Workshop

Part 1

Security risk management
Workshop (part I) plan

• Team formation
• Presentation of the workshop tasks
• Work on the tasks
• From the mid of lecture 2
  – Result (*so far*) overview – presentation:
    • 120 seconds max per team
Workshop (part I) plan

• Team formation
  
  Workload is estimated for 4-member team
  • Maximum team size – 5 members
  • You can form smaller teams or do the workshop task individually
    • You are expected to submit a report which equals to workload of 4-member team
  
  • Once you create your team:
    • Write its name and name of all its members in the course Message board
    • Your report will not be checked if the team name and members are not registered in the Message board:

<https://piazza.com/ut.ee/spring2019/mtat03307/home>
Workshop (part I) plan

• Team formation
• Presentation of the workshop tasks
• Work on the tasks
• From the mid of lecture 2
  – Result (so far) overview – presentation:
    • 120 seconds max per team
Workshop (part I) plan

• Team formation
• Presentation of the workshop tasks
• Work on the tasks
• From the mid of lecture 2
  – Result (so far) overview – presentation:
    • 120 seconds max per team
Workshop (part I) plan

- Team formation
- Presentation of the workshop tasks
- Work on the tasks
- From the mid of lecture 2
  - Result (*so far*) overview – presentation:
    - 120 seconds max per team

At the beginning of the presentation say:
- your team name
- the names of the team members
Workshop (part I) plan

• Team formation

• Presentation of the workshop tasks

• Work on the tasks
  – From the mid of lecture 2

  • Result (so far) overview
  – Presentation:
    • 120 seconds max per team

• At the beginning of the presentation say:
  • your team name
  • the names of the team members

• If your team is not present at the workshop, OR

• If less than 51% of the team members are present at the class
  • The team have to submit the recorded video presentation (of the final solution) together with the workshop solution.
Workshop (part I) plan

- Team formation
- Presentation of the workshop tasks
- Work on the tasks
  - From the mid of lecture 2
  - Result (so far) overview
  - presentation:
    - 120 seconds max per team
    - At the beginning of the presentation say:
      - your team name
      - the names of the team members
  - If your team is not present at the workshop, OR
  - If less than 51% of the team members are present at the class
    - The team have to submit the recorded video presentation (of the final solution) together with the workshop solution
  - If you are not present at the workshop, but the majority of your team was present at the class, make sure that you contribute equally to the workshop solution
 Tasks and Steps

1. Read the workshop scenario description and discuss the scenario within the team
Tasks and Steps

2. 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
Tasks and Steps

3. Discuss and define the scope of your further analysis

• It is much better to choose a narrow scope and provide extensive analysis in the narrow scope (then broad scope and shallow analysis in the broad scope)

Where to report?
• Section 1.2
Tasks and Steps

4. 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
- Textually (or graphically) explain the support below the Table 2.
Tasks and Steps

5. Analyse security risks

Each team should elicit 6 security risks.

- 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
Tasks and Steps

5. Analyse security risks

Each team should elicit 6 security risks.

- 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 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

Where to report?
- Section 2, Table 3
- Each security risk should have its “Table 3”.
  - Include additional tables
  - Change table captions to Table 3.1, Table 3.2 …
6. Define security countermeasures to mitigate security risks

For each risk separately!

Where to report?
- Section 3, Table 4.
- Each security risk should have its countermeasures reported in “Table 4”
  - Include additional tables
  - Change table captions to Table 4.1, Table 4.2 …
Workshop Tasks and Steps

7. Agree on the security metrics

For each risk and its security countermeasure!

Which risk(s) needs to be mitigated first?

• Use plots:
  – Risk reduction level versus Cost
  – Risk reduction level versus Value
  – Value versus Cost
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.
• 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 4.2-4.4, Fig. 1, Fig. 2, Fig. 3
- Section 4.5, Table 6
- Write the answer to the question below Table 6 (conclude your analysis)
Workshop Tasks and Steps

8. Estimate effort of each team member in the workshop

Where to report?
• Section 5, Table 7
Submission

• To submit:
  – Use the course Website

• Deadline:
  8.April, 23:59

Penalty of late submission minus 50% from the evaluation grade