Expected : 86/100

Homework 4. Internetworking. EP2120 . Pierre FLEITZ

I) DNS: 23/30

a) Command used : dig +short –x 192.16.125.102
Result : mail.ssvl.kth.se.
Therefore, the domain name is mail.ssvl.kth.se. 5/5

b) We can divid the address into several zones of hierarchical way :
Zone 1 : .
Zone 2 : se.
Zone 3 : kth.se.
Zone 4 : ssvl.kth.se.
Zone 5 : mail.ssvl.kth.se.

With the command dig –x 192.16.125.102 we can have access to the AUTHORITY SECTION that gives us the domain names and IP addresses of the name servers for the zone :

- gaia.it.kth.se -> 130.237.212.6 10/15
- ns.ssvl.kth.se -> 192.16.124.50
- ns2.ssvl.kth.se -> 192.16.125.100

c) In order to find the delegations we use the command : dig +trace mail.ssvl.kth.se.

- root (".") delegates mail.ssvl.kth.se to 127.0.1.1 : .se
- se delegates mail.ssvl.kth to 202.12.27.33 (m.root-servers.net.): kth
- kth delegates mail.ssvl to 199.254.63.1 (j.ns.se.) : ssvl 8/10
- ssvl finds the result through 130.237.72.246 (a.ns.kth.se) : mail

II) IPsec : 13/15

a) IPsec provides differents security services :

- *Defining Algorithms and Keys :* The 2 entities that want to create a secure channel between themselves can agree on some avaible algorithms and keys to be used for security pruposes.
- *Packet Encryption :* The packet exchanged between 2 parties can be encrypted for privacy using one of the encryption algorithms and a shared key agreed upon ih the first step.

Note : This makes the packet sniffing attack useless !

- *Data Integrity :* Data integrity guarantees that the packet is not modified during the transmission. If the received packet does not pass the data integrity test, it is discarded.

Note : This prevents the packet modification attack.

- *Origin Authentication :* IPsec can authenticate the origin of the packet to be sure that the packet is not created by an imposter.

Note : This can prevent IP spoofing attack.

5/5

b) What to do when you receive an ESP encapsulated IP Packet : 3/5

1) Look up the Security Association based on the destination address and SPI (Security Parameter Index) -> If the packet is unsecured (there is no IPsec) then search through SPD (Security Policy Database) for match. -> If there is no matching entry OR if policy is PROTECTED or DISCARD then the packet is discarded.

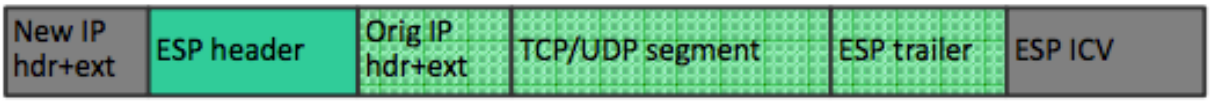
2) After that you need to find the algorithm, the algorithm key, the sequence number etc in the SA databased (reminder : SA determines how packets are processed : cryptography, algorithms, key, ESP (or AH) etc..). -> That's how the destination figures out what cryptographic to use to decrypt the packet.

3) Finally when finished decrypting the message, deliver packet to the next higher layer.

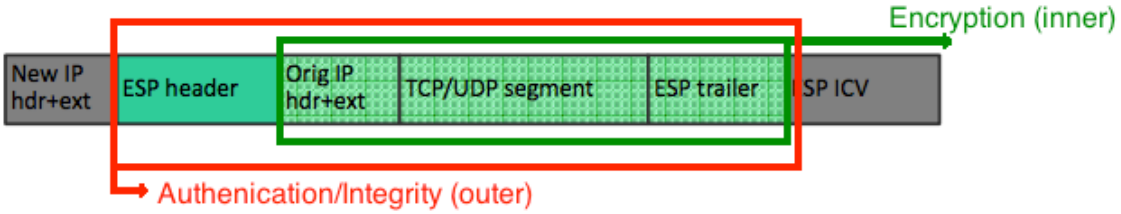
c) We can notice the presence of the « Orig IP hdr + ext » therefore this is tunnel mode.

