Question 1: Modeling (35%)

We consider again the recruitment system that you know from the three obligatory exercises, although some of the specifications are slightly changed.

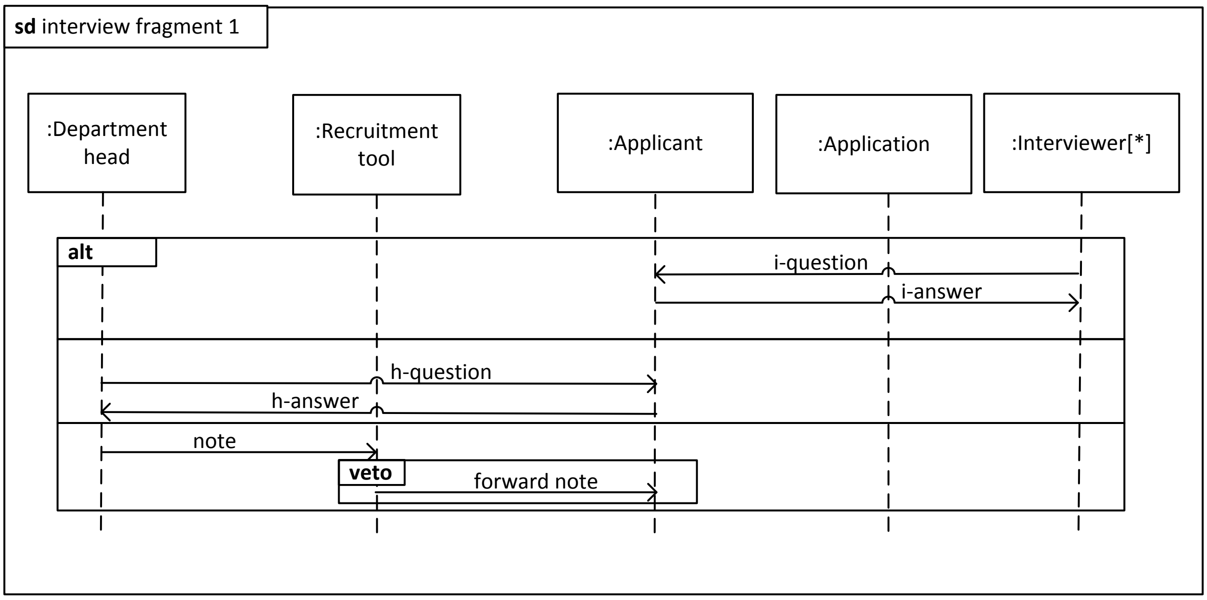

Figure 1

(weight 5%)

a) What is/are the potential initial event/events in the sequence diagram **sd** *interview fragment 1* in Figure 1? Explain your answer.

There are three possible initial events:

!i-question, !h-question, !note

The alt allows us to select freely between the three operands. Each operand has only one first event due to weak sequencing.

(weight 5%)

b) Describe the negative trace/traces of the sequence diagram **sd** *interview fragment 1* in Figure 1. Describe each trace on the form **<e1,e2,...,en>** where **e1,e2,...,en** are events.

There is only one such trace:

<!note,?note,!forward note,?forward note>

Only one of the operands can produce a negative trace and it obtained weak sequencing with the first message.

(weight 5%)

c) What is the shortest inconclusive trace with respect to the sequence diagram **sd** *interview fragment 1* in Figure 1?

The empty trace <>, since this trace is neither positive nor negative in the diagram.

