Brandenburg University of Technology
Cottbus-Senftenberg
IT Security Group

Practice Class
“Introduction into Cyber Security”
Winter Term 2019/2020

Introduction into Cyber Security
– Authenticity –

Deadline: 28th November, 2019

Topics

In this second practical exercise we deal with Authenticity. More specifically, we take a hands-on approach on the famous Man-In-the-Middle attack to steel a secret which is send between Alice and Bob. In our simplified Laboratory environment this will be just some basic data. However, in a real world scenario the obtained secrets could be partial information of a Diffie-Hellman key exchange, or even a whole symmetric key. This makes the attack under consideration so dangerous if there are nor counter measures installed. Later within the lecture, we will learn how to deal with such authenticity issues. However, you can sill think about solutions to overcame the problems arising in this laboratory task now.

1 Preparation

If you are not already familiar with the UNIX/Linux operation system it is now a good point in time to get to know the basic command line operation possibilities of UNIX. Therefore go through the *Linux-Challenge* provided below. If you are already familiar with UNIX, feel free to skip this part.

https://www.b-tu.de/owncloud/s/jm3iFoSq7XW65zx

Also you will need some basic understanding of the C/C++ programming language. If you are not yet familiar with it, you should get to know it in a self-studying manner. In the next task it will be assumed that you have basic C/C++ programming skills, when we deal with stack based buffer overflows.

1.1 Setting up the Laboratory Environment

Consider a switched Ethernet network that contains 3 computers: Alice, Bob and Mallory. You will assume Mallory's role in this experiment. The computers will be given by the means of three

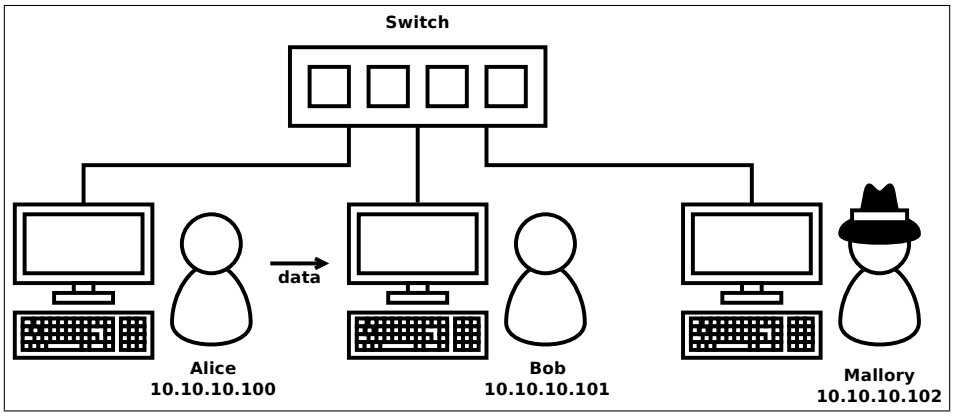

Figure 1: Sketch of the network scenario with ARP

virtual machines. Occasionally the PCs of Alice and Bob send data packets through the network. To make this possible they use the ARP (Address Resolution Protocol) to determine their target's MAC address. The switched nature of the network makes it impossible for possible attackers to simply listen and evasdrop on their network port. However, this network is still far from secure.

In this preparation step you will have to setup the three given virtual machines either on your own computer, or within your account in the BTU PC pool. The images for the virtual machines will be provided in moodle after the 14.11.2019. Your experimental assembly should be as sketched in the figure above. As a virtualization solution you are allowed to use any existing library or program, however we recommend to use *VirtualBox* due to its easy of use. Also *VirtualBox* comes preinstalled with the computers provided in the BTU pc pool.

Beside the provided virtual machines, you will work with the C-program `RAW_Pacet.c` which was provided in the encrypted Zip file from our previous task.[1] Read through the source code, try to understand it and compile it on the Mallory machine. Also it is worth to take a look into the structure of the Address Resolution Protocol.

[1] If you were not able to decrypt the Zip in the previous task, you are not allowed to use this provided program. You have to program your own network packet builder using any programming language of your choice.

2 Main Task

Use ARP Spoofing (ARP Cache Poisoning) to impersonate a PC and perform a Man-in-the-middle-attack. Beside the `arp` system command and the may provided `RAW_Pacet.c`, you are not allowed to use any third party programs not written on your own. If you have established *Mallory* as the Man-in-the-Middle, steal the secret that Alice sends to Bob constantly. Take special care that Alice and Bob won't notice your attack. In such a case you might get caught and the attack fails. After you have obtained the secret, upload it contents to the moodle platform before the deadline ends.

Hints:

1. You work with sudo privileges on the machine `mallory`, using the username `mallory` and password `mallory`.

2. In case you require internet access, edit the file `/etc/network/interfaces` and uncomment the configuration for the interface `enp0s8`.

3. You can build custom network packets with the socket API in C. Don't forget to make use of the tool `arp` to check the contents of the ARP cache.

4. Make sure that Alice and Bob won't notice your attack.

3 Preparation for the Consultation

Please prepare yourself for a consultation of approximately 15-20 minutes. During this consultation you should be able to demonstrate and explain your attack. Thereby describe each step you have done to obtain the secret data and reason about it. Especially explain any written/used code and/or program; even the given ones. Take notice, that the examiners will ask additional questions around the topic of authenticity and Man-In-the-Middle attacks. Especially, if they were directly or indirectly discussed within the lectures. Thus, be prepared to answer them as well an keep in mind that these tasks are part of approval for the final exam. Thank you.

References

[1] *Linux Man Page of arp*. URL: http://man7.org/linux/man-pages/man8/arp.8.html (visited on 10/30/2019).

[2] *Linux Man Page of socket interface*. URL: http://man7.org/linux/man-pages/man7/socket.7.html (visited on 10/30/2019).

[3] Oracle. *Oracle® VM VirtualBox® User Manual*. URL: https://www.virtualbox.org/manual/UserManual.html (visited on 10/30/2019).

[4] D. C. Plummer. *An Ethernet Address Resolution Protocol*. 1982. URL: https://tools.ietf.org/html/rfc826 (visited on 10/30/2019).

Good luck!