

## National Exams December 2018

### 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 a CLOSED BOOK EXAM.  
No calculator is permitted.  
Candidates are allowed to bring **ONE** aid sheet 8.5" X 11" hand-written on both sides containing notes and formulae
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 - full marking scheme on page 4.
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 stream cipher works. How can a block cipher be used as a stream cipher?
  - c. What is an advantage of the one time pad versus a stream cipher? What is a disadvantage of the one time pad versus a stream cipher?
  
2.
  - a. Suppose both parties have a public/private key pair, how can they communicate securely?
  - b. Explain the role of the certificate authority. What kind of attack does the certificate authority prevent?
  - c. Under what circumstances would you use a public key algorithm like RSA over a key exchange algorithm like Diffie-Hellman?
  
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. What is two-factor authentication? Give an example.
  - b. What is a single-sign-on system? What are some security advantages of single-sign-on systems?
  - c. What are some reasons to store the hash of a user's password instead of the password itself in a system? What is the purpose of a password salt?
  
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 a network 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[24];
5:
6:      len = strlen(arg);
7:
8:      if (len-1 > 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. Suppose an attacker compromises a computer system and copies the password file to a remote system. Which security property has the attacker violated: confidentiality, integrity or availability?
- b. Give an example of a violation of one of the other 2 remaining properties.

**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) 10 marks, (b) 10 marks