IPsec and Transport Layer Security

Lab Report 4

Information Systems Security course (01TYM, 02KRQ)

prepared by:

Anuar Elio Magliari (s317033@studenti.polito.it)

George Florin Eftime (s303483@studenti.polito.it)

Alekos Interrante Bonadia (s319849@studenti.polito.it)

1) IPSec and security at IP level

3.1 Setting IPsec policies and Security Associations

- Which commands do you need to run to flush the SAD and SPD? Which commands do you need to run to check the content of the SAD and SPD databases?
  - In order to flush the SAD the command needed is:
    - *ip xfrm state flush*
  - For the SPD database the command needed is:
    - *ip xfrm policy flush*
- which type of traffic is protected with IPsec?
  - In IPsec we protect the payload not the header (AH encapsulates also the real header). We do it with ESP or AH strategy ESP is ok for confidentiality, authentication, integrity and also for protection against replay attacks. Using AH we does not give encryption so usually ESP is preferred. In this solution we are using only ESP algorithm.
- which IPsec protocol is used?
  - The IPsec protocol used are AH and ESP protocols
- which security services are provided?
  - AH: authentication, integrity and protection against replay attacks
  - ESP: almost same functions provided by AH, plus confidentiality
- Which are the cryptographic algorithms used?

    - AES-128-CBC is used in this case
- what are respectively the roles of the Security Association Database (SAD) and of the Security Policy Database (SPD) in the IPsec architecture?
    - SAD (Security association database) is required to offer a valid policy between two IP addresses so between two devices with specific IP. The association is saved in the “DB” and could be then checked using an index (SPI). In this case we are using the indexes 0x1000 for Alice DB and 0x2000 for Bob DB.
- which directives are processed every time Alice sends a new IP packet?
    - The directives that are processed every time Alice sends a new IP packet are: verification of valid index in the SAD and the policies, encryption then encapsulation of payload IP packet then finally sending to the destination
- why are two SAs necessary?
    - The SAs associations are two because even if the association is unidirectional, for a secure bidirectional channel we need to have SA policies in both nodes so that the channel can be secure and both DB (for Alice IP and Bob IP device) should be filled with the other index, key, IP and algorithm. Then, there are two tables, one for outgoing packets and one for incoming packets in each of the two nodes connected.
- which is the purpose of the field SPI present in the IP packets exchanged?
    - SPI is a specific index for each connection channel so there is always a single and unique index of 32 bits associated with a IP in the SAD. The SPI can be manual or random value but always it should be unique
- Which is the scope of the field Seq Number?
    - The purpose of the sequence number within packets is to prevent replay and filtering attacks. In other words, it is a method to protect packets from manipulation by an attacker. It is also used for the integrity check of a packet by the endpoints.

3.2 Setting IPsec policies and Security Associations

- ESP with AES-128-CBC and HMAC-SHA1;
  - *ip xfrm state add src 192.168.1.43 dst 192.168.1.42 proto esp spi 0x1000 enc aes 0xaa22334455667788990aabbccddeeff auth sha1 0xbbccddeeff00112233445566778899aabbccddeeff*
  - *ip xfrm state add src 192.168.1.42 dst 192.168.1.43 proto esp spi 0x2000 enc aes 0xbb22334455667788990aabbccddeeff auth sha1 0xaaccddeeff00112233445566778899aabbccddeeff*
  - *ip xfrm policy add src 192.168.1.43 dst 192.168.1.42 dir out tmpl proto esp mode transport level required*
  - *ip xfrm policy add src 192.168.1.42 dst 192.168.1.43 dir in tmpl proto esp mode transport level required*
- AH with HMAC-SHA1:
  - *ip xfrm state add src 192.168.1.43 dst 192.168.1.42 proto ah spi 0x3000 auth sha1 0xbbccddeeff00112233445566778899aabbccddeeff*
  - *ip xfrm state add src 192.168.1.42 dst 192.168.1.43 proto ah spi 0x4000 auth sha1 0xaaccddeeff00112233445566778899aabbccddeeff*
  - *ip xfrm policy add src 192.168.1.43 dst 192.168.1.42 dir out tmpl proto ah mode transport level required*
  - *ip xfrm policy add src 192.168.1.42 dst 192.168.1.43 dir in tmpl proto ah mode transport level required*
- ESP with AES-128-CBC and AH with HMAC-SHA1:
  - *ip xfrm state add src 192.168.1.43 dst 192.168.1.42 proto esp spi 0x1000 enc aes 0xaa22334455667788990aabbccddeeff*
  - *ip xfrm state add src 192.168.1.42 dst 192.168.1.43 proto esp spi 0x2000 enc aes 0xbb22334455667788990aabbccddeeff*
  - *ip xfrm state add src 192.168.1.43 dst 192.168.1.42 proto ah spi 0x3000 auth sha1 0xbbccddeeff00112233445566778899aabbccddeeff*
  - *ip xfrm state add src 192.168.1.42 dst 192.168.1.43 proto ah spi 0x4000 auth sha1 0xaaccddeeff00112233445566778899aabbccddeeff*
  - *ip xfrm policy add src 192.168.1.43 dst 192.168.1.42 dir out tmpl proto esp mode transport level required*
  - *ip xfrm policy add src 192.168.1.42 dst 192.168.1.43 dir in tmpl proto esp mode transport level required*