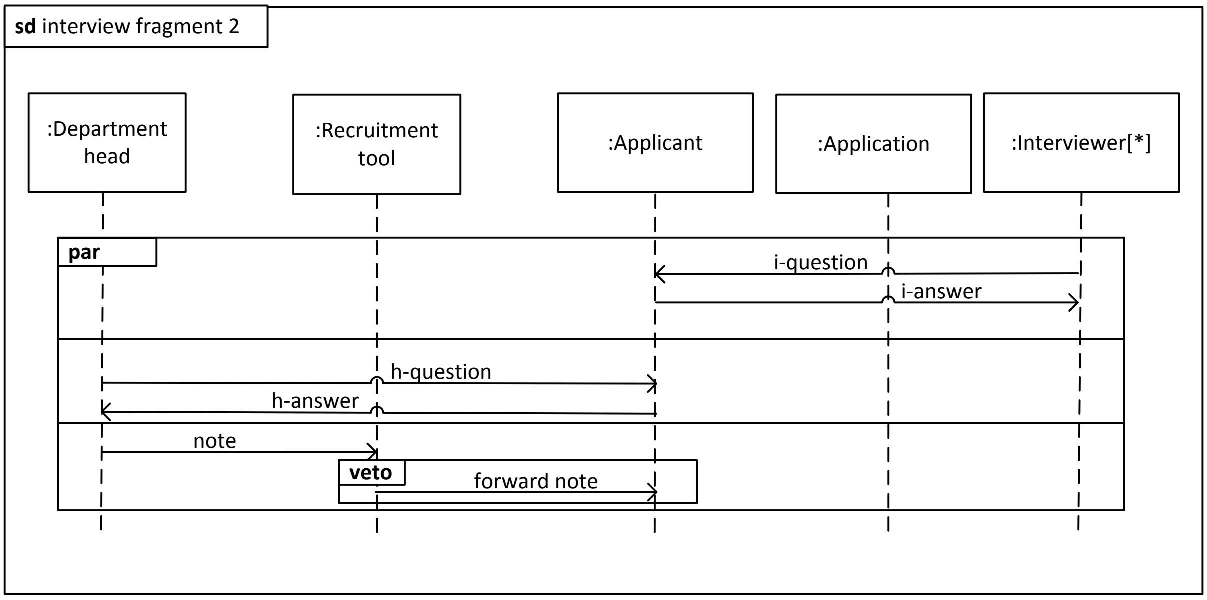

Figure 2

(weight 6%)

d) What is the length of a negative trace of **sd** *interview fragment 2* in Figure 2? Explain your answer. (Note that in **sd** *interview fragment 2,* the **alt** in **sd** *interview fragment 1* has been replaced by **par**.)

The length is 12. We get two events per message, and positive traces of the first two operands are interleaved with the negative one of the last.

