Fall, 2015 Name: _____

(Please *don't* write your id number!)

CIS 4615 — Secure Software Development and Assurance

Test on Secure Design and Coding

Special Directions for this Test

This test has 6 questions and pages numbered 1 through 5.
This test is open book and notes, but no electronics.
If you need more space, use the back of a page. Note when you do that on the front.
Before you begin, please take a moment to look over the entire test so that you can budget your time.
Clarity is important; if your answers are sloppy and hard to read, you may lose some points.

For Grading

Question:	1	2	3	4	5	6	Total
Points:	10	10	10	10	10	50	100
Score:							

1. (10 points) [SecurelyConstruct] Suppose you need to write a client program for a client-sever system, like Quicken Bill Pay, that does not use a browser to connect to the server. Which of the following is the best option for the design of how the client authenticates the server? (Choose one and write a brief justification for your choice.)

    A. Write your own protocol to use PKI to authenticate the server, following the design of SSL/TLS. You have the company's approval to hire some security experts to do testing to see if they can find flaws in the protocol or its implementation when it is finished.

    B. Write your own protocol design in UMLSec notation and use the UMLSec tools to validate the security of the protocol. You have the company's approval to hire some security experts to do testing to see if they can find flaws in the protocol or its implementation when it is finished.

    C. Use a SSL library to connect to the server, trusting that it will do all the work. Then you can brag to your co-workers about how much money you saved the company by not designing and implementing all of the PKI checks yourself.

    D. Use a SSL library to connect to the server, and carefully check the documentation and options used to ensure that all certificates are validated properly and that the communications on the channel are confidential and tamper resistant.

    E. Both B and D would work well.

2. (10 points) [SecurelyConstruct] At the online file backup service company where you work, you have a co-worker, Claude, a math PhD who has been studying ecliptic curve problems for use in crytography. Claude proposed a fix to the RC4 algorithm that will make it possible to quickly encrypt traffic within the company's LAN. Which of the following is the best response to Claude's proposal? (Choose one and write a brief justification for your choice.)

    A. Reject the proposal, as it does not use a known algorithm that has been tested by experts.

    B. Study the proposal carefully yourself, to decide if it is secure. There is no need to hire experts since the algorithm will only be protecting traffic on the LAN.

    C. Accept the proposal, provided adequate testing is done to ensure that the algorithm is reasonably difficult to break.

    D. Accept the proposal. This is adequate because network traffic within the company's LAN does not need to be confidential or have a great deal of integrity.

3. (10 points) [SecurelyConstruct] The company you work for is growing rapidly and needs to use a more capable database on its Linux server machines, so you talk to two database vendors.

   A database from Rochester has very good performance numbers, but when you ask the company, they say that their database runs as the privileged user "root." They also say that their database software has been thoroughly audited to ensure a high level of security.

   A database from Utica has performance numbers with slightly higher latency, and when you ask the company, they say that their database runs in a non-privileged user account. They also say that their database software has been thoroughly audited to ensure a high level of security.

   Which of the following is the best decision for your company's database needs? (Choose one and write a brief justification for your choice.)

   A. The Rochester company's database has better performance, and performance should always be the most important consideration from a technical perspective, so the Rochester database should be chosen.

   B. Both databases have be audited to achieve a high level of security, so it makes sense to go with the Rochester company, since it has higher performance.

   C. Although the Utica company's database has slightly lower performance, their overall design follows the principle of least privilege, and thus has a more secure design, making it preferable. So the Utica database should be chosen.

   D. Since the Utica company's database software does not execute as root, it seems like it will always run with a bit more latency than the Rochester company's software, due to the way that privilege checks are coded in Linux. Thus the best option is to buy the Utica company's software and also rewrite the Linux kernel to make the code run faster.

4. (10 points) [SecurelyConstruct] They company you work for writes all their software in Python, but does not use design or code reviews. Their chief security officer says that because they are not writing software in a dangerous language like C, it is unnecessary to have design and code reviews. Which of the following is the best response to this policy? (Choose one and write a brief justification for your choice.)

   A. You point out that there are several vulnerabilities that can result from poor design, such as the way passwords are handled, and thus that design reviews are needed. Furthermore, you point out that in Python one can still make coding mistakes that make a program vulnerable to attacks, thus code reviews should also be in place.

   B. You commend the chief security office on his wisdom in choosing Python, because you are well aware of the many pitfalls in C coding from your courses at UCF.

   C. You commend the chief security officer on getting the company to only code in Python, because in Python buffer overflow attacks are impossible and it is well known that they are the most important and most frequent kind of attacks.

   D. You volunteer to do code reviews yourself, since you know you can impress the chief security officer when you find some coding mistakes that affect security.

5. (10 points) [SecurelyConstruct] The following Java code compiles and works fine on non-malicious tests. Your task is to review the code and identify all security-related coding problems. You *don't* need to write corrections for this code. Just identify the statements in the code that have security-related problems, and give comments or other clear indications of what the problems are or what attacks the code is vulnerable to. In your review assume that the string argument (`id`) could be a user input.

```
import java.sql.*;
public class QueryHelpers {
  public static ResultSet doQuery(Connection con, String id) {
    ResultSet ret = null;
    try {
        ret = con.createStatement().executeQuery(
              " SELECT ccnum FROM cust WHERE id = " + id);
    } catch (Exception e) {
        System.err.println(e.toString());
    }
    return ret;
  }
  // ...
}
```

6. (50 points) [SecurelyConstruct] The following C code compiles and works fine on non-malicious tests. Your task is to review the code, identify the security-related coding problems and attacks that the code is vulnerable to, and correct those. The corrected code should have equivalent behavior on non-malicious tests. You can edit the code by: (a) crossing out vulnerable lines of code, (b) writing the corrected code next to crossed out code, and don't forget to (c) indicate the kind of attack being prevented by a comment.

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include "prompt.h"
#define NAMESIZE 30
#define SCORESFILE "c:/secure/scores.csv"

static char* readname() {  /* read name from stdin */
  char* buf = (char*) malloc(NAMESIZE);   /* holds input */
  strcpy(buf, "\n"); /* initialize buf */
  return gets(buf);
}

static int getscores(char* name, int exgr[]) {
  /* if name is found, return 1 with the scores in exgr
     otherwise return 0. */
  char recbuf[NAMESIZE+20];
  char* nameend = NULL;
  FILE* sf;
  sf = fopen(SCORESFILE, "rw");
  if (sf == NULL) {
    fprintf(stderr, "Cannot open scores file %s\n", SCORESFILE);
    perror("Reason");  /* prints the OS error string */
  }
  while (fgets(recbuf, NAMESIZE+20, sf) != NULL) {
    nameend = strchr(recbuf, ','); /* find first comma */
    if (strncmp(name, recbuf, nameend-recbuf) == 0) { /* same? */
      sscanf(nameend+1,"%d,%d,%d", &exgr[0],&exgr[1],&exgr[2]);
      return 1;
    }
  }
  return 0; /* name not found */
}

int main(int argc, char *argv[]) {
  char *name = NULL;
  int exgr[3];
  prompt(stdin, "name? ");
  name = readname();
  if (getscores(name, exgr) == 1) {
    printf("Scores for ");
    printf(name);
    printf(":\n");
    printf("exam1 = %d, exam2 = %d, exam3 = %d\n",
           exgr[0], exgr[1], exgr[2]);
  } else {
    fprintf(stderr, "Name \"");
    fprintf(stderr, name);
    fprintf(stderr, "\" not found\n");
    return 1;
  }
  return 0;
}
```