Security on the Internet, summer 2006

MICHAEL NÜSKEN

2. Exercise sheet
Hand in solutions on Tuesday, 2nd of Mai, at the b-it info desk.
Deadline for key server signatures is the same Tuesday, 23:59.

Exercise 2.1 (Signature verification). (4 points)

You got two mails with the subjects `[SotI] PGP signed mail` and `[SotI] Thawte signed mail`. Consider the signature verification for each of them.

(i) Describe the steps that you need to perform in order to verify the PGP signature. [2]

(ii) Describe the steps that you need to perform in order to verify the S/MIME signature. [2]

Exercise 2.2 (Trust model). (7 points)

(i) The fingerprint of my PGP key is [3]

```
E49D 218D B622 51E0 DE04 DF1E 7142 20BB A085 1EB4
```

Find my key in your key management tool, after verification give it some or full trust, sign and submit your decision to the key server. (Make sure that things are visible on the server! Join with your fellow students to synchronize you.)

Find the fingerprint of your own PGP key. Write it down (on paper!) so that I can do the above for you.

(ii) My Thawte certificate has the serial number `41:CD:2D:35:37:92:B0:DE:DF:5D:8A:80:42:D5:B2:10`. Verify it.

`95:80:D5:DA:DE:0A:59:2E:0B:B6:06:5C:71:D2:A2:D5:F4:EE:62:0E` is the SHA1-fingerprint of my Thawte certificate changed at one position. Determine that position. [1]

`AE:7A:F2:17:1E:11:B2:9D:DF:4D:D5:74:C8:17:00:C4` is the MD5-fingerprint of my Thawte certificate changed at one position. Determine that position. [1]

(iii) Can you "tell" the world that you trust my Thawte key? Does the trust model give you a way of doing so? If that is not possible, what can you do? What is "WOT"? [2]