Oblig III: Security Risk Assessment of the Gestalt Principles Service

In this compulsory exercise (Oblig III) you will be trained in security risk assessment of the Gestalt Principle Service you know from Oblig I.

You are free to make assumptions as long as they are stated explicitly by you in your oblig-solution.

The solution in the form of a single pdf-document should be sent to kst@sintef.no by midnight November 16.

THE SOLUTION SOULD BE EASILY READABLE WHEN PRINTED IN A4 FORMAT. THIS INCLUDES TEXT IN THE CORAS DIAGRAMS.

You may work in groups of maximum three students or you may work alone. Hence, one solution may have up to three names. There should be no collaboration or copying between different groups. Hence, each group should solve the exercise independently.

You should use the new CORAS-tool: https://stverdal.github.io/#/try-it

With respect to likelihood reasoning, you should use the rules for frequencies presented in the lectures on Security Risk Assessment. (In the CORAS book there are also rules for probability reasoning. They **should not** be used.)

It is a very good idea to start by carefully reading Chapter 3 of the CORAS book unless you have already done so.

Remember to put your real names (not usernames) in the solution-paper so that I can see who wrote it when it is printed on paper.

Gestalt principle service

As I tried to explain in Lecture I, modellers need to be aware of the theory of Gestalt psychology. Gestalt psychology implies that the mind understands external stimuli as wholes rather than as the sums of their parts. Gestalt psychology has proposed principles or laws that govern the workings of human perception. In Lecture I we briefly mentioned the following laws:

1. Law of proximity: objects that are close are perceived to form a group
2. Law of similarity: objects are perceptually grouped together if similar
3. Law of closure: objects are perceived as complete ignoring gaps
4. Law of symmetry: symmetrical objects are perceptually connected to form a coherent shape

There are many more and they are well documented and explained both in the literature and on the internet. See for example:

- https://www.toptal.com/designers/ui/gestalt-principles-of-design
- https://www.usertesting.com/blog/gestalt-principles

A new business Gestalt Principle Service is developing a tool to guide modellers on the impact of gestalt principles. The idea is to offer a service that allows modellers to submit models to get them analysed with respect to gestalt principles. The service solution will not grasp the intended semantics

of the models. Hence, it does not know what the models it gets means, but it can nevertheless identify potential "gestalt-traps" and communicate them back to the modellers. When receiving a model, the service will analyse the model and present the result in the form of a report that is sent back to the service user which are the customers of the Gestalt Principle Service.

Task

Assume you are under contract to conduct a security risk assessment of size 250 man-hours on behalf of the Gestalt Principle Service. Your task is to conduct a security risk assessment **of the service offered by** the Gestalt Principle Service.

In the following we address some of the aspects that such a risk assessment may involve.

Question I

Identify at least seven assets **of relevance for the Gestalt Principle Service**. Minimum two assets should be indirect and minimum three assets should be direct.

Two of the direct assets should be "confidentiality of service design" and "availability of service". One indirect asset should be "reputation of service".

Make a CORAS asset diagram that correctly relates them.

For detailed advice, see Section 7.2.2 in the CORAS book.

Question II

Make a good **qualitative scale** for measuring harm (consequence) to the asset "reputation of service". It should have at least 5 values.

Question III

Make a good **quantitative scale** for measuring harm (consequence) to the asset "confidentiality of service design". It should have at least 5 values.

Question IV

Make a good **quantitative interval scale** for measuring harm (consequence) to the asset "availability of service". It should have at least 5 values.

Question V

Make a good **quantitative interval scale** for measuring frequency. It should have at least 5 values.

Question VI

Make relevant threat diagrams with respect to the two direct assets "confidentiality of service design" and "availability of service". The diagrams should all together capture at least seven risks. The diagrams should be annotated with consequences and likelihoods in such a way that **they are consistent**. Every initiate relation, unwanted incident and threat scenario should be assigned a **likelihood in the form of a frequency interval**. Every leads-to relation should be assigned a **conditional probability different from 1**. Moreover, all **initiate and leads-to relations should have at least one vulnerability associated with them** (i.e. represented in the diagram).

Question VII

Present the identified risks in a risk-matrix.

Question VIII

Make a treatment diagram by annotating the threat diagrams from Question VI with relevant treatments.

Question IX

Assume that the Gestalt Principle Business requires treatments for at least the three most important risks to be implemented. Use the CORAS before-after style to illustrate the effect of these treatments on the already identified risks. The threat diagrams you have already drawn (Question VI) corresponds to the before situation. You are to "translate" these threat diagrams into threat diagrams expressed in the so-called before-after style reflecting the situation both before and after the implementation of the treatments.

For detailed advice, see Section 6 of
http://www.uio.no/studier/emner/matnat/ifi/INF5150/h11/undervisningsmateriale/2011.FOSAD-preprint.pdf

Question X

Any risk treatment will introduce some new risks (possibly with respect to some new assets). Update the threat diagrams from Question IX to capture at least two new risks.

Question XI

Present the risk matrix as it looks after the risk treatment (also considering the results from Question X).