

MSc project plan template

Einar Snekkenes



Master's Thesis Project Description
Master of Science in Information Security
5 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2007

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Revision history

Version #	Description of change (why, what where - a few sentences)
0.1	First version is made available via Fronter

Abstract

Abstract (1/2 page) This document provides format and guidelines for the MSc project descriptions. The document has been produced using MikTeX and TeXnicCenter.

The objective of the abstract is to provide the reader with an understanding of the work to be done and put him in the position to make a 'correct' decision regarding reading/not reading the report.

The abstract of the project description *must* include

- a summary of the problem description,
- motivation and
- a summary of the planned contribution from the master project in terms of *new* results.

Control questions

1. Does the abstract have a 'reasonable' length?
2. Is it clear to a non expert (e.g. a typical reader of a newspaper) what problem is addressed?
3. Does a person that has been working in the field find the text informative?
4. Do the results that might be obtained have the potential to be interesting to a lot of people? How interesting to how many and why?
5. Would a decision maker/manager be willing to pay NOK 400.000 to have the project completed (estimated salary costs + overheads) after having read the abstract? Why/why not?

Contents

Revision history	iii
Contents	iii
1 Contents of the project description	1
2 Introduction (1-2 pages)	3
2.1 Topic covered by the project	3
2.2 Keywords	3
2.3 Problem description	4
2.4 Justification, motivation and benefits	4
2.5 Research questions	5
2.6 Planned contributions	5
3 Related work (3-10 pages)	7
3.1 Handling Potential problems	7
4 Choice of methods (2-5 pages)	9
5 Milestones, deliverables and resources (2-5 pages)	11
6 Feasibility study (1/2-3 pages)	13
7 Risk analysis (1/2-2 pages)	15
8 Ethical and legal considerations (1/4-1 page)	17

1 Contents of the project description

The project description must use the gucmasterproject class file and contain the following elements/chapters:

Front page

Table of contents

Abstract

1 Introduction

1.1 Topic covered

1.2 Keywords

1.3 Problem description

1.4 Justification motivation and benefits

1.5 Research questions

1.6 Planned contributions

2 Related work

3 Choice of methods

4 Milestones, deliverables and resources

5 Feasibility study

6 Risk analysis

7 Ethical and legal considerations

Bibliography

Appendix

A Acronyms and abbreviations

Each chapter must contain the information specified in this document and further explained in lectures or included in lecture notes.

2 Introduction (1-2 pages)

The introduction chapter should not include detailed information on how you intend to solve the problem, what you're going to do etc. This belongs more in the 'method' and 'feasibility study' section of the research proposal.

Make sure you read several of the past project proposals. Make your own judgment on how 'good' they are.

2.1 Topic covered by the project

This section specifies the general area of the project. It should preferably be understandable by everybody, also those not familiar with the field. (e.g. all your relations and friends).

The purpose of the topic section is to:

- Very quickly give the reader some idea of the perspective taken with respect to problem addressed.
- Help a reader to decide if the project is within the readers area of interest and scope.
- Help the author (you!) to see if he has the necessary skills, if he/she needs to get access to specific expertise etc. Do you have the right skills/ background/ knowledge to be able to carry out the project?

Control questions:

1. Does it have the right length?
2. Is it focused or is it just a non-focused brain dump going all over the place?
3. Is it clear from the text what skills would be required/beneficial in order to do/participate in the project?

2.2 Keywords

There are several sources of keywords. Rather than 'inventing your own' you should select an appropriate set of keywords from a reputable source such as the one published by the IEEE computer society (IEEE Computer Society - Keywords). The taxonomy by Avizienis et al[?] provides an overview of of the subject area and an alternative set of keywords/classifications.

Control questions:

1. Does the collection of keywords 'pin down' the project or is it to 'wide'?
2. Are the keywords too specific, making it difficult for people with a closely related interest to recognize the keywords?
3. Why is it likely that a person working in the field would use the keywords you have selected when doing a search in this area?
4. Is the number of keywords appropriate?

2.3 Problem description

The one of the main and indecipherable problem in security discipline is formulating general threat definition and recognizing malicious activity and all this problems unsurprisingly reflect on information and computer security concept. Security is defined by system's identification, which involve with purpose, crowd, design structures, network model and so on, and today's information system which is designed with various architectural forms is protected against malware by general purpose protection tools. In the market, The anti malware tools producers focused on pragmatic solutions to survive, but it leads to that most of these tools are utterly reverse engineering process which works on result instead of reason.

