Dissertation Plan

MASTER IN COMPUTER SCIENCE AND ENGINEERING

NOVA University Lisbon

Draft: *December 9, 2024*

Dissertation Plan
MASTER IN COMPUTER SCIENCE AND ENGINEERING

NOVA University Lisbon
Draft: *December 9, 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 LaTeX (novathesis) (LaTeX) 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 (LaTeX) 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

Acronyms

novathesis NOVAthesis LaTeX *i, ii)*

1

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.

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.

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.

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.

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.

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.

1.2 Objective

O objetivo principal desta tese é desenvolver um protocolo de modelagem de ameaças especificamente adaptado para organizações não-hierárquicas, como cooperativas de trabalhadores, sindicatos, grupos ativistas e projetos de software de código aberto. Este protocolo visa abordar os desafios únicos enfrentados por essas organizações em termos de segurança cibernética, considerando a horizontalidade como um ativo e não como uma limitação.

O desenvolvimento de um protocolo de modelagem de ameaças que leve em consideração a estrutura participativa e democrática das organizações não-hierárquicas é essencial para garantir que as soluções de segurança não comprometam os princípios de igualdade e participação. A avaliação da eficácia do protocolo desenvolvido será realizada com membros de diferentes organizações que exibem variados níveis de horizontalidade, analisando como o protocolo se adapta a diferentes contextos e necessidades específicas de cada tipo de organização.

Além disso, será feita uma comparação entre o novo protocolo e os modelos de ameaças tradicionais, como STRIDE e DREAD, destacando as vantagens e desvantagens de cada abordagem em contextos horizontais. A identificação dos principais desafios de segurança enfrentados por organizações não-hierárquicas e a proposição de soluções que respeitem e reforcem a estrutura participativa dessas organizações são passos cruciais para o sucesso do protocolo.

Por fim, a documentação de casos de uso reais onde o protocolo foi implementado fornecerá exemplos práticos de como ele pode ser aplicado e os resultados obtidos.

1.3 Contributions

Esta tese pretende apresentar várias contribuições significativas para o campo da segurança cibernética em organizações não-hierárquicas. Primeiramente, desenvolveremos um protocolo de modelagem de ameaças que considera a horizontalidade como um ativo, abordando os desafios únicos enfrentados por cooperativas de trabalhadores, sindicatos, grupos ativistas e projetos de software de código aberto. Este protocolo será projetado

para respeitar e reforçar a estrutura participativa dessas organizações, garantindo que as soluções de segurança não comprometam os princípios de igualdade e participação.

Em segundo lugar, realizaremos uma avaliação detalhada da eficácia do protocolo desenvolvido, envolvendo membros de diferentes organizações com variados níveis de horizontalidade. Esta avaliação permitirá analisar como o protocolo se adapta a diferentes contextos e necessidades específicas, fornecendo insights valiosos sobre sua aplicabilidade prática e eficácia em ambientes reais.

Além disso, compararemos o novo protocolo com modelos de ameaças tradicionais, como STRIDE e Attack trees, destacando as vantagens e desvantagens de cada abordagem em contextos horizontais. Esta comparação não apenas ilustrará a necessidade de soluções de segurança adaptadas para organizações não-hierárquicas, mas também fornecerá uma base sólida para futuras pesquisas e desenvolvimentos no campo.

1.4 Structure

O primeiro capítulo, Introdução, apresenta o contexto e a motivação do estudo, destacando a necessidade de um protocolo específico para organizações horizontais e delineando os objetivos da pesquisa. O segundo capítulo, Background and Related Work, revisa a literatura existente sobre modelagem de ameaças e as características das organizações não-hierárquicas, fornecendo uma base teórica para o desenvolvimento do protocolo. O terceiro capítulo, Design, descreve o novo protocolo. O quarto capítulo, Conclusion, sintetiza os principais achados da pesquisa, discutindo as implicações dos resultados e sugerindo direções para trabalhos futuros. Finalmente, o capítulo Work Plan detalha o cronograma e as etapas previstas para a implementação e validação do protocolo.

