EP2120 Internetworking/Internetteknik
IK2218 Internets protokoll och principer

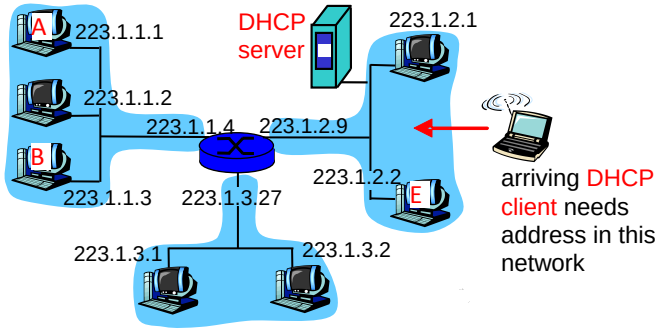
Homework Assignment 4

Solutions due 17:00, October 14, 2016
Review due 17:00, October 18, 2016

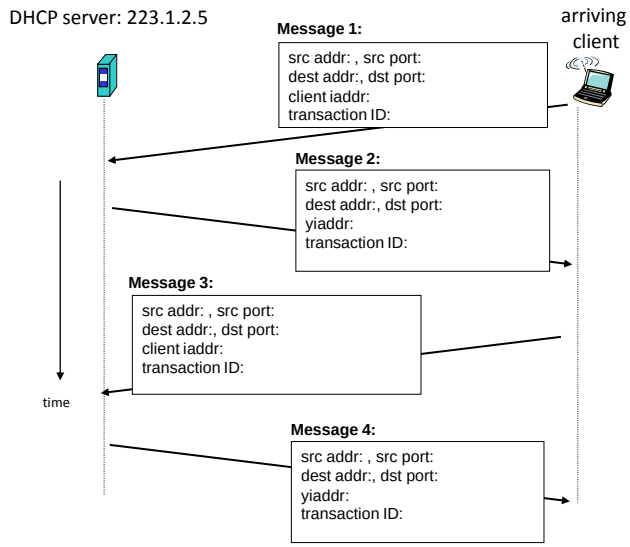
Problems

1. DHCP (20 p)

Consider the following scenario, where a DHCP client arrives and requests an IP address from the DCHP server.



In the simplest case, four DHCP messages will be exchanged according to the figure below. Name these four DHCP messages (message type) and fill in the missing fields in each message. You can assume that the subnet to which the DHCP client arrives is a /24 network and that all addresses below 223.1.2.10 are occupied. Based on that, you can let the DHCP server hand out a suitable IP address. You also have to select reasonable transaction IDs.



2. IPv6 autoconfiguration (10 p)

In IPv6 stateless autoconfiguration, the client can create an IP address based on its MAC address instead of requesting it from a DHCP server. Discuss advantages and problems with using an IPv6 address generated from the MAC address and explain how IPv6 privacy extensions address the problems.

3. IPsec (15 p)

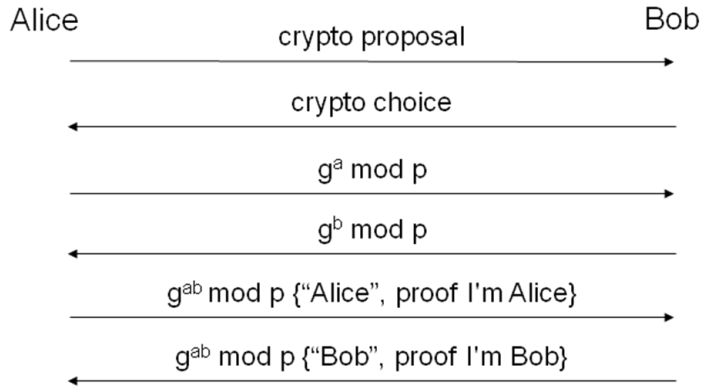
a) Draw an IP packet where IPsec AH (Authentication Header) is used in transport mode. You don't need to show any header fields, just headers/trailers and payload. (5 p)

b) Draw an IP packet where IPsec ESP (Encapsulated Security Payload) is used in tunnel mode for both encryption and authentication. You don't need to show any header fields, just headers/trailers and payload. Mark the parts of the IP packet that are encrypted and the parts that are authenticated. (5 p)

c) 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)

4. 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)

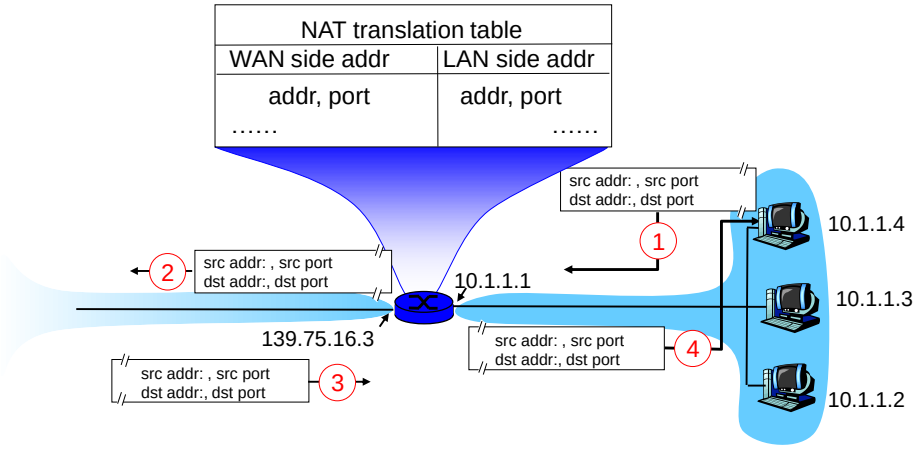
b) Briefly explain *how* the use of a cookie helps against the attack you mentioned in your answer to a) above. Furthermore, the cookies used in IKE should be *stateless*. What does this mean and how is it achieved in IKE? (10p)

5. Firewalls (15 p)

Firewalls can be placed in a number of different places, providing different protection. Give at least three examples of places where deploying firewalls is motivated, and explain the motivation for placing them there.

