Research Methods in Cybersecurity

Raimundas Matulevičius

rma@ut.ee
Introductory Seminar

• How to write 2-page problem statement?
• How to perform literature review?
• How bibliography needs to be organised?
• Few more quick tips for presentation
Introductory Seminar

- How to write 2-page problem statement?
- How to perform literature review?
- How bibliography needs to be organised?
- Few more quick tips for presentation

Does the abstract matter?
Requirements for 2-page problem statement

• Outline the following:
  • Short overview
  • Main research question
  • More specific research questions
  • Objectives
  • The initial plan for the Masters project
Abstract

• Two or three sentences about the current state of the art, identifying a particular problem

• One or two sentences about what this paper contributes to improving the situation

• One or two sentences about the specific result of the paper and the main idea behind it

• A sentence about how the result is demonstrated or defended
Six Questions

1. What is the problem?

2. Is this a real problem?

3. What is your solution (technical contribution)?

4. How does this solve the problem?

5. Is this a real solution?

6. Why is this good?
Six Questions

1. What is the problem?
   • Goal modelling is emerging as a central technique for dealing with trust in information systems development and aligning information systems with enterprise strategy. Unfortunately, current goal-oriented languages are not interoperable and easily comparable with one another, nor with other modelling languages used to represent other perspectives on enterprises and their information systems.

2. Is this a real problem?
   • This is a problem because the emerging generation of model-driven information systems will depend on coordinated use of several modelling languages to represent different perspectives on the enterprise and its proposed information system.

3. What is your solution (technical contribution)?
   • The paper applies a structured approach to describe the goal-oriented KAOS language, by mapping it onto a philosophically grounded, but extensible, ontology.
Six Questions

4. How does this solve the problem?
   • As other goal-oriented languages and languages representing other perspectives become described using the structured approach, they are made interoperable and available for comparison through their mappings onto the common ontology. The structured approach can thereby act as an intermediate language for comparison, consistency checking, update reflection, view synchronisation and, eventually, model-to-model translation across language and perspective boundaries.

5. Is this a real solution?
   • This shows that model driven security development improves the certain qualitative aspects of the system without affecting existing quality types.

6. Why is this good?
   • Because goal modelling is central to dealing with trust in information systems development, the paper contributes to developing trusted model-driven information systems.
Service orientation is a relatively new software development paradigm. It inherits a number of concepts and principles from earlier paradigms but differs from these paradigms in the manner in which the separation of concerns in the software system is done. In addition to this, it provides an additional software system abstraction layer – business logic layer. Service oriented architecture (SOA) is an architectural style that implements service-orientation approach. SOA raises new problems in software requirements engineering. As a result, new requirements engineering sub-discipline – service-oriented requirements engineering (SORE) – emerges. SORE focuses mainly on the identification of services and workflows used to modelling applications and on their reuse. The thesis highlights existing issues and concerns in SORE and discusses how one type of service specification issues – non-functional requirements capturing, analysis and conflicts resolution could be solved. The thesis defines a spiral process model for capture and analysis of non-functional requirements for Enterprise Service-Oriented Architecture – ESOA (a sub-style of SOA, operating in a less open environment than ordinary SOA and aimed at supporting enterprise business strategy and objectives) systems. The process model is based on classical as well as service-oriented RE process models, i* based modelling languages, viewpoints that are widely used Enterprise Architecture (EA) standards and frameworks, service-oriented architecture layers and can be applied in conjunction with service-oriented systems development methodologies. The experimental research – a case study – demonstrated that the proposed process model can be successfully applied to real-world ESOA systems as it facilitates capturing, analysis and resolution of conflicting non-functional requirements and improves the system’s quality.
Security level of the enterprise is one of the main elements that should be taken under control in the organization. It is difficult to maintain high security level of Information System. Since development of enterprise architecture is targeted on continues business flow modeling, it sometimes does not take into account security requirements.

The paper provides an approach to improve security countermeasures to contribute with secure Enterprise Architecture. Filling the gap between Enterprise Architecture model and Security Risk Management is done through Information System Security Risk Management domain model (ISSRM). To build the Enterprise Architecture model, ArchiMate modelling language is being used. Among different risk-oriented languages, selection was done in favor of Mal-activity diagrams, which help to provide visual concept of Security Risk Management. Structured alignment can show the mapping between aforementioned terms and provide the information about most vulnerable points of the system. The maintenance of security level will help to make business flow independent from the state of Information System.

