Name: ________________________________

- You may not use any reference materials during this exam.
- Electronic devices, including calculators, cell phones, mp3 players, and laptops are all prohibited.
- You may not use your own scratch paper. The exam has plenty and you can ask for more if needed.
- You may not leave the classroom once the exam has been distributed.
- Communicating with other students in any way is prohibited.

Academic Honesty: I understand that if I cheat on this exam in any way, I will receive the maximum possible penalty, including an F in this course.

Name (print): ________________________________

Signature: ________________________________
1 Usable Access Control

You have designed a new blogging system that let’s users declare simple access control rules like, “All my posts about ‘parties’ are only visible to my ‘College Buddies’.” Users must define the ‘College Buddies’ group, but the blogging system will automatically figure out which posts are about ‘parties’ and apply the above rule.

• (10 points) Show how to reduce this access control system to an access control matrix. The columns of the access control matrix should be labeled by topic, and the rows should be labeled by groups. How is an access-control decision made using your access-control matrix?

• (10 points) You want to perform a user study to determine whether bloggers would use this new form of access control and whether they would be able to use it correctly. You are considering two different types of studies:
  
  – Running a public blogging service and letting anybody on the internet use it. You will collect statistics on how they use the access control features.
  
  – Having subjects come in and perform certain tasks using your system while role-playing.

List two advantages of each type of study.
2 Terra-based DRM

(20 points) One of the problems with Sony DRM was that they had to use the existing CD format. Imagine you could redesign the format of CDs. Design a secure CD DRM system using Terra. You should clearly state what is stored on a CD, and what happens when the user plays the CD in his computer.
3 Electronic Voting with RFID Tokens

Suppose that, in order to address some of the attacks described in the voting machine paper, the voting machine company replaces the insecure voter cards with RFID tokens. However, they are aware of the weaknesses of the DST-40 algorithm, so they use RFID tokens that implement the secure AES cipher, instead. Give protocols for

- (5 points) Initializing a token before giving it to a voter.

- (10 points) Starting the voting procedure and cancelling the token so voters cannot vote twice.

(5 points) Furthermore, give an attack against your system.
4 SFI+ASR?

Imagine a server that supports mini-server plugins, i.e. plugins that provide additional services through the main server’s interface. The authors of the main server wish to protect it from potentially buggy plugins, so they propose to combine two technologies: address-space randomization to make buffer overflow attacks against the mini-servers less likely to succeed, and software fault isolation to protect the main server from compromised plugins.

• (5 points) What will be one of the major challenges when designing this system?

• (10 points) How can the authors overcome this problem?
5 Queueing Theory of Client Puzzles

Suppose a server can handle $R$ requests/second, and has $C$ legitimate requests every second. Suppose also that an attacker is performing a TLS DoS attack using a botnet of $B$ computers. The server uses client puzzles and adjusts the difficulty of the puzzles depending on the load it sees.

- (10 points) How long must it take to solve a single puzzle in order for the server to be able to handle the load from the clients and botnet?

- (5 points) If it takes too long for legitimate clients to solve the puzzle, they will effectively be denied service. Is this more likely to happen with a large, busy server, or a small, infrequently-visited server?
6 Program Transformations against Side-Channel Attacks

As we saw in class, it is often possible to rewrite code to avoid timing attacks. In general, we can eliminate all timing attacks by rewriting almost any program using the following idea:

<table>
<thead>
<tr>
<th>Original</th>
<th>Transformed</th>
</tr>
</thead>
<tbody>
<tr>
<td>if (e)</td>
<td>mask = 0xffffffff * (e != 0);</td>
</tr>
<tr>
<td>a = b;</td>
<td>a = (b &amp; mask)</td>
</tr>
</tbody>
</table>

- (5 points) What can go wrong with pointers? (Hint: if (p != NULL) *p = 42;)

- (10 points) How can you fix it?
7 Economics of Proof-Carrying Code

(10 points) Does the economics of security predict that proof-carrying code will be successful or not? Why or why not?
8 Race Conditions

(10 points) Describe the access-open race condition and how to attack it.

(10 points) Describe two different ways you could change the UNIX system calls to enable programs to avoid the access/open race.