2

Background and Related Work

2.1 Modelagem de Ameaças: Conceitos

A modelagem de ameaças é um processo estruturado que visa identificar, analisar e mitigar riscos de segurança em sistemas e aplicações. Na sua base, um modelo de ameaças genérico oferece uma abordagem sistemática para entender as vulnerabilidades potenciais de um sistema e as possíveis ações que os adversários podem tomar para explorá-las. Ele serve tanto como uma ferramenta de design quanto um quadro de avaliação, apoiando o desenvolvimento seguro de sistemas e a mitigação proativa de riscos.

O processo geralmente começa com a caracterização do sistema em análise. Isso envolve definir sua arquitetura, identificar ativos críticos e mapear o fluxo de dados através de seus componentes. Um entendimento completo das fronteiras de confiança — pontos onde os dados transitam entre áreas com diferentes níveis de segurança — é essencial. Essas fronteiras frequentemente destacam áreas de vulnerabilidade aumentada, onde as ações adversárias são mais prováveis de ocorrer.

Uma vez que o sistema é mapeado, o foco se desloca para a identificação de ameaças potenciais. Técnicas como STRIDE fornecem uma estrutura para categorizar sistematicamente as ameaças. Alternativamente, representações gráficas como árvores de ataque mapeiam visualmente caminhos de ataque potenciais, oferecendo uma maneira intuitiva de avaliar vulnerabilidades.

Após as ameaças serem identificadas, seu impacto potencial é analisado. Esta análise envolve avaliar a probabilidade de cada ameaça e a gravidade de seu impacto na funcionalidade e segurança do sistema. Ferramentas que variam de métodos qualitativos, como revisões de especialistas, a modelos formais, como redes de Petri, apoiam esta fase. O objetivo é priorizar riscos, garantindo que os esforços de mitigação se concentrem nas vulnerabilidades mais críticas.

Estratégias de mitigação são então desenvolvidas para abordar os riscos identificados. Essas estratégias podem incluir controles técnicos, como criptografia ou gestão de acesso, bem como medidas organizacionais como políticas e treinamentos. Um modelo de ameaças genérico também inclui loops de feedback, garantindo que, à medida que o

sistema evolui, o modelo de ameaças seja atualizado para refletir novas vulnerabilidades e ameaças.

Embora os métodos de modelagem de ameaças variem amplamente, eles compartilham um foco comum na análise metódica e defesa proativa. Seja aplicado manualmente ou com ferramentas automatizadas, o processo fornece uma visão abrangente dos riscos potenciais, permitindo que desenvolvedores e profissionais de segurança abordem proativamente as vulnerabilidades antes que possam ser exploradas.

2.1.1 STRIDE

A metodologia STRIDE é uma das mais maduras e amplamente utilizadas para modelagem de ameaças. Desenvolvida por Loren Kohnfelder e Praerit Garg em 1999 e adotada pela Microsoft em 2002, STRIDE evoluiu ao longo do tempo para incluir novas tabelas específicas de ameaças e variantes como STRIDE-per-Element e STRIDE-per-Interaction. A metodologia STRIDE é baseada na criação de Diagramas de Fluxo de Dados (DFDs) para identificar entidades do sistema, eventos e limites do sistema. A precisão dos DFDs é crucial para o sucesso da aplicação do STRIDE, embora seu uso exclusivo possa ser limitante, pois não representa decisões arquitetônicas relacionadas à segurança.

O acrônimo STRIDE representa seis categorias de ameaças: Spoofing (falsificação de identidade), Tampering (manipulação de dados), Repudiation (repúdio), Information Disclosure (divulgação de informações), Denial of Service (negação de serviço) e Elevation of Privilege (elevação de privilégio). Cada uma dessas categorias corresponde a uma propriedade de segurança violada, como autenticação, integridade, não-repúdio, confidencialidade, disponibilidade e autorização, respectivamente. A metodologia STRIDE é utilizada para identificar ameaças conhecidas com base nessas categorias, auxiliando na navegação pelo modelo do sistema criado na fase inicial.