Validation of our approach is done on the example, which is taken from CoCoME case study. It is shown on number of illustrative pictures. After getting the results, there is a comparison of the output between presented method and approach developed by Grandry et.al. (2013).
• Testing is an essential part of the software development lifecycle for gaining trust in the quality of the delivered product. Concerns have been raised over the maturity of existing test processes and techniques, and the desire to improve has been acknowledged. Unfortunately, the decisions on how the improvement should be carried out are not straightforward.

• This poses a variety of problems because even though there are test process improvement models available on the market, the guidelines on how to use them are unsatisfactory. Furthermore, insufficient information is available on how to choose the best model.

• The current thesis describes the literature study conducted on existing test process improvement models. As a result of this research, the potentially best model was chosen from the perspective of Playtech Estonia’s Casino unit. To evaluate the choice, we conducted a single-object case study of test process assessment and improvement process based on the selected Test Maturity Model integration (TMMi) in the Casino unit. As part of the assessment process, a survey was carried out and staff interviews were performed to obtain an understanding of test process maturity. Based on the outcome, improvements were proposed to Casino unit’s testing activities.

• We provide an overview of the test process maturity concept of the framework and suggest how the described best practices could be considered in the organisation’s improvement process. As a result of the assessment and improvement case study, we show the importance of understanding the reasons and objectives for test process improvement in consideration with the needs of the organisation. Identifying the best model is primarily dependent on defining organisation-side requirements for an improvement framework.

• An evaluation on the performance and suitability of TMMi in a software development organisation is presented based on the case study experience, raising also the concerns of its applicability in agile environments. Improvement possibilities for TMMi are described, which have been also forwarded to the model publisher TMMi Foundation, and contribute to the potential enhancement of the framework.
Introductory Seminar

• How to write 2-page problem statement?
• **How to perform literature review?**
• How bibliography needs to be organised?
• Few more quick tips for presentation
Systematic Review

Phase 1: Plan Review
1. Specify Research Questions
2. Develop Review Protocol
3. Validate Review Protocol

Phase 2: Conduct Review
4. Identify Relevant Research
5. Select Primary Studies
6. Assess Study Quality
7. Extract Required Data
8. Synthesise Data

Phase 3: Document Review
9. Write Review Report
10. Validate Report
1. Specify Research Question

- **Effect** of a software engineering technology
- **Frequency or rate** of a project development factor
  - (adoption of a technology, frequency or rate of project success or failure)
- **Cost and risk factors** associated with a technology
- Impact of technologies
  - reliability, performance and cost models
- **Cost / benefit** analysis of employing specific software development technologies or software applications
1. Specify Research Question

- Effect of a software engineering technology
- Frequency or rate of a project development factor (adoption of a technology, frequency or rate of project success or failure)
- Cost and risk factors associated with a technology
- Impact of technologies reliability, performance and cost models
- Cost / benefit analysis of employing specific software development technologies or software applications

- What evidence is there that cross-company estimation models are not significantly different from within-company estimation models for predicting effort for software/Web projects?

- Which experimental procedure is most appropriate for studies comparing within- and cross-company estimation models?
2. Developing Review Protocol

- Background
- The research questions
- The strategy that will be used to search for primary studies
  - including search terms and resources to be searched
- Study selection criteria
- Study selection procedures
- Study quality assessment checklists and procedures
- Data extraction strategy
- Synthesis of the extracted data
- Dissemination strategy
- Project timetable
3. Evaluating a Review Protocol

- If appropriate funding is available
  - a group of independent experts should be asked to review the protocol
  - same experts can later be asked to review the final report.

- Students should present their protocol to their supervisors for review and criticism
4. Identify Relevant Research

- Find as many primary studies relating to the research question as possible using an unbiased search strategy

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Library</td>
<td>Name of database</td>
</tr>
<tr>
<td></td>
<td>Search strategy for the database</td>
</tr>
<tr>
<td></td>
<td>Date of search</td>
</tr>
<tr>
<td></td>
<td>Years covered by search</td>
</tr>
<tr>
<td>Journal Hand Searches</td>
<td>Name of journal</td>
</tr>
<tr>
<td></td>
<td>Years searched</td>
</tr>
<tr>
<td></td>
<td>Any issues not searched</td>
</tr>
<tr>
<td>Conference proceedings</td>
<td>Title of proceedings</td>
</tr>
<tr>
<td></td>
<td>Name of conference (if different)</td>
</tr>
<tr>
<td></td>
<td>Title translation (if necessary)</td>
</tr>
<tr>
<td></td>
<td>Journal name (if published as part of a journal)</td>
</tr>
<tr>
<td>Efforts to identify unpublished</td>
<td>Research groups and researchers contacted (Names and contact details)</td>
</tr>
<tr>
<td>studies</td>
<td>Research web sites searched (Date and URL)</td>
</tr>
<tr>
<td>Other sources</td>
<td>Date Searched/Contacted</td>
</tr>
<tr>
<td></td>
<td>URL</td>
</tr>
<tr>
<td></td>
<td>Any specific conditions pertaining to the search</td>
</tr>
</tbody>
</table>
4. Identify Relevant Research

