



DEPARTMENT OF
COMPUTER SCIENCE

THIAGO ARAUJO MONTEIRO

BSc in Computer Science and Engineering

CREATING A THREAT MODELING PROTOCOL FOR NON-HIERARCHICAL ORGANIZATIONS

Dissertation Plan
MASTER IN COMPUTER SCIENCE AND ENGINEERING

NOVA University Lisbon

Draft: December 1, 2024



DEPARTMENT OF
COMPUTER SCIENCE

CREATING A THREAT MODELING PROTOCOL FOR NON-HIERARCHICAL ORGANIZATIONS

THIAGO ARAUJO MONTEIRO

BSc in Computer Science and Engineering

Adviser: Kevin Gallagher

Full Professor, NOVA University Lisbon

Dissertation Plan
MASTER IN COMPUTER SCIENCE AND ENGINEERING

NOVA University Lisbon

Draft: December 1, 2024

ABSTRACT

Regardless of the language in which the dissertation is written, usually there are at least two abstracts: one abstract in the same language as the main text, and another abstract in some other language.

The abstracts' order varies with the school. If your school has specific regulations concerning the abstracts' order, the NOVAthesis L^AT_EX (`novathesis`) (L^AT_EX) template will respect them. Otherwise, the default rule in the `novathesis` template is to have in first place the abstract in *the same language as main text*, and then the abstract in *the other language*. For example, if the dissertation is written in Portuguese, the abstracts' order will be first Portuguese and then English, followed by the main text in Portuguese. If the dissertation is written in English, the abstracts' order will be first English and then Portuguese, followed by the main text in English. However, this order can be customized by adding one of the following to the file `5_packages.tex`.

```
\ntsetup{abstractorder={<LANG_1>,...,<LANG_N>}}  
\ntsetup{abstractorder={<MAIN_LANG>={<LANG_1>,...,<LANG_N>}}}
```

For example, for a main document written in German with abstracts written in German, English and Italian (by this order) use:

```
\ntsetup{abstractorder={de={de,en,it}}}
```

Concerning its contents, the abstracts should not exceed one page and may answer the following questions (it is essential to adapt to the usual practices of your scientific area):

1. What is the problem?
2. Why is this problem interesting/challenging?
3. What is the proposed approach/solution/contribution?
4. What results (implications/consequences) from the solution?

Keywords: One keyword, Another keyword, Yet another keyword, One keyword more, The last keyword

RESUMO

Independentemente da língua em que a dissertação está escrita, geralmente esta contém pelo menos dois resumos: um resumo na mesma língua do texto principal e outro resumo numa outra língua.

A ordem dos resumos varia de acordo com a escola. Se a sua escola tiver regulamentos específicos sobre a ordem dos resumos, o template (L^AT_EX) *novathesis* irá respeitá-los. Caso contrário, a regra padrão no template *novathesis* é ter em primeiro lugar o resumo *no mesmo idioma do texto principal* e depois o resumo *no outro idioma*. Por exemplo, se a dissertação for escrita em português, a ordem dos resumos será primeiro o português e depois o inglês, seguido do texto principal em português. Se a dissertação for escrita em inglês, a ordem dos resumos será primeiro em inglês e depois em português, seguida do texto principal em inglês. No entanto, esse pedido pode ser personalizado adicionando um dos seguintes ao arquivo `5_packages.tex`.

```
\abstractorder(<MAIN_LANG>):={<LANG_1>,...,<LANG_N>}
```

Por exemplo, para um documento escrito em Alemão com resumos em Alemão, Inglês e Italiano (por esta ordem), pode usar-se:

```
\ntsetup{abstractorder={de={de,en,it}}}
```

Relativamente ao seu conteúdo, os resumos não devem ultrapassar uma página e frequentemente tentam responder às seguintes questões (é imprescindível a adaptação às práticas habituais da sua área científica):

1. Qual é o problema?
2. Porque é que é um problema interessante/desafiante?
3. Qual é a proposta de abordagem/solução?
4. Quais são as consequências/resultados da solução proposta?

Palavras-chave: Primeira palavra-chave, Outra palavra-chave, Mais uma palavra-chave, A última palavra-chave

CONTENTS

List of Figures	iv
Acronyms	v
1 Introduction	1
1.1 Context	1
1.2 Your Time is Precious	2
2 Background and Related Work	3
2.1 Introduction	3
2.2 Quick Start	3
2.2.1 With a Local L ^A T _E X Installation	3
3 Research Design	4
4 Conclusion	5
5 Work Plan	6
Bibliography	7

LIST OF FIGURES

ACRONYMS

novathesis NOVAthesis L^AT_EX (*pp. [i](#), [ii](#)*)

INTRODUCTION

1.1 Context

A segurança cibernética moderna frequentemente pressupõe a existência de estruturas hierárquicas, o que pode não ser adequado para organizações que operam de maneira horizontal, como cooperativas de trabalhadores, sindicatos, organizações ativistas, etc. Essas organizações, que evitam deliberadamente estruturas hierárquicas, enfrentam desafios únicos em termos de segurança, pois as soluções tradicionais não consideram a horizontalidade de todo. Este projeto visa desenvolver protocolos de modelagem de ameaças que valorizem a horizontalidade, especificamente para as organizações mencionadas.

Organizações hierárquicas são estruturadas de forma que o poder e a tomada de decisões fluem de cima para baixo. Em uma organização hierárquica típica, há uma cadeia de comando clara, onde cada nível da hierarquia tem autoridade sobre o nível abaixo. Por exemplo, em uma empresa tradicional, o CEO toma decisões estratégicas que são implementadas por gerentes de nível médio e, finalmente, executadas por funcionários de nível operacional. Este modelo facilita a tomada de decisões rápidas e a implementação de políticas de segurança, pois há uma clara atribuição de responsabilidades e controle [4].