Apesar de a Microsoft não manter mais o STRIDE, ele ainda é implementado como parte do Ciclo de Vida de Desenvolvimento Seguro da Microsoft (SDL) com a Ferramenta de Modelagem de Ameaças, que continua disponível. A metodologia STRIDE é fácil de adotar, mas pode ser demorada, especialmente à medida que a complexidade do sistema aumenta. Estudos descritivos da técnica de modelagem de ameaças da Microsoft mostram que o STRIDE tem uma taxa moderadamente baixa de falsos positivos e uma taxa moderadamente alta de falsos negativos.

A aplicação do STRIDE não se limita a sistemas cibernéticos, mas também a sistemas ciber-físicos, demonstrando sua versatilidade. Além disso, a metodologia STRIDE pode ser combinada com outras abordagens de modelagem de ameaças para criar uma visão mais robusta e abrangente das potenciais ameaças. A escolha da metodologia de modelagem de ameaças deve considerar áreas específicas a serem abordadas, o tempo disponível para a modelagem, a experiência com modelagem de ameaças e o nível de envolvimento dos stakeholders.

Em resumo, a metodologia STRIDE é uma ferramenta poderosa para identificar e

mitigar ameaças em sistemas complexos. Sua aplicação em organizações não hierárquicas pode ser particularmente valiosa, pois permite uma abordagem sistemática para a segurança, considerando a horizontalidade como um ativo. A adoção de STRIDE, juntamente com outras metodologias de modelagem de ameaças, pode proporcionar uma defesa mais focada e eficaz contra ameaças cibernéticas.

2.1.2 Attack trees

As árvores de ataque são uma das técnicas mais antigas e amplamente aplicadas para modelagem de ameaças em sistemas cibernéticos, ciber-físicos e físicos. Desenvolvidas por Bruce Schneier em 1999, inicialmente foram aplicadas como um método independente e, desde então, têm sido combinadas com outros métodos e frameworks. As árvores de ataque são essencialmente diagramas que representam ataques a um sistema em forma de árvore. A raiz da árvore é o objetivo do ataque, e as folhas são as maneiras de alcançar esse objetivo. Cada objetivo é representado como uma árvore separada, resultando em um conjunto de árvores de ataque para a análise de ameaças do sistema.

A construção de uma árvore de ataque geralmente requer algumas iterações de decomposição do objetivo. Uma vez identificados todos os nós folha, podem ser atribuídos marcadores de possibilidade, que devem ser definidos após uma pesquisa relevante sobre cada etapa. Durante o exame de diferentes métodos para alcançar o objetivo, pode-se perceber que isso pode ser realizado de várias maneiras. Para incorporar essas diferentes opções na árvore, devem ser usados nós AND e OR. Nós AND indicam que ambos os nós devem ser realizados para avançar para a próxima etapa, enquanto nós OR representam alternativas. Em sistemas complexos, árvores de ataque podem ser construídas para cada componente, em vez de para o sistema como um todo.

As árvores de ataque são fáceis de entender e adotar, mas são úteis apenas quando o sistema e as preocupações de segurança são bem compreendidos. O método assume que os analistas possuem alta expertise em cibersegurança e, portanto, não fornece diretrizes para avaliar sub-objetivos, ataques ou riscos. Nos últimos anos, essa técnica tem sido frequentemente usada em combinação com outras técnicas e dentro de frameworks como STRIDE, CVSS e PASTA. A aplicação de árvores de ataque pode ajudar a tomar decisões de segurança, verificar se os sistemas são vulneráveis a um ataque e avaliar um tipo específico de ataque.

Um objetivo adicional do método é gerar portas de ataque para componentes individuais. Essas portas de ataque, que são efetivamente nós raiz para as árvores de ataque dos componentes, ilustram atividades que podem passar risco para os componentes conectados. A pontuação auxilia no processo de realização de uma avaliação de risco do sistema. Se uma porta de ataque depende de um nó raiz de componente com uma alta pontuação de risco, essa porta de ataque também terá uma alta pontuação de risco e uma alta probabilidade de ser executada. O oposto também é verdadeiro. Este método foi utilizado em um estudo de caso para uma rede de comunicações ferroviárias, demonstrando sua

aplicabilidade prática.

