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.

Signature: ______________________________________

<table>
<thead>
<tr>
<th>Problem</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>/20</td>
</tr>
<tr>
<td>2</td>
<td>/10</td>
</tr>
<tr>
<td>3</td>
<td>/15</td>
</tr>
<tr>
<td>4</td>
<td>/15</td>
</tr>
<tr>
<td>5</td>
<td>/15</td>
</tr>
<tr>
<td>6</td>
<td>/15</td>
</tr>
<tr>
<td>7</td>
<td>/20</td>
</tr>
<tr>
<td>Total</td>
<td>/</td>
</tr>
</tbody>
</table>
1 Phishing Counter-measures

(5 points each) Which of the following phishing counter-measures will be successful. Explain why or why not in one sentence.

- Instead of having the SiteKey displayed above the user’s login prompt, the web page uses the SiteKey image as the background for the user’s password field.

- To prevent users from visiting the wrong website when they mis-type the URL, the browser requires users to enter URLs twice.

- To prevent users from visiting the wrong website when they mis-type the URL, the browser submits the URL to Google. If the first search result returned is not from the same domain, then the browser displays a warning dialog to the user.

- Browsers maintain a list of known-safe websites and display the URL on a green background when visiting one of these sites.
2 Indirect Information Flow

(10 points) Imagine a programming language in which each variable is labeled as PUBLIC or SECRET. Constants can be labeled as either PUBLIC or SECRET. The compiler forbids assignments from SECRET to PUBLIC. Example:

PUBLIC x;
SECRET y;
x = 5; // OK
y = x; // OK
x = y; // ERROR

Give an example program where secret information is copied to a public variable, without causing a compiler error. (Hint: use an if statement. You only need to write about 4 lines of code.)
3 Side Channel Attacks

(5 points each) Give a two-sentence explanation of how each of the following components can be used to perform a side-channel attack. You explanation should describe an example application that is vulnerable to attacks through the side channel, and then explain how to attack the application.

- TLB (Translation Lookaside Buffer)

- Disk (i.e. the file-system)

- Frame buffer (i.e. graphics memory)
4 Applications of Proof-Carrying Code

(5 points each) For each of the following scenarios, give a one-sentence explanation why proof-carrying code would or would not be an appropriate solution.

- Apple wishes to ensure that iPhone’s can only run Apple-approved software.

- Netflix provides software for streaming rented movies online. The software should support arbitrary plugins as long as those plugins don’t violate Netflix’s security goals.

- A wireless networking card supports user-defined firmware, but that firmware should never cause the network card to transmit outside of a certain frequency range or with too much power.
5 Intrusion Detection Systems

Intrusion-detection systems require a model of the application’s correct behavior in order to detect intrusions. The model can be created in one of three ways: by analyzing the source code of the application, by analyzing execution traces of the application, or through manual specification by the programmer. Give two advantages of each approach.

• Static analysis

• Execution traces

• Manual specification
6 Address-Space Randomization

(15 points) Address space randomization can randomize several layout details: stack top, variable layout, interframe padding, code segment position, function locations, heap location, and allocation sizes. For each of the following memory corruption attacks, indicate which randomizations make the attack harder:

- Stack buffer overflow

-Heap overflow

-Return-to-libc attack

-Intra-structure overflow (i.e. corrupting one field of a structure by overflowing another)

-Local variable corruption
(20 points) Recall that Terra offered VMs a sealed-storage service, i.e. an encrypted disk that could only be read by the same VM that created it. Terra implemented this feature by encrypting the disk under a key, \( k_{\text{disk}} \), and storing \( k_{\text{disk}} \) encrypted under Terra’s key. This means that the encrypted disk is tied to the machine on which it is created.

Design a sealed storage system appropriate for use with removable media, i.e. the encrypted disk would be readable on any machine running the designated VM.