Name:

Information Assurance: Homework 1 - Comments

Due September 2, 2009 on compass.

Everyone got full points for the first 5 questions. The remaining questions were broad and also graded fairly leniently.

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

Fairly small set of expectations shared among you. Gain an overview of the security area. Learn some practical skills to help your machines and your friends' machines.

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

Cryptography was the top vote getter.

Malware/attacks and network work security roughly tied for second and third.

A fair number of folks wanted to learn about OS security, web security, DB security, wireless security, secure programming/design, authentication.

Most of the topics people identified we will address to some degree. I don't currently have web security on the schedule, but maybe we can rejigger some networking topics to make space. Otherwise, we do discuss web security in the lab course. Privacy is one topic identified that we won't be covering this semester.

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

Most folks are comfortable with C/C++. Some with Java. Some with a wide variety of scripting languages.

We'll be doing some exercises this semester using security tools. You should not need to program anything. These tools you can run on your home machines with the OS of your choice. I'll be certain that the exercises can be performed on linux machines that everyone should have access to.

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

   a) I can recite the seven layers of the OSI network model.

   25%

   b) I am familiar with the differences between IP, TCP, and HTTP.

   43%

   c) I have used sockets to create a networking application.

   15%

Name:

d) I have used a network.

16%

Most of you have some previous networking experience. We will be reviewing some basic networking while covering network security, but those of you with less experience please work with the TAs or me if you feel that you are being left behind.

5. Ensure that you can access the various communication mechanisms used in class

   a) Access the cs461 newsgroup

   b) Enter the cs461 jabber chat room

   c) Access the c461 compass page

   Some folks had issues accessing the jabber chat room. Plus TSG seemed to be having stability problems the weekend before this assignment was due. Hopefully things have stabilized. If you are still having problems accessing the chat room, please contact one of us to get things worked out. One of the students also noted that there were multiple chat rooms that had cs461 in the name. I assume that one of you accidentally created a chat room while figuring out the interface. The TA's and I will be hanging out in the chat room named "cs461".

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

   a) Alice uses Bob's bus pass.

   Availability – Alice can't use the pass

   Integrity – Bob is passing himself off as Alice

   b) Charles installs a game that includes some malware

   Integrity – His system now includes some undesirable code. The game was not as advertised.

   c) Dave learns Ed's ATM pin.

   Confidentiality – Dave learns Ed's confidential PIN.

   Availability – Ed will soon lose availability to his money.

   d) Fran steals George's car.

   Availability – George doesn't have access to his car.

   Integrity – Fran runs a red light and is caught on camera. Ticket is issued and mailed to George.

   e) Hank's latest browser upgrade causes his laptop to crash.

   Integrity – The brower is not operating as it should

   Availability – Hank no longer has access to the web from his laptop.

Name:

7. Give an example of a situation in which a compromise of confidentiality leads to a compromise in integrity.

There are a large number of cases. Most answers generalized to the following.

Alice's login information to a system (e.g. online bank or email) is acquired by Bob. He can login as Alice and perform unauthorized actions (e.g. money transfer, change account info, etc.).

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

The most popular answers to question 8 were:

1. Recent DoS attacks on twitter

2. Theft of credit card information in large scale (e.g. from TJ MAX or Radisson)

Two other answers include:

"Recently, two renowned hackers claimed they have discovered security issues in the popular iphone platform. They said that it is possible to exploit the security weakness of iphone just by sending a sms message which can eventually lead to gain control of the entire phone. After being hacked, this attack gives the hacker full control over the phone to make calls, send messages and using the internet. In the above security failure scenario, all four of the broad classes of threats would be involved: disclosure, deception, disruption, and usurpation. Since a hacker in this case will gain unauthorized access to the iphone, it is a threat of disclosure. The hacker can make unauthorized calls or send messages/data to other people from the phone acting as the user which might give rise to threat of deception. Since the hacker gets full access to the phone, he can easily change/delete certain data/features from the phone that can lead to interruption of normal usage of the phone which might become threat of disruption. Threat of usurpation can be a concern here as the hacker gets complete control of the phone without the owner's authorization."

*"In April, the Wall Street Journal reported cyberspies had stolen classified information regarding the Lockheed Martin F-35 Lightning plane (*Note: Lockheed Martin refuted the claim). This potential breach of security is of the disclosure type, because sensitive information had been taken by unauthorized people."*