- *ip xfrm policy add src 192.168.1.43 dst 192.168.1.42 dir out tmpl proto ah mode transport level required*
- *ip xfrm policy add src 192.168.1.42 dst 192.168.1.43 dir in tmpl proto ah mode transport level required*

- ESP with AES-128-GCM (RFC-4106) Authenticated Encryption with Associated Data (AEAD).
  - *ip xfrm state add src 192.168.1.43 dst 192.168.1.42 proto esp spi 0x1000 aead rfc4106(gcm(aes)) 0xaa223344556677889900aabbccddeeff12345678 96*
  - *ip xfrm state add src 192.168.1.42 dst 192.168.1.43 proto esp spi 0x2000 aead rfc4106(gcm(aes)) 0xbb223344556677889900aabbccddeeff12345678 96*
  - *ip xfrm policy add src 192.168.1.43 dst 192.168.1.42 dir out tmpl proto esp mode transport level required*
  - *ip xfrm policy add src 192.168.1.42 dst 192.168.1.43 dir in tmpl proto esp mode transport level required*
- How many SAs and SPs do you need to define to implement the security mechanism 3 (above)?4
  - Sas and 2 Sps
- Which is the difference among the configurations 1 and 3 in terms of the structure of the IP packets obtained?

```
▾ Internet Protocol Version 4, Src: 172.22.16.169, Dst: 172.22.16.190
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 136
    Identification: 0x5f83 (24451)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: Encap Security Payload (50)
    Header Checksum: 0x612d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.22.16.169
    Destination Address: 172.22.16.190
▾ Encapsulating Security Payload
    ESP SPI: 0x00001000 (4096)
    ESP Sequence: 372
```

  - ip xfrm policy update src 172.22.16.169 dst 172.22.16.190 dir in tmpl proto esp mode transport

```
▾ Internet Protocol Version 4, Src: 172.22.16.169, Dst: 172.22.16.190
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 124
    Identification: 0xac2c (44076)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: Encap Security Payload (50)
    Header Checksum: 0x1490 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.22.16.169
    Destination Address: 172.22.16.190
▾ Encapsulating Security Payload
    ESP SPI: 0x00001000 (4096)
    ESP Sequence: 45
```

- ip xfrm policy update src 172.22.16.190 dst 172.22.16.169 dir out tmpl proto ah mode transport

```
▸ Internet Protocol Version 4, Src: 172.22.16.190, Dst: 172.22.16.169
▾ Authentication Header
    Next header: ICMP (1)
    Length: 4 (24 bytes)
    Reserved: 0000
    AH SPI: 0x00004000
    AH Sequence: 42
    AH ICV: 1cd7a24e90a58b5310c3e53d
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xb7db [correct]
    [Checksum Status: Good]
    Identifier (BE): 49931 (0xc30b)
    Identifier (LE): 3011 (0x0bc3)
    Sequence Number (BE): 19 (0x0013)
    Sequence Number (LE): 4864 (0x1300)
    Timestamp from icmp data: Dec  1, 2023 12:39:13.000000000 CET
    [Timestamp from icmp data (relative): -33.404614242 seconds]
```

- when is the configuration 2 useful?
  - It is useful when the purpose is to authenticate the packets and the intermediate nodes. Furthermore, it’s faster because it does not need to encrypt.
- what advantage do we have using the configuration 4?
  - With configuration 4 we have a single algorithm for encryption and integrity so low overhead, more efficiency and simpler to implement.
- Choose one of the previous configurations and modify the SPs so that to protect only the TCP protocol messages (and not the messages corresponding to the other protocols). Verify subsequently that the ping packets are not protected, while the TCP traffic remains protected (for example the HTTP traffic).
  - ip xfrm policy add proto tcp dir out priority 1 **(da testare)**

- Finally, indicate which information is contained in the SAD and in the SPD.
    - **Scattare uno screenshot del SAD e SPD**

Performance measurement

	10 KB	100 KB	1MB	10 MB	100 MB
			No IPsec/TLS		
time [s]	0,8	0,34	0,29	3,92	42,4
speed [kB/s]	12,5	288	3402	2493	2088
			ESP transport AES-128-CBC		
time [s]					
speed [kB/s]					
			ESP transport AES-128-CBC HMAC-SHA1		
time [s]					
speed [kB/s]					
			AH transport HMAC-SHA1		
time [s]					
speed [kB/s]					
			ESP AES-128-CBC + AH HMAC-SHA1		
time [s]					
speed [kB/s]					

- Now, execute the same performance measurements for the various IPsec configurations encountered in the previous exercises; write down the results in the Table 1, and compare them with the previous ones.