Milwaukee School of Engineering

Electrical Engineering and Computer Science Department

SE-4920 – Computer Security
Midterm Exam

Print Name: _____

- This is a take-home exam.
- The exam will be emailed to the class before 8:00 A.M. on Thursday 10 April 2008.
- **Email your completed**, typed responses to the exam in Word, PDF, or other nicely styled format to the instructor by **5:00 P.M. on Friday**. You must be finished with the exam by this time. Any **handwritten items** (*e.g.*, figures for the final problem) may be submitted to the instructor's mailbox by **4:00 P.M. on Friday**.
- You may not consult with anyone except the instructor about the content of this exam.
- The instructor will be available during his office hours to answer questions. He will also be available at other times, and will answer any emailed questions about the exam as quickly as possible.
- You **are allowed to use** both textbooks, the PDF notes the instructor provided on the online course outline, and any class notes that you had before this midterm was distributed. You **are not allowed to use** any other materials.
- You are allowed to work on this exam for a **maximum of 2 hours**. You must complete the time log below. Any time spent actively working on the exam (writing/typing ideas, reading it) must be included. (Thinking about the exam does not need to be logged as long as you are not referring to any references, the exam itself, or your written/typed responses.)
- You **must sign** a hardcopy of this page in ink below, signifying that you have followed these rules.

Sign Here: _____

I have neither given nor received aid on this exam, and have followed all the above rules.

Time Log

(Enter times as "hh:mm A.M./P.M." Use local time (CDT-0500). Enter durations as "hh:mm".)

Begin	*End*	*Interruption*	*Total*	*Notes*
Total				

Problems

1. (10 points) Roughly estimate the distance at which you can read normal email in your normal viewing size on your laptop computer. This defines a zone of control (optical, not electronic) for your monitor. Provide a brief description of as many factors or assumptions (maximum of 10) that you can think of that would modify the zone of control.
2. (5 points) Why do faster computers generate a greater relative benefits for the users of cryptography than the attackers of it?
3. (5 points) For a two-argument function, reversible means that if the output and one input are known, the other input can be calculated. Which of the following operations are reversible?
    a. left rotate
    b. left shift
    c. AND of 2 bitstrings
    d. XOR of 2 bitstrings
4. (5 points) Discuss the differing reversibility requirements of hash and encryption algorithms.
5. (15 points) Review the Therac-25 discussion on pages 142-144 of Rice. Identify 2-4 of the information security principles that apply to this case and clearly explain why they apply or how they were violated.
6. (20 points) Consider a large project with which you are or were recently involved (*e.g.*, senior design project, SDL project).
    a. Provide a brief statement of the system's purpose.
    b. List several parties who have some sort of access to the system.
    c. Briefly summarize the value of each of the following properties of this system: confidentiality, integrity, availability.
    d. Imagine now that you are given the above information and are given the job to attack the system in order to help the developers make it more secure before releasing it to the customer. Describe 2 approaches that you would take.

Continued on next page...

7. (40 points) Consider a encryption scheme that has a block size of 1 B (8 b) and a key size of 1 B (8 b). The first 3 (MSB) bits of the key indicate a rotation offset and the remaining 5 bits are an XOR mask. The encryption procedure is: 1) XOR the 5 MSBs of the message with the mask, 2) rotate the resulting value ***right*** by the offset and 3) XOR the 5 MSBs of the result with the inverse of the mask.

   For example:

```
   E(m, k) = E(0x5A, 0x65) = E(0b0101 1010, 0x0110 0101)
1) 0b0101 1010 XOR 0b0010 1000 = 0b0111 0010
2) 0b0111 0010 >>> 0b011       = 0b0100 1110
3) 0b0100 1110 XOR 0b1101 0000 = 0b1001 1110 = 0x9E
```

   a. (5 points) State the decryption algorithm
   b. (5 points) Apply the decryption to the algorithm to example encryption and note whether the result is correct.
   c. (5 points) Some encryption algorithms are criticized because they have “weak keys” -- keys that do little to hide the data, perhaps applying only trivial manipulations of the data. What is the weakest key for the given encryption algorithm? Explain your answer.
   d. (15 points) Using the key 0x40, encrypt the message “ 10” (2 leading spaces) using the CBC mode of operation with the IV 0x3B. You may refer to the ASCII chart at <http://www.physik.fu-berlin.de/~goerz/misc/ascii.gif> if needed.
   e. (5 points) Assume that an attacker knows what the plaintext is, but not the key. Also assume that a brute force attack is infeasible. Given that the attacker is able to modify messages on their way to the destination, how would the attacker modify the message in order to turn the ‘1’ in the message into a ‘9’? (It is not necessary to decrypt the message to verify a correct result)
   f. (5 points) In what other way would the message be (unintentionally) modified as a result of this attack?