Em resumo, as árvores de ataque são uma ferramenta poderosa para identificar e mitigar ameaças em sistemas complexos. Sua aplicação em organizações não hierárquicas pode ser particularmente valiosa, pois permite uma abordagem sistemática para a segurança, considerando a horizontalidade como um ativo. A adoção de árvores de ataque, juntamente com outras metodologias de modelagem de ameaças, pode proporcionar uma defesa mais focada e eficaz contra ameaças cibernéticas.

2.1.3 Security Cards

2.1.4 Personna non Grata

2.1.5 PASTA

2.2 Trabalhos Relacionados

A modelagem de ameaças é um campo dinâmico e em constante evolução, com várias abordagens e frameworks desenvolvidos ao longo dos anos para atender a diferentes necessidades e contextos. Este capítulo revisa alguns dos trabalhos mais relevantes na área de modelagem de ameaças, com foco em métodos que podem ser adaptados ou servir de inspiração para o desenvolvimento de um protocolo específico para organizações não-hierárquicas.

No artigo "ABC: A Cryptocurrency-Focused Threat Modeling Framework", os autores Ghada Almashaqbeh, Allison Bishop e Justin Cappos propõem um modelo de ameaças específico para criptomoedas, destacando a necessidade de frameworks especializados para lidar com as particularidades desses sistemas.

O framework ABC introduz a matriz de colusão como uma inovação chave, permitindo cobrir um amplo espectro de casos de ameaças sem tornar o processo excessivamente complexo. Este modelo é particularmente eficaz em identificar riscos financeiros, como demonstrado em estudos de caso reais e em um estudo de usuários, onde 71% dos participantes que utilizaram o ABC conseguiram identificar ameaças financeiras, em comparação com apenas 13% dos que usaram o STRIDE. Esta abordagem é particularmente importante em criptomoedas permissionless, onde qualquer pessoa pode participar e onde a colusão entre atacantes é uma preocupação significativa.

No contexto de organizações não-hierárquicas, a modelagem de ameaças deve considerar a horizontalidade como um ativo. Nós visamos desenvolver protocolos de modelagem de ameaças que valorizem a horizontalidade, avaliando esses novos protocolos com membros de grupos com diferentes níveis de horizontalidade.

Assim como o framework ABC aborda as especificidades das criptomoedas, o trabalho busca adaptar a modelagem de ameaças para contextos onde a ausência de hierarquia é uma característica fundamental. Ambos os trabalhos destacam a importância de frameworks especializados que considerem as particularidades dos sistemas e organizações que

visam proteger.

2.3 Princípios de Organizações Horizontais

Aqui está o texto traduzido e revisado para melhorar a coesão:

—

As organizações horizontais, como cooperativas de trabalhadores, sindicatos, organizações ativistas e projetos de software de código aberto, operam com base em princípios que promovem a igualdade, a participação coletiva e a ausência de hierarquia rígida. Esses princípios são fundamentais para assegurar que todos os membros tenham voz ativa e que as decisões sejam tomadas de maneira democrática e inclusiva.

Um dos princípios centrais dessas organizações é a eleição dos organismos dirigentes, da base ao topo, com o direito de destituição de qualquer eleito pelo coletivo que o escolheu. Isso garante que os líderes sejam responsáveis perante os membros e que possam ser substituídos caso não desempenhem suas funções de maneira satisfatória.

Outro princípio relevante é a obrigatoriedade de os organismos dirigentes prestarem contas regularmente de suas atividades às respectivas organizações. Esse processo inclui considerar atentamente as opiniões e críticas dos membros, valorizando-as como contribuições para a reflexão e as decisões coletivas, de modo a aprimorar o funcionamento organizacional.

A livre expressão de opiniões e o debate cuidadoso sobre elas também são características essenciais. As organizações horizontais buscam assegurar que o maior número possível de membros participe do trabalho, da reflexão, da tomada de decisões e da ação coletiva, incorporando contribuições individuais. Esse modelo promove um ambiente colaborativo e inovador, onde todas as vozes são ouvidas e valorizadas.