Em contraste, organizações não-hierárquicas, ou horizontais, distribuem o poder de forma mais equitativa entre seus membros. Nessas organizações, a tomada de decisões é frequentemente feita de forma coletiva, através de processos democráticos e participativos. Por exemplo, em uma cooperativa de trabalhadores, todos os membros podem ter uma voz igual nas decisões importantes, e não há uma cadeia de comando rígida. Isso pode levar a uma maior transparência e inclusão, mas também pode criar desafios únicos em termos de segurança, como a dificuldade em gerenciar o acesso a informações sensíveis sem criar uma hierarquia implícita [4].

Um dos principais desafios de segurança em organizações horizontais é a gestão de segredos, como senhas e chaves de criptografia. Em uma organização hierárquica, esses segredos são frequentemente controlados por um pequeno grupo de administradores que têm autoridade para gerenciar o acesso. No entanto, em uma organização horizontal,

decidir quem deve ter acesso a esses segredos pode ser mais complicado. Se todos os membros tiverem acesso, há um risco maior de abuso ou erro humano. Por outro lado, restringir o acesso a um pequeno grupo pode criar uma hierarquia de fato, minando os princípios de horizontalidade [4].

Ao desenvolver protocolos de modelagem de ameaças para organizações horizontais, é crucial considerar a horizontalidade como um ativo. Isso significa criar sistemas de segurança que não apenas protejam contra ameaças externas, mas que também respeitem e reforcem a estrutura participativa da organização. Por exemplo, em vez de confiar em um único administrador para gerenciar o acesso a recursos críticos, pode-se implementar um sistema de autorização coletiva, onde múltiplos membros devem concordar antes que o acesso seja concedido. Isso não só distribui a responsabilidade, mas também aumenta a resiliência contra ataques internos, pois um único indivíduo não pode comprometer o sistema [4].

Além disso, a horizontalidade pode ser usada para melhorar a detecção e resposta a incidentes de segurança. Em uma organização hierárquica, a detecção de ameaças pode ser centralizada, o que pode levar a pontos únicos de falha. Em uma organização horizontal, a detecção de ameaças pode ser distribuída entre todos os membros, aumentando a probabilidade de que atividades suspeitas sejam rapidamente identificadas e respondidas [1].

Ao considerar a horizontalidade como um ativo na modelagem de ameaças, podemos desenvolver protocolos de segurança que não apenas protejam as organizações horizontais, mas que também reforcem seus princípios fundamentais de participação e igualdade. Este projeto busca explorar essas possibilidades e criar um novo paradigma de segurança cibernética que seja verdadeiramente adequado para organizações não-hierárquicas [6].

1.2 Your Time is Precious

BACKGROUND AND RELATED WORK

This manual is outdated and must be revised!

2.1 Introduction

This Chapter describes how to use the

2.2 Quick Start

2.2.1 With a Local \LaTeX Installation

Follow these steps to get started with a local \LaTeX installation:

RESEARCH DESIGN

This Chapter aims at exemplifying how to do common stuff with \LaTeX . We also show some stuff which is not that common! ;)

Please, use these examples as a starting point, but you should always consider using the *Big Oracle* (aka, [Google](#), your best friend) to search for additional information or alternative ways for achieving similar results.

CONCLUSION

This Chapter aims at exemplifying how to do common stuff with \LaTeX . We also show some stuff which is not that common! ;)

Please, use these examples as a starting point, but you should always consider using the *Big Oracle* (aka, [Google](#), your best friend) to search for additional information or alternative ways for achieving similar results.

WORK PLAN

This Chapter aims at exemplifying how to do common stuff with \LaTeX . We also show some stuff which is not that common! ;)

Please, use these examples as a starting point, but you should always consider using the *Big Oracle* (aka, [Google](#), your best friend) to search for additional information or alternative ways for achieving similar results. Citing something online [2, 3, 5].

BIBLIOGRAPHY

- [1] G. Almashaqbeh, A. Bishop, and J. Cappos. “ABC: A Cryptocurrency-Focused Threat Modeling Framework”. In: *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2019, pp. 859–864. DOI: [10.1109/INFOCOMW.2019.8845101](https://doi.org/10.1109/INFOCOMW.2019.8845101) (cit. on p. 2).
- [2] W. contributors. *Shunting-yard algorithm* — *Wikipedia, The Free Encyclopedia*. 2017-03. URL: https://en.wikipedia.org/w/index.php?title=Shunting-yard_algorithm&oldid=817901155 (visited on 2018-03-01) (cit. on p. 6).
- [3] *Fast Lexical Analyser*. URL: <https://github.com/westes/flex> (visited on 2020-07-26) (cit. on p. 6).
- [4] K. Gallagher et al. “COLBAC: Shifting Cybersecurity from Hierarchical to Horizontal Designs”. In: *Proceedings of the 2021 New Security Paradigms Workshop*. NSPW ’21. Virtual Event, USA: Association for Computing Machinery, 2022, pp. 13–27. ISBN: 9781450385732. DOI: [10.1145/3498891.3498903](https://doi.org/10.1145/3498891.3498903). URL: <https://doi.org/10.1145/3498891.3498903> (cit. on pp. 1, 2).
- [5] *Gnu Bison*. URL: <https://www.gnu.org/software/bison/> (visited on 2020-07-26) (cit. on p. 6).
- [6] M. Howard and S. Lipner. *The Security Development Lifecycle: SDL, a Process for Developing Demonstrably More Secure Software*. Secure software development series. Microsoft Press, 2006. ISBN: 978-07356-2214-2 (cit. on p. 2).

