CIS 170 Security Fundamentals
Spring 2009 Final Exam
Matthew Franz

This exam is worth 40% of your course grade and must be electronically sent in RTF, Microsoft Word or PDF (you can use Google Docs for this) format to mdfranz@gmail.com no later than 9 PM on Monday, May 18th. I will be submitting grades on Tuesday afternoon and grades are due 10 AM Wednesday, May 20th so don't be late!

Part I: Essay (20 points each)

Pick ***two*** *of the following essay questions to answer in a well-reasoned and clearly written essay. Essays must be at least 250 words in length and will be graded based on the evidence you provide from readings, classroom activities, lectures, and any other research.*

1. In your opinion, what is the single biggest problem affecting the security of computer systems and networks? Can this problem be solved? If so, why? If not, why not? Justify your answer with detailed examples of threats, vulnerabilities, and security countermeasures we have discussed in class.

2. Define what it means for a networked computer system to be secure. Your answer should include a discussion of the security principles (confidentiality, integrity, availability, and authenticity) and discuss vulnerabilities and security countermeasures that are available within operating systems, the network infrastructure, and network services.

3. What type of applications are harder to secure? Clients or servers? You must pick one and make a case for its [in]security based on researching the evidence and applying the security principles we have learned in the class. Use examples of design, implementation, and misconfiguration, vulnerabilities that have impacted real applications.

4. Find a security job on a site such as Dice, Monster, or HotJobs. Convince me that you are qualified for this job based on what you have learned and what you want to learn. Be sure to include the job description and skills listed in your answer.

Part II: Short Answer (5 points each)

Answer **seven** of the following questions in 3-4 sentences. Your answers should be based on lectures and lab activities.

1. How do firewalls enforce a network security policy?
2. How do security administrators can identify vulnerabilities and attacks against systems?
3. What is the difference between symmetric and asymmetric cryptography?
4. What is the difference between a hash algorithm and an encryption algorithm?
5. What is the purpose of a web framework that runs on a web server?
6. How has the way that the world wide web changed over the last 15 years?
7. Describe the components & functions of malware using a real type of malware you researched in class.
8. Describe how security is implemented in the HTTP protocol.
9. Describe the parts of an operating system

Part II: Practical (25 points)

Answer **one** of the following questions

1. Using one of the Web Application tools such as FireBug or Webscarab document the type of messages exchanged between your web browser and the web server when you login to a web site that requires authentication such as Gmail, Facebook, or Yahoo Mail. Identify which messages are encrypted. What functions of the browser are used and any information you can discover about the web server.

2. Describe how you use GPG4Win to ensure message confidentiality and authenticity. List and describe the steps you would use to encrypt and sign a message using one of the public keys of your classmates listed on the google groups site.