Index

Slide 1 – Introduction

Welcome to this presentation for the Research Methods and Professional Practice Module of the Master of Science Cyber Security course. My name is Jan Küfner, I will walk you through the following slides where I will discuss certain aspects like for example aims and objectives, methodology utilized, research design and so on for my potential Master Thesis.

1. The title of my thesis will be “Tools & technology to secure IoT endpoints in a modern AI railway maintenance system”

Slide 2 – Significance

On this slide I will talk about the significance of the research problem

1. It is a fact that IoT devices due to cheap hardware will become more and more
2. It is also shown that AI can be utilized to predict railway maintenance in a better way. In the next slide I will explain more about the literature, where the afore mentioned statements come from
3. As conclusion to the afore mentioned facts, it can be stated that IoT device do influence railway safety, since not conducted maintenance can be a safety issue.
4. It is also a known fact that if you mess with training data coming from the IoT sensors, you will likely influence the AI
5. Therefore it is of urgency to protect AI controlled IoT endpoints in railway maintenance.

Slide 3 – Key literature

Now I will present you key literature on the topic. The literature chosen is a small subset of literature that is being used in the thesis. Additionally, considerably more literature is even looked at that will

not directly be cited in the master thesis but is nonetheless integrated in the thesis for evidence of wider reading.

The first article from the Journal of rail and rapid transit is called Cybersecurity for railways- A maturity model. It is written by Kour, Karim and Thaduri. This rather short article provides a good start in the thesis, since considerable work was conducted to map the situation in the railway sector with real life companies. This article showcases how necessary it is currently to implement cyber security tools in the railways sector.

The next article by Valdivia, which was featured in an IEEE magazine. IEEE magazines are by the way are great source for relevant literature on this topic, since they have several groups that publish about transportation, railway transportation and modern ICT driven transportation systems in general. This article is another very great supportive article that again maps the situation perfectly, but also provides a transition to the real Issue. The maintenance.

Kour as well as others dove more into the topic of railway maintenance. They clearly point to a future very dominant issue, that cheap IoT sensors everywhere in the field need to be analyzed, likely by AI and therefore sufficiently controlled against any malicious attacks. They however don`t suggest tools to efficiently do this.

Slide 4 – Significance/contribution to the discipline/research problem

Let`s come back to the question about significance of the topic.

1. As I stated earlier the need for the topic “Tools & technology to secure IoT endpoints in a modern AI railway maintenance system” is there
2. Now combined with the information about key literature it can be stated that the topic is not yet sufficiently discussed in literature. There is a considerable GAP within literature. The closure of this gap / my MSc Thesis will therefore contribute to the discipline by narrowing in on that gap.

Slide 5 – Research Question

Now let’s discuss the underlying research question, I plan to start with. This research question is likely to change within the 6 months of my MSc thesis, since by reading literature and by conducting experiments I am likely to have to adapt the question, since I gain knowledge a long the way. This iterative process of evolving the research question, is ideal to close the gap in literature and to provide a significant contribution to the topic.

1. “What tools & technology can secure IoT railway endpoints cost effectively and what is their performance?”
   Is the research question I am planning on starting with. This question is clear, focused and appropriately complex.

Slide 6 – Methodology/development strategy/research design

On this slide I will talk about the methodology, development strategy and the research design utilized.

1. I will be conducting quantitative research since I am gathering numerical data.
   Qualitative Research would not fit here, since qualified people, that can be interviewed or asked to fill out a questionnaire are very likely hard to find for this specific topic.
2. I will conduct an experiment. Within this experiment

3. I will create IoT nodes feeding to an AI.
   the IoT nodes can for example be coded in Docker to easily simulate their manifold.
4. Use various cyber security methods to secure the nodes.
   Methods here could for example be simple and typically also obligatory authentication, an intrusion detection system IDS and a block chain for integrity control.
5. Then I will attack the system and measure the impact on the performance of the AI.
   Attacks could be typical replay attacks, denial of Service attacks, node tampering attacks etc.
6. Lastly the cyber security methods are rated by performance impact, cost and exploitability.
7. I will be doing conclusive research. More precisely I will be doing a descriptive research design.

