Information Assurance
Midterm notes
Spring 2007

This note is intended to help you prepare for the midterm on Thursday, March 1st. It should give you an idea of what to expect and some hints on how to prepare.

My exam philosophy

Sometimes, while I was going through my education, I encountered professors who would seem to think that an exam was a good time to get their students to learn something new. They would give questions on the exam that was new material, with the expectation that students would somehow figure out the answer and learn something new in the process. I don't believe in that approach.

I believe that exams should provide students with an opportunity to demonstrate their facility with the material that has been presented in class up to that point. I also believe there are different levels of learning, and write tests to try and determine which level individual students have achieved (for those interested, the model I like to look at is well presented at:

`http://www.coun.uvic.ca/learn/program/hndouts/bloom.html`

I would test up to the analysis or synthesis level in this class on topics that we spent significant time on.) I also try and use exams to discover topics I may have covered poorly in class.

My exam actualities

This class is a bit different than other classes I teach. Because we are going over so much material, we don't have time to discuss everything thoroughly in class. Therefore, as I mentioned in the beginning of the semester, I expect you to be keeping up with the readings assigned in the syllabus, and I will feel free to ask questions based on that information. The topics will therefore center on what we have covered in class, but I will ask questions that cover more detail than we went into in lecture.

In terms of difficulty, I try and write exams so that about 50% of the material can be completed relatively easily in about 1/3 of the exam time. The average grade on tests I write tends to be between 75%-85%, which I consider too high - I'd rather have about a 70% average. I also have a tendency to make my exams too long for the time alloted.

One type of question that you may not have seen before is a true/false question with corrections. The idea is that if the statement is true, you need only to mark it as true. If it is false, you mark it as false, but then correct it to be true. You may not simply negate the statement to make it true.

The instructions for questions like this would read:

```
The statements below are either true or false.
  If true, mark them with a T.
  If the false, mark the statement with an F and then show a correction that
  would make it true.
  Do this by either crossing out a single term (word or related words), by
  drawing an insertion mark and writing a single term to be inserted, or
  by circling a term and showing a single term to replace it.
```

You cannot simply negate the statement to make it true.

For example, the statement "Today is a day in the year 1972" would be made correct by circling 1972 and writing "2007" next to or above the statement. You would not get credit for inserting the word "not" to make the statement "Today is not a day in the year 1972".

How to study and take the test

First, do the readings and make sure that you have an understanding of the material. The review your notes.

Once you have done this you are ready to study with others. I highly recommend that you do find some others in the class to study with Take turns coming up with questions on the material, perhaps similar to homework questions. This is a good opportunity for the person who is making up the question to get others to help them through a topic that they don't understand.

When you take the test, read through it before you start. Look at the questions to figure out which ones seem easy, and which are worth the most points. Skip around between questions so that you do the easiest, most valuable questions first. Don't get caught on a hard question if it keeps you from doing an easy one.

Topics and expectations

- Know and understand the model of information assurance, threats under that model, and basics of how we can work to mitigate or prevent threats.
- Know the three-step cycle used to work towards achieving security.
- Be able to outline how a risk assessment would be conducted. Also be able to describe the benefits of conducting a risk assessment.
- Be able to show how an attack tree can be used to describe particular threats to information.
- Know the different common types of attackers and what their capabilites might be.
- Be able to define what ”security through obscurity” is, and provide arguments for or against it. The example we discussed in class was about cryptographic algorithms.
- Understand what a security policy is, be able to describe the important elements of writing one, and be able to make arguments about why those elements are important.
- Understand the elements of a physical security plan, and the threats that this plan will protect against.
- Be able to explain what procedures should be followed regarding system back-ups.
- Understand and be able to describe personnel security measures for employees and new hires. This includes policies to guard against personnel conspiracy.

- Be able to describe the differences between public and private key cryptosystems. Be able to give examples of each type of cryptosystem, and differentiate between them as to their security.
- Understand how hashing and message digests are done, and know what uses they have.
- Understand how digital signatures are computed and used.
- Be able to explain how passwords are used, how they can be attacked, and defenses against those attacks.
- Be able to suggest mechanisms for creating strong and memorable passwords.
- Know and understand alternatives to reusable passwords.

  they can be attacked.
- Know and be able to describe the four general mechanisms that can be used for authentication.
- Understand and be able to describe and differentiate between false positive and false negatives in a detection system.

  occur.
- Be able to answer questions regarding common themes in the bugtraq and RISKS mailing lists, particularly those linked to from the class web page.
- Be able to describe what different Unix commands covered in Project 1 do, and be able to write commands to meet a particular stated purpose.