With usual and pragmatic signature based methods, there are two mainstream techniques to detect malicious code which are called static and dynamic analysis. Static analysis identifies malwares mainly with code flow graph and data flow graph on stored file which is not processing. However, On the dynamic side it is a bit more tricky to analyze process, because you are working on the running pieces of codes without knowledge of structures and worse than this, it must concern race condition and memory coherency flaws.

The detection methods and techniques have been adequately worked so far because of the simplicity of architectures and usage of the massive generic computers, However, with increasing of the not standardized, parallel and popular devices like arm's SoC, it is not hard to estimate their new challenges. It is really likely to evade and obfuscate properly your on-the-fly processes with using uncertain charactership of parallel processing, complexity of concurrent programming, and structure of "Non Uniform Memory Architecture".

2.4 Justification, motivation and benefits

This section should be understandable by everybody including your family and relatives. In particular, it should be understandable to those who will benefit. NOTE : 'I want to do zz' does not count as a legitimate motivation!

- Why is important to solve the problem you have identified?
- Why would 'mankind' benefit from a solution to the problem identified?
- Who would benefit (the stakeholders)?
- What are the primary and secondary benefits - what's in it for the stakeholders?

You should try to find a journal, conference or newspaper article identifying the problem you will be adresssing. This can be used to substantiate your claim that the problem you are adresssing is significant.

Control questions

1. For each of the issues listed above, has the issue been addressed properly/thoroughly?
2. What is the information density of your text and why?
3. If the project results was to be put in an auction when the project was completed - what price would it fetch and who would put in what bids?
4. What would be the overall ROI (Return On Investment) of your project if carried out?

2.5 Research questions

Describe the types of information you need in order to solve the research problem, e.g. We need to find out

- what factors affect xx (where xx is the 'parameter' you want to improve, e.g. cost, time, usability, security, etc.)
- to what extent will activity/ method/procedure yy (where yy is some method of improving the parameter, e.g. a program for simplifying access) improve factor xx?
- have somebody solved this or some closely related problem?
- how well has the problem been solved?
- what is the theoretically 'best' one can achieve?

Control questions:

1. Are there any questions at all? Look for '?'...
2. Why are the research questions relevant to the research problem?
3. What other research questions might also be relevant?
4. why/why not are the chosen research questions the most relevant?

2.6 Planned contributions

A short summary of what kind of *new* results the master thesis will produce. Ideally, the potential novelty of the results should be justified by means of references provided. E.g. if an article describes the problem you will be addressing as *unsolved*, you should include this reference. Similarly, if you e.g. have some ideas on how an authentication method can be improved in terms of FAR/FRR, you should specify the best FAR/FRR figures published and a reference to where this was published. The goal of the master thesis will be to produce the new results identified in this section.

Control questions

1. Is the length of the section appropriate and why?
2. Why/why not are the contributions 'significant'?
3. Why/why not is it realistic that the planned contribution can be achieved? You may want to have a look at relevant literature/ other completed master thesis to answer this question.

3 Related work (3-10 pages)

The purpose of this chapter is to explain to the reader what knowledge is already available from the literature.

The purpose of the related work chapter is to:

- Identify to what extent information identified in the 'Research questions' section is provided in the literature.
- Give an overview of why/how the literature provides the answer to the research questions identified.
- Identify areas/ research questions where the literature appears to be weak or non-existent.

The Related Work Chapter is NOT:

- A list of abstracts and summaries of more-or-less-relevant literature.

If you have

- found some relevant literature
- made summaries of what you have written

you should

- reorganize these summaries to focus on the research questions you have identified.

This chapter should include one subsection for each of the research questions identified in section 2.5.

3.1 Handling Potential problems

When searching for literature, you usually get too many hits or none at all...

Question 1

I don't find any relevant literature.

Answer 1.A

Make a list of words, phrases, applications, abbreviations, organizations, terminology etc. relevant for your area of interest. Ask a librarian to sit with you for 20 minutes to formulate relevant queries to available databases. Record your findings.

