

Computer Networking and IT Security (INHN0012)

Tutorial 13

Problem 1 DNS Zonefile

You are a student assistant at the chair and have been given the task of creating a zone file for grnvs.net.. Relevant servers and their domain names and IP addresses are shown in Figure 1.1.

Fill in the following template so that the requirements of the individual subtasks are fulfilled. Enter the letter of the corresponding subtask in the box at the end of each line.

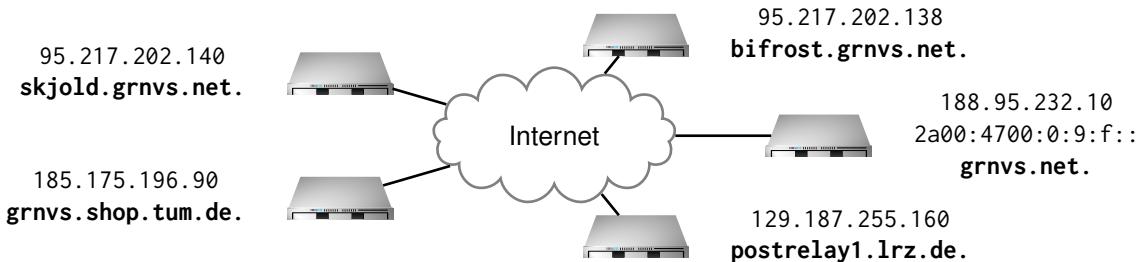


Figure 1.1: Servers relevant for the zone grnvs.net. with domain names and IP addresses

grnvs.net.	600 IN SOA	bifrost.grnvs.net. 164214 3600 900 604800 900	moepi.grnvs.net.	
grnvs.net.	NS	bifrost.grnvs.net.	a)	
grnvs.net.	A	188.95.232.10	c)	

a)* The primary name server of the zone is bifrost.grnvs.net and is already entered. For fault tolerance, the server reachable under skjold.grnvs.net shall act as the secondary name server.

b)* Ensure that the name servers are reachable under their respective IP addresses.

c)* When accessing grnvs.net in the browser, the GRNVS website should be displayed. This currently only works for IPv4; it should also be reachable via IPv6.

d)* In order for students to send an email to info@grnvs.net, a mail server must be configured. To avoid operating one yourself, the LRZ email service Postrelay shall be used with priority 10.

e)* In the next semester, merchandise and bonus points will be sold in a webshop. To avoid operating an online shop, a cooperation with the TUM Shop has been arranged. For access, shop.grnvs.net shall serve as an alias for grnvs.shop.tum.de.

f)* Why is it not possible to configure grnvs.net.in.tum.de. as an alias for grnvs.net. in this zone file?

Problem 2 Alice in Cryptoland

Alice and Bob want to securely communicate over an insecure channel. Therefore, they want to define a means of message transportation that provides authenticity, integrity, and confidentiality.

Alice has come up with a scheme for a protocol. It is a hybrid scheme: both parties possess a keypair which is used to exchange a shared key. This key is then used for symmetric encryption after the initial exchange is completed. Since Alice and Bob don't know each other's public keys yet, the protocol includes them in the initial handshake.

To initiate the communication, the requesting party sends a message request which contains their public key. The requestee responds with the freshly generated secret k as well as their public key. The message containing k is encrypted with the requesting party's public key that was received in the first message. The exchange is completed by an acknowledgement by the requesting party, encrypted with the requestee's public key.