O trabalho coletivo e a direção compartilhada são pilares dessas organizações. A tomada de decisões por consenso ou maioria, junto com a iniciativa mais ampla possível de todas as organizações dentro de sua esfera de atuação, é incentivada, sempre em conformidade com os princípios estatutários e as resoluções dos organismos de responsabilidade superior.

Além disso, o respeito pelas decisões coletivas e opiniões divergentes é fundamental. As organizações horizontais estimulam e valorizam o estudo, a reflexão, a intervenção e as contribuições de cada membro, combatendo o individualismo e a imposição de opiniões ou decisões pessoais. Isso cria um ambiente de unidade de pensamento e ação, onde a disciplina consciente e voluntária é promovida.

Esses princípios são indispensáveis para o funcionamento eficaz de organizações horizontais, assegurando que a horizontalidade seja mantida como um ativo valioso. No contexto da modelagem de ameaças, é crucial desenvolver protocolos que respeitem esses princípios, garantindo que as soluções de segurança sejam compatíveis com a estrutura e os valores dessas organizações.

Com base nos estatutos do Partido Comunista Português (PCP), propõe-se a seguinte seção de tese, que explora o funcionamento interno de organizações não hierárquicas, com atenção especial aos mecanismos de segurança voltados para prevenir ameaças, como **"Representante Malicioso"**, **"Abuso de Poder em Emergências"**, **"Quórum Artificial por Colusão"** e **"Negação de Quórum por Colusão"**.

—

Estrutura e Segurança Interna em Organizações Não Hierárquicas

Organizações não hierárquicas, como o PCP, estruturam-se de forma a promover a participação coletiva e descentralizada, ao mesmo tempo em que mantêm mecanismos de coordenação e coesão que asseguram sua funcionalidade e segurança interna. Esse modelo organizacional enfatiza a democracia interna, a transparência e a responsabilidade compartilhada como fundamentos para a construção de confiança mútua e interação eficaz com tecnologias de suporte. A seguir, detalham-se os principais elementos estruturais e os mecanismos de segurança que buscam prevenir riscos organizacionais e de governança.

Organização e Princípios Fundamentais

De acordo com seus estatutos, o PCP adota o princípio do centralismo democrático, que equilibra a autonomia das unidades organizacionais de base com a uniformidade de orientação política definida por organismos centrais. Sua estrutura baseia-se na participação ativa dos membros em células organizacionais, que atuam como elo direto com a comunidade. As decisões são tomadas coletivamente, respeitando a pluralidade de opiniões até que se alcance um consenso ou maioria, assegurando um processo inclusivo e deliberativo.

Mecanismos de Prevenção de Riscos

1. **Representante Malicioso:** O processo de seleção e eleição dos representantes é regulado por normas claras, incluindo critérios de fidelidade aos princípios do partido e avaliação de conduta prévia. Adicionalmente, o direito de destituição pelo coletivo que os elegeu funciona como mecanismo preventivo contra abusos de poder.

2. **Abuso de Poder em Emergências:** Situações extraordinárias são regulamentadas de forma a limitar a autonomia nas decisões emergenciais, com supervisão e revisão posterior pelos organismos superiores. Essa abordagem visa prevenir decisões arbitrárias ou desvios em momentos críticos.

3. **Quórum Artificial por Colusão:** Para evitar a formação de quóruns artificiais, o PCP promove a rotatividade e a diversidade nos órgãos de direção. O princípio de distribuição de tarefas entre diferentes níveis organizacionais e a fiscalização contínua garantem que as decisões não sejam controladas por grupos restritos ou facções internas.

4. **Negação de Quórum por Colusão:** A ampla mobilização dos membros nas decisões coletivas reduz o risco de bloqueios deliberados. O estímulo à participação regular e a garantia de acesso a informações relevantes fortalecem a transparência e impedem práticas que dificultem deliberações fundamentais.

Relação com Tecnologias

Organizações não hierárquicas como o PCP têm o potencial de interagir eficazmente com tecnologias horizontais, especialmente aquelas que suportam comunicação distribuída, deliberação coletiva e registro imutável de decisões (como blockchain). Essas tecnologias podem reforçar os valores de igualdade, transparência e segurança, mitigando riscos de centralização e abuso de poder.

