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 1:00 P.M. on Tuesday 17 April 2007.
- **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 Thursday**. 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 **6:00 P.M. on Thursday**.
- You may not consult with anyone except the instructor about the content of this exam.
- The instructor will be available during his posted 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 (2 pages)

1. (20 points) Most, if not all, of the 12 information security principles apply to the design of a variety of security systems, including the combination lock discussed in class. Pick any 5 of the 12 IS principles and explain how (and perhaps whether) each is addressed by a system using a combination lock.

2. (10 points) A vendor of RFID equipment states that the $20 reader installed at point of sale terminals (*i.e.,* registers) can only reliably detect their RFID tags (used to identify both customers and merchandise) at a range of 1 m and therefore the system is reasonably safe from eavesdropping. This argument has numerous flaws. Discuss at least 2 of them.

3. (5 points) Describe and briefly explain a place in a software development lifecycle where it may be advantageous to "build in" security (as opposed to "bolting it on" later).

4. (10 points) Why do faster computers generate a greater relative benefits for the users of cryptography than the attackers of it?

5. (15 points) We discussed 3 classes of cryptographic functions (secret key, public key, and hash function). Which of these functions must be reversible (*i.e.,* invertible) and which must not be reversible? Explain your answers.

Continued on next page...

6. (40 points) Construct an example of 4-bit cipher feedback (CFB) mode using an 8-bit encryption function. The encryption function is defined as E(x) = x + k, where x is a 8-bit number, '+' represents normal addition with carries out ignored, and k is the key. Then, we have the decrypting function $D(x) = E^{-1}(x) = x - k$. Let k = 1011 0110. The message to send consists of 4-bit values and is m_1=0101, m_2=1101, 0110, 0111, 1111, 0010, 1000, m_8=0100. Use an IV of 0000 0011.
    A. (16 points) Compute the ciphertext, c_1 through c_8.
    B. (8 points) Show how to decrypt the first 3 messages, verifying that you get the correct results, m_1 through m_3.
    C. (16 points) Assume the received ciphertext is missing c_1 and c_2, perhaps because a processor was too busy and its UART receive buffer overflowed. So, the receiver sees c_3 through c_8, thinking they are c_1 through c_6 and that there was only a 6-nibble message. Run the decryption algorithm on this 6-nibble message. How many of the messages were received correctly? Comment on the pros and cons of using CFB when incoming ciphertext units may be randomly dropped.