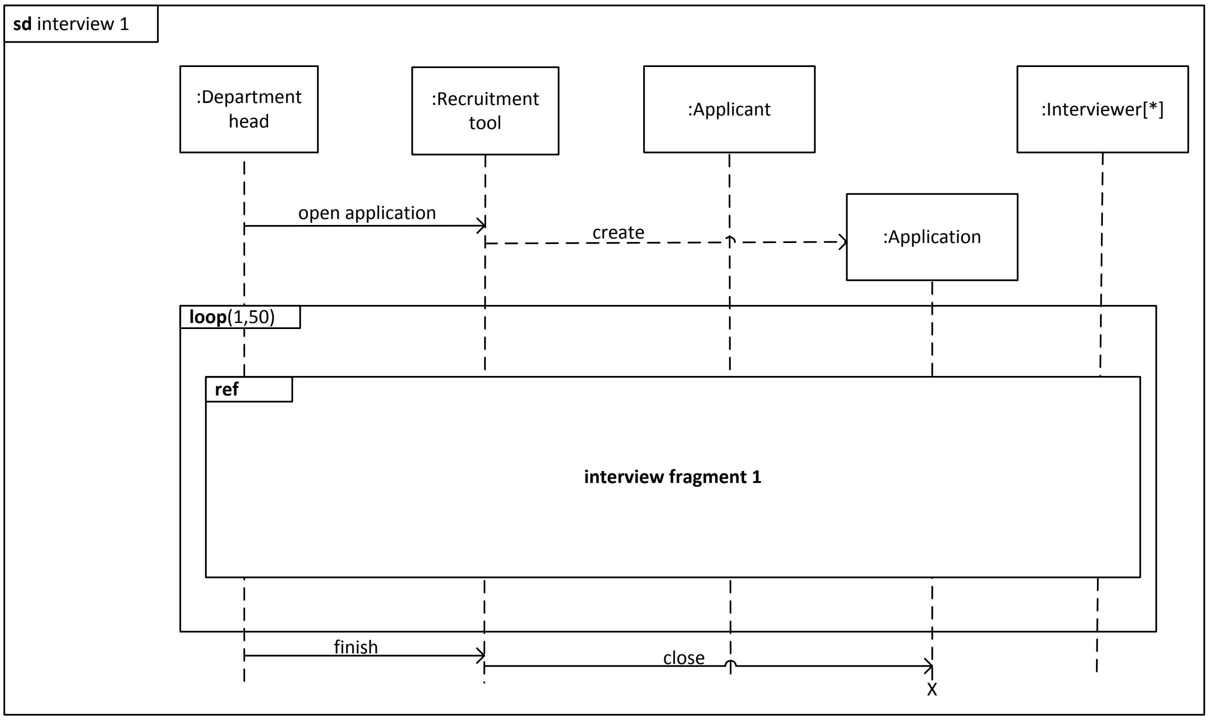

Figure 3

(weight 6%)

e) What is the minimal length of a positive trace of **sd** *interview 1* in Figure 3? Explain your answer.

10, since we may loop only once and choose the alt-operand with positive trace of length 2. If they answer 8, because they do not count create, then that is also ok.