5/5

Original packet :

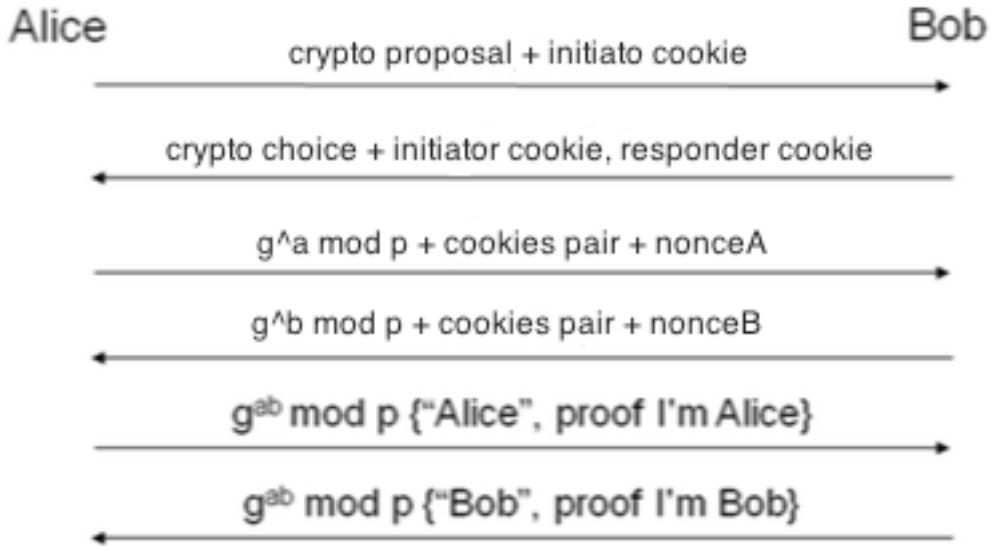


Redrawed packet to show how the differents parts of the packet can be protected :



III) IKE : 15/20

a) Cookies are used against denial-of-services attacks and Nonces are used against replay attack.
Redraw of the figure to show where to add cookies and nonces :



10/10

b) A stateless protocol is a communication protocol that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of request and response. In IKE it is achieved that way : Cookies ensure that the responder is stateless until initiator produced at least 2 messages :

5/10

- Responder's state is stored in an unforgetable cookie and sent to initiator.
- After initiator responds, cookie is regenerated and compared with the cookie returned by the initiator.

V) Firewalls : 15/15

We briefly discussed about 2 types of firewalls :

1) Packet-filter firewall : It can forward or block packets based on the information in the network layer and transport layer. A packet-filter firewall is a router that uses a filtering table to decide wich packets must be discarded (not forwarded).

But sometimes we need to filter a message based on the information avaible in the message itself, and that's why we have proxy firewalls !

2) Proxy firewall : A proxy firewall (also called Application firewall or Gateway firewall) will therefore protect network ressources by filtering message at the application layer : i tacts as an intermediary between in-house clients and servers on the internet but i twill not only intercept internet requests and responses it will also monitor incoming traffic for layer 7 protocol (http and ftp for example). In addition to determining wich traffic is allowed and wich traffic is denied, a proxy firewall uses

stateful inspection technology and deep packet inspection to analyse incoming traffic for signs of attack.

VI) NAT : 20/20

Packet 1 :

- src @ : 10.1.1.4
- src port : 2225 (randomly choosed)
- dest @ : 130.237.20.12
- dest port : 80

Packet 2 :

- src @ : 139.75.16.3
- src port : 4378 (randomly choosed again)
- dest @ : 130.237.20.12
- dest port : 80

NAT Translation Table	
WAN side addr (public)	LAN side addr (private)
139.75.16.3 , 4378	10.1.1.4 , 2225

Packet 3 :

- src @ : 130.237.20.12
- src port : 80
- dest @ : 139.75.16.3
- dest port : 4378

Packet 4 :

- src @ : 130.237.20.12
- src port : 80
- dest @ : 10.1.1.4
- dest port : 2225