Network Security Lab
Experiment#5
IPSec Basic Configuration

Dr. Ahmed Awad & Eng. Ibrahim Amreyeh

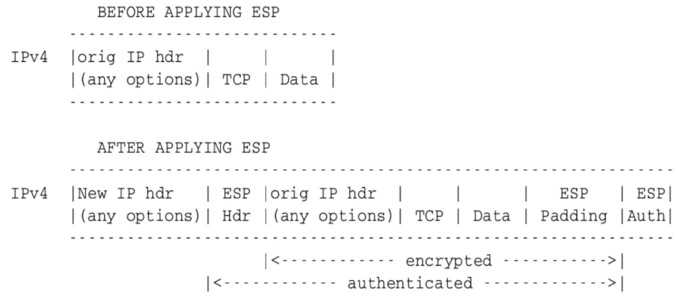
March 21, 2021

1 Objectives

The purpose of this experiment is to implement a simplified version of IPSec to demonstrate the integration of cryptography algorithms in TCP/IP protocols.

2 Introduction

IPsec is a set of protocols developed by the Internet Engineering Task Force (IETF) to support secure packet exchanging in the network layer. IPSec exemplifies a number of security principles including: encryption, hashing, authentication, and key management. It is important to mention that cryptography algorithms are integrated in TCP/IP protocol stack in a transparent way, so that the existing programs do not have to be aware of the existence of IPSec. There are two modes when IPSec protection is applied: **The transport mode** and the **Tunnel mode**. Furthermore, two headers are inserted in the IP packet: Authentication Header (AH) and Encapsulating Security Payload (ESP). Figure 1 illustrates the ESP header insertion in IPv4 packet.



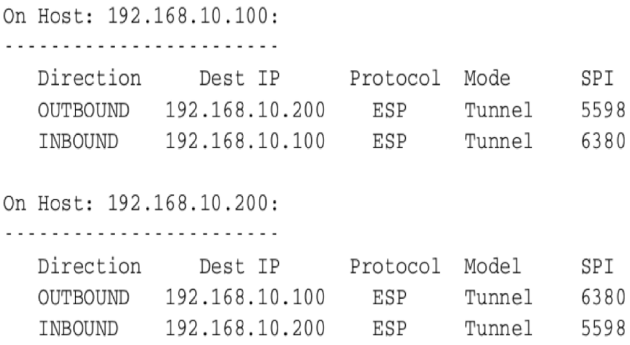
```
         BEFORE APPLYING ESP
      ----------------------------
IPv4  |orig IP hdr  |     |      |
      |(any options)| TCP | Data |
      ----------------------------

         AFTER APPLYING ESP
      ---------------------------------------------------------------
IPv4  |New IP hdr   | ESP |orig IP hdr  |     |      |   ESP   | ESP|
      |(any options)| Hdr |(any options)| TCP | Data | Padding |Auth|
      ---------------------------------------------------------------
                          |<------------ encrypted ----------->|
                    |<------------ authenticated ------------>|
```

Figure 1: ESP Header Insertion

2.1 Security Associations (SAs)

To enable IPSec between two hosts, a Security Association (SA) is required between those hosts. SA is a connection that affords security services to the traffic carried to it. Usually an SA is uniquely identified by a triple that consists of: Security Parameter Index (SPI), destination IP address, and the security protocol identifier (ESP and AH). As an example, consider the host with IP address 192.168.10.100 with any outbound packet to the destination 192.168.10.200. with tunneled ESP mode to process the packet. Assume that the SPI equals to 5598. This value will be attached to the ESP packet so that the receiving host can lookup this entry using the SPI and get all necessary security parameters. Notice that the SA should be unique for each node in the network. Furthermore, for a bi-directional communication, SAs should be set on each host, therefore, two SAs should be found in each host. Figure 2 demonstrates the aforementioned example.



```
On Host: 192.168.10.100:
-----------------------
   Direction     Dest IP      Protocol  Mode      SPI
   OUTBOUND   192.168.10.200    ESP     Tunnel    5598
   INBOUND    192.168.10.100    ESP     Tunnel    6380

On Host: 192.168.10.200:
-----------------------
   Direction     Dest IP      Protocol  Model     SPI
   OUTBOUND   192.168.10.100    ESP     Tunnel    6380
   INBOUND    192.168.10.200    ESP     Tunnel    5598
```

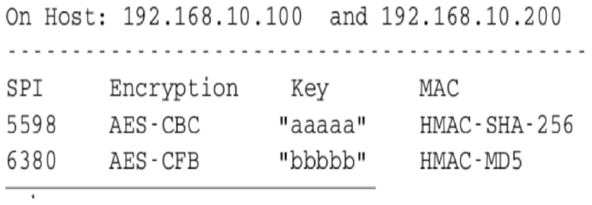
Figure 2: Security Association (SA) Example.

The key parameter in SA is the SPI which is a 32-bit identifier that serves as the index into the security table for some communication. For example, all security parameters for the communication from the host whose IP 192.168.10.100 to the host whose IP 192.168.10.200 are associated with SPI value of 5598 (see Figure 2). On the other hand SPI value of 6380 is used to identify the security parameters from the communication from host 192.168.10.200 to the host whose IP is 192.168.10.100. Figure 3 illustrates an example of a security table stored in the hosts shown in Figure 2.