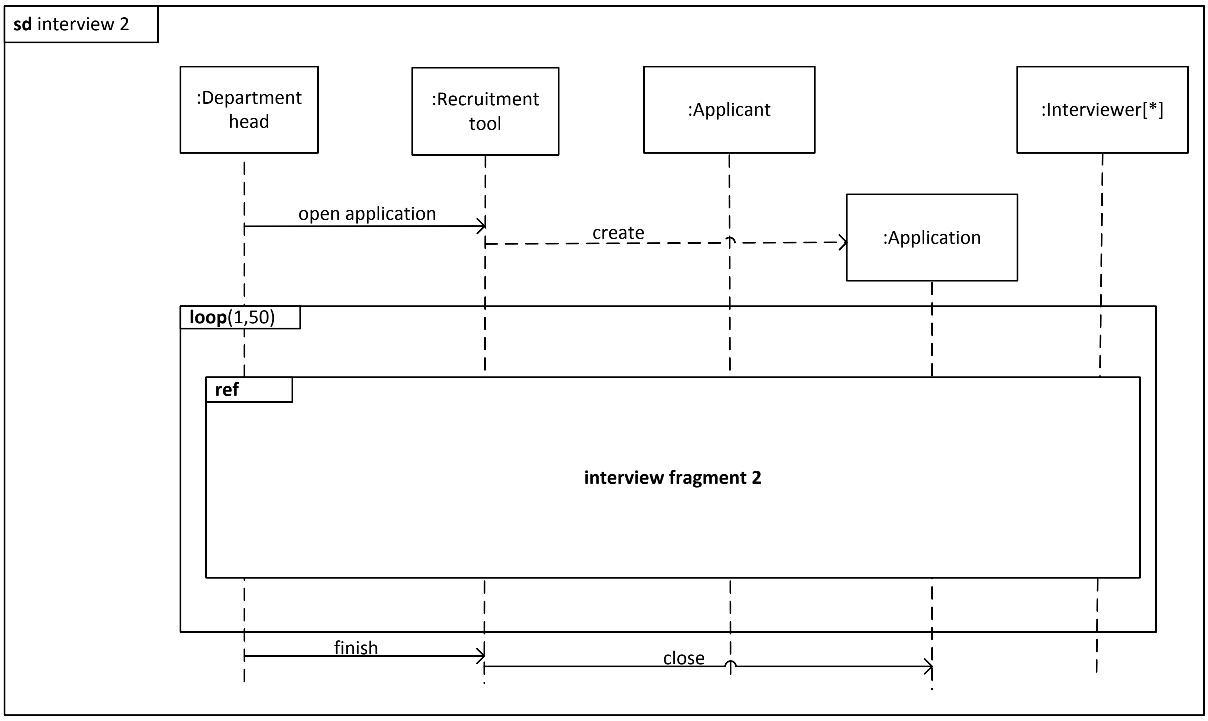

Figure 4

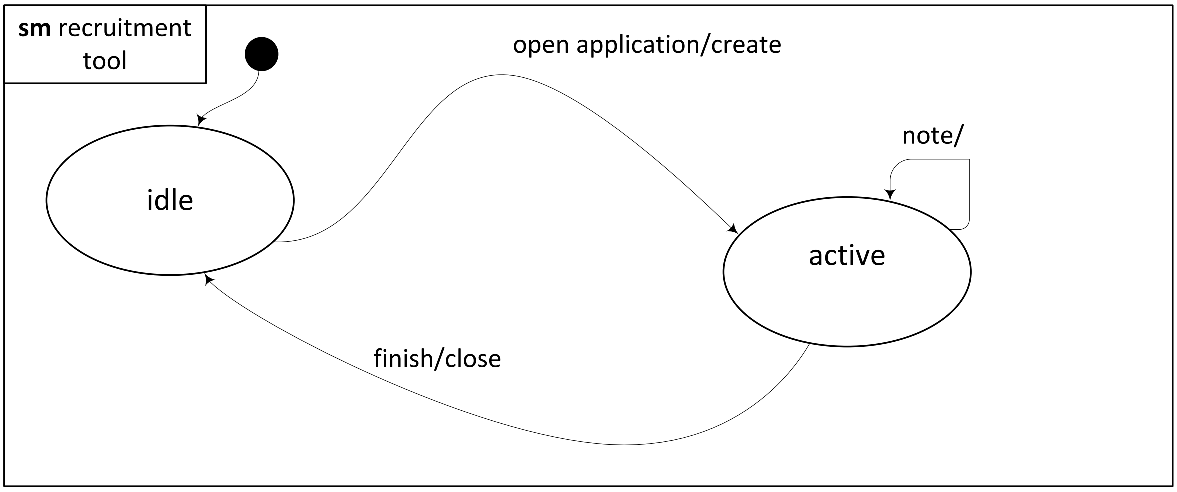

Figure 5

(weight 8%)

f) Explain how **sm** *recruitement tool* can be updated so that it describes all possible positive traces of **sd** *interview 2* with respect to the lifeline *:Recruitement tool*, but not all positive traces of **sd** *interview 1* with respect to the same lifeline.

My idea is to insert another state in-between **idle** and **active** and require **note** as an input signal in order to get from the new state to **active.** Then any trace ending with **!close** must have at least one !note.

Question 2: Refinement (35%)

We consider the recruitment system as specified above.

(weight 5%)

a) Explain how the sequence diagram **sd** *interview fragment 1* in Figure 1 can be modified into a sequence diagram **sd** *interview fragment 1'* so that **sd** *interview fragment 1'* is a (pure) narrowing of **sd** *interview fragment 1.*

(weight 5%)

My idea is **refuse** within one of the **alt** operands.

b) Explain how the sequence diagram **sd** *interview fragment 1* in Figure 1 can be modified into a sequence diagram **sd** *interview fragment 1''* so that **sd** *interview fragment 1''* is a (pure) supplementing of **sd** *interview fragment 1.*

(weight 5%)

My idea is to add another operand to **alt**.

c) Explain how the sequence diagram **sd** *interview fragment 1* in Figure 1 can be modified into a sequence diagram **sd** *interview fragment 1'''* so that **sd** *interview fragment 1'''* is a refinement of **sd** *interview fragment 1* without being a (pure) supplementing or a (pure) narrowing.

