Workshop Day 1

Tabular-based security risk management
Tasks and Steps

1. Describe what is “system” in the given scenario.
   - Products/components of the system
   - Its infrastructure applications
   - Information technology staff
   - Internal users and management
   - Customers
   - Other external users
   - Environment

Where to report?
- Section 1.1, Table 1, page 2
Workshop Tasks and Steps

2. Discuss and define the scope of your further analysis
   • It is much better to choose a narrow scope (e.g., only one business asset!!!) and provide extensive analysis in the narrow scope

Where to report?
• Section 1.2, page 2
Workshop Tasks and Steps

3. Define assets and their security criteria

- What are the business assets and their security criteria?
- Explain how these business assets are supported by the system assets

Where to report?
- Section 1.3, Table 2, page 3.
- Textually (or graphically) explain the Support relationship below the Table 2.
5. Analyse security risks

Each team member should propose at least 2 security risks

Consider:

• Functionality Decomposition Layers and/or Information processing functions to determine targeted system assets
• Taxonomy of Seven pernicious kingdom (or any other vulnerability database) to determine vulnerabilities of the systems assets
• Characteristics of Threat agent to characterize Capabilities, Motivation and Expertise of the Threat agent
• STRIDE and/or Taxonomy of Threats to (Distributed) Systems to determine Threats and Attack methods
• Symptoms of malicious software to indicate the harm to the assets. Indicate what could be the possible negation of the security criterion.
• Fill in the table (for each risk) to state explicit risk definition

For each risk:

• it must be clear what are threat agent, attack method, vulnerability and impact.
• it must be clear which system asset(s) is (are) targeted by the identified risk
Workshop Tasks and Steps

5. Analyse security risks

Each team member should propose at least 2 security risks

Consider:

- Functionality Decomposition Layers and/or Information processing functions to determine targeted system assets
- Taxonomy of Seven pernicious kingdom (or any other vulnerability database) to determine vulnerabilities of the systems assets
- Characteristics of Threat agent to characterize Capabilities, Motivation and Expertise of the Threat agent
- STRIDE and/or Taxonomy of Threats to (Distributed) Systems to determine Threats and Attack methods
- Symptoms of malicious software to indicate the harm to the assets. Indicate what could be the possible negation of the security criterion.

For each risk:

- it must be clear what are the threat agent, attack method, vulnerability and impact.
- it must be clear which system asset(s) is (are) targeted by the identified risk

Where to report?

- Section 2, Table 3, page 3.
- Each security risk should have its “Table 3”.
- Include additional tables
- Change table captions to Table 3.1, Table 3.2, … and Risk IDs to ID1, ID2, …
Workshop Tasks and Steps

6. Define security countermeasures to mitigate security risks

For each risk separately!

Where to report?

- Section 3, Table 4, page 3.
- Each security risk should have its countermeasures reported in “Table 4”
  - Include additional tables
  - Change table captions to Table 4.1, Table 4.2 …
  - Security requirements must have unique ID and they must correspond to criteria of “good requirements”
Workshop Tasks and Steps

7. Agree on the security metrics

For each risk and its security countermeasures separately!

Which risk(s) needs to be mitigated first?

• Use plots:
  – Risk reduction level versus Cost
  – Risk reduction level versus Value
  – Value versus Cost
Workshop Tasks and Steps

7. Agree on the security metrics

For each risk and its security countermeasures separately!

Which risk(s) needs to be modelled first?

- Use plots:
  - Risk reduction level versus Cost
  - Risk reduction level versus Value
  - Value versus Cost

Where to report?
- Section 4.1, Table 5, page 4.
- Each tuple of business asset, security risk, and security countermeasure should have its “Table 5”
  - Include additional tables
  - Change table captions to Table 5.1, Table 5.2 …
Workshop Tasks and Steps

7. Agree on the security metrics for each risk and its countermeasures separately.

Which risk(s) needs to be mitigated first?

- Use plots:
  - Risk reduction level versus Cost
  - Risk reduction level versus Value
  - Value versus Cost

Where to report?
- Section 4.2, Fig. 1, Fig. 2, Fig. 3, pages 5-7
- Section 5, Table 6, page 8
- Write the answer to the question below Table 6 (conclude your analysis)