Homework

Information Security II

Summer Term 2018

17 May 2018

1) SPA of RSA Using CRT (3, 1 Points) Assume that there exists a side channel in RSA decryption using CRT that, if the most-significant bits of the input x (down to about half the size of x) are zero, reveals if:

$$x \mod p > x \mod q.$$

1.a. How can you learn the secret key by repeatedly using this side channel?

1.b. Can proper verification of padding after RSA decryption protect against active attacks?

2) No Covert Channel? (4 Points) Some military officers want to prevent every covert channel and thus build a datacenter in a hermetically sealed building (this means, there is no data connection to the outside and it is not possible to see variations in electro-magnetic radiation or measure sound). They pay attention that the power consumption of the datacenter is constant over time and defective computers will not be sent to the manufacturer for repair, but will be replaced with new ones. Furthermore, the personell of the datacenter is selected in such a way that they would rather die than disclosing information. They claim that not a single bit will leave the datacenter.

2.a. Can you still think of a covert channel?

2.b. What is the capacity of this channel?

(Assume that computers fail on average every 10 years.)

3) PINs, Pollen, Probability (Part II) (1, 3, 1 Points) Consider a key pad that gives you access to a building. You know that one 5-digit PIN is used, but you can see from the key pad that only 4 keys are worn off.

3.a. How many trials do you need on average to open the door without prior knowledge of the PIN?

3.b. It's springtime and pollen are everywhere. How and by how much can you reduce the number of trials if you can selectively wipe keys before a person enters the building and inspect the key pad thereafter? Assume that the person uses only one finger. If this finger has first touched a dusty key, traces of the dust will be visible on all subsequently pressed clean keys.

3.c. How would you proceed if only 3 keys were worn off?

4) Game Theory (1, 2, 2, 1, 1 Points) Assume the following situation to be modeled as a one-shot game: two system administrators keep their `ssh` private keys on their laptops. These keys grant access to the server on which the company secrets are stored. Each of the system administrators can decide to either connect his laptop to the Internet or to have it air-gapped (from the Internet). There is no way for the company or the other system administrator to find out if a laptop was always air-gapped or not.

Internet connection allows the respective system administrator to play Minecraft online, which adds utility of $+1.5$ for the system administrator. But, if a laptop is connected to the Internet, there is a risk of 20 % that an attacker steals the private key and compromises the server. If such an incident happens, the company's digital forensics team can find out with probability 75 % which key was used. In that case, the responsible system administrator loses his job. If the company cannot find the responsible party, both system administrators are fired. Assume that losing the job "adds" utility of -7 for the system administrator.

4.a. Formulate the utility functions for the players.

4.b. Specify the game in matrix form.

4.c. Find the Nash equilibria (if any) and the social optima of the game.

4.d. Which canonical game applies in this situation?

4.e. Would you apply for the job?

Submission Instructions Please combine your solution into a single legible PDF file (preferably no scans of hand-written notes) and hand it in via OLAT no later than **23 May 2018, 23:59h**.

Grading Information The grade of this assignment counts 20 % of the final proseminar grade. So, every point of this sheet corresponds to 1% of your overall grade. Full points are only given for a detailed derivation of the solution.