Computer Security

Exercise 1

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

It will impact Availability.

2. What is the difference between authenticity and integrity.

Authenticity is about being **certain** that the information received or accessed by us is from the from the entity we believe it to be from. Integrity is about making sure that information has not been corrupted (due to natural causes), changed or added to by human activity (either accidental or intentionally) either during transit or in storage.

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

- Who is the adversary and what abilities and access do they have.
- Where are they in relation to the objects we are trying to secure.
- What is the aim of the adversary, or in other words, what are we trying to prevent them from doing at the high-level.
- What particular threats are we trying to prevent that, if successfully taken advantage of, will lead to the adversary achieving their goals.
- Are there more than one type of adversary and can they collude.

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.

This question is to get used to thinking in terms of the situation rather than the "right" answer.

A tracking chip in a laptop can be a form of deter and recover defences.

It is deter if it is common knowledge (or there is a prominent sign on the laptop itself) that your laptop has a chip inside. Then the would-be laptop thieves may think twice about stealing a laptop that could lead Law enforcement to their door step. It is also recover since once the laptop is stolen you can use the tracking feature to locate it. This assumes that the tracking chip is still operational and within range of the tracking system.

One may also argue that this is deflect since the thieves may then steal nearby laptops instead and avoid yours. However, this is not as strong a defence in this particular setting as the above two.

It is not prevent since the presence of the chip can not physically prevent someone from walking away with the laptop. It is not detect since the tracking chip is not what would tell you that the laptop is lost, you would know that using just your eyes.

If a tracking chip is cost effective depends on the cost of the laptop, the value of the information it contains, and the cost of the tracking chip and the operation of the infrastructure required to track the chip once the laptop was stolen. Some laptops have this functionality built in, like Macbooks. Here, the cost is absorbed by Apple. However, if you had to deploy it yourself would it still make sense?

Also important is the adversary who this tracking chip is supposed to work in the face of. If it is an opportunistic laptop swiper at a café this might be workable. However, if a criminal organization was trying to steal your laptop's secrets, they may have a way of disabling the tracking chip, so it might not thwart them. Furthermore, you may also consider the probability, or likelihood, of the different sorts of adversaries occurring, and that is also another factor that can go into the decision of the cost effectiveness of the tracking chip.

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).

256^3, or 2^24 = 16,777,216 (give or take some reserved addresses).

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

IPv4 will be exhausted first. The difference is 2^48 – 2^32 = 281,470,681,743,360 more MAC addresses.

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?

10+12+12+12=46 bytes.

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

2x(5+12+12+12)= 82 bytes.

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.

NAT can help to hide the number of machines on the private network. By hiding the number of hosts on the network we do not present an attractive target for attackers who are looking to maximise their gains given the cost of running the attack. The size of the network could also reveal the potential operational capabilities of the network (for instance dedicated database servers or printers) that might give clues to the attack on how best to attack the network hosts.

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)?

We could try to poison the DNS cache of name servers so that they point to our own IP address. If we are the ISP or other router on the path of the victim, we could alternatively divert their traffic to the fake website by rewriting the destination IP in the packet header.

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

The DNS cache attack may be noticed by the cache servers after the attack since they may keep logs. The diversion may be more stealthy since there is no record of the change except at the network node that rewrote the header.

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.

Imagine 1 million visits.

TP = 500,000 * .9599 = 479950, FP = 75000.

Precision = TP/(TP+FP) = 479950/(554950) = 0.865 or **86.5%.**