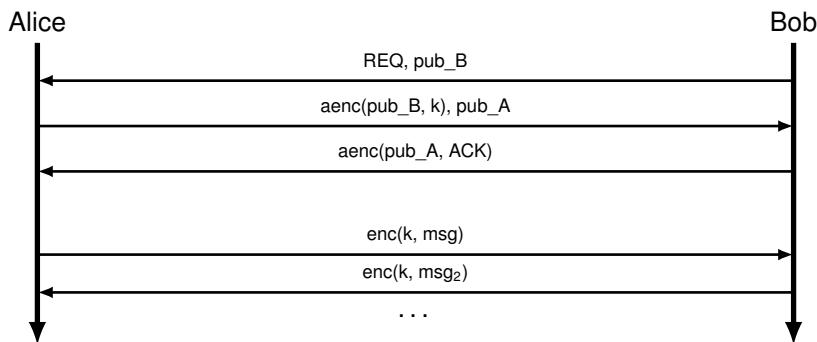
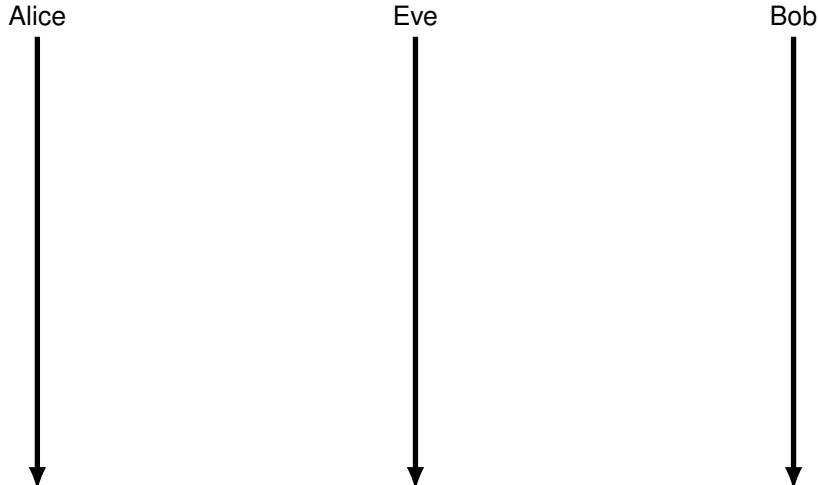


Figure 2.1: The communication protocol proposed by Alice.

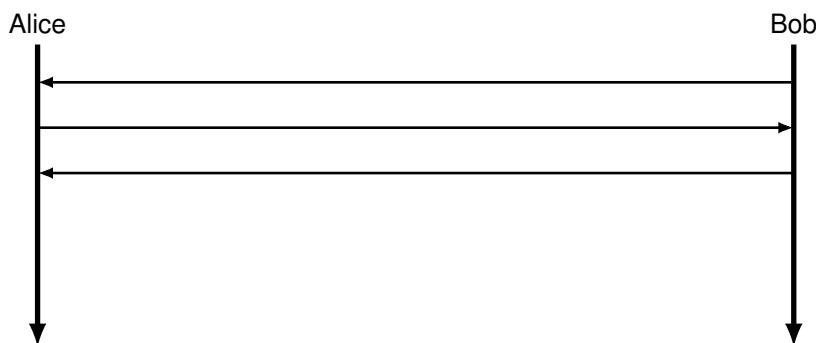
For this task, assume an active man-in-the-middle attacker Eve, who can see and tamper with all traffic between Alice and Bob. You can use the following primitives: `hash(msg)`, `sign(asymm_key, msg)`, `MAC(key, msg)`, `aenc(asymm_key, msg)` and `adec(asymm_key, msg)` for asymmetric cryptography as well as `enc(key, msg)` and `dec(key, msg)` for symmetric cryptography primitives. $x \mid y$ denotes the concatenation of x and y .

a)* Is this protocol secure? If not, list what it is vulnerable to.

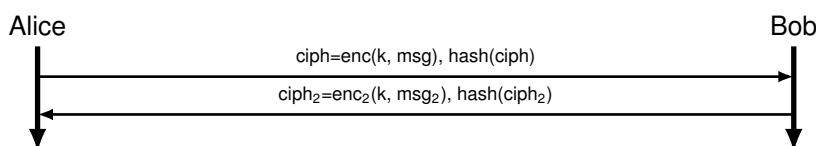
b)* Eve wants to eavesdrop on the encrypted messages exchanged. Sketch how Eve can manipulate the key exchange in order to retrieve k. Assume that Bob initiates the communication. Use the key exchange from Alice's protocol in Figure 2.1.



c) Extend Alice's protocol to enable authenticity and integrity protection for the key exchange, thereby preventing Eve from getting the key. How can you solve the problem that Bob initially does not know and trust Alice's key?



d) Alice proposes the following as integrity protection. Evaluate Alice's proposal.



In the following tasks, assume that Bob and Alice have exchanged their public keys through a secure channel in advance.

e) The protocol provides neither integrity nor authenticity for data messages exchanged after k has been established. Extend the protocol with a MAC scheme to protect the messages.

Alice and Bob have defined a key exchange that provides authenticity and integrity protection as shown below. Thereby, Eve cannot eavesdrop on the key and therefore cannot decrypt the following symmetrically encrypted data messages.

f) Modify your so-far proposed protocol such that replays are detected.

