ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Spring Term 2016
Prof. Adrian Perrig

# Operating Systems and Networks
# Assignment 10

Assigned on: **May 31, 2016**

## 1 Port Numbers

(1) Can the source and destination ports be the same in a UDP packet?

(2) Is it possible for a web server to listen on port 79? What about port 7900? Explain what the difference is between these two cases, focusing on necessary user privileges to make this configuration possible

## 2 TCP Three Way Handshake

Explain, using the TCP three way handshake, why it is not possible for one of the parties to "spoof" their source IP address.

## 3 TCP/UDP

(a) When host A sends data to host B using TCP, can it happen that two blocks of data generated by the application at A are grouped by TCP into one single IP datagram?

(b) When an application receives data from TCP, can the application assume that the data was sent as one message by the source?

(c) When an application receives data from UDP, can the application assume that the data was sent as one message by the source?

(d) Assume host A sends one block of data to host B using UDP. Can it happen that the blocks of data generated by the application at A is fragmented by the IP layer at A into several IP packets?

## 4 Vulnerabilities on TCP — let's be evil

The last assignment briefly covered IP address spoofing. Let's have a closer look in this exercise. Recall that when crafting IP packets, a host can specify an arbitrary source IP address, that is, instead of putting the host's correct IP address in the IP packet header, the host chooses an arbitrary address to appear in the packet header.

(a) Faking the source address and thus camouflaging the host's real identity can have several reasons. Mention at least two.

(b) Specify what network requirements are necessary to enable address spoofing. Consider middleboxes, NATs, and ISPs.

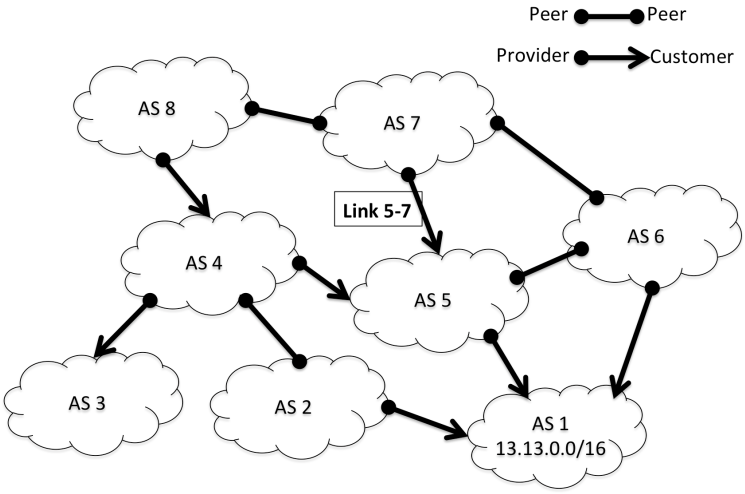
(c) Specify protocol requirements necessary to enable address spoofing. Consider particularities of TCP and UDP. How does TCP's built-in mechanism work to prevent requests with spoofed addresses?

(d) Assume address spoofing is ruled out by the network or by the protocol. An adversary can thus not fool a server into believing a connection is established from an IP address different than the client's actual address. How can the adversary still launch an attack against the server, for instance a denial-of-service attack? Think about how (a group of) clients can exhaust the server's resources by not replying to SYN/ACK packets. How exactly does the attack work?

(e) What are possible countermeasures? Hint: The TCP protocol specification does not impose particular restrictions on the choice of the first sequence number. How can the 4 bytes of the sequence number be used in a clever way to encode the state that would usually be stored in the SYN queue?

# 5 BGP

Consider the AS-level topology in the picture below. Say AS1 starts by announcing prefix 13.13.0.0/16 into the network at time 0. All routing messages exchanged in this problem pertain to the prefix 13.13.0.0/16. At time 1, each of AS1's neighbors – AS2, AS5 and AS6 – propagate the route to their neighbors, and so on. Hint: Note that ASes only announce paths for traffic for which they can earn money and they prefer paths that increase their revenue. Your answers should follow the format shown in the "Routing Message Format" below.




| Routing Message Format |
|---|
| Prefix : 13.13.0.0/16 |
| Path : {AS1} |
| Send To: AS2, AS5, AS6 |

(a) Show the path vector that AS5 sends out at time 1. Which of its neighbors does AS5 send this path vector to?

(b) Show the path vector that AS7 sends out at time 2. Which of its neighbors does AS7 send the path vector to?

(c) A valid AS level path is one that is allowed by economic policies. List all possible, valid, AS level paths from AS8 to the prefix 13.13.0.0/16. Argue why {AS8,AS7,AS6,AS1} is a valid (or invalid) AS level path from AS 8 to the prefix 13.13.0.0/16?

(d) Which path will AS8 use to route to the prefix 13.13.0.0/16? Why?

(e) Assume that Link 5–7 is removed from the topology. Would AS7 announce the prefix 13.13.0.0/16 with {AS7,AS6,AS1} to AS8? Briefly explain.