TDT4237 Exercise 4 censor guide (20 points in total)

Identify business assets (at least 3) and goals (at least 3). (1 + 1 points)

The candidate should know the difference between business goals (what to achieve) and assets (what to protect).

Examples of business goals:

- Protect refugees from kidnapping, misuse and other criminal acts.
- Manage the identity and role of volunteers and refugees.
- Easily verify the identity and role of volunteers and refugees.
- The system developed and in operation within a week.
- Provide a free-to-use system to the volunteers.
- The client software runs on common devices (smart phones).
- The system has an uptime of 99%.
- A system resilient to hostile actors and unforeseen events.

Examples of business assets:

- Digital identities.
- Safety of users (volunteers and refugees).
- Personal data.
- QR-codes.
- Trustworthy system.
- Technical equipment (software, servers, clients, infrastructure). NB: This is often regarded as secondary assets in some risk management approaches. However, we have not talked about the difference between primary and secondary assets in this course.
- Trust towards volunteers.
- Reputation of helper organisations.

Identify business risks (at least 5) and specify which scales you are using. At least one of the risks should be related to privacy. (1 + 1 points)

It is expected that the candidates mention something about the risk dimensions and scales they are using (topic in the Risk management lecture).

Likelihood could be based on expected frequency or be attacker-centric (from the Threat modelling lecture).

Expected frequency:

Low: Once every year or less

Medium: One per Month or less

High: Once per day or less

Extreme: Once per hour or less

Attacker-centric:

Low: There are no known threat agents present or able to perform.

Medium: There are a few threat agents able and willing to do this.

High: There are many threat agents with this potential.

Extreme: There is a massive number of threat agents operating.

Impact dimensions, e.g. related to Confidentiality, Integrity, Availability, Financial, Safety, Privacy.

Example scale privacy:

Low: No or minimal exposure of individual personal data.

Medium: Breach of personal data for an individual.

High: Breach of personal or sensitive data of many individuals.

Extreme: Severe breach of all personal or sensitive data.

Business risk examples:

BR1: System too difficult to use (unnecessary mistakes).

BR2: System unavailable (unable to do register or lookup identities).

BR3: User identity is disclosed (privacy breach).

BR4: System not installed and operational in time (no help).

BR5: System misused by malicious actors (people exploited or put in danger).

BR6: The system provides false information (lack of trustworthiness).

BR7: The technical equipment is not compatible with the software (unable to deploy).

BR8: Identities are stolen, swapped or false (identity manipulation).

BR9: The system is easy to sabotage (lack of protection).

Identify technical risks (at least ten) through threat models (here, you need to show us that you know how to make misuse cases and attack trees. You need to choose at least two use cases and make their corresponding misuse cases. In addition, you need to choose at least two high-level attacks and make two corresponding attack trees.) (2 +2 +4 points)

Here the candidate should show proper use of misuse case diagrams, including normal use cases. The level of abstraction should not be too technical, but rather on the level of intention from the attackers' point of view.

Example threat agents:

- Cyber warriors (state sponsored, sabotage)
- Traffickers (kidnapping)
- Criminals / crooks (financial gain, theft)
- Dishonest refugee (swap identity/QR)
- Dishonest volunteer /insider (blackmail, corruption, sabotage)
- Warmonger (stop evacuation, sabotage)

The ranking can be based on elements from the threat modelling lecture, such as number, opportunity, (required) means, opportunity, technical skills, potential profit, etc. The important thing here is that the candidate shows some sort of reasoning and justification for the ranking.

Attacks trees: The candidate should show how a misuse case activity can be used as a top goal node in an attack tree and that there are several ways (branches) of achieving this goal. Very few nodes (3-4) should receive a lower score.

The technical risks should correspond to the contents of the threat models. They should be properly defined (not just single words like “DDOS”, but rather “Phone network jammed by DDOS attacks”). The Risk management lecture showed how to link business and technical risks, and how to place business risks within a matrix.

Example technical risks:

TR1: Malware on mobile device made to quickly expend battery.

TR2: Fake QR codes links to spoofing server.

TR3: Attacker brute force administrator password.

TR5: Injection attack on database.

TR6: QR-codes can be read by attacker from afar.

TR7: Phone network jammed by DDOS attacks.

TR8: Volunteer device physically stolen by attacker.

TR9: The firewall (if any) is misconfigured to not let anyone in.

TR10: The load balance is misconfigured to overload one application server.

We expect that the students show how the business risks and technical risks are related, e.g., in a table (see lecture slides on Risk management).

Derive security requirements (at least ten) from the technical risks based on your misuse cases and attack trees. (4 points)

The requirements should follow the criteria for good requirements as presented in the Risk management lecture:

- What you require, not how to achieve it
    - Being open to different solutions
    - Avoid premature design or implementation decisions

- Understandability, clarity (not ambiguous)
- Cohesion (one thing per requirement)
- Testability
    - Clear acceptance criteria
    - Often requires quantification

It is OK to pick from ASVS, but they should be relevant and linked to the selected technical risks.

Example: Two-factor authentication should be required for administrators.

Create a test plan addressing (at least five of) the security requirements (You do not need to execute the test plan). (4 points)

Each test should obviously and effectively validate the requirements. Tests that only evaluate specific cases without covering the whole requirements are given less points. For instance:

- Test sanitation to prevent SQL injection by using a specific injection, e.g., “username’; --.”

- Test sanitation to prevent SQL injection by using a dictionary of possible injection attacks.