Conclusão

A estrutura não hierárquica do PCP demonstra que é possível equilibrar a participação democrática com mecanismos robustos de segurança, assegurando a continuidade organizacional e a proteção contra ameaças internas. Esse modelo oferece uma base teórica e prática para o desenvolvimento de tecnologias de segurança alinhadas aos princípios de horizontalidade e coesão coletiva.

—

Se precisar de ajustes adicionais ou um foco mais específico, é só pedir!

2.4 Lacunas na Literatura

Embora a modelagem de ameaças tenha sido amplamente estudada e aplicada em diversos contextos, ainda existem lacunas significativas na literatura, especialmente no que diz respeito à segurança em organizações não-hierárquicas. A maioria das ferramentas e técnicas de segurança cibernética foi desenvolvida com base em pressupostos hierárquicos, refletindo as necessidades de entidades militares ou corporativas, onde há uma clara cadeia de comando e responsabilidades bem definidas. No entanto, essas tecnologias não são adequadas para setores horizontais e participativos, como cooperativas de trabalhadores e grupos ativistas, que operam com base em processos democráticos e coletivos.

Uma das principais lacunas identificadas é a falta de exploração na área de segurança horizontal, ou seja, técnicas e tecnologias de segurança que utilizam a participação democrática para a tomada de decisões de segurança. O trabalho COLBAC: Shifting Cybersecurity from Hierarchical to Horizontal Designs destaca a necessidade de desenvolver tecnologias que beneficiem a comunidade limitando os privilégios dos poderosos dentro de uma organização por meio da participação democrática. No entanto, o estudo também aponta que a implementação de tais sistemas requer mais opções de configuração e interações não mediadas, o que pode ser um desafio significativo.

A pesquisa etnográfica também pode fornecer insights valiosos sobre como essas organizações trabalham com sistemas centralizados e hierárquicos, e como essas práticas estabelecidas podem ser usadas para gerar métodos de design de interfaces entre COLBAC e sistemas mais centralizados. A observação de como a introdução de técnicas de segurança horizontais afeta a organização das comunidades pode ajudar a refletir essas mudanças em novas tecnologias.

Por fim, é crucial garantir que as soluções desenvolvidas sejam utilizáveis. A criação de um sistema de segurança horizontal, ou qualquer sistema, deve considerar a usabilidade

para garantir que os membros da organização possam efetivamente utilizar e manter o sistema sem comprometer os princípios de participação e igualdade.

Essas lacunas na literatura destacam a necessidade de mais pesquisa e desenvolvimento na área de segurança cibernética para organizações não-hierárquicas. Abordar esses desafios permitirá a criação de sistemas de segurança que não apenas protejam contra ameaças externas, mas também respeitem e reforcem a estrutura participativa dessas organizações.

3

Design

3.1 Desafios na Modelagem de Ameaças para Organizações Não-Hierárquicas

Organizações não-hierárquicas, como cooperativas de trabalhadores, sindicatos, grupos ativistas e projetos de software de código aberto, enfrentam desafios únicos em termos de segurança cibernética devido à sua estrutura participativa e democrática. A maioria das ferramentas e técnicas de segurança cibernética foi desenvolvida com base em pressupostos hierárquicos, refletindo as necessidades de entidades militares ou corporativas, onde há uma clara cadeia de comando e responsabilidades bem definidas. No entanto, essas tecnologias não são adequadas para setores horizontais e participativos, como cooperativas de trabalhadores e grupos ativistas, que operam com base em processos democráticos e coletivos.

Um dos principais desafios enfrentados por 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.

Outro desafio significativo é a implementação de políticas de controle de acesso de forma horizontal. Sistemas de controle de acesso tradicionais, como MAC Mandatory Access Control, DAC Discretionary Access Control e RBAC Role-Based Access Control, tendem a forçar a criação de uma hierarquia, onde certas entidades na organização têm o poder de implementar as regras de controle de acesso que foram democraticamente criadas pela organização. Se os indivíduos que têm a capacidade de aplicar as regras decidirem não fazê-lo, as políticas de controle de acesso recém-criadas tornam-se ineficazes, formando uma hierarquia com as entidades capazes de aplicar o controle de acesso no topo.