(weight 6%)

My idea is to combine the two steps corresponding to the two first questions.

d) Is **sd** *interview 2* in Figure 4 a refinement of **sd** *interview 1* in Figure 3? Explain your answer.

No, because positive traces become inconclusive.

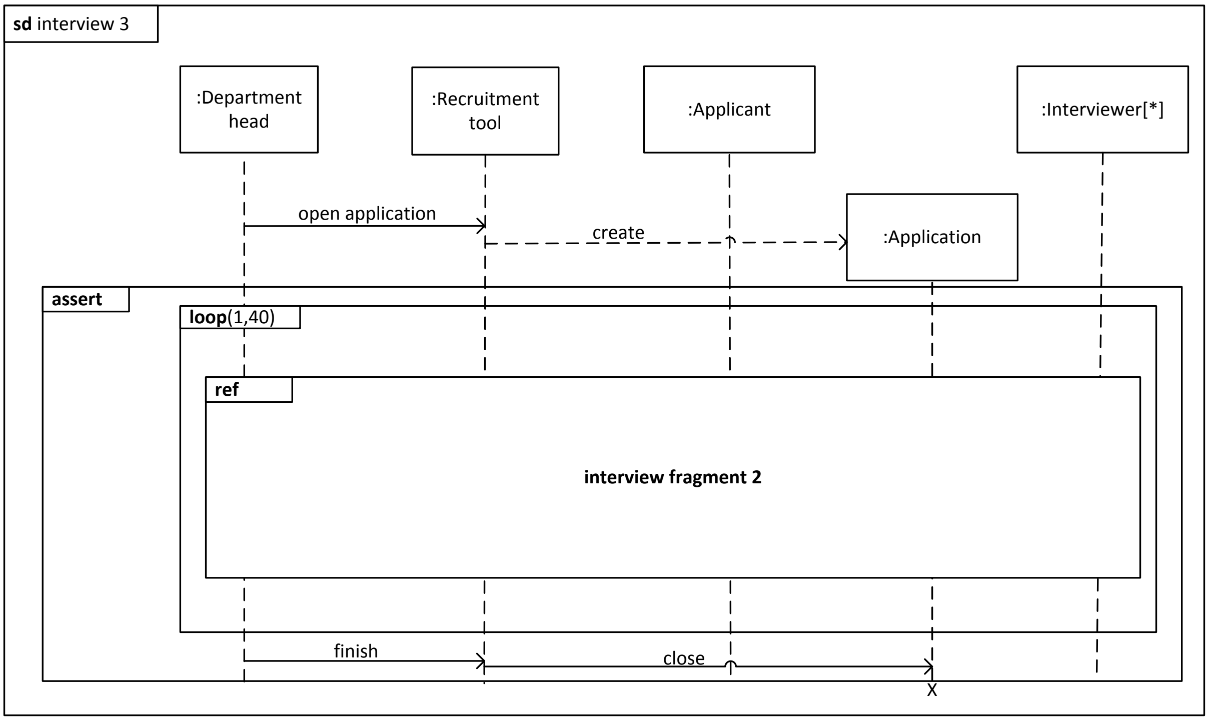

Figure 6

(weight 7%)

e) Is **sd** *interview 3* in Figure 6 a refinement of **sd** *interview 2* in Figure 4? Explain your answer. (Note that **sd** *interview 3* contains two modifications *wrt* **sd** *interview 2* – the **loop** construct is restricted to maximum 40 iterations and we have introduced an **assert**.)

Yes. The positive traces of the new diagram are positive also in the old. The positive traces of the old diagram that are not positive in the new have become negative.

