EP2120 Internetworking/Internetteknik
IK2218 Internets protokoll och principer

Homework Assignment 4

Solutions due 17:00, October 8, 2015
Review due 17:00, October 12, 2015

Problems

1. DNS (30 p)

Use a tool such as "dig", together with your recently acquired knowledge about DNS, to answer the following questions. Important: whenever you answer with a domain name, it must be a Fully Qualified Domain Name (FQDN).

a) What is the domain name that corresponds to IP address "192.16.125.102"? Your answer should include the dig command you use. (5 p)

b) To which zone does it belong? Give all domain names and IP addresses of the name servers for the zone. What dig command(s) did you use? (15 p)

c) What are the delegations that lead to this zone? Give the full chain of delegations. For each step, specify the zone that it is delegated (as a domain name), and the zone from which it is delegated (as a domain name). *Hint: you will find "dig +trace" to be a useful command.* (10 p)

2. IPsec (15 p)

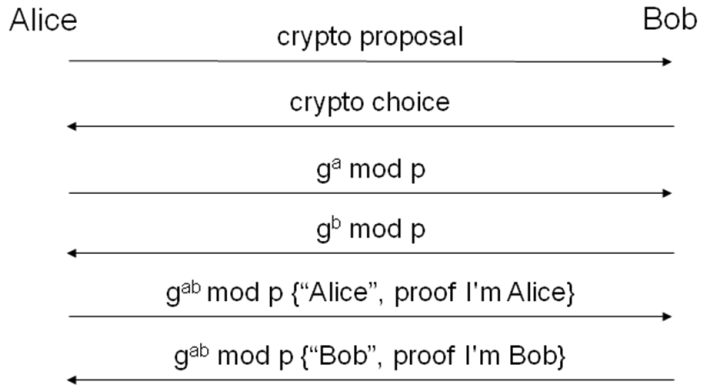
a) Briefly summarize the security services that IPsec provides. (5 p)

b) An ESP encapsulated IP packet arrives to the destination. Briefly describe how the destination figures out what cryptographic algorithm to use to decrypt the packet. (5 p)

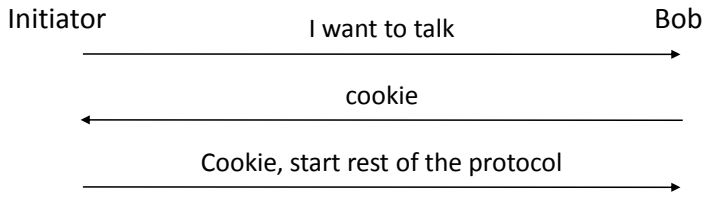
c) The packet below illustrates and IPv6 packet protected using IPsec. Is it tunnel mode or transport mode? Redraw the packet and show how the different parts of the packet can be protected using the services mentioned in a) above. (5 p)

3. IKE (20 p)

a) The following picture illustrates the general idea for IKE phase-1 protocols, main mode. Note that the message exchange is simplified in several ways.

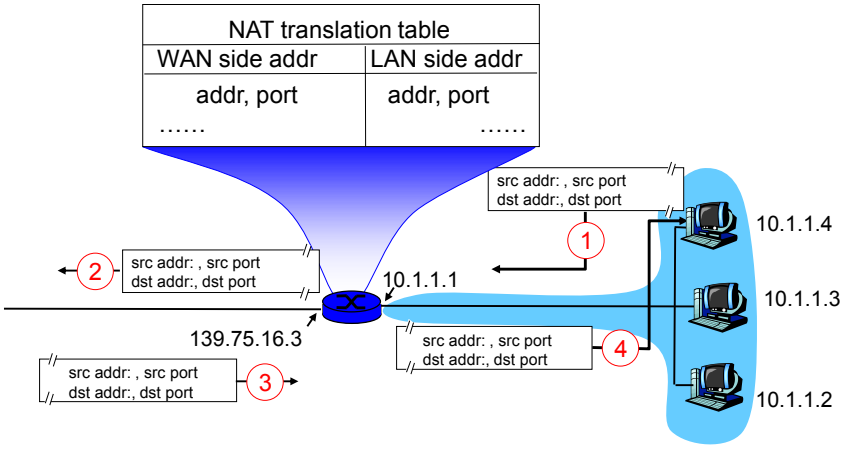


To protect against certain attacks, cookies and nonces are used in IKE. Redraw the figure and show where to add cookies and nonces. Against what type of attack are cookies used? Against what type of attack are nonces used? (10p)
Cookies are used in IKE to protect against denial-of-service attacks where an impostor launches packets with forged IP source addresses, according to the simple illustration below. The cookies used should be *stateless*. What does this mean and how is it achieved in IKE? (10p)



4. Firewalls (15 p)
We have discussed two types of firewalls. Mention these two types and briefly describe how they work.

5. NAT (20 p)
Consider the figure below. Assume that host 10.1.1.4 on a private network (10.1.1.0/24) sends an HTTP request through its NAT box to a web server on address 130.237.20.12 and that this web server answers with an HTTP response back to the host. Fill in source address, source port, destination address, and destination port in the IP packets 1-4 in the figure. Also, fill in the NAT table as it will look when the four packets have been exchanged.


NAT translation table
WAN side addr
LAN side addr
addr, port
addr, port
……
……
src addr: , src port
dst addr:, dst port
1
10.1.1.4
2
src addr: , src port
dst addr:, dst port
10.1.1.1
10.1.1.3
139.75.16.3
src addr: , src port
dst addr:, dst port
4
3
src addr: , src port
dst addr:, dst port
10.1.1.2