

Name:

Information Assurance: Homework 1 Answer Comments

1. What do you hope to get out of this class?

Most people are taking this class to get a general introduction into the area of computer security. Some people are looking to build a basis for a career in security or research in the area of security.

2. What are the top three topics you hope are covered in this class?

There were a large number of topics mentioned. I grouped the topics into chunks that made sense to me. Cryptography was the most mentioned topic. Network Security and malicious code/hacking were also very frequently mentioned. Database, OS, and program security also got significant mentions.

I think we will cover most of the topics mentioned. Some of the less mentioned topics will also influence how I direct some of the latest lectures. One of you suggested a lecture on "The greatest hacks of all time". Sounds like a cool talk, but I doubt I'm the person to give that one. We will be addressing malicious code techniques and numerous defensive mechanisms that are addressing specific types of attacks.

3. What programming languages and operating systems are you comfortable working with?

About what I expected. We won't be doing considerable programming in this course. But you will need to compile a few tools and run a few tests. Also to understand the malicious code, you will need to understand how process stacks are laid out, so being comfortable with memory layouts and C will be beneficial.

4. How familiar are you with IP networking? Choose the most appropriate.

- a) I can recite the seven layers of the OSI network model. 11%
- b) I am familiar with the differences between IP, TCP, and HTTP. 28%
- c) I have used sockets to create a networking application. 18%
- d) I have used a network. 43%

I was a bit surprised by the distribution here. I would have thought more people would be in the b or c case. As we get into network security, I'll try to back fill a bit on basic IP network layers. Please talk with Ravinder or me, if you get lost on the basic network structure and we will adjust lectures or work with you individually to make sure you have the right background.

5. Name three computer controls you use or encounter. What vulnerabilities are they protecting?

Name:

There are any number of answers here. Some examples from my head and student papers include:

- *Passwords – protecting against unauthorized access.*
- *VPN tunnels – protecting against unauthorized access and leaking data over the network.*
- *Antivirus programs – protecting against software flaws.*
- *Doors locks – protect against unauthorized access to hardware or equipment.*
- *Computer case – protecting fragile computer parts.*
- *Firewalls – Protect against unauthorized network traffic. Unauthorized packets may trigger vulnerabilities in the software of network services running behind the firewall.*

6. Consider a program to accept and tabulate votes in an election. Who might want to attack the program? What types of harm might they want to cause? What kinds of vulnerabilities might they exploit to cause harm?

Potential attackers

- *political group, candidate, or party*
- *Subversive group trying to cause panic and break down trust in the democratic party*

Potential harms

- *Add votes to favored candidate by changing votes or adding votes.*
- *Remove votes from candidate by causing a mistrust in the integrity of entire precincts*
- *Remove votes by preventing precincts from voting.*
- *Learn results before polls close to better address later phases of election*

Vulnerabilities:

- *Use poor physical access controls to gain unauthorized access to voting machine.*
- *Tap into weakness in electronic communication to gather information or change information as it is passed from precinct to centralized vote tallying location.*

7. Describe a computer security failure you read about recently in the news. What major security component(s) was violated in this attack? Confidentiality, availability, or integrity?

Looking for a sentence or two description, not just a URL.

Any number of attacks here:

- *Accidental inclusion of a spreadsheet of student personal information into an unrelated email sent to a large number of people. This is a failure of confidentiality.*

Name:

- *Users of monster.com were sent directed emails that appeared to come from monster. These emails included URL's that installed malware on the computer if the user clicked it. The malware in turn gathered sensitive information about the user and used the new machine to send additional tainted emails. - By gathering sensitive information about the users, this is also a failure in confidentiality.*
- *In the well publicized attack on Estonia, the information infrastructure was placed under denial of service attacks. These were standard bot net attacks, but they were enough to make most of the Estonia information infrastructure unusable. - This was an attack on availability.*
- *iPhone hacking – A failure to adequately handle bad input causes the safari browser to crash. With the right “bad input”, a malicious user can take over the browser process and fetch other sensitive data the user may have on his iPhone. This is a failure of integrity in the web browser software. With the attack, new code is running in the browser process. It is also a failure of confidentiality. Data the iPhone user is storing on his device under the assumption that it is private, is not. (http://www.mercurynews.com/opinion/ci_6668195).*