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 12:01 A.M. on Monday 3 April 2006. You may also pick up a hard copy of exam at the instructor's office (CC27) between 3:00 P.M. and 3:30 P.M. on Monday.
- **Email your completed**, typed responses to the exam in Word, PDF, or other nicely styled format to the instructor by **11:00 P.M. on Tuesday**. 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 **12:00 P.M. (noon) on Wednesday**.
- You may not consult with anyone except the instructor about the content of this exam.
- The instructor will be available in his office from 1:00-2:00 P.M. on Tuesday 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** the textbook, 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 (9 problems on 2 pages)

1. (10 points) Consider mandatory and discretionary access controls in light of the 8 security mechanism design principles. For both mandatory and discretionary access controls, select the principle that you feel is most compromised by that type of control. Justify both responses.

2. (10 points) Given our discussion of HIPAA, would you say that "need to know" clearances imply mandatory access controls? Justify your response. Your justification should include a brief discussion of the different motivations of the mandatory vs. discretionary models. (Note: Either a 'yes' or a 'no' might be accepted with supporting discussion.)

3. (5 points) "Failure to validate input" is a common cause of security defects. Which basic principle is not being sufficiently addressed when such a failure occurs?

4. (10 points) Why do you think vulnerability analysis **by defect type** is an important area of TSP-Secure research?

5. (10 points) Why do faster computers generate a greater relative benefits for the users of cryptography than the attackers of it?

6. (10 points) Give two reasons that you might want to use a secret key algorithm like Triple-DES even if you have access to a state-of-the-art public key cryptosystem.

7. (5 points) What is the key difference between a random and a pseudorandom number generator?

8. (5 points) Why is it difficult to build a good random number generator with regular computer hardware?

Continued on next page...

9. (35 points, parts A-F) Construct an example of CBC Threat 1 ("Modifying Ciphertext Blocks", text, page 99). Let E (the encrypting function) be the Caesar cipher. Assume, for the purposes of your example, that E is difficult to invert (true in general, but false for the Caesar cipher). Use a 6-bit code where 0 represents a space, 1-26 represent the characters 'a' through 'z', 27-31 represent "$().,", 32-41 represent the characters '0'-'9' (so that 0b10xxxx represent the characters, where xxxx represent the corresponding digits, analogous to ASCII) and 42-63 represent "!@#%^&*-+=<>?/;:[]{}\|".

   A. (3 points) What is the block size (in bits and characters)?

   B. (10 points) Encode the plaintext " $42" using the IV 13 and the key 7 (i.e., 'a' encrypts to 'h'). Note: There is a space before the '$' in this string. (I recommend that you draw a single diagram showing your calculations for parts B, C, and D, using a different color for C and D than for B.)

   C. (6 points) Now, assume this is an approved amount on Bob's expense report, he knows the plaintext and the message format, he can modify the ciphertext in transit to the check printer, and he wishes to change the 4 to a 6. How would Bob modify the ciphertext stream? (Note that he cannot merely encrypt " $62" since he cannot perform the E function.)

   D. (6 points) What is the corresponding plaintext due to this modification?

   E. (3 points) If this were input to a check-writing program that constructed the dollar amount by looking for numeric digits starting from the right and stopping when it found a non-numeric digit, how much would Bob be paid?

   F. (7 points) There are several ways to rectify the above problem (undetected modification), but a fairly simple one would be to use the CBC residue for message integrity. What is given up when taking this approach? Justify your response.