2.2 ESP Tunnel Model Outer IP Header Construction

The source and destination IPs in the outer header in ESP tunnel are constructed depending on the type of the IPSec tunnel which can be categorized as:

a. Host-to-Host Tunnel: The tunnel has to be established between two hosts.



```
On Host: 192.168.10.100  and 192.168.10.200
-------------------------------------------
SPI     Encryption    Key       MAC
5598    AES-CBC      "aaaaa"    HMAC-SHA-256
6380    AES-CFB      "bbbbb"    HMAC-MD5
```

Figure 3: Security Parameters Associated with SA.

In this case, the source and destination IP addresses in the outer header are simply copied from the inner header.

b. Host-to-Gateway Tunnel: In this tunnel, the source IP is copied from the inner header. However, the destination outer IP becomes the IP of the gateway. This means, the original packet is wrapped in an IPSec packet with the gateway as a destination IP address. When the packet is received by the destination, it unwraps the IPSec packet and gets the original packet which then will be forwarded to the destination stated in the original (inner) IP packet.

c. Gateway-to-Gateway Tunnel: In this tunnel, both the source and destination IPs in the outer header are different from that in the inner header. In this case, the settings of source and destination IPs should be defined in the SA.

2.3 Virtual Private Network (VPN)

A VPN brings geographically distributed computers together to form a virtual network. For example, a host X creates a host-to-gateway ESP tunnel type with a gateway G that is located in another country. In this case, G treats X as it is directly connected to it and X can be considered as a member of this private network.

2.4 Key Management in IPSec

Key management can be simply performed manually in IPSec, wherein, the administrator manually configures each with keying material and SA management. This approach is acceptable when the number of sites to be securely connected in small. However, it does not properly scale for large number of sites. Therefore, Internet Key Exchange (IKE) is used as the default key management protocol under the IPSec domain.

2.5 Encryption and Hashing in IPSec

AES is typically used as an encryption algorithm for IPSec. Therefore, the IPSec should support the AES with 128-bit, 192 bit, and 256-bit keys. If the message

to be encrypted exceeds one AES block size (128 bits), then a mode of operation should be applied with padding, if necessary. Notice that if Initialization Vector (IV) is needed, then it is sent followed by the ciphertext (all form the encrypted ESP packet).
For the authenticated part of ESP packet, the IPSec supports Hashed Message Authentication Code (HMAC) with various underlying hashing algorithms. For example HMAC-SHA-256 is commonly used.

3 Procedure

3.1 Host-to-Host IPSec Communication

a. Construct a simple peer-to-peer network using two Linux machines (virtual or standalone). Write down the IP address for each host.

b. Make sure that each host is reachable by the other. **How can you do that?**

c. What are the basic requirements to create host-to-host secure communication with IPSec?

d. Install the IPSec tool with all its needed dependencies using the command: **apt-get install ipsec-tools strongswan-starter**.

e. Open the IPSec configuration file **ipsec.conf**.

f. At the end of the file ipsec.conf, add the following lines with the IPs you have used in your network (instead of IPX and IPY):

```
conn host-to-host
authby=secret
auto=route
keyexchange=ike
left=IPX
right=IPY
type=transport
esp=aes128gcm16!
```

g. Explain each item in the above lines you have added to the file **ipsec.conf**.

h. Open the file **ipsec.secrets** under the etc directory. What does this file contain?

i. Add the following line to the file **ipsec.secrets**. Make sure to include the IPs you have in your network instead of IPX and IPY. In addition, choose a strong password that meets the general security requirements.
IPX IPY : PSK "Your password here!".

j. Now restart the IPSec process. **How can you do that?**

k. Why do you need to re-start the IPSec process?

l. Run the command **ipsec statusall** and explain the output.

m. Now repeat all steps (d-j) on the other host but with using the proper IP. Show all your steps in details.

3.2 Testing the Constructed Tunnel

a. Issue a ping command from the first host to the second host. Set the packet size to be 4048 bytes. **How can you do that?**

b. Run the command **watch ipsec statusall**.

c. Keep the above process running and state your conclusions.

d. Use tcpdump to capture ESP packets. Write those packets to a file named **ESP.cap**

e. Open the file **ESP.cap** using Wireshark and select a captured ESP packet. Write down the SPI of that packet.

f. Show the Security Associations (SAs) that have been implemented on the first host. **How can you do that?**

g. Now do ping from the second host to the first host. Capture an ESP packet on the first host and check its SPI.

h. Change the pre-shared key value in one of the hosts, restart the IPSec process, and do ping again. **Is there any captured packet?**

3.3 SSH With the Constructed Tunnel

a. Install an SSH client on both machines. Make sure that it is installed using the command **ssh**.

b. Install an SSH server on both machines. If it is not installed, then you have to use the following command **sudo apt-get install openssh-server ii**.

c. Run the tcpdump on one machine and try to capture ESP packets.

d. Connect SSH from one machine to another. You can use the command **ssh username@host-ip-address** with the password of the host you are connecting to.

e. Capture ESP packets and analyze one of the packets.

References

https://seedsecuritylabs.org/
https://wiki.strongswan.org/projects/strongswan/wiki/IntroductiontostrongSwan