Exercise 4

Exercises Peer-to-Peer-Systems and Security (SS2010)

Monday 14.6 2010
Hand-in: Monday 28.6. 2010 in lecture or per mail
Exercise: to be announced

Dipl.-Inform. Heiko Niedermayer
Lehrstuhl für Netzarchitekturen und Netzdienste
Technische Universität München

<u>Rules:</u> There will be five exercise sheets with each 10 points. You have to achieve 50 % of the points and present a solution in the exercise course to get the 0.3 bonus.

Task 1 (2 Points) Eclipse Attack

In this task we discuss node and data eclipse.

a) It is possible in Chord to eclipse a node for messages to the node with one other node. Where do you need to position yourself as attacker and describe why this is the case?

b) Why is data eclipse trivial in standard DHTs like Chord (in the lecture we have seen that it is not easy in the KAD network)?

Task 2 (2 Points) 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.)

Protocol for Task 2:

Prerequisites:
S is a TTP.
Each participant X has a shared key with S. This key is called k kXS.
Let kab = Nb.
Protocol:

```
A -> B: Na, A
B -> S: Na, A, B,{Nb}kBS
S -> A: B, {Na, Nb}kAS
A -> B: {Nb}kab
```

Task 3 (2 Points) Authentication

Do the same as in task 2, yet with a different protocol. Hint: Use information from previous runs to attack the protocol. Sig_X stands for encryption with private key.

Prerequesites: 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 4 (2 Points) Some questions

Anwer the questions with knowledge from the lecture..

a) Cryptographic identities seem to make authentication a lot easier. Lets 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 to authenticate the communication partners? What problem do they try to resolve?

Task 5 (2 Punkte) Sybil Attack

In the lecture, we introduced the sybil attack.

a) Why is the sybil attack fatal for the security of a Peer-to-Peer network?

b) Does requiring an email address prevent nodes from launching a sybil attack?

c) How could an attacker profit from a sybil attack in an auction site with a reputation system like Ebay?