Advanced cryptography: Cloud & More, winter 2013/14

MICHAEL NÜSKEN

1. Exercise sheet
Hand in solutions until Wednesday, 6 November 2013, 23:59

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. You need 50% of the credits to be admitted to the final exam. As an additional motivation, you will get a bonus for the final exam if you earn more than 70% or even more than 90% 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). (4 points)

(i) Send a digitally signed email with the subject 2

`[13ws-ac] hello`

to me at

`nuesken@bit.uni-bonn.de`

from your personal account. The body of your email must be nonempty and 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 at `http://pgp.mit.edu/`.

Choose yourself among this solution and possible others. In any case use a pgp key pair.

(ii) Find the fingerprint of your own PGP key. Bring two printouts of it and an identification document to the next tutorial. (Do not send an email with it. Guess, why!) 2

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.

Exercise 1.2 (Privacy?). (4 points)

4 Check the electronic frontier foundation's web page `https://panopticlick.eff.org/`. How unique is your browser? Discuss user privacy related to this observation.

Exercise 1.3 (Cloud vendors). (6 points)

6 Pick one cloud provider, eg. AT&T, Amazon, BitRefinery, Google, HP, Lunacloud, Microsoft Azure, Nephoscale, OpSource, Rackspace, Salesforce, Softlayer, Terremark, Tier3, ...

- What kind of services does it offer?
- What do they advertise and promise?
- How much usage is for free?
- Which cloud software are they using? Is it open-source?
- Where are the computing centers?
- Who is using it?