- Find as many primary studies relating to the research question as possible using an unbiased search strategy

**Software Engineering Digital Libraries**

- IEEExplore
- ACM Digital library
- SpringerLink
- Google scholar (scholar.google.com)
- Citeseer library (citeseer.ist.psu.edu)
- Inspec (www.iee.org/Publish/INSPEC/)
- ScienceDirect (www.sciencedirect.com)
5. Select Primary Studies

- **Study selection criteria** are intended to identify those primary studies that provide direct evidence about the research question.
  - selection criteria should be decided during the protocol definition, although they may be refined during the search process.
6. Assess study quality

• Detailed inclusion/exclusion criteria
  • Investigate whether quality differences provide an explanation for differences in study results
  • As a means of weighting the importance of individual studies when results are being synthesised
  • To guide the interpretation of findings and determine the strength of inferences
  • To guide recommendations for further research
6. Assess study quality

• Detailed inclusion/exclusion criteria

• Investigate whether differences in study design and methods are responsible for differences in study results
• As a means of weighting the importance of individual studies when results are being synthesised
• To guide the interpretation of findings and determine the strength of inferences
• To guide recommendations for further research

• Checklists of factors that need to be evaluated for each study
  – Quantitative and qualitative studies
7. Extract required data

• Design data extraction forms to accurately record the information researchers obtain from the primary studies
  • Linked to the research questions
8. Synthesise data

• Collating and summarising the results of the included primary studies
  • Descriptive (non-quantitative)
  • Quantitative

• The data synthesis activities should be specified in the review protocol
  • However, some issues cannot be resolved until the data is actually analysed
9. Write review report

- Specifying the dissemination strategy
  - Journal, conference paper, technical report,
- Formatting the main systematic review report
  - Section in thesis report
10. Validate report

• Journal articles will be peer reviewed as a matter of course

• Experts review theses as part of the examination process

• Technical reports are not usually subjected to any independent evaluation
Your report

At least 5-7 articles
Introductory Seminar

- How to write 2-page problem statement?
- How to perform literature review?
- **How bibliography needs to be organised?**
- Few more quick tips for presentation
How bibliography needs to be organised?

References should appear as

- **Book with one author:**

- **Book with two authors:**

- **Book with more than two authors:**

- **Journal article:**

- **A publication in press:**
How bibliography needs to be organised?

References should appear as

• **Edited book:**

• **Chapter in an edited book:**

• **Report from a university:**

• **Published proceedings:**
How bibliography needs to be organised?

References should appear as

- **Unpublished doctoral dissertation or master’s thesis:**

- **A presented paper:**

- **Web site:**
How bibliography needs to be organised?

**In-Text Citations**

- In-text citations should appear with author surname followed by publication year in parentheses
  
  (Brown, 2002)

- Citing several references in-text:
  - In most organizations, data resources are considered to be a major resource (Brown, 2002; Krall & Johnson, 2005; Smith, 2001).
  - Brown (2002) states that the value of data is recognized by most organizations
  - “In most organizations, data resources are considered to be a major organization asset” (Smith, 2001, pp. 35-36) and must be carefully monitored by the senior management.
  - Brown (2002) states that “the value of data is realized by most organizations” (p. 45).
How bibliography needs to be organised?

In-Text Citations

- If you have organised the citations with number in brackets
  - In most organizations, data resources are considered to be a major resource [15; 30; 84].
Introductory Seminar

• How to write 2-page problem statement?
• How to perform literature review?
• How bibliography needs to be organised?
• Few more quick tips for presentation
Presentation

• Present the following:
  • The problem statement
  • Background
  • Review of the state of the art
  • Identified gaps in the state of the art
  • The expected contribution given the identified gaps (objectives)

• Each student has a time-slot of 30 minutes:
  • 20 minutes for the talk + 10 minutes for Q&A
How **not** to do presentation

- Don McMillan: Life After Death by PowerPoint
  - [http://www.youtube.com/watch?v=WGiePuNFXwY](http://www.youtube.com/watch?v=WGiePuNFXwY)
  - [http://www.youtube.com/watch?v=zDvm1PVtgWo](http://www.youtube.com/watch?v=zDvm1PVtgWo)
  - [http://www.youtube.com/watch?v=lpvgfmEU2Ck](http://www.youtube.com/watch?v=lpvgfmEU2Ck)