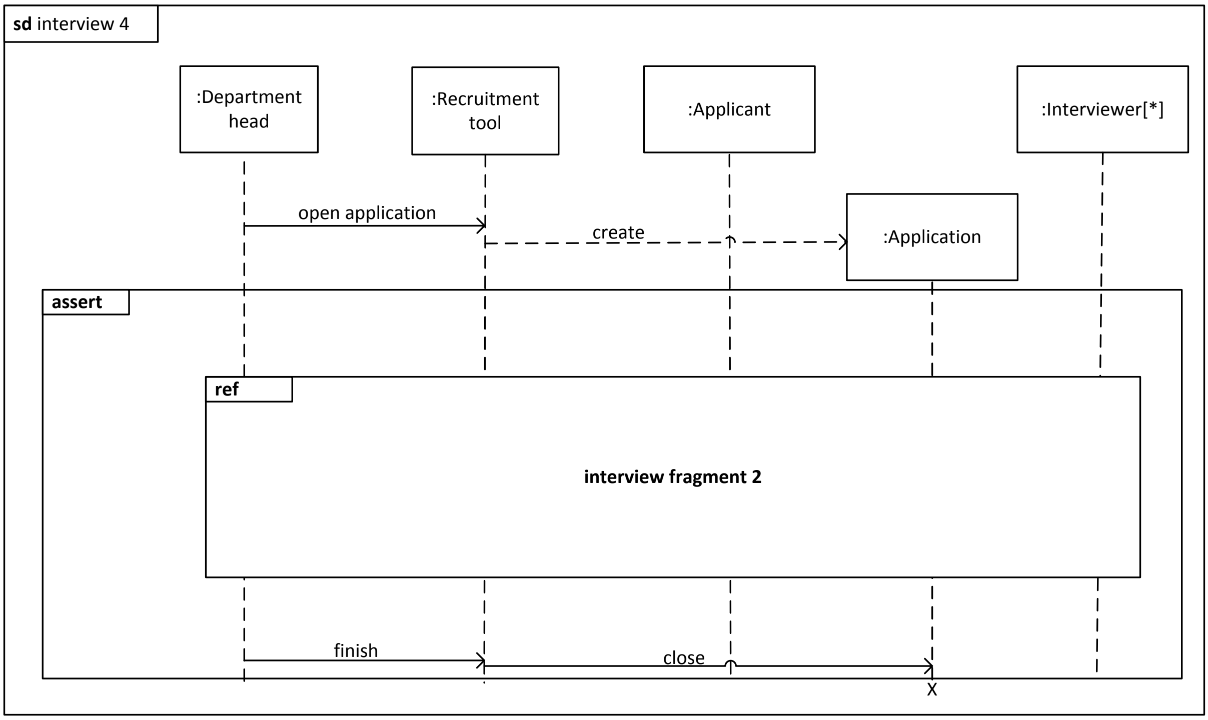

Figure 7

(weight 7%)

g) Is **sd** *interview 4* in Figure 7 a refinement of **sd** *interview 3* in Figure 6? Explain your answer. (Note that **sd** *interview 4* has no **loop** construct)

Yes. The argument is basiccally the same as above since we basically loop once in interview 4.

Question 3: Security Risk Assessment (30%)

