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

Secure Software and Hardware Systems

Main Summer Examinations 2023

Time allowed: 2 hours

[Answer all questions]

Note

Answer ALL questions. Each question will be marked out of 30. The paper will be marked out of 60, which will be rescaled to a mark out of 100.

Question 1

Consider the case of a web server, accessible from the Internet.

(a) Why is it important that the software uses buffers located on the stack correctly, paying proper attention to their size? **[8 marks]**

(b) Explain how modern operating systems and hardware platforms reduce the impact of problems with buffers located on the stack, without requiring any recompilation? **[8 marks]**

(c) You have recently been appointed to the post of web security specialist, and are concerned that the webservers that your company runs may have exploitable weaknesses. Write a one-page memo to your manager explaining the measures you think should be taken to reduce the harm that an attacker can do if they manage to find a stack overflow or similar vulnerability. **[14 marks]**

Question 2

You are the designer of a hardware device that uses encryption as part of an authentication protocol. You have the choice between two microcontrollers: MCU-A has a dedicated hardware engine for AES, while MCU-B lacks this.

(a) Briefly describe (i) two advantages and (ii) two disadvantages of using a hardware implementation of AES. **[6 marks]**

(b) MCU-A runs at 4 MHz and the AES hardware engine uses 200 clock cycles to encrypt a 128-bit block. MCU-B runs at 100 MHz and a software implementation of AES consumes 2000 clock cycles to encrypt a 128-bit block. If execution time is the main concern, which microcontroller is the better choice? Explain your answer. **[9 marks]**

(c) In the software implementation on MCU-B, the `xtime()` function is implemented as follows:

```
uint8_t xtime(uint8_t B) {
   uint16_t tmp = ((uint16_t)B) << 1;
   if(tmp & 0x100 == 0x100)
      tmp ^= 0x1B;
   return tmp & 0xFF;
}
```

Assume a remote attacker who can only interact with the device but does not have physical access. Which type of side-channel attack is this implementation then vulnerable to? Briefly explain your answer. **[6 marks]**

(d) Rewrite the code from (c) so that the side-channel issue is fixed. To do this, assume that integer multiplication `a * b` has constant runtime independent of the operands `a` and `b`. **[9 marks]**

End of Paper

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.