Workshop 1

Security Risk Management
Discuss the selected case and perform the following tasks

Summary of workshop tasks:

1. Describe what the system is
2. Discuss and define the scope
3. Define system assets, business asset and their security criteria
4. Analyse security risks
5. Define security countermeasures to mitigate security risks
6. Agree on the security metrics

7. Prepare report with the answers to the above tasks
8. Record 3-5 minute presentation on the workshop results
9. Submit the report and presentation
Steps and Tasks

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

2. Discuss and define the scope

• It is much better to choose a narrow scope (e.g., only one business asset supported by few system assets) and provide extensive analysis in the narrow scope
Steps and Tasks

3. Define system assets, business asset and their security criteria

– What are the *business assets* and their *security criteria*?

– Explain how these business assets are supported by the *system assets*
Steps and Tasks

4. 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. Define security countermeasures to mitigate security risks

For each identified risk, consider:
– What security risk treatment decision is taken?
– What are security requirements to mitigate the risk?
– What controls implement the security requirement?

Security requirements must be defined following criteria of good requirements?
Workshop Tasks and Steps

6. Agree on the security metrics
   For each risk and its security countermeasures separately!
   • What are the security need?
   • What is the business asset value?
   • What is the vulnerability level, threat likelihood, event potentiality, impact level, and risk level?
   • What is the risk reduction level?
   • What is the cost of countermeasures?
Workshop Tasks and Steps

6. Agree on the security metrics

Which risk(s) needs to be mitigated first? You must explain your answer – for example, you can use plots:

- Risk reduction level versus Cost
- Risk reduction level versus Value
- Value versus Cost
Workshop Tasks and Steps

7. Prepare report with the answers to the above questions

8. Record 3-5 minute presentation

9. Submit the report and presentation
   - Submit report as the PDF file using Upload function in the course Website
   - Email the link of presentation to rma@ut.ee with email Subject [SSD-workshop]

Submission deadline – 3. March
Evaluation

• Workshop 1 report – **10 points**
  – You will receive feedback and will be able to improve the solution. The grade will be given for all three workshop solutions at the same time

• Workshop 1 presentation – **5 points**
  – The grade will be given after the presentation

• Post- workshop 1 questionnaire – **2 points**
Useful references
