15-441 Computer Networks
Homework 4

Due: 5:00pm, 5th April 2019

1 DDOS-ing Blackholes

You have just taken the Computer Networks course at CMU. After watching an episode of the popular TV series, Mr. Robot, you decide to become a 'hacker'. In order to gain notoriety, you decide to carry out a Denial-of-Service attack on Netflix's server.

(a) As a beginner hacker, you only have access to your own laptop. Conceptually, why can't the traffic from your laptop be enough to bring down a Netflix server?

(b) After doing some research (even being a 'hacker' is hard work) you figure out a vulnerability in Windows 10 that lets you take control of the device and send traffic from it. Unfortunately, due to the computation required for this exploit, a single device and only handle two outgoing connections (as in a single device can at most hack into and control two other devices).

(i) After some more research, you find out that taking down a single Netflix server requires a burst of 1024 Mbps of simultaneous traffic. Given that each device you can compromise has an uplink capacity of 2 Mbps, and assuming they do not interfere with each other, what is the minimum number of devices you need to compromise (including your own laptop) to be able to carry out a successful DDOS attack on one Netflix server? (The devices are geographically distributed and your control only lasts while the connection is active, so you can't install scripts to run later)

(ii) Given a setup with k max connections possible, an uplink capacity of d Mbps, and a server that requires a burst of C Mbps to take down, give a closed form formula for the minimum number of devices needed to carry out a successful DDOS attack on this server. You can assume that $\frac{C}{d}$ is an integer power of k.

(c) You have gained notoriety but as a result, Microsoft has started patching the vulnerability in Windows that allowed you to take control of their devices. Meanwhile, you discover a vulnerable public server that runs the memcached protocol. You decide to carry out an amplification attack using this server. Is it possible now to carry out a successful DOS attack on a Netflix server using only your own laptop? What is required for this to be possible? (assume link and server capacities from part (a)(i) and assume the memcached server has unlimited uplink capacity) Is it possible to do a similar attack using a public DNS server? Why?

2 Symmetric and Asymmetric key encryption

Prof. Sherry wants to send Prof. Steenkiste a copy of the final exam over the network. Prof. Sherry and Prof. Steenkiste have public/private keys and know each others' public keys. They also have a pre-shared secret key. These keys have not been compromised.

Suppose students can intercept and modify packets on the network. For each of the following methods, circle whichever is appropriate to indicate whether the protocol is safe, whether the exam can be overheard, whether the exam can be modified, or whether it can be overheard and modified.

(i) Prof. Sherry sends the exam in plaintext.

Safe Overheard Modified Overheard & Modified

(ii) Prof. Sherry signs the exam with her private key, sends it.

Safe Overheard Modified Overheard & Modified

(iii) Prof. Sherry encrypts the exam with Prof.Steenkiste's public key, sends it.

Safe Overheard Modified Overheard & Modified

(iv) Prof. Sherry encrypts the exam with Prof.Steenkiste's public key, signs it with his private key.

Safe Overheard Modified Overheard & Modified

3 Attacking SSL

1. Suppose Alex is accessing CMU website over an SSL session. Suppose an attacker, who does not have any of the shared keys, inserts a bogus TCP segment into a packet stream with correct TCP checksum and sequence numbers (and correct IP addresses and port numbers). Will SSL library in the CMU webserver accept the bogus packet and pass the payload to the web server application? Why or why not?

2. Visit www.baidu.com. Can an attacker who has 'tapped' your network link read your connection data? Why or why not?

   Can you be sure that you are talking to the 'real' Baidu server? Why or why not?

3. Visit www.nytimes.com. Can an attacker who has 'tapped' your network link read your connection data? Why or why not?

Can you be sure that you are talking to the 'real' New York Times server? Why or why not?

4. (Very few points, do this tricky one for the glory!) What are the differences or similarities in privacy, integrity, and authentication guarantees between the SSL configurations for www.nefeli.io and www.cmu.edu?