Answer 1.B

Go to the ACM (www.acm.org) or IEEE (www.ieee.org) web pages. Identify the SIGs (Special Interest Groups) of these organizations. Select the SIGs which looks the most interesting. Most SIGs publish one or more journals and/or organize workshops or conferences. Get hold of a few journals or proceedings and see if they're any interesting.

Question 2

I've found a lot of papers. They all look interesting, but I don't have time to read them all.

Answer 2.A

Narrow your search. Be more specific in your search. Read the abstracts of the relevant articles before you read the full papers.

Answer 2B

Find a citation index (e.g. <http://citeseer.ist.psu.edu/>). Read those papers with a high citation score first (a citation index rates papers according to 'academic popularity'). Alternatively, read those papers published in 'prestigious' conference proceedings or journals first.

Control questions:

1. Why can we have confidence that the most relevant literature has been identified?
2. is the related literature grouped in a sensible way such that the reader gets a good understanding of 'existing knowledge' relating to th research questions/problem description?
3. Is the chapter sufficiently comprehensive?

4 Choice of methods (2-5 pages)

This section is to include a description of the methods to be used, including references to literature describing the methods to be used (e.g. qualitative, quantitative, interviews, surveys, questionnaire, model building etc.) For each of the research questions to be addressed, the chapter is to explain why the method is

- appropriate
- likely to provide the desired knowledge/information.

5 Milestones, deliverables and resources (2-5 pages)

The purpose of this chapter is to convince the reader that you know exactly what to do. This chapter gives a description of how the project is to be broken down into smaller parts and activities.

1. What is it you have to do in order to obtain the desired knowledge?
2. What deliverables are to be produced (MSc thesis report, software,...)
3. When are the various deliverables going to be available?

For each deliverable, identify 4 versions, having an 'increasing' degree of completeness/quality. Students are strongly recommended to review each others drafts. For each version of a deliverable explain why and how this version is to be better/more complete. E.g. v1.0: my first draft - chapter text includes 1/2 page summaries only. v2.0: Like v1.0, but comments by NN(who? fellow student) has been incorporated. v3.0:....

This section is to include a preliminary table of contents for the MSc thesis (only include 2 levels).

For each of the activities identified, specify

1. the time you need to complete each activity both calendar time and 'man-hours'.
2. hours needed by you
3. things you need to buy (consumables)
4. equipment, lab space or facilities you need access to
5. contributions from others (e.g. survey/interview participants) and how much each will have to contribute in terms of resources (probably time)

At the beginning of this section, provide a 2-3 line summary of the resource requirements. This is particularly useful if you have broken down the task into a lot of small tasks.

6 Feasibility study (1/2-3 pages)

An analysis of why it is likely that the desired results can be produced within the given time and resource bounds. This may include a description of

- similar projects completed by others and their 'resource consumption',
- an attempt to answer parts of the research questions
- the 'difficult' elements of the work and an explanation of why/how these problems can be solved. Alternatively you can explain an 'approximate' solution.

7 Risk analysis (1/2-2 pages)

In this project, there five inevitable risks which we can face during development.

- The thesis is highly dependent on the hardware, and the cost of the hardware constitute risk on its own. Any case of hardware defect leads to comprise obstacle.
- Hardware dependency is also leads to logistical and time consuming risk which could result with latency on submit time.
- Firmware codes which we are planning to work on are mostly undocumented. We could discover their usage by proper reverse engineering and fuzzing process when required, however it is obviously manpower.
- Most important and highlighting risk is there isn't proper research on this particular area. That means there are strongly possibly hidden risks which could cause other mental and physical result.
- During testing and purification part, Anti-malware tools could come out with unreliable result. To analyze result properly, we may need to inspect mentioned tools with reverse engineering process which could violate proper usage agreement. To mitigate that kind of risks, we could request research agreement from companies.

8 Ethical and legal considerations (1/4-1 page)

The content of this document could be used in order to malicious purpose, but any matter or information could be misused in the life and ignorance is not known well as a defense strategy. In this purpose, this thesis aims to enlighten security specialist and system developers against recent way of the possible attacks.

However, in order to act ethical responsibility, we tried to eliminate practice of tools and piece of codes which could leads malicious usage. In any case, there is no doubt that it is critical to discover and publish vulnerabilities which could cause deep impact before malicious people discover and abuse them.

Virus don't harm, ignorance does.
- VxHeaven