Além disso, a tomada de decisões coletivas em sistemas de segurança pode ser

vulnerável a ataques específicos, como o ataque Sybil, onde um usuário mal-intencionado pode se passar por vários votantes legítimos, comprometendo a integridade do processo democrático. A interrupção do sistema por um grupo de usuários mal-intencionados também pode impedir o funcionamento adequado do sistema, interrompendo operações de votação e outras atividades críticas.

Esses desafios destacam a necessidade de desenvolver tecnologias e protocolos de segurança que permitam uma organização ser flexível e dinâmica em sua horizontalidade, sendo participativa ou hierárquica conforme necessário, sem comprometer a capacidade de retornar à horizontalidade quando desejado. A criação de sistemas que utilizem processos democráticos para a tomada de decisões de segurança pode ajudar a resolver esses desafios, permitindo que as organizações horizontais mantenham seus princípios fundamentais de participação e igualdade enquanto protegem seus ativos e dados sensíveis.

3.2 Horizontality as an Asset

We also show some stuff which is not that common!

4

Conclusion

4.1 Introduction

We also show some stuff which is not that common!

5

Work Plan

5.1 Evaluation

A avaliação será conduzida em duas etapas principais: um estudo de caso prático e um estudo de usuários.

Na primeira etapa, será realizada a aplicação do protocolo em organizações reais que operam de maneira horizontal, como cooperativas de trabalhadores, sindicatos, grupos ativistas e projetos de software de código aberto. Cada organização participante será analisada para identificar suas necessidades específicas de segurança e como o protocolo pode ser adaptado para atender a essas necessidades. Durante esta fase, serão coletados dados sobre a eficácia do protocolo em identificar e mitigar ameaças, bem como sobre a facilidade de uso e a aceitação pelos membros da organização.

A segunda etapa consistirá em um estudo de usuários, onde participantes de diferentes organizações horizontais serão convidados a utilizar o protocolo desenvolvido. Este estudo será comparativo, envolvendo também a aplicação de um protocolo de modelagem de ameaças tradicional, como STRIDE, para servir como base de comparação. Os participantes serão divididos em dois grupos: um grupo utilizará o novo protocolo, enquanto o outro grupo utilizará o protocolo tradicional. Durante o estudo, os participantes serão solicitados a identificar ameaças em cenários específicos fornecidos. A eficácia de cada protocolo será medida com base na quantidade e na qualidade das ameaças identificadas. Espera-se que o novo protocolo demonstre uma maior eficácia na identificação de ameaças e cenários de colusão, refletindo a necessidade de soluções de segurança adaptadas para organizações não-hierárquicas.

Os dados coletados durante o estudo de caso prático e o estudo de usuários serão analisados quantitativa e qualitativamente. A análise quantitativa incluirá métricas como o número de ameaças identificadas, a taxa de falsos positivos e negativos, e o tempo necessário para completar a modelagem de ameaças. A análise qualitativa envolverá feedback dos participantes sobre a usabilidade do protocolo, a clareza das instruções e a percepção geral de segurança proporcionada pelo protocolo.

Para fornecer uma visão abrangente da eficácia do novo protocolo, os resultados

serão comparados com os obtidos utilizando protocolos tradicionais, como STRIDE. Esta comparação destacará as vantagens e desvantagens de cada abordagem em contextos horizontais, fornecendo uma base sólida para futuras pesquisas e desenvolvimentos no campo da segurança cibernética para organizações não-hierárquicas.

A avaliação proposta permitirá uma compreensão detalhada da eficácia do protocolo de modelagem de ameaças desenvolvido, considerando a horizontalidade como um ativo. Os resultados fornecerão insights valiosos sobre como melhorar e adaptar o protocolo para diferentes tipos de organizações horizontais, garantindo que as soluções de segurança respeitem e reforcem os princípios de participação e igualdade.

5.2 Scheduling

We also show some stuff which is not that common!