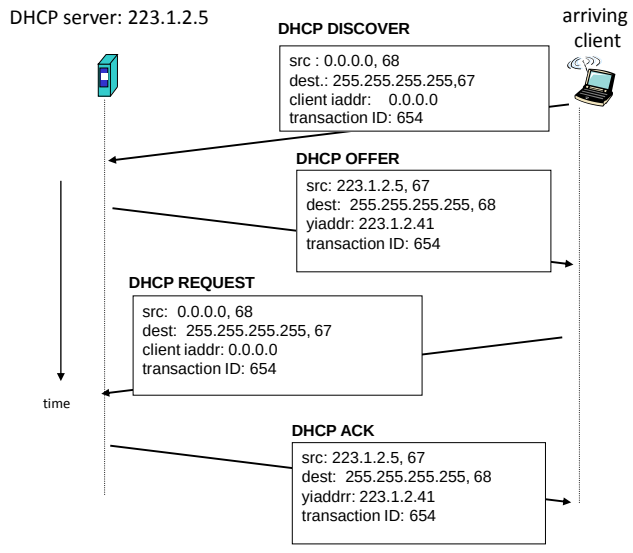
6. NAT (20 p)

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.



Solutions

1. Valid IP addresses for yiaddr from server are 223.1.2.10-223.1.2.254. Transaction ID should be the same value for all four messages (DHCP DISCOVER, DHCP OFFER, DHCP REQUEST, and DHCP ACK).



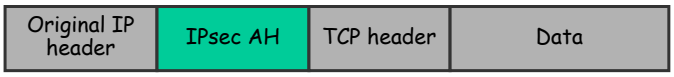
1

2. IPv6 autoconfiguration

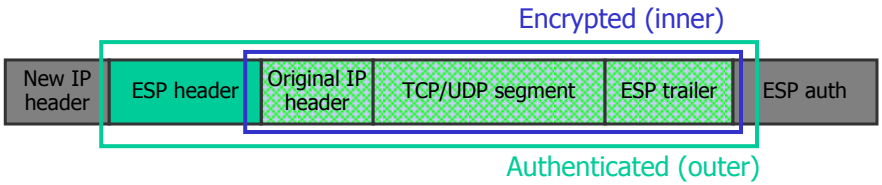
A MAC-derived IPv6 address is a straight forward way to generate a unique IP address automatically and L3/L2 address translation can be done locally by the sender (no ARP needed). The problem is that the MAC address reveals information about the interface card, such as identity and vendor of the interface card so that e.g. potential bugs could be exploited. IPv6 privacy extensions solve this problem by using a randomly assigned interface ID instead and this number can change over time (temporal address).

3. IPsec

a) See below:



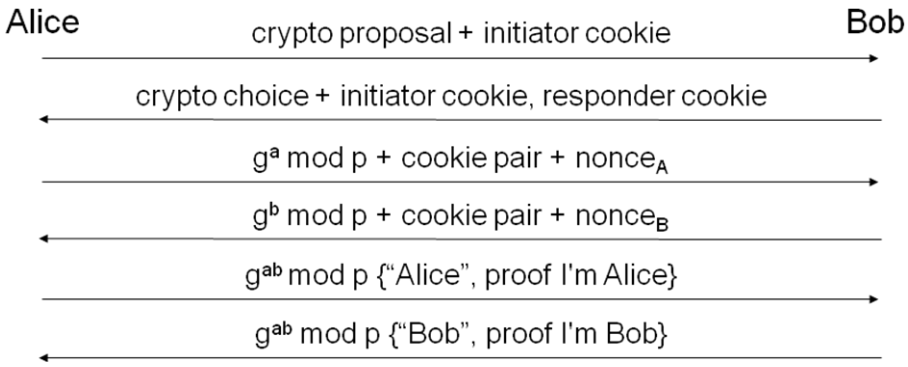
b) See below:



c) The receiver needs to lookup the correct SA (Security Association) in the security association database, and the SA will contain information about the cryptographic algorithm. The SA lookup is based on the {SPI, destination IP address, flags} retrieved from the ESP encapsulated IP packet.

4. IKE

a) Cookies are used to protect against denial-of-service attacks. Nonces are used to protect against replay attacks.



b) When Bob has sent a cookie to the initiator, he will not continue the execution until he receives the same cookie from the initiator. In a DoS attack, there could be a large amount of fake initiators and the cookies should be stateless so that "Bob" doesn't have to keep track of all cookies he has sent. A stateless cookie can be created by doing a hash of the initiator's IP address and a single secret number that Bob uses: hash(Initiator's IP addr, Bob's secret)

5. Firewalls

1. On the host itself, i.e., a *personal firewall*. Common in operating systems. Placed here to protect the host itself, and to regulate access to and from the host. Because you may still want to be able to access, e.g., shared filesystems etc, on the LAN, this firewall is often more permissive than other firewalls.

2. Between the host and the rest of the Internet. This is the classic firewall, protecting the LAN from outside threats and especially access to services used on the LAN which are not meant to be accessed from the outside, such as printers, file servers etc. It may also serve to limit access from the LAN to the outside (e.g., corporate firewalls limiting access for the employees, national firewalls preventing access to pages belonging to political dissenters).
3. Between departments and LANs inside a company. Sometimes done because some departments are more sensitive (payroll), but it is also a good practice in general to compartmentalize access, since this means that even if an attacker gets into a corporate LAN, they do not have unlimited access.

6. NAT