Advanced cryptography: Cloud & More, winter 2013/14

MICHAEL NÜSKEN

2. Exercise sheet
Hand in solutions until Wednesday, 13 November 2013, 23:59

Exercise 2.1 ("IT-Grundschutz"). (20 points)

At

`https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html`

you find the BSI documents about IT-Grundschutz [basic protection for IT]. Say, you are the Security Officer responsible for setting up a computing centre for a new cloud for a government-secure voice phone service. (Speculate where additional information is needed.)

(i) Consider the threats catalogue and name at least one example of a threat that [6]

- (a) is a natural disaster.
- (b) maybe seen as a random attack.
- (c) is a human factor.
- (d) is an intentional attack.
- (e) is an internal attack.
- (f) is an availability issue.

Now we turn to BSI 100-2.

(ii) What are your first steps for the security process? [2]

(iii) Illustrate the security risks and effects of security incidents. [4]

(iv) Illustrate the processing of a phone call: which data has to be handled, classify in short-term and long-term data? Which long-term data must be available? When is short-term data it created, stored, modified, deleted? [4]

(v) Sketch a security policy. (At most half a page.) [4]

Exercise 2.2 (DDoS). (8+4 points)

Have a look at the Digital Attack Map by Google Ideas and Arbor Networks at `http://www.digitalattackmap.com/`.

[1] (i) Where does the data come from?

[1] (ii) Does an attack's source country indicate the location of the attacker?

Find the attack with the largest peak data rate observed during the last two month.

[1] (iii) When did it occur and how long did it endure?

[1] (iv) What type of attack was it?

[1] (v) What has been its target?

[1] (vi) Which port(s) were attacked?

[2] (vii) Are these port(s) registered? For which application?

[+2] (viii) Was it an attack?

And finally:

[+2] (ix) What can individual sites do to protect themselves from DDoS attacks?