before hashing it. If an attacker is carrying out a type-I dictionary attack (meaning they have the hashes for every user), then without salting they could compute one hash per dictionary word and compare that to all user hashes. With salting, the attacker has to compute one hash for every *pair* of dictionary word/salt possibilities, which makes their necessary work increase linearly with the number of possible salts (For the most part, one of the reasons UNIX systems only use 4096 salts is that unless a salt is used by at least one user the attacker need not consider it so really it scales with the number of users defined in the password file).*

#11 (6 points) List at least three major differences between the Access Control Matrix Model and the Take-Grant model:

- 1. Access control matrix model is more expressive than Take-Grant model*
- 2. In the take-grant model, security (in terms of leaked rights) can be decided in linear time whereas in the access control matrix model the general case is formally undecidable.*
- 3. Changes to the access controls are explicit in the take-grant model's representation, whereas the access control matrix model has a separate set of protection state transitions.*

#12 (5 points) When I `chroot()` to jail myself in a directory, e.g., `/home/capitals`, there are two important steps. The first and most obvious is `chroot("/home/capitals")`. What is the other step? (Hint: the answer is another function call like `function("argument")`, and this is a simple example of why understanding the UNIX security API is important).

`chdir("/")`;

#13 (2 points) Where on the Internet can I find a simulator or emulator for an Elbrus computer built by Boris Babayan, such as the Elbrus E2K?

If somebody had actually found one, I would have been very happy since I can't find one myself.

#14 (1 point) Which Black Sabbath song has a bell in it and the theme of being singled out by some dark, mysterious figure?

Black Sabbath (song name is the same as the band name)