Name:

Computer Security I: Homework 1 Comments

Due August 30, 2010 on compass.

This homework was graded very liberally. Don't be surprised when future homeworks and exams have harder questions and are graded as such. We had a mis-communication between the graders. So the last question was graded to 6 points instead of 12. Everyone got the extra 6 points for free.

1. What are your goals for this class?

Most folks stated the general "learn more about computer security". Some folks have the goal of getting a good job (or progressing in their current job), earning an A in the course, or being better able to manage their personal computer/network systems. At least one person is preparing for the CISSP exam.

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

The biggest vote getter was cryptography. Followed by hacking/malware, security programming/design, network security, system attack/defense, system authentication, and secure operating systems.

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

Most people listed C/C++/C# and Java for programming languages and Linux/Windows for OS. We won't be using Mac OS for any assignments, so those of you with MacOS concerns can rest easy.

A handful of people have no programming experience or no C/C++ programming experience. We are not doing much programming in this class. A few assignments may involve compiling programs on the EWS Linux machines. One assignment may involve minimal programming. Contact the Professor if you have issues with these assignments, and we can arrange for an alternate assignment or extra help.

4. How familiar are you with IP networking? Choose the most appropriate.
   a) I can recite the seven layers of the OSI network model.
   b) I am familiar with the differences between IP, TCP, and HTTP.
   c) I have used sockets to create a networking application.
   d) I have used a network.

There is still a fair bit of a spread over networking background. Almost ¾ of you have either already had a class in networking or have done some extensive networking on your own, but that leaves ¼ of you with minimal networking background. When we get

Name:

into the networking section of the course, I'll try to strive for a middle ground. Please ask questions and contact the teaching staff if we go too fast.

5. Ensure that you can access the various communication mechanisms used in class
   a) Access the cs461 newsgroup. Report on the "magic" word posted by Prof. Hinrichs.

Some people lost points due to not listing the magic word, "synergy".

   b) Access the c461 compass page

Figured you got this if you successfully submitted the assignment.

6. Classify each of the following as a violation of confidentiality, integrity, availability, or some combination:

Three points for each section.

   a) Alice uses Bob's smart phone to post to his facebook account.

   Violates:

   - *origin integrity – Alice is pretending to be Bob. Could post things as Bob and trick others.*
   - *Confidentiality – Alice could see information from some of Bob's friends that she would not normally be able to see.*
   - *Could maybe make an argument for Availability but I think that is pretty weak. At worst Bob should be able to go to a public terminal at the library and gain access to his facebook account. If she used the smart phone access to change his password, then you might have a decent argument.*

   b) Charles reads his roommate's letter from home on the way back from picking up the mail.

   Violates:

   - *Confidentiality – Assuming the letter was in a sealed envelop not addressed to Charles, he is access information he is not authorized for.*

   c) Bob leaves himself logged onto facebook, and Alice changes his password.

   Violates:

   - *Availability – Bob can no longer access his facebook account.*
   - *Origin integrity – Alice is pretending to be Bob.*

   d) Diana installs a free game that corrupts her system.

Name:

Violates:

- *Availability – Diana can no longer use her system*
- *Data Integrity – The data on her system is no longer correct*

7. Consider two options Ernie has to check his balance and pay bills.

Three points for each vulnerability. Three points for each exploit.

a) He uses his bank's web interface to check his balance and pay bills. Identify a vulnerability in this scenario. How could an attacker exploit this vulnerability?

Vulnerability/exploit

- *Inadequate password authentication system/ Attacker guesses or brute forces the customer's password to gain full access to his bank account.*
- *Inadequate network encryption between browser and server / Attacker is able to break the encryption between the browser and server and gain information about Ernie's bank account.*
- *Unscrupulous insider/ bank employee sets up transfers from Ernie's account into an account controlled by the employee.*
- *Malware on client adds a layer onto the bank interface / Performs action on the attacker's behalf whenever the user interacts with bank server. The recent Zeus malware is an example of this case.*
- *Falling for phishing attempts that lure Ernie to a web site that looks like his legitimate banking site, but isn't. The vulnerability is the user interface issues that trick Ernie into visiting the wrong site. The exploit is to steal sensitive information from Ernie for later access to his real accounts.*
- *Trick Ernie into installing keylogging software. The vulnerability is the user naivity/OS issues that enable the installation of surprising software. The exploit looks at Ernie's key presses to steal passwords and other sensitive information for later access to Ernie's accounts.*

b) He calls on the phone to check his balance, and he sends paper checks to pay his bills. Identify a vulnerability in this scenario. How could an attacker exploit this vulnerability?

Vulnerability/exploit:

- *Unscrupulous insider/ bank employee sets up transfers from Ernie's account into an account controlled by the employee.*
- *Loss of checks in the mail/ either maliciously or accidentally checks never reach biller resulting in late fees or critical services being turned off.*
- *Interception of checks in the mail/ Attacker grabs checks and convinces a bank to cash the checks into an account controlled by attacker.*

Name:

- *Overhearing phone conversation/ Someone overhears Ernie's conversation checking on his bank account. He makes note of account numbers and pins and uses the information later to access Ernie's account*

8. Describe a computer security failure you read about recently. What classes of threats were involved in the attack? Disclosure, deception, disruption and/or usurpation?

I'm expecting the student to provide a paragraph or two discussing a current security event. Perhaps the recent admission from the DoD that several restricted networks were compromised as the result of malware introduced into the system by a USB thumbdrive. This particular case would involve threat classes:

- *Disclosure – the malware gained access to information that it was not authorized for.*
- *Deception – presumably the DoD employee through the thumbdrive was a completely passive storage device.*

If they give an event but don't discuss threat classes take away 6 points.

If they give an event and list threat classes but don't say why take away 3 points. This is where people tended to lose points.