Advanced cryptography: Cloud & More, winter 2013/14

MICHAEL NÜSKEN

3. Exercise sheet
Hand in solutions until Wednesday, 20 November 2013, 23:59

Exercise 3.1 (SSL/TLS status). (16 points)

Many operations for clouds can be done via web interfaces. These are typically secured by SSL/TLS. Consider

- `https://www.trustworthyinternet.org/ssl-pulse/`,
- `http://www.isg.rhul.ac.uk/tls/`, and
- `http://www.isg.rhul.ac.uk/tls/Lucky13.html`.

(i) Which versions of SSL/TLS are used? Which ones are widely used, which ones should? [2]

(ii) Discuss briefly the most prominent attacks: [4]

- BEAST, CRIME, Lucky13,
- attack on RC4.

(iii) Describe how to disable RC4 in your favorite web browser. (You may want to check `https://cc.dcsec.uni-hannover.de/` to see what your browser offers.) [2]

(iv) Check your favorite high-security target (for example, an online banking site) at SSL pulse. Interpret the results. Would you feel safe with them? [4]

(v) Find out a reasonable value for the Apache parameter `SSLCipherSuite`. Print the answer of `openssl ciphers -v 'MY-REASONABLE-VALUE'` and explain your choice. [4]

Exercise 3.2 (Authentication). (7+3 points)

Authentication factors can be grouped into ownership factors like your identity card, knowledge factors like a password and inherence factors like a signature.

(i) Give an additional example for each group. 3

4 (ii) Discuss reasonable combinations for two-factor authentication of

(a) a cloud administrator, or

(b) a cloud customer.

+3 (iii) What does single sign on provide? Describe the basic idea for their realization.