Calculators may be used in this examination provided they are not capable of being used to store alphabetical information other than hexadecimal numbers

UNIVERSITY OF BIRMINGHAM

School of Computer Science

Computer Security and Networks

Previous Exam Questions

Time allowed: 2 hours

[Answer all questions]

Turn Over

Note

Answer ALL questions. Each question will be marked out of 20. The paper will be marked out of 60, which will be rescaled to a mark out of 100.

Question 1

(a) What is a Block cipher mode? **[5 marks]**

(b) Bob gives instructions to buy or sell shares to his broker over the internet. When Bob gives an instructions, he sends two messages. The first message consists of the RSA-encryption with the broker's public key of a 128-bit key which is shared between Bob and the broker. The second message consists of the RSA-encryption with the broker's public key of the instruction. If an attacker manages to obtain the encrypted messages, is it possible for the attacker to send an instruction to the broker which is different from all previous instructions? **[7 marks]**

(c) Assume Alice and the bank share a symmetric key. Alice encrypts "Pay Tom 1000 pounds" in AES-counter mode using this key, and signs the encrypted message with El-Gamal using her private key. The bank accepts this message if it can decrypt it, and the signature matches. If the attacker has obtained the encrypted message and the signature, is it possible for the attacker to change the message so that message is the encryption of "Pay Bob 9999 pounds" and moreover create a matching signature which the bank will accept? If this is possible, describe how the attacker can do this. If this is not possible, explain why. **[8 marks]**

Question 2

(a) What is a replay attack? **[5 marks]**

(b) Is it safe to replace nonces by timestamps in a security protocol? Justify your answer. **[5 marks]**

(c) Consider the following protocol:

$$\begin{array}{lcl} A & \rightarrow & B : N_A, B \\ B & \rightarrow & A : E_A(N_A), E_A(Sign_B(\text{Pay Elvis } \pounds 5), \text{Pay Elvis } \pounds 5) \end{array}$$

Assume different protocol runs produce different payment messages. Is this protocol secure? If yes, explain why. If not, give an attack in Alice-Bob notation. **[5 marks]**

(d) Consider the following protocol:

$$\begin{array}{lcl} A & \rightarrow & B : E_B(N_A, A) \\ B & \rightarrow & A : E_A(N_B, B) \\ A & \rightarrow & B : E_B(N_B) \end{array}$$

where N_A and N_B are nonces, and $\#(N_A, N_B)$ is a symmetric key based on the hash of N_A and N_B. By giving an attack in Alice-Bob notation, show that this protocol does not satisfy key agreement. **[5 marks]**

Question 3

You review a C program that performs a password check:

```
1  int check_authentication(char *password) {
2      int authenticated = 0; // 0: not authenticated, else authenticated
3      char password_buffer[16];
4
5      strcpy(password_buffer, password);
6      password_buffer[15] = '\0'; // prevent long strings!
7      if(strlen(password_buffer) > 15)
8          return 0;
9
10     if(strcmp(password_buffer, "mahgnimrib") == 0)
11         authenticated = 1;
12
13     return authenticated;
14 }
```

(a) Assume that the program is compiled for x86 in 32-bit mode.

(i) Sketch the state of the stack *before* line 5 is executed. Clearly indicate where top and bottom of the stack are located. Assume that all variables are aligned at 4-byte boundaries.

(ii) Explain which vulnerability is present in this code?

(iii) Indicate which part of the stack has been changed *after* the `strcpy` on line 5 has been executed when the input password is 20 characters long.

[9 marks]

(b) For each of the following exploits, explain how you would craft an input to the function to achieve it. If possible, give a concrete example.

(i) Circumvent the password check. Your input should make the function return 1 without knowing the correct password.

(ii) Achieve an arbitrary code execution?

[6 marks]

(c) The author of the code intended to prevent this type of vulnerability using the code in lines 6–8. Explain why these checks do not achieve the intended purpose and explain how you would need to change the code instead. **[5 marks]**

This page intentionally left blank.

Do not complete the attendance slip, fill in the front of the answer book or turn over the question paper until you are told to do so

Important Reminders

- Coats/outwear should be placed in the designated area.
- Unauthorised materials (e.g. notes or Tippex) must be placed in the designated area.
- Check that you do not have any unauthorised materials with you (e.g. in your pockets, pencil case).
- Mobile phones and smart watches **must** be switched off and placed in the designated area or under your desk. They must not be left on your person or in your pockets.
- You are not permitted to use a mobile phone as a clock. If you have difficulty seeing a clock, please alert an Invigilator.
- You are not permitted to have writing on your hand, arm or other body part.
- Check that you do not have writing on your hand, arm or other body part – if you do, you must inform an Invigilator immediately
- Alert an Invigilator immediately if you find any unauthorised item upon you during the examination.

Any students found with non-permitted items upon their person during the examination, or who fail to comply with Examination rules may be subject to Student Conduct procedures.