Exercise 4

Exercises Peer-to-Peer-Systems and Security (SS2012)

Thursday 28.6 2012
Hand-in: Thursday 5.7. 2012 in lecture or per mail
Exercise: Monday 9.7. 2012

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

Task 1 Authentication

In this task we specify a cryptographic protocol which is meant to be used for mutual authentication.

a) Specify on what information and when in the protocol do the entities A,B, and S detect a successful authentication run?
b) The protocol is insecure. Find an attack. (The strength of the attacker is that it can read, send, fake, and drop messages in the network, yet it cannot break cryptography. This is a common security model in network security.)

Hint: Use information from previous runs to attack the protocol. Sig_X stands for encryption with private key.

Protocol:

Prerequisites: S is TTP and for each participant X S knows the corresponding public key PK_X. All participants know the public key PK_S of S.
Let kab = hash(Na,Nb).
Protocol:

```
A -> S: A, Enc_PK_S(Na, B)
S -> A: PK_B, Enc_PK_A(Sig_S(Na, A))
A -> B: Enc_PK_B(Na, A, B, Sig_S(Na, A))
B -> A: Nb, {Na}kab
A -> B: {Nb}kab
```

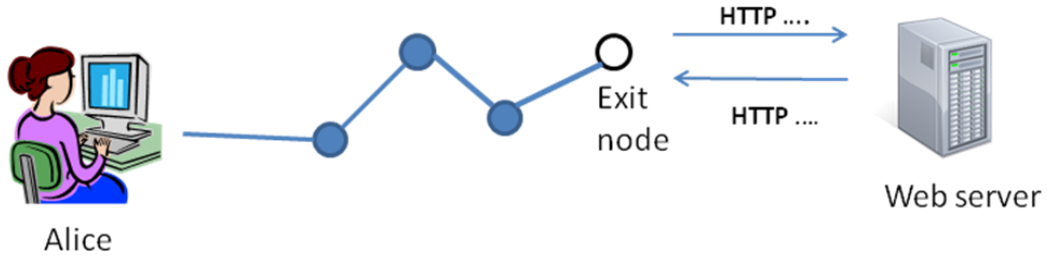
Task 2 Some questions

Answer the questions with knowledge from the lecture.

a) Cryptographic identities seem to make authentication a lot easier. Let assume, we use cryptographic identities. Do we still need a Certificate Authority? If yes, for what? If no, why not?
b) Why is trust important for key distribution?
c) Why does Zfone or SSH in the Baby Duck model not simply use a conventional authentication protocol like in SSL to authenticate the communication partners? What problem do they try to resolve?

--- continues on next page ---

The following graph sketches the situation for 2d):



d) 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)

Task 3 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 4 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 5 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?