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 Wednesday 15 April 2015.
- **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. (15 points) A hashing algorithm generates a 160-bit hash value by starting with a 160-bit 0 in a register and then XORing in 160 bits at a time from the object (e.g., file or message) to be hashed until the end of the object is reached. For most types of data, this generates an expensive but high quality hash for efficient hash table storage. In contrast, it generates a reasonably priced but unacceptably low quality / unusable hash for cryptographic purposes. Use this example to describe the key differences between regular and cryptographic hash functions.
3. (15 points) In your own words, describe as you would to a skeptical colleague why "security through obscurity" is not a sound design mechanism. Be convincing. Ideally, address some reasonable, limited exceptions, perhaps drawing on Schneier's "Beyond Fear."
4. (10 points) Describe a situation in which the security interests of citizens as individuals might be in conflict with the security interests of society as a whole.
5. (50 points) Consider a significant engineering project with which you are or were recently involved (*e.g.*, senior design project, SDL project).
    a. (10 points) Background
        1. Provide a brief statement of the system's purpose.
        2. List several parties who have some sort of access to the system.
        3. Describe a security measure for the system that you have implemented or that you considered during the system design. You may also invent a security for the purposes of this test. Be sure to state which you are doing.
    b. (30 points) Apply Schneier's Steps
        1. What assets are you trying to protect?
        2. What are the risks to these assets?
        3. How well does the security solution mitigate those risks?
        4. What other risk does the security solution cause?
        5. What costs and trade-offs does the security solution impose?
    c. (10 points) 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.