**Introduction to Computer Security**, exercise 4, 14.-16. 2. 2012

1. Each time a malware designer, Pierre, sells a product on a chat server in the underground economy for fraudulent products and services, there is a chance that he will get caught and be fined by law enforcement officials. Suppose the probability that pierre will get caught because of any one sale of malware is $p$, and this value is known to both Pierre and the law enforcement officials. What should be the minimum fine for selling a keystroke logger so that it is worth the effort for a rational malware designer like Pierre to sell it? What about the minimum fine for selling a botnet? (Assume that the price of a keystroke logger is 25 e and the price of a botnet 250 e.)

2. **a)** In a salami-slicing attack, a program performs a large number of small, hardly noticeable malicious actions, which add up to a large aggregate malicious action. In a classic example, a programmer for a bank has 1 cent of the monthly interest calculation on each bank customer's account transfered into his account. Thus, if the bank has 1,000,000 customers, then this programmer would get $ 10,000 each month from this salami slicing attack. What type of malware is such a program?

   **b)** Bobby says that a computer virus ate his homework, which was saved as a Word document. What kind of virus is the most likely culprit?

   **c)** Jack encrypts all his email and insists that everyone who sends him email encrypt it as well. What kind of spyware attack is Jack trying to avoid?

   **d)** Eve installed some spyware software on 100 USB ash drives and has designed this software to autoload from these drives along with some nude photos. She then painted the logo of a well-known adult magazine on each one and randomly scattered these ash drives in the parking lots of several of the big defense companies in her town. What type of malware attack is this and what vulnerability is she trying to exploit in order to get her malware code past the network

   rewalls of these companies?

3. Suppose you want to use an Internet cafe to login to your personal account on a bank web site, but you suspect that the computers in this cafe are infected with software keyloggers. Assuming that you can have both a web browser window and a text editing window open at the same time, describe a scheme that allows you to type in your userID and password so that a keylogger, used in isolation of any screen captures or mouse event captures, would not be able to discover your userID and password.

4. **a)** Can two network interfaces have the same IP address? Why or why not?

   **b)** Can two network interfaces have the same MAC address? Why or why not?

   **c)** In the three-way handshake that initiates a TCP connection, if the SYN request has sequence number 156955003 and the SYN-ACK reply has

sequence number 88370339, what are the sequence and acknowledgement numbers for the ACK response?

5. Suppose you suspect that your session with a server has been intercepted in a man-in-the- middle attack. You have a key, $K$, that you think you share with the server, but you might be only sharing it with an attacker. But the server also has a public key, $K_P$ , which is widely known, and a private secret key, $K_S$, that goes with it. Describe how you can either confirm you share $K$ with the server or discover that you share it only with a man-in-the-middle. Also, be sure your solution will not be discovered by a packet sniffer.

6. Either party in an established TCP session is allowed to instantly kill their session just by sending a packet that has the resdet bit, RST, set to 1. After receiving such a packet, all the other packets for this session are discarded and no further packets for this session are acknowledged. Explain how to use this fact in a way that allows a third party to kill an existing TCP connection between two others. This attack is called a *TCP reset attack*. Include both the case where the third party can sniff packets from the existing TCP connection and the case where he cannot.