NOVA SCHOOL OF SCIENCE & TECHNOLOGY

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 17, 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 17, 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 *(pp. 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 e grupos ativistas. Essas organizações enfrentam desafios específicos em termos de segurança devido à inadequação das soluções tradicionais, que geralmente ignoram a horizontalidade em sua concepção. Por exemplo, métodos como STRIDE, amplamente utilizados em modelagem de ameaças, dependem fortemente de diagramas de fluxo de dados (DFDs) e processos hierárquicos de decisão, mas enfrentam limitações significativas ao abordar organizações horizontais, conforme explorado por Shostak (2014) e outros autores [12, 4, 3].

Organizações hierárquicas normalmente facilitam a implementação de políticas de segurança devido à clara atribuição de responsabilidades e controle. Essa abordagem é evidente em práticas tradicionais como STRIDE e DREAD, que estruturam as ameaças em categorias bem definidas, tornando o processo mais direto, ainda que por vezes oneroso [7, 3, 10]. Em contraste, organizações horizontais distribuem o poder de forma equitativa, baseando decisões em processos coletivos e participativos. Essa estrutura, enquanto mais inclusiva e transparente, apresenta desafios únicos, como a gestão de segredos e o controle de acesso, temas amplamente debatidos na literatura sobre segurança para estruturas horizontais [2, 9, 11].

Além disso, autores como Uzunov e Fernandez (2014) destacam que a modelagem de ameaças frequentemente ignora as complexidades de governança horizontal, requerendo ferramentas que incorporem múltiplas perspectivas [12]. Por outro lado, metodologias participativas, como a descrita por CoReTM, demonstram a eficácia da colaboração e da diversidade de expertise na modelagem de ameaças, mas ainda enfrentam desafios de implementação [11].

A horizontalidade, porém, pode ser vista como um ativo estratégico. Protocolos de segurança que respeitem essa estrutura podem reforçar os princípios fundamentais de participação e igualdade das organizações. Esse conceito é destacado em trabalhos como

COLBAC, que explora tecnologias para suporte a organizações democráticas e horizontais, enfatizando a importância de integrar políticas de autorização baseadas na coletividade [2]. No entanto, como aponta o estudo da COLBAC, soluções eficazes para segurança horizontal exigem não apenas tecnologias, mas também adaptações sociotécnicas e um alinhamento entre estruturas organizacionais e suas ferramentas tecnológicas.

Finalmente, para organizações horizontais, a gestão de segredos, como senhas e chaves de acesso, precisa ser distribuída de forma justa e segura, evitando concentração de poder. Isso contrasta diretamente com práticas hierárquicas tradicionais, onde essas responsabilidades são centralizadas [2].

1.2 Objective

O objetivo desta pesquisa é desenvolver um protocolo de modelagem de ameaças adaptado para organizações não hierárquicas, como cooperativas, sindicatos e projetos de software de código aberto. Esse protocolo busca resolver os desafios específicos enfrentados por essas organizações, valorizando a horizontalidade como um diferencial positivo. A abordagem aqui proposta considera tanto as ameaças externas quanto os processos democráticos internos, garantindo soluções que respeitem a igualdade e a participação [5, 4, 9].

Para validar o protocolo, serão conduzidas avaliações em diferentes organizações horizontais, comparando seus resultados com abordagens tradicionais, como STRIDE e DREAD. Esses métodos tradicionais, ainda que robustos, frequentemente dependem de diagramas de fluxo de dados e abordagens sistemáticas, como checklist, que não capturam nuances participativas [12, 7]. A comparação irá destacar vantagens e desvantagens de cada abordagem no contexto de organizações horizontais.

1.3 Contributions

As contribuições desta pesquisa incluem o desenvolvimento de um protocolo de modelagem de ameaças inovador que considera a horizontalidade como um ativo estratégico. Este protocolo será projetado para abordar os desafios específicos enfrentados por cooperativas, sindicatos e projetos de código aberto [12, 11, 9]. Além disso, será realizada uma avaliação comparativa detalhada do protocolo com métodos tradicionais, como STRIDE, para ilustrar a aplicabilidade prática e eficácia em diferentes contextos [4, 8, 7, 6].

Por fim, espera-se que este trabalho contribua para o avanço das práticas de segurança cibernética, promovendo soluções inclusivas e respeitando os princípios de participação e igualdade [2, 1].

1.4 Structure

O primeiro capítulo apresenta o contexto e os objetivos do estudo. No segundo capítulo, são revisados trabalhos relacionados e fundamentos teóricos, com ênfase em abordagens participativas e tradicionais de modelagem de ameaças. O terceiro capítulo detalha o protocolo proposto. O quarto capítulo sintetiza os resultados e propõe direções futuras. Finalmente, o capítulo Work Plan apresenta o cronograma e as etapas de validação.

