Computer Security

Exercise 1

1. A DDoS attack prevents you from connecting to your bank website. Which of the security properties will this impact?

2. What is the difference between authenticity and integrity.

3. What are the basic elements of a threat model?

4. Image that you have important data on your laptop. You place a tracking chip inside it in a tamper resistant enclosure. Is this a cost effective way to protect your laptop? Relate your answer to the different types of defences one could employ to protect their assets. Make sure to include your assumptions.

5. ARP allows address translation between IP and MAC addresses.

a. How many MAC addresses are allocated to each manufacturer for their use (assuming one prefix each).

b. Which of the two address spaces would be exhausted first, MAC or IPv4? Give the (approximate) difference.

6. Recall encapsulation. Imagine that a packet of 10 bytes needs to go through 3 layers of the stack before it is transmitted to another machine. Each layer added 10bytes of header and 2 bytes of footer.

a. What is the size of the packet that is transmitted?

b. Imagine that the original 10byte packet is fragmented into two. Now what is the total size (in bytes) of transmitting that original packet?

7. NAT is useful to ease the exhaustion pressure on the IPv4 address space. It can also hide the internal information of a private network from external observers. Give at least one type of information that could be prevented from being observed? Give reasons why this is good to protect.

8. Imagine you want to divert internet traffic to your own knock-off bank website that is a duplicate of the original bank website.

a. What could you do to divert the traffic from the real website to yours (assume that certificates or other forms of authentication are not present)?

b. Would this be a stealthy attack, or would it be traceable?

9. Imagine that an IDS has been trained to detect website-X (that serves malware) and the IDS has a TPR = 95.99% and an FPR = 15%. Suppose that website-X is very popular and 50% of all website visits that the IDS observes are to it. What is the probability that when the IDS detects a visit to website-X it is correct? Show your intermediate steps.