

Advanced cryptography: Cloud & More,
winter 2013/14
MICHAEL NÜSKEN

4. Exercise sheet

Hand in solutions until Wednesday, 27 November 2013, 23:59

Exercise 4.1 (Data protection and transport paths). (8+6 points)

Find out on which path packets are transported:

- (i) Use traceroute (Windows: tracert) and a tool for IP to location to determine the geographic path from your home location to your favourite cloud provider. (For some targets no information can be obtained beyond entering the backbone. If you cannot obtain reasonable information, state that and pick a more open target.) 6

Hints: You may use

- <http://www.iplocation.net/index.php>,
- <http://www.spy-ip.com/>,
- <http://whatismyipaddress.com/ip/> or
- <http://www.geobytes.com/IpLocator.htm>

find a geographic location from an IP.

From which data can the geographic location of an IP be determined? +2
How precise is that?

- (ii) Can you find a target IP where the traffic is routed from a country in Europe to the US and back to the same country? +4
- (iii) Why may it be important to know the path of a transmission for a (cloud) user operating with data subject to some data protection law? 2

Exercise 4.2 (Confidentialty and integrity).

(8+4 points)

Consult the documentation of your favourite cloud service provider.

(i) Which provider and which service do you consider?

4 (ii) What kind of confidentiality protection is automatically provided? Distinguish the phases: during upload/download, during storage, during computation, during communication (in particular, user data transfer!).

4 (iii) What kind of integrity protection is automatically provided? Distinguish the phases: during upload/download, during storage, during computation, during communication (in particular, user data transfer!).

+4 (iv) What additional possibilities are provided or recommended?

