CHALMERS
EXAMINATION / TENTAMEN

Course code/kurskod	Course name/kursnamn			
EDA263	Computer Security			
Anonymous code Anonym kod		Examination date Tentamensdatum	Number of pages Antal blad	Grade Betyg
EDA263-51		2015-03-21	9+tes	5

Solved task Behandlade uppgifter No/nr		Points per task Poäng på uppgiften	Observe: Areas with bold contour are to completed by the teacher. Anmärkning: Rutor inom bred kontur ifylles av lärare.
1	X	10-	
2	X	3	
3	X	3	
4	X	9	
5	X	4	
6	X	6-	
7	X	9	
8	X	7..	
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
Total examination points Summa poäng		51	

1) a) The inference threat means that you are able to infer information about an individual from a statistical database from different statistics. 3

b) Query size restriction means that statistics from queries with small (or big) size will not be returned. 2
If $|X(C)| \leq k$ or $|X(C)| \geq N-k$ the query will not be returned.

c) If we have a query C with $|X(C)| \leq k$ we can find a disjoint set $X(C')$ and then we can 2
find statistics for C with $X(C' \cup C) - X(C')$.
If $|X(C)| \leq k$ and a C' have $|X(C')| > k$, $|X(C') \cup X(C)| < N-k$ and $X(C) \cap X(C') = \emptyset$ then $(X(C') \cup X(C)) \setminus X(C') = X(C)$ where both C' OR C (gives $X(C') \cup X(C)$) and C' are valid characteristic formulas. Thus we pass the query restriction.

d) C:= Sex='female' AND Dep='CS' AND Pos='Prof'
We try disjoint sets C' and find one with 3
count(C') within the bounds. e.g. C:= Sex='male' AND Pos='Prof' then we query sum(C', "Salary")=212 and we query sum(C' OR C, "Salary")=272 thus Dodd's salary is 272-212=60 (\$1K). Both querys are within the limits so it works.
Note: C' OR C is the query: (Sex='male' AND Pos='Prof') OR (Sex='female' AND Dep='CS' AND Pos='Prof')

a) The three security objectives are (CIA): confidentiality, integrity and availability. Confidentiality means that a non-user cannot see the information in the system. Integrity means that a non-user can't change anything regarding the system and availability means the the system still (always) is available to the user.

b) Two such concepts are reliability and safety. Reliability means that the system outputs things that are correct i.e. a non-user cannot make the system output wrong things. Safety means that even if a fault or something similar is introduced the system should never harm anyone or anything.

3 She should focus on prg2 becaus it is a SUID-program. This means that anyone who runs it gets its EUID set to the owner which in this case is root. If there is a bug or some exploit in this program then an attacker might abuse it to get root priviliges which basically means that the attacker controls the system. The security consultant should make sure that setuid(ruid) is called before any fault might occur.

4

4 a) No, given the same key-length SC is generally more secure.

b) No, read above. AC is often used for key sharing and SC afterwards.

c) No, AC often depends on calculations that take more time than SC.

d) Yes, in SC a key must somehow be secretely be shared but in AC everyone can know your public key.

e) No, the symmetric key cannot be used for signing. and at least two people know it.

f) No, anyone with your public key might have sent it.

g) No, you can sign a plaintext and everyone can still read the plaintext.

h) No, you use public and private keys which is AC.

i) No, RSA needs a longer key length to be secure. AES 256-bit is secure though (for now).

j) No, one is public and one is private/secret.

5

EDA263-51 4 5

5 a) Side-channel attacks tries to gather information through some other channel such as measuring the time for certain computations or the power consumption when decrypting a message. One might also (with access to the hardware) introdues a fault (by e.g. changing the volt) to make a program leak secrets.

2

b)
```
isPasswordCorrect(String pw){
    String realPw = "verysecret";
    for(int i=0;i<realPw.length;i++){
        if( realPw.at(i) != pw.at(i) ){
            return false;
        }
    }
    return true;
}
```

2

Since it will take longer time for every character in the begining that is correct we know that every time the calculation is longer we guessed another character right.

