Security on the Internet, winter 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

1. Exercise sheet
Hand in solutions until Monday, 3 November 2008.

For future exercises it might be important to use b-it computers. So please register an account for the b-it. (Ask at the infodesk for the procedure.)

A word on the exercises. They are important. Of course, you know that. Just as an additional motivation, you will get a bonus for the final exam if you earn more than 60% or even more than 80% of the credits. The bonus does not help passing the exam, but if you pass the bonus will increase your mark by up to two thirds.

Exercise 1.1 (Secure email). (6 points)

(i) Send a digitally signed email with the subject "`[08ws-soti] hello`" (without the quotation marks) to us at [4]

`08ws-soti@bit.uni-bonn.de`

from your personal account. The signature must be verifiable and correct. [It is a good idea to verify this by sending a blind carbon copy (Bcc) to oneself.]

With Thunderbird I recommend using `enigmail` and `gpg`. In any case make sure to register your key eg. at `http://wwwkeys.de.pgp.net/`.

Choose yourself among this and possible other solutions. In any case use a pgp key pair.

Note: Future exercise hand-ins will only be accepted via signed email. Then a bonus point will be awarded for a correct signature and a malus for a missing or invalid signature.

(ii) Send a second email with the subject "`[08ws-soti] student id`" containing your student identification number. (How should that be secured?) You have only one trial here! [If you need testing then test with yourself or with a friend.] [2]

Deadline for earning these credits: Monday, 3 November 2008, 23:59:59 (valid timestamp of your emails).

Exercise 1.2 (Trust). (4 points)

[2] (i) Find the fingerprint of your own PGP key. Bring two printouts of it to the next tutorial. (Do not send us an email with it. Guess, why!)

[2] (ii) Sign our two keys: The corresponding fingerprints of our PGP keys are

```
F753 FA1F 70C8 0B4A 0181 8B50 B6EF 9CA3 B967 0465
```

and

```
FC11 51FB 995E 58A0 186B B701 306A DAFE 965F 1E54
```

Find our keys 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.)

Additionally, sign your collegues' public keys using the authenticated list that we will distribute as soon as possible.