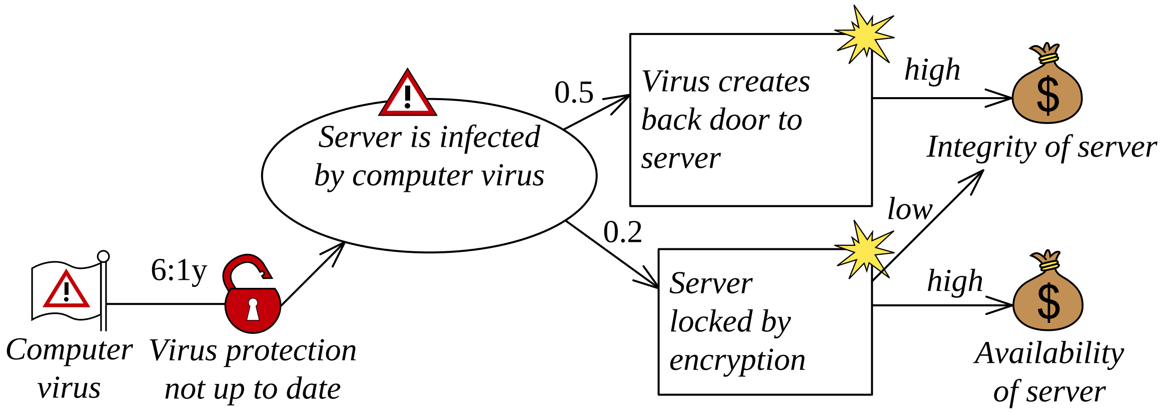
Server is infected by computer virus
0.5
Virus creates back door to server
high
Integrity of server
low
0.2
Server locked by encryption
high
Availability of server
6:1y
Computer virus
Virus protection not up to date

Figure 8

(weight 5%)

a) Determine frequencies for the threat scenario and the two unwanted incidents in Figure 8 in such a way the threat diagram is consistent under the assumption that it is complete.

(weight 5%)

Threat scenario: 6:1y.

3:1y and 1.2:1y by leadsto rule. (Multiplication)

b) Determine frequencies for the threat scenario and the two unwanted incidents in Figure 8 in such a way the threat diagram is inconsistent under the assumption that it is complete, but consistent under the assumption that it is not incomplete.

We could for example assign the frequency 199:1y to one of the unwanted incidents. Then it is consistent if incomplete because there may be additional scenarios, but inconsistent otherwise.

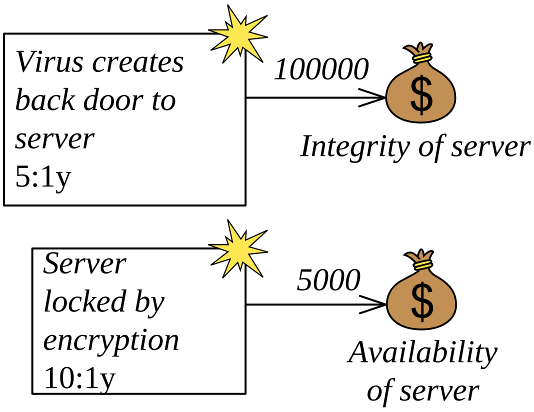
Virus creates back door to server 5:1y
100000
Integrity of server
Server locked by encryption 10:1y
5000
Availability of server

Figure 9

(weight 5%)

c) Calculate the frequency of the aggregated risk corresponding to the two unwanted incidents in Figure 9.

Here there such be argument that they are separate in which case the answer is 15:1y. If they are not separate then the maximum is 15:1y and the minimum is 10:1y.

(weight 5%)

d) Assume consequence values in Figure 9 represent the average loss in EURO per occurrence. What is then the average loss in EURO per occurrence of the aggregated risk corresponding to the two unwanted incidents?

(100000*5 + 5000*10) / 15 = 36666,66

This depends on the issue of separation.

(weight 5%)

e) The party of the security risk assessment in Oblig-III was the company Bang!. It could also have been the applicant. Consider the asset "trust of applicant". In the setting of a security risk assessment would "trust of applicant" be a suitable asset for the company Bang!, the applicant, for both or for neither? Explain your answer.

Trust of applicant should never be an asset for applicant. If I'm mislead to trust the director then f.eks. this is not a good thing for me. It may be an asset for the company (want to be trusted by the public) or it may not (not sufficiently important).

(weight 5%)

f) Define a good qualitative scale with 6 values to measure trust (in the general case).

Six values all defined with good explanations in natural language so that it is "easy" to decide which one to choose in a practical situation. The explanations should be trust-oriented.