EDA263-51 6- 6

6 a) Teleological theory means that the only things that matters are the consequenses or the outcome. On the individual level I only care about my consequences and on the universal level I care about the total outcome for all parts involved. 2

b) Deontology means that one should do what is right, that there are rules to follow. On a universal level there are laws to follow and on the individual level one has a perception about what is morally right as well. 2

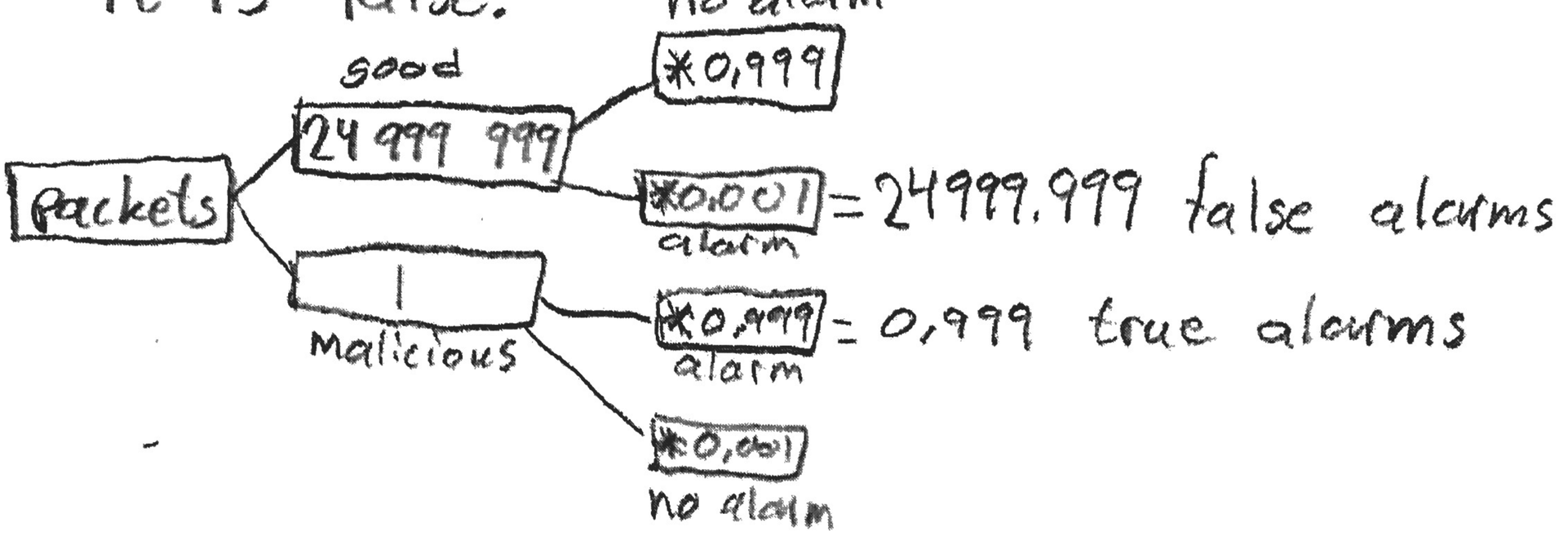
c) I see three options: Sell information to possible attacker, blackmail owner of system or tell said owner. To sell information might be good individually you get money but there is a chance that you will get caught and/or loose electricity. Thus your pay should be more than the possible damage for your outcome to be good. Universally many people might loose power which seems like a bad consequence. Blackmail might give money but you might get caught and the might fix it if they know that a →

6.c) critical bug exists. I would not do this since the expected outcome seems bad. To tell the owner might give you a reward but probably not so it can be seen as ±0, everything is as usual. The best thing would probably be to sell it to an attacker if the pay is good enough otherwise tell the owner and hope for a good outcome such as a pay or a job.

2

You use egoism mostly.
Most would argue selling to attacker a bad outcome

7 It is false.



$$\frac{\text{true alarms}}{\text{total alarms}} = \frac{0{,}999}{24999{,}999 + 0{,}999} \simeq \frac{1}{25000} = \frac{4}{100\,000} = 0{,}004\%$$

Since there will be about 25 000 false alarms and about 1 real alarm the probability of a packet being malicious if the IDS raises an alarm is about 0,004% (or 1 in 25 000).

9

8

8 a) The first action is to take the risk, this is good if it is expensive to avoid and might not cause that much damage. An example might be to get robbed of your computer, it is not likely and if it is encrypted the consequences are not that bad so it might be worth to not pay for guards or protection.

The next action is to avoid the risk e.g. (have guards at your office so unauthorized persons might not enter.) It will cost you but if anyone could come and go that might cost you more.) bra ex

The last action is to insure yourself. In the unlikely event that something gets stolen you will get money from an insurance company though you will pay them monthly for the service.

b) You can reduce the likelihood of a risk happening e.g. do penetration tests so that the likelihood of someone unauthorized getting access to your system is smaller. The other thing is to reduce the consequences e.g. to have all your data encrypted, which limits the damage if the data is stolen.