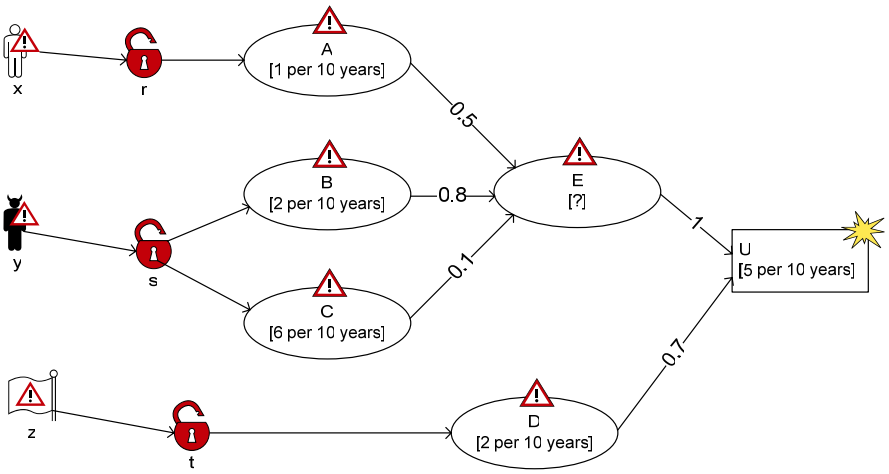
INF5150 Exercises 30/10-2007

Exercise 1

Consider the following figure, where we assume that all threat scenarios A, B, C and D are statistically independent:



I: What is the minimum likelihood that can be assigned to threat scenario E?
II: Assume threat scenario E is assigned likelihood 4 per 10 years. Is this consistent with the likelihood assigned to the unwanted incident U?

Exercise 2

Exercises in using the CORAS modelling language.

We will model the results of several steps of a security risk analysis in the CORAS modelling language based on natural language descriptions.
The example is taken from a larger analysis; therefore names/numbers of unwanted incidents etc. may seem strange.

PHASE I: establishing the context

Target description

- The target of analysis is a web portal that serves as a communication medium between ordinary citizens and various public entities (for example the tax office).
- The service must be available 24/7.
- A lot more information could be given, but this is all we need to know for this exercise.

Stakeholder(s)

- The company management (CM) of the company that develops and delivers the service is the client of (and pays for) the analysis, and is the only stakeholder in this analysis.

Assets:

- **CM1 – Users personal information** (damage is measured by the type of information disclosure, for example major = the information is available to the public for one day, medium = the information is available to the public for one hour, minor = the information is available to an unauthorized employee in the company for a week)
- **CM2 – Company reputatio**n (damage is measured by the type of negative media publicity in TV, radio, large newspaper or small newspaper, negative rumours etc.)
- **CM3 – Availability of service** (damage is measured as down time of the service)
- **CM4 – User efficiency** (damage is measured as the increased effort needed to use the functions provided by the service)

Relations between assets:

- Company reputation (CM2) can only be harmed if at least one of the other assets is harmed first.
- Only damage to the availability of service (CM3) may affect user efficiency (CM4).

Exercise Ia: Draw an asset diagram from the information above.

The analysis team chooses the following scale for likelihood: *seldom* (= 1 time per 5 years or less), *sometimes* (= more than 1 time per 5 years and less than 1 time per year), *often* (= 1 time per year or more).

The analysis team has chooses the following scale for consequence: *minor*, *moderate* and *major*. The interpretation of these depends on the asset. For example: minor damage to the availability asset could correspond to “system down in 2 minutes”.

The analysis team chooses the following scale for risk: *low*, *medium*, *high*.

Exercise Ib: A risk value matrix shows how likelihood and consequence values combine into a risk value. Draw a risk value matrix that uses the above scales for likelihood and consequence. (It is up to you to decide exactly how a consequence value and a risk value combines into a risk value.)

The analysis team chooses the following risk evaluation criteria:

Asset	**Max accepted risk level**
Users personal information	low risk
Company reputation	medium risk
Availability of service	medium risk
User efficiency	high risk

Phase II: Identifying risks

Note: We limit ourselves to non-human threats (and related vulnerabilities, threat scenarios and unwanted incidents). The full analysis would also include other threats.

The analysis team identifies the following threats:
• **Internal infrastructure (non-human)**: hardware or software, part of the service, may fail and initiate unwanted incidents.
• **External resources (non-human)**: resources that deliver data to the service.
• **Virus attack (non-human)**: an environmental circumstance outside the company's control.

The analysis team identifies the following vulnerabilities:
• **Shared infrastructure resources**: the service runs on hardware or software that is shared with other less critical services. This means that if one of the other services encounter a problem it may affect the service.
• **Low robustness**: in cases of high traffic to the portal, the server tends to degrade in performance and response time increases.
• **External resource failure:** a resource that provides data to the web portal service may fail, and the service is dependent on the availability of these databases.
• **Internal hardware or software failure:** the internal infrastructure may fail due to hardware or software errors.

The unwanted incidents (named Ux) that are identified by the analysis team are listed below, followed by a description of the threat scenarios (which are indented and numbered) that may lead to the incident:

U2: Unauthorized modification of users' personal information:

1. Virus attack on the service may cause high traffic on the service. This may lead to a server crash, so that all active user sessions are deleted along with their previous data modifications, leaving the information partly incorrect.

U4: Unavailability of service due to infrastructure failure:

1. Hardware or software, part of the service infrastructure, may fail or malfunction and make the service fully or partly unavailable.
2. External sources of information may fail or malfunction making the service unavailable.

U5: Unavailability of service due to malicious code:

1. A virus attack may cause extensive traffic so that the server crashes.

U6: Damage to company reputation:

1. If the service is unavailable it may harm the company's reputation.

U7: Reduced user efficiency:

1. If the service is unavailable it may reduce the users' efficiency.

Exercise IIa: Document the above information in a threat diagram.

Phase III: Estimating risks

The analysis team has named the risks and estimated consequences and likelihoods according to the following table:

Risks	**Asset harmed**	**Consequence estimate**	**Likelihood estimate**
R2CM) Unauthorized modification of user's personal information	CM1	Major	Seldom
R4CM) Unavailability of service due to infrastructure failure	CM3	Moderate	Sometimes
R5CM) Unavailability of service due to malicious code	CM3	Moderate	Seldom
R6CM) Damage to company reputation	CM2	Moderate	Seldom
R7CM) Reduced user efficiency	CM4	Minor	Sometimes

Exercise IIIa: Add consequence and likelihood estimates to the threat diagram from Exercise 2a.
Exercise IIIb: Draw a risk evaluation matrix with all identified risks.

Phase IV: Evaluating risks

Exercise IVa: Draw a risk overview diagram showing whether risks are acceptable or not.

Phase V: Identifying treatments

The analysis team identifies the following treatment options for the unacceptable risk:

• **TO1: Upgrade to more robust infrastructure solution** that have lower failure rate.
• **TO2: Install redundant system** that will take over in case of infrastructure failure or attack.
• **TO4: Install intrusion detection system** that will detect the attack rapidly and make it possibly to switch to manual routines.

Exercise Va: Draw a treatment diagram showing where these treatments have an effect.