National Exams May 2014

04-Soft-B3, Security/Safety

3 hours duration

NOTES:

1. If doubt exists as to the interpretation of any question, the candidate is urged to submit with the answer paper, a clear statement of any assumptions made.

2. This is an CLOSED BOOK EXAM.
   No calculator is permitted.

3. FIVE (5) questions constitute a complete exam paper.
   The first five questions as they appear in the answer book will be marked.

4. Each question is of equal value.

5. Most questions require an answer in essay format. Clarity and organization of the answer are important.

1.
   a. Explain how a one time pad cipher works.
   b. Explain how a block cipher works. Given two examples of common block ciphers.
   c. What is an advantage of the one time pad over a block cipher? What is a disadvantage of the one time pad versus a block cipher?

2.
   a. Suppose two parties who have never had contact with each other and share no information want to communicate securely. How can they do this?
   b. Now suppose both parties have a public/private key pair, how can they communicate securely?
   c. Explain the role of the certificate authority. What kind of attack does the certificate authority prevent?

3.
   a. What properties differentiate a cryptographic hash from a non-cryptographic hash?
   b. Explain the difference between a cryptographic hash and a message authentication code (MAC).
   c. What security properties do digital signatures provide?

4.
   a. Give three fundamentally different ways a user can authenticate herself to a computer system across a network.
   b. What is two-factor authentication? Give an example.
   c. What is a single-sign-on system? What are some security advantages of single-sign-on systems?

5.
   a. What is a network firewall? What purpose does it serve?
   b. What is a demilitarized zone (DMZ) in network security terminology? How does one implement a DMZ?
   c. What is an intrusion detection system? What is a Honeypot? How are they similar?

6. Consider the program below and answer the questions:

Program:

```
1:   int foo(char *arg)
2:   {
3:     int i, len;
4:     char buf[16];
5:
6:     len = strlen(arg);
7:
8:     if (len > 24)
9:       len = 24;
10:    for (i = 0; i <= len; i++)
11:      buf[i] = arg[i];
12:    return 0;
13:  }
14:
15:  int main(int argc, char *argv[])
16:  {
17:    char string[12];
18:
19:    strncpy(string, argv[1], 12);
20:    foo(argv[2]);
21:    return 0;
22:  }
```

a. Is there a security vulnerability in this program? If so, explain the vulnerability
b. How would you make this program more secure?

7.

a. Explain the "principal of least privilege."
b. Explain "defense in depth."
c. Explain "separation of privilege."

Marking Scheme

1. (a) 6 marks, (b) 7 marks, (c) 7 marks
2. (a) 7 marks, (b) 6 marks, (c) 7 marks
3. (a) 6 marks, (b) 7 marks, (c) 7 marks
4. (a) 7 marks, (b) 6 marks, (c) 7 marks
5. (a) 6 marks, (b) 7 marks, (c) 7 marks
6. (a) 10 marks, (b) 10 marks
7. (a) 7 marks, (b) 7 marks, (c) 6 marks