

Cybersecurity - Homework 9

Vlad Turno (1835365)

December 28, 2025

1) Introduction

SafeGuard is a VPN solution that uses cryptographic techniques in order to provide secure communications between clients and servers over potentially insecure networks (like the whole internet). The general cryptographic principles underlying the VPN protocols include the following:

- **Confidentiality:** a VPN protocol ensures that transmitted data is encrypted so that even if an attacker intercepts the communication the data cannot be read.
This property is usually achieved by using symmetric encryption with a shared secret key to encrypt and decrypt the data.
- **Integrity:** the integrity of data is protected by using cryptographic hashing and MACs (message authentication codes) to ensure the data cannot be tampered within the traffic intransit.
- **Authentication:** before establishing any kind of connection, both clients and servers authenticate themselves to ensure that they are communicating with the correct party.
This operation can be guaranteed by using asymmetric encryption (through public and private key pairs) and certificates.
- **Forward Secrecy:** it ensures that even if an attacker compromises the VPN server or manage to gather any of the session keys, the previous communication sessions cannot be decrypted.
This mechanism is implemented using key exchange protocols like *Diffie-Hellmann* to ensure session keys to be generated secretly and not stored.

2) Configuration

Using *VMware* as hypervisor I deployed two *Linux* virtual machines (specifically *Ubuntu 18.04*) for both client *C* and server *S*, connected over the same local network.

On both of them I installed *SafeGuard-VPN* and set it on the basic standard configuration and used *OpenSSL* to generate encryption keys in order to securely authenticate and encrypt communications between *C* and *S*.

Then, I edited the VPN configuration files to set ports, netmask and server address:

```
# Server VM configuration
$ sudo apt-get update
$ sudo apt-get install safeguard-vpn

$ openssl genpkey -algorithm RSA -out server.key
$ openssl req -new -key server.key -out server.csr
$ openssl x509 -req -in server.csr -signkey server.key -out server.crt

$ nano /etc/safeguard-vpn/server.conf
server_ip = 192.168.1.1
vpn_network = 10.8.0.0/24
vpn_subnet_mask = 255.255.255.0
vpn_port = 1194
vpn_protocol = UDP
server_certificate = /etc/safeguard-vpn/server.crt
server_key = /etc/safeguard-vpn/server.key
dh_param = /etc/safeguard-vpn/dh2048.pem

$ sudo systemctl start safeguard-vpn-server
```

```
# Client VM configuration
$ sudo apt-get update
$ sudo apt-get install safeguard-vpn

$ openssl genpkey -algorithm RSA -out client.key
$ openssl req -new -key client.key -out client.csr
$ openssl x509 -req -in client.csr -signkey client.key -out client.crt

$ nano /etc/safeguard-vpn/client.conf
server_ip = 192.168.1.1
vpn_network = 10.8.0.0/24
vpn_port = 1194
vpn_protocol = UDP
client_certificate = /etc/safeguard-vpn/client.crt
client_key = /etc/safeguard-vpn/client.key
dh_param = /etc/safeguard-vpn/dh2048.pem

$ sudo systemctl start safeguard-vpn-client
```

3) Usage

Now I test the VPN functionality by executing a *curl* command from the client VM to fetch a file from *Cloudflare*'s test server and measure the time needed to download 5GB of data with and without VPN on:

```
# VPN off
$ curl -o /dev/null -w "%{time_total}\n" "https://speed.cloudflare.com/_down?
  bytes=500000000"
% Total      % Received % Xferd  Average Speed   Time      Time      Time  Current
          Dload  Upload   Total Spent  Left Speed
100  500000000  0  5000     0       0  34728       0 --::-- --::-- --::--  35211
1.43973

# VPN on
$ curl -o /dev/null -w "%{time_total}\n" "https://speed.cloudflare.com/_down?
  bytes=500000000"
% Total      % Received % Xferd  Average Speed   Time      Time      Time  Current
          Dload  Upload   Total Spent  Left Speed
100  500000000  0  5000     0       0  34728       0 --::-- --::-- --::--  34790
2.71462
```