Exercise 5

Exercises Peer-to-Peer-Systems and Security (SS2011)

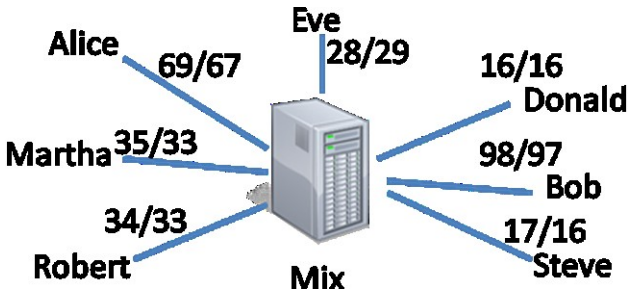
Monday 11.7 2011
Hand-in: Monday 18.7. 2011 in lecture or per mail
Exercise: Thursday 21.7. (together with lecture)

Dr. Heiko Niedermayer
Lehrstuhl für Netzarchitekturen und Netzdienste
Technische Universität München

Rules: There will be five exercise sheets. You have to hand-in 70 % of the assignments, attend atleast 3 exercise courses and present a solution in the exercise course to get the 0.3 bonus..

Task 1 Anonymity / Encryption
Some questions with short answers.

a) Assume that Alice, Bob, and Cleta use SSL to communicate with each other. Alice sends a message via SSL to Bob and Bob forwards it via SSL to Cleta. Does the message look the same on both paths (Alice→Bob, Bob→ Cleta) for a global observer? Is this true for all properties of the message?
b) Now look at the following graph. A passive observer was able to observe all communication around a mix (some anonymity system that makes packets unlinkable). All packets are perfectly encrypted and when passing the mix they are re-encrypted by the mix. The observer counted how many packets the entity sent to the mix (first number) and how many packets the mix sent to the entity (second number). Can you still guess who communicates with whom?



Task 2 Eclipse Attack on Chord
Assume that you want to attack a node in Chord and eclipse it from the rest of the network. You have as many resources as you like, but significantly less than 50 % of all nodes.

a) What do you have to do to be able to intercept all of his outgoing messages to other nodes? (Eclipse the outgoing links)
b) What do you have to do to prevent packets towards the node reach the node? (Eclipse ingoing links)

Task 3 Eclipse Attack on Kademlia
Assume that you want to attack a node in Kademlia and eclipse it from the rest of the network. This is a bit harder than in Chord and will most likely be less perfect. You have as many resources as you like, but significantly less than 50 % of all nodes.

a) What do you have to do to be able to intercept his outgoing messages to other nodes? (Eclipse the outgoing links)
b) What do you have to do to prevent packets towards the node reach the node? (Eclipse ingoing links)

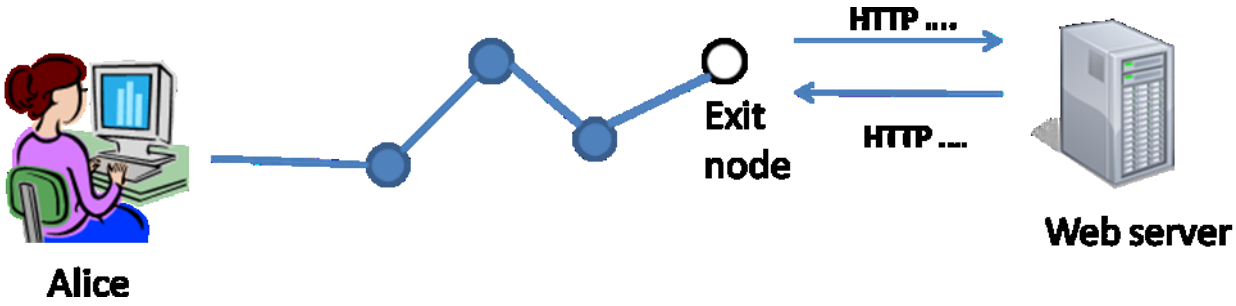
Task 4 Bootstrap Tree and Social Network Graph

In the lecture we discussed defences against Sybil and Eclipse attack based on the bootstrap graph and based on social network graphs. Brief answers are sufficient.

a) Why is it not possible to *only* use the bootstrap graph to route to a certain ID (node with certain ID)?
b) Why is it not possible to *only* use the social network graph to route to a certain ID (node with certain ID)?
c) How could you use either the bootstrap graph or the social network graph in your normal DHT routing to defend against routing attacks?

Task 5 Exit Nodes and Anonymity

The following graph sketches the situation:



Alice is using an anonymity system (like Tor) to access a web server. Lets assume the communication within the anonymity system along the dark thick lines is all-encrypted and highly secure and anonymous. To exit the anonymity network towards the normal Internet, exit nodes are used in such systems. The exit node (white node) operates as proxy that executes the HTTP requests to the web server for Alice.

Question: How can this so-called exit node attack Alice's private data or break her anonymity if she is not careful? (Hint: consider what the exit node can read)