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 8 April 2014.
- **Email your completed**, typed responses to the exam in Word, PDF, or other nicely styled format to the instructor by **11:59 P.M. on Sunday**. 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 and articles 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.)
- "A"-level answers will thoroughly, insightfully, and ***concisely*** answer the questions.
- You **must sign** a hardcopy of this page in ink below and submit it by the end of the class meeting following the exam due date, 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

Day/Date	*Begin Time*	*End Time*	*Duration*	*Notes*
Total				

Problems

1. (10 points) Why do faster computers generate a greater relative benefits for the users of cryptography than the attackers of it?
2. (10 points) Explain why traditional use cases are insufficient for describing system security properties.
3. (10 points) What are 2 reasons that cybercrime cost estimates are widely believed to be inaccurate?
4. (30 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. Most, if not all, of the 12 information security principles apply to the design of a variety of systems. Pick any 5 of the 12 IS principles and explain how (and perhaps whether) each is addressed by your project.
    e. 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.

5. (40 points) Consider an encryption scheme that has a block size of 1 B (8 b) and a key size of 1 B (8 b). The (big endian) key bits are interpreted, in order, as follows
   a. The first (left) 2 bits are an unsigned number representing the amount of an initial left rotation of the message.
   b. The next 2 represent an XOR mask to apply to the 2 LSBs of the message.
   c. The next 2 bits represent another rotation as in (a).
   d. The final 2 bits represent a final XOR mask as in (b).

   For example:

```
   E(m, k) = E(0x5A, 0x6E) = E(0b0101 1010, 0x01 10 11 10)
1) 0b0101 1010 <<< 0b01    = 0b1011 0100
2) 0b1011 0100 XOR 0b10    = 0b1011 0110
3) 0b1011 0110 <<< 0b11    = 0b1011 0101
4) 0b1011 0101 XOR 0b10    = 0b1011 0111 = 0xB7
```

   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. There various sets of keys that result in the ciphertext equaling the plaintext in this example. Describe one such set and list ***all*** of its members.
   d. (15 points) Using the key 0x95, encrypt the message “ 10” = 0x203130 (1 leading space) using the CBC mode of operation with the IV 0xB3.
   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’? You may refer to the ASCII chart at <http://commons.wikimedia.org/wiki/File:ASCII-Table-wide.svg> if needed. (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?