Slide 7 – Aims and objectives incl. timeline

Now let me introduce you to my planned Objectives and timelines

1. The first objective is to get a profound overview of state of the art in technology by finding reading and paraphrasing relevant scientific literature
2. This is planned to be done in the beginning of the project.
3. The 2nd objective is to "Investigate technologies that can be utilized for the experiment"
4. This will be done also in an early stage of the project.
5. The 3rd objective is to code the IoT nodes, train the chosen AI, run the simulation, and gather test data. Different cyber defense tools like blockchain as stated earlier for example will now be used.
6. This phase will contain most of the workload and therefore is planned for a long time without any parallel actions.
7. The 4th objective is reporting. Generally, I will be writing the MSc thesis, curating the GitHub repository, and creating the test reports in parallel, but most of the work is happening at the end of the literature review and tools selection section as well as obviously at the very end of the project, once the experiment is concluded.

Slide 8 – Ethical considerations

On this slide I will talk about ethical considerations

1. As it is planned right now, I will not conduct any surveys, interviews or similar. This will mean that there is no direct human participation to my work.
2. There will also be no data collection from any external source as it is planned right now. The data will only be created by experiment which is designed conducted and analyzed by me with no further participation from others.
3. I will also not analyze data that contains sensitive or personal identifiable information
4. In conclusion I can state that there is currently no University of Essex Online ethics approval necessary. If due to the iterative nature of a Master thesis, I plan to change any of the afore mentioned items, I of course have to revisit this conclusion

Slide 9 – Risk assessment

This slide shows the major risks involved.

1. Risks are shown within a table. To quantify a risk, I have its severity and its likeliness evaluated. A severe risk such as realizing in the last month that I cannot use the material created with a likely occurrence would be rated as a very high risk for example

2. The first and biggest risk I identified is that the implementation of the technology will be too complex. The severity is according to my judgment medium, since I have sufficient experience with AI, docker and pen-testing tools to cover a minimum. The overall risk is considered medium since it might likely happen that I will run into my limitations, since the topic chosen is challenging.
3. The next risk I identified is that I will identify literature that discusses exactly what I am trying to research. I think this is unlikely. Additionally, I would realize this in a very early stage and could easy alter my research question to fix this issue.
   This are not all risks that I might encounter in the project obviously. Due to time constraints of this presentation, I however was limited to only show a few.

Slide 10 – Description of artefacts that will be created

On this slide I will talk about the artefacts I will create

1. I will obviously strive to create a Master of Science Thesis.
2. I will also create the code for the IoT nodes, and the security counter measures within those nodes. I will choose the AI. I will create with the IoT nodes training data, which I will also version control in the GitHub repo, to have traceability, if I suspect issues or conclusions in the training data. Additionally, I try to create test scripts to automatize the comparative testing as much as possible.
3. Lastly the deliverables will contain human readable test reports as an appendix to the thesis.

Slide 11 – Conclusion

In conclusion it can be stated that the topic “Tools & technology to secure IoT endpoints in a modern AI railway maintenance system” is a good choice, since

1. I will close a significant gap in literature. Significant, since the manifold of IoT devices which are controlled via an AI in railways is very likely to come.
2. There is also sufficient literature available as a base. But there is also an appropriate gap so I can still do my Master of Science thesis.
3. The aims and objectives are clearly defined, and they also will fit into a six-month timeline
4. The methodology chosen (experiment) is fit for this purpose
5. Ethical considerations are conducted
6. Only medium risks are expected
7. To sum it up, the topic is suitable, challenging, relevant and doable

References

British Research Methodology (BRM) (n.d.) Research Design

Dawson, C. (2015) Projects in Computing and Information Systems A Student’s Guide Third Edition

Mitchell, J. (2018) Ethics vs Morality

Miessler, D. (2020) The Difference between Deductive and Inductive Reasoning

Sage (2021) Sage Research Methods: Methods Map

Saunders, M., Lewis, P. & Thornhill, A. (2012) Research Methods for Business Students 6th ed. Pearson Education Limited