CMPSCI 177 - Computer Security
Fall 2013
Seventh Homework - Malware, Security Policies, and Internet Security

Due: 4 DEC 13 2:00pm

Part I: Malware

1. As a virus writer, give three techniques that you would use to make your virus more difficult to detect. Briefly explain each of the techniques.

Part II: Security Policies

1. In Bishop's text, section 4.5.1, he discusses what should be included in a general University Acceptable Use Policy. I would like you to locate the College of Engineering Acceptable Use Policy, read it, and then briefly (but explicitly) discuss whether or not it includes all of the things that Bishop discusses in the text. Also, if it includes things that were not discussed in Bishop, tell why you think these things are or are not important to include.

2. Which of the Bell & LaPadula rules presented in class makes it clear that the permission matrix represents discretionary access control? Be sure to explain your answer.

3. Answer question 2 at the end of Chapter 5 in Bishop's text.

Part III: BBC - Defeating the Hackers Movie

(If you missed class, you can view the movie at http://www.youtube.com/watch?v=_4NrrKTYmBI)

1. In the section on generating large primes, what is the size of the largest prime number that they generated?

2. In the section discussing the use of quantum computers to factor semiprimes, what is the largest semiprime that they factored?

3. In the section on storing information in people's brain without them knowing it, what musical instrument do the researchers use to introduce the sequence that is remembered by muscle memory.

4. How was the stuxnet malware introduced into the Iranian facility?

Part IV: Internet Security

1. (i) What is the difference between a MAC address and an IP address?
   (ii) Who assigns MAC addresses?
   (iii) Who assigns IP addresses?

2. In the three-way handshake that initiates a TCP connection, if the SYN request has sequence number 163421094 and the SYN-ACK reply has sequence number 672319601, what are the sequence and acknowledgment numbers for the ACK response?

3. Use nmap to determine what hosts are up on subnetwork 128.111.43. What is this type of scan called?

4. Using the results of question 3, choose a host name that starts with the same letter as your last name, and use nmap to determine what TCP services are available on that host. If there is no host whose name begins with the first letter of your last name, then choose a host whose name is alphabetically closest to your last name.

5. Use the traceroute tool to determine the hosts that are on the path from your computer to depcos.pwr.wroc.pl.