Homework 3

Submission into the *green SEC mailbox* in front of Room 2.041 until December 19, 2017, 17:30.

General Notes

- If you encounter difficulties, you SHOULD[1] ask the teaching assistants in the tutorial sessions.
- To solve the homework, you SHOULD form teams of 3 people.
- Your team size MUST NOT exceed 3 people.
- You MUST submit your homework on paper (one submission per team).
- You are free to choose whether you write your solutions in German or in English.
- If your submission contains multiple sheets, you MUST staple them.
- Each sheet of your submission MUST include all team member's names and matriculation numbers.
- If you do not adhere to these rules, you risk loosing points.

Problem 1: BGP

Consider the network depicted in Figure 1 with the IP networks listed in Table 1.

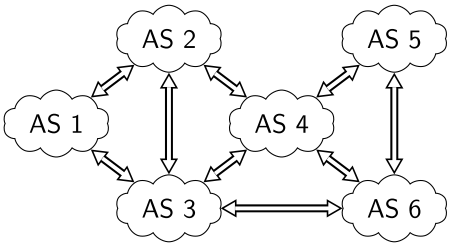

Figure 1: A network with six autonomous systems.

AS	IP Networks
1	1.2.3.0/24 17.9.8.0/25
2	5.2.0.0/16
3	92.18.2.0/24
4	18.2.1.0/26
5	80.90.42.0/24
6	15.23.2.0/24

Table 1: IP networks.

(a) What is the content of the BGP tables of each AS (after BGP has been running for a while)? Consider that BGP only takes the shortest path. If two different announcements for the same IP network have paths of the same length, one of the announcements is ignored (based on a random choice that the AS remembers). (5 points)

(b) AS 5 maliciously starts announcing the IP network 1.2.3.0/24. What is the outcome, i.e., how are the BGP tables affected? (5 points)

Problem 2: Network Trace

Consider the network setting depicted in Figure 2. Alice and the attacker are connected to a Wifi network. This Wifi network is connected via a router to the internet (which we consider as a black box here, i.e., we do not care about the structure of the internet). The router also acts as a recursive DNS resolver for all parties in the Wifi network.

In the following, we assume that there are no caches at all, i.e., if some party needs some information, this party needs to retrieve that information.

[1] SHOULD, MUST, and MUST NOT are used as defined in RFC2119.

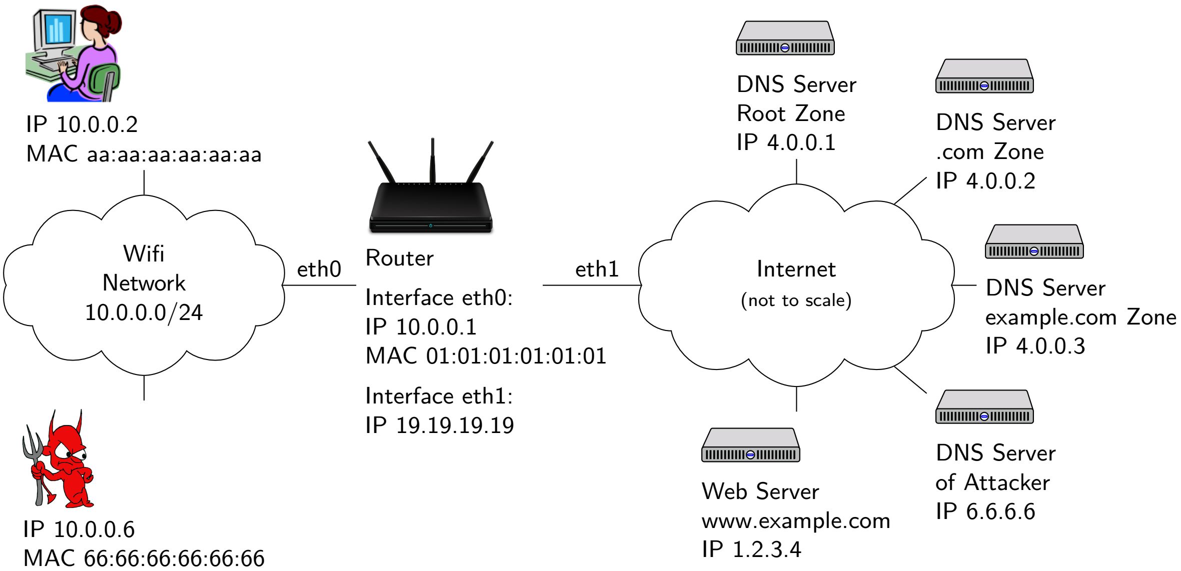

Figure 2: Network setting

(a) Alice opens the web page at http://www.example.com in her browser. Write down a trace of all messages that are exchanged between any of the parties as a result of Alice's action. (The attacker does not take any action.) (5 points)

(b) How does the trace look like, if the attacker performs an ARP spoofing attack in order to replace the contents of the web page that Alice's browser receives? Note that the attacker cannot intercept or block any messages that are not addressed to him (in particular, he cannot spoof MAC addresses). The attacker may create arbitrary new messages with the knowledge that he gained. (5 points)

Remarks:

- The trace should only contain messages and message properties that we know from the lecture.
- In the Internet, you only need to consider the Internet, transport, and application layer, while in the Wifi network, you also need to consider the data link layer.
- For the individual messages, use the following notation:

  Protocol 1 (Property A = foo, property B = bar) / Protocol 2 (. . .) / . . .

  where Protocol 1 is on a lower layer than Protocol 2, and so on.

  For example:

  Data link (Source MAC = cc:cc:cc:cc:cc:cc, Dest. MAC = ee:ee:ee:ee:ee:ee) / IP (Source IP = 1.2.3.4, Dest. IP = 4.3.2.4) / TCP (. . .) / . . .
- We advise you to write down your solution with a computer as the trace will be very long and will contain many similar messages.

Problem 3: Probability of Successful DNS Spoofing

Alice uses the recursive DNS resolver 9.9.9.9.

(a) Alice queries the resolver for the A record of `www.example.com` via UDP. The attacker knows this. In order to spoof the DNS response from the resolver to Alice, which properties does the attacker need to guess? How many possible values are there for these properties? What is the probability that the attacker guesses all values correctly at the first try? (5 points)

(b) Now, the attacker performs Kaminsky's attack on the resolver. Assume that one round of the attack (see Slide Set 8, Slide 22) takes 0.1 second and the attacker can send 2000 spoofed responses to the resolver in one round. How long does the attacker need (on average) to succeed? (5 points)