2

Background and Related Work

2.1 Modelagem de Ameaças: Conceitos e Estratégias

A modelagem de ameaças é um processo estruturado que permite identificar, analisar e mitigar vulnerabilidades em sistemas, compondo um elemento essencial para a segurança cibernética. Este processo também serve como base para a definição de requisitos de segurança e é amplamente utilizado no desenvolvimento de sistemas mais resilientes. Segundo Torr [10], a modelagem de ameaças deve ser integrada aos processos de design e especificação desde o início, como uma prática preventiva essencial.

2.1.1 Definições e Objetivos da Modelagem de Ameaças

Diversos autores oferecem definições que destacam aspectos fundamentais da modelagem de ameaças. Uzunov e Fernandez [12] descrevem-na como um processo para analisar ataques potenciais, utilizando bibliotecas de ameaças ou taxonomias. Em um contexto mais específico, Shull et al. [8] destacam que a modelagem de ameaças cria uma abstração do sistema de software para identificar habilidades e metas dos atacantes, gerando catálogos de possíveis ameaças que precisam ser mitigadas.

As metodologias de modelagem de ameaças são ferramentas valiosas para responder a perguntas como: "Quais são os ativos mais críticos?", "Quem são os adversários?" e "Quais vulnerabilidades podem ser exploradas?" [5].

2.1.2 Ferramentas e Representações Visuais

As ferramentas desempenham um papel crucial na eficácia da modelagem de ameaças. *Data Flow Diagrams* (DFDs), por exemplo, são amplamente usados para mapear fluxos de dados e identificar fronteiras de confiança [6]. As árvores de ataque são outro exemplo comum, oferecendo uma maneira hierárquica de decompor ameaças [3].

2.1.3 Desafios e Limitações

Embora eficaz, a modelagem de ameaças enfrenta desafios, como a dependência de DFDs precisos e a complexidade crescente em sistemas maiores [6]. Almashaqbeh et al. [1] destacam que modelos específicos para domínios emergentes, como criptomoedas, ainda estão em estágios iniciais de desenvolvimento.

2.1.4 Futuras Direções

Para melhorar a modelagem de ameaças, é crucial integrar abordagens colaborativas e adaptativas [11]. Modelos que considerem dinâmicas horizontais, como o COLBAC, e a participação ativa dos usuários, como o Participatory Threat Modeling, mostram promessas significativas [2, 9].

Com uma evolução constante nas metodologias e ferramentas, a modelagem de ameaças continuará sendo uma área essencial para avanços em segurança cibernética e resiliência organizacional.

2.1.5 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.

2.1.6 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.

2.1.7 Security Cards

2.1.8 Personna non Grata

2.1.9 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

Organizações horizontais buscam minimizar ou eliminarminimizam hierarquias tradicionais, promovendo participação igualitária em processos de tomada de decisão. Este modelo de organização reflete práticas que priorizam odecisões. Este modelo prioriza trabalho coletivo e a inclusão das bases, elementos característicos de organizações horizontaisinclusão das bases. Esta análise explora o funcionamento e a estruturação dessas organizações com base em princípios geraisseu funcionamento e estruturação.

Organizações horizontais são frequentemente constituídas por núcleos ou células que representam sua organização de base. Esses núcleos podem ser formados em locais de trabalho, residências ou áreas de atividade específicas, destacando a descentralização operativa. Essa formação permite que cada grupo atue em conformidade com a realidade local, promovendo a ligação direta entre a organização e suas bases. Ao contrário de organizações hierárquicas, onde as decisões são impostas de cima para baixo, os núcleos em organizações horizontais têm autonomia relativa para definir suas atividades, desde queSão organizadas em núcleos ou células de base, formadas em locais de trabalho, residências ou áreas específicas, destacando descentralização. Esses grupos atuam conforme a realidade local e prestam contas a organismos coordenadores, equilibrando autonomia e coesão. Diferente de organizações hierárquicas, onde as decisões são impostas, os núcleos têm liberdade para definir atividades alinhadas aos princípios gerais do coletivo. Essa autonomia é equilibrada pela prestação de contas a organismos coordenadores, assegurando coesão sem comprometer a descentralização.

