# Assignment 2

Yuri Shafet, Itay Azaria

January 23, 2016

## Question 1

You can find pcap of spoofing attack in pcap folder. Attack proceed as follows:

We first perform ARP poisoning(code only on client side), by listening to ARP packets, and sending fake response. After ARP poisoning is done we perform 3 way handshake with server, and using fake IP for spoofing.

## Question 2

To prevent IP spoofing now every legitimate client has his unique secret(only client and server knows it), secret is unique per IP, when client wants to send HTTP request, it has to add *secret* header to request and add following : sha1(unique-secret + data). When server receives requests, it looks in its secret table, where all secret/ip stored for client secret, calculates hash and compares it. If it is equal, know client wants to communicate, if not, request will be denied with error message. Because key is unique per IP, even if IP was changed in the middle, server will decline spoofed IP.

You can find in pcap folder 2 pcaps, one when request is spoofing and error is returned to client, and second is legitimate one.

## Question 3

1. You can find caps of blocked communication when client wants to download file with ending that should be stopped. One of caps is normal request, the other one is fragmented(2 fragments). You also can use our scripts for testing. One of them sending fragmented packets.

   We also take care of fragmented packets by storing packets in buffer and reconstructing them when possible. Packets released from buffer using timeout timer.

2. We use two knocks for user to open SSH port. First knock to port 4242 with specific HMAC, if HMAC correct, server will send back challenge to client, and client will have to return HMAC (client uniquekey+challenge) to 4243 port. Because key is unique per IP , it prevents IP spoofing(like in question 2), and challenge-response prevents replay attacks. Server will open port if HMAC is correct. You can find relevant pcaps in pcap folder. You can use q3-magician.py script to knock(after that you can use ssh).