Homework

Information Security II

Julia Wanker

23 May 2018

// TODO: check all

1 SPA of RSA Using CRT

// TODO

1.1 Learn Secret

We can observe the result of $x \bmod p < x \bmod q$. So we choose x to be equal to 0 (where $x \bmod p < x \bmod q$ will be false) and reqeatedly set the least significant bits to 1 (up to about half the size of x) and check when $x \bmod p < x \bmod q$ gets true. This x then is our chosen ciphertext. We don't know whether p or q is larger at this point.

!!! need to find p or q here in order to find n and with p or q and n we can compute p or q and further d – didn't have a good idea of how one could do this yet.. maybe one could use the chosen x in some way for p or q - need to further think about that !!!

1.2 Protection through Padding

2 No Covert Channel?

2.1 Possible Covert Channel

An adversary could monitor the **frequency of replacing computers** or in case that those are destroyed inside the datacenter where the attacker cannot observe it, he could take the average period of 10 years. The adversary can further interpret the replacement pattern as a string of bits, forming a covert channel. (Need malware on running computers inside datacenter which interprets bitstring ?)

2.2 Capacity of Covert Channel

In the worst case (where the attacker cannot observe the replacements and thus needs to hold on the average case of replacing computers every 10 years) the channel has a capacity of

$$\frac{\frac{1}{10}bit}{year} * amountPCs$$

.
Since the attackerr can transfer 1 bit per replacement, in a very good case (at least for the attacker), where each day one computer is replaced, he would be able to reach a capacity of

$$\frac{1bit}{day}$$

.

3 PINs, Pollen, Probability (Part II)

3.1 Trials without prior Knowledge

Assuming we have a key of 5 digits where only 4 digits are worn off on the keypad, then within the key there might be one of those numbers two times. So we have 60 trials in total:

$$\binom{5}{2,1,1,1} = \frac{5!}{2!} = \frac{5 * 4 * 3 * 2}{2} = \frac{120}{2} = 60$$

Which will lead to **30 trials on average**.

3.2 Trials when selectively cleaning Keys

When we can selectively clean keys I would suggest to **wipe all keys except one** (where we know that it is contained in the overall key, one of the worn offs), since we know from the discussion of the optional exercise sheet that the number of trials gets less the more keys we clean (down to one leaving dirty).

$$4! + 3! + (2! + 2!) + 3! + 4! = 24 + 6 + 4 + 6 + 24 = \frac{64}{5} = 12.8$$

which leads to **6.4 trials on average**.

The components for the formula were constructed as follows:

- dirty key is **first number** of the overall key: 4! different permutations
- dirty key is **second number** of the overall key: 3! different permutations
- dirty key is **middle number** of the overall key: 2! different permutations for each side, which gives us 2*2! permutations in total
- dirty key is **second to the last number** of the overall key: 3! different permutations
- dirty key is **last number** of the overall key: 4! different permutations

3.3 Progress of three worn off Keys

Assuming we have now only 3 digits worn off on the keypad, then the overall key might contain exactly two digits for two times each or one digit is included three times. Then the total number of trials reduces to 30 or 20, respectively:

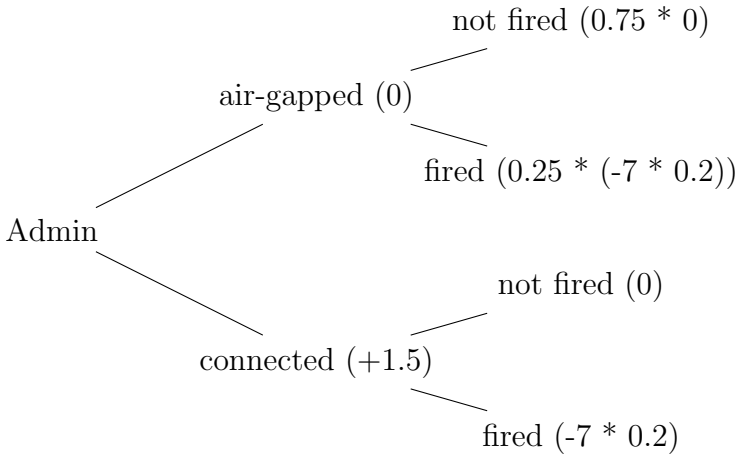
$$\binom{5}{2,2,1} = \frac{5!}{2! * 2!} = \frac{5 * 4 * 3 * 2}{2 * 2} = \frac{120}{4} = 30$$

$$\binom{5}{3,1,1} = \frac{5!}{3!} = \frac{5 * 4 * 3 * 2}{3 * 2} = \frac{120}{6} = 20$$

Thus we have an **average amount of 12.5 trials** ($\frac{(\frac{30}{3} + \frac{20}{2})}{2}$)

4 Game Theory

N := {1, 2} S1 := {connected (c), disconnected (d)} S2 := {connected (c), disconnected (c)}



4.1 Utility Functions

u1(d, d) = 0
u1(d, c) = 0 + 0.2 * (0.25 * (-7))
u1(c, d) = 1.5 + 0.2 * (-7)
u1(c, c) = 1.5 + 0.2 * (-7)

u2(d, d) = 0
u2(d, c) = 0 + 0.2 * (0.25 * (-7))
u2(c, d) = 1.5 + 0.2 * (-7)
u2(c, c) = 1.5 + 0.2 * (-7)

4.2 Game Matrix

	Admin2:connected	Admin2:disconnected
Admin1:connected	(0.1, 0.1)	(0.1, -0.35)
Admin1:disconnected	(-0.35, 0.1)	(0, 0)

4.3 Nash Equilibrium and Social Optimum

Since every game with a finite number of players and a finite set of actions has at least one Nash equilibrium, we also have one here, which is when both are connected to the Internet. (0.1 is the best response to 0.1)

The social optimum is when both administrators have an air-gapped system.

4.4 Appropriate Canonical Game

The corresponding canonical game is the *Prisoners' Dilemma*.

4.5 Apply for Job?

NO, I would not apply for the job, since I would always have a 25% chance of getting fired although I kept my system air-gapped. Further, in case I do not know my colleague's decision, I would need to connect to the Internet such that he cannot improve by changing his strategy and thus my system would possibly be vulnerable.