Um dos pilares das organizações horizontais é a eleição dos organismos coordenadores em todos os níveis, da base ao topo. Isso contrasta fortemente com organizações hierárquicas, onde lideranças são muitas vezes designadas ou hereditárias. Além disso, os membros têm o direito de expressar opiniões livremente, criticar decisões e propor alternativas em todos os níveis da estrutura. Essas organizações também promovem a prática da crítica e autocrítica como ferramenta para aperfeiçoar o trabalho coletivo. Essa prática assegura que todos os membros possam contribuir ativamente para a reflexão e elaboração das diretrizes doA eleição dos organismos coordenadores é um pilar fundamental. Contrapondo-se a lideranças designadas em sistemas hierárquicos, membros

expressam opiniões, criticam decisões e propõem alternativas. Crítica e autocrítica são ferramentas essenciais para aperfeiçoar o trabalho coletivo.

A direção coletiva é uma característica fundamental dessas organizações, baseada no princípio de que as decisões devem refletir o consenso ou a vontade majoritária dos membros. Embora exista uma estrutura de responsabilidade coordenadora, essa é orientada a estimular o trabalho conjunto e evitar tendências autoritárias ou centralistas. Para garantir a coesão, todas as decisões tomadas por consenso ou maioria são vinculativas, o que reforça o compromisso coletivo. Esse formato evita a divisão em facções, frequentemente observada em organizações hierárquicas, onde disputas internas podem enfraquecer a unidadereflete o consenso ou a maioria, estimulando trabalho conjunto e evitando centralismo. Decisões são vinculativas, fortalecendo o compromisso coletivo e prevenindo divisões internas, comuns em organizações hierárquicas.

A disciplina é voluntária e baseada na aceitação coletiva das diretrizes. Em contraste com imposições verticais em hierarquias, medidas disciplinares horizontais são transparentes, com direito de apelação, promovendo confiança interna e comprometimento.

Organizações horizontais enfatizam a disciplina consciente e voluntária, baseada na aceitação coletiva de suas diretrizes e princípios. Essa disciplina é vista como um fator essencial para a unidade prevenindo a fragmentação interna. Em contraste, organizações hierárquicas muitas vezes dependem de imposições verticais para manter a ordem, o que pode gerar resistência e descontentamento. As medidas disciplinares em organizações horizontais tendem a ser aplicadas de forma transparente e incluem direitos de apelação, assegurando justiça processual. Essa prática promove a confiança interna e fortalece o comprometimento dos membros.

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!

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/INFCOMW.2019.8845101 (cit. on pp. 2, 5).

[2] 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. URL: https://doi.org/10.1145/3498891.3498903 (cit. on pp. 1, 2, 5).

[3] S. Hussain et al. "Threat Modelling Methodologies: A Survey". In: vol. 26. 2014-01, pp. 1607–1609. URL: https://api.semanticscholar.org/CorpusID:111533730 (cit. on pp. 1, 4).

[4] N. R. Mead et al. "A hybrid threat modeling method". In: *Carnegie MellonUniversity-Software Engineering Institute-Technical Report-CMU/SEI-2018-TN-002* (2018) (cit. on pp. 1, 2).

[5] S. Myagmar, A. J. Lee, and W. Yurcik. "Threat modeling as a basis for security requirements". In: (2005) (cit. on pp. 2, 4).

[6] N. Shevchenko et al. "Threat modeling: a summary of available methods". In: *Software Engineering Institute| Carnegie Mellon University* (2018), pp. 1–24 (cit. on pp. 2, 4, 5).

[7] A. Shostack. "Experiences Threat Modeling at Microsoft". In: *MODSEC@ MoDELS* (2008) (cit. on pp. 1, 2).

[8] F. Shull et al. *Evaluation of Threat Modeling Methodologies*. Tech. rep. Approved for public release and unlimited distribution. SEI Research Review 2016. DM-0004095. Carnegie Mellon University, Software Engineering Institute, 2016-10. URL: https://insights.sei.cmu.edu/documents/4027/2016_017_001_474200.pdf (cit. on pp. 2, 4).

[9] J. Slupska et al. "Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity". In: *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI EA '21. Yokohama, Japan: Association for Computing Machinery, 2021. ISBN: 9781450380959. DOI: 10.1145/3411763.3451731. URL: https://doi.org/10.1145/3411763.3451731 (cit. on pp. 1, 2, 5).

[10] P. Torr. "Demystifying the threat modeling process". In: 3.5 (2005), pp. 66–70. DOI: 10.1109/MSP.2005.119 (cit. on pp. 1, 4).

[11] J. Von Der Assen et al. "CoReTM: An Approach Enabling Cross-Functional Collaborative Threat Modeling". In: *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*. 2022, pp. 189–196. DOI: 10.1109/CSR54599.2022.9850283 (cit. on pp. 1, 2, 5).

[12] W. Xiong and R. Lagerström. "Threat modeling - A systematic literature review". In: 84 (2019), pp. 53–69. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2019.03.010. URL: https://www.sciencedirect.com/science/article/pii/S0167404818307478 (cit. on pp. 1, 2, 4).