Milwaukee School of Engineering
Electrical Engineering and Computer Science Department
Dr. Durant

CS-4920 – Information 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 Tuesday 13 April 2010.
- **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.
- 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 2.5 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.)
- "A"-level answers will thoroughly, insightfully, and ***concisely*** answer the questions.
- 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) 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. (5 points) Roughly estimate the distance at which you one read normal email on a current generation smartphone. This defines a zone of control (optical, not electronic). 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.
3. (5 points) Why do faster computers generate a greater relative benefits for the users of cryptography than the attackers of it?
4. (10 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.
5. (10 points) Review the National ID card discussion on pages 97-102 of Schneier. Identify 3 of the information security principles that apply and clearly explain why or how they apply.
6. (15 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.
7. (10 points) A hash function takes an arbitrary length message and generates a 256-bit hash value. It begins with a hash output of 0, and XORs successive blocks of 256 message bits to update the hash output. All word and bit orders are big endian. If there are fewer than 256 bits in the final block of the message, it is right-aligned and 0-padded. Discuss why this hash is not cryptographically secure.

Continued on next page...

8. (35 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 LSBs of the message with the mask, 2) rotate the resulting value ***right*** by the offset and 3) XOR the 5 LSBs of the result with the transpose of the mask.

For example:

```
   E(m, k) = E(0xA5, 0xB3) = E(0b1010 0101, 0x1011 0011)
1) 0b1010 0101 XOR 0b0001 0011 = 0b1011 0110
2) 0b1011 0110 >>> 0b101       = 0b1011 0101
3) 0b1011 0101 XOR 0b0001 1001 = 0b1010 1100 = OxAC
```

a. (5 points) State the decryption algorithm
b. (5 points) How many I/O mappings are possible for this encryption algorithm? How many are possible, for any possible private key algorithm, given the block size?
c. (5 points) Apply the decryption to the algorithm to example encryption and note whether the result is correct.
d. (10 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.
e. (10 points) Discuss the design of this algorithm in terms of permutations, substitutions, rounds, and key length.