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 20, 2024*

NOVA SCHOOL OF
SCIENCE & TECHNOLOGY

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 20, 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.

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.

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

Contents

List of Figures

Acronyms

CGTP Confederação Geral dos Trabalhadores Portugueses *(p. 10)*

COLBAC Collective based access control system *(p. 9)*

STRIDE Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege *(pp. 2, 6, 7, 10)*

1

Introduction

1.1 Governança Organizacional: Uma Perspectiva Histórica

A governança organizacional reflete as estruturas sociais, econômicas e tecnológicas de cada época. Desde os primeiros agrupamentos humanos até as organizações complexas da contemporaneidade, as formas de organizar o poder e a tomada de decisão foram moldadas para responder a contextos específicos. O modelo hierárquico, amplamente adotado, emergiu como solução para demandas de controle e eficiência. Contudo, a história também registra experimentos que desafiaram essa lógica, sugerindo a possibilidade de novas abordagens na gestão e coordenação de atividades.

Mesmo em sistemas considerados pioneiros na horizontalidade, como a democracia ateniense, a governança enfrentou limitações significativas relacionadas à inclusão e à aplicabilidade prática, evidenciando fragilidades na operacionalização da participação igualitária [2]. Com o avanço da Revolução Industrial, a centralização hierárquica intensificou-se para lidar com o crescimento e a complexidade organizacional [24]. Adicionalmente, experiências como as cooperativas e os movimentos sindicalistas do século XIX delinearam alternativas à centralização absoluta, enquanto tecnologias modernas, como o blockchain, expandem essas ideias, oferecendo estruturas descentralizadas que desafiam paradigmas tradicionais de controle [8, 19].

Enquanto tecnologias de vigilância em massa reforçam estruturas centralizadoras, bloqueando a adoção plena de governança horizontal, inovações como o blockchain abrem novas possibilidades de descentralização, ainda que enfrentem desafios na distribuição equitativa de poder e recursos, como evidenciado na concentração de mineradores em redes públicas [23].

Essas evoluções históricas e tecnológicas não apenas moldam as estruturas de governança, mas também introduzem desafios únicos na modelagem de ameaças. A análise crítica dessas tentativas permite identificar vulnerabilidades e forças que fundamentam a construção de protocolos de segurança em organizações horizontais.

1.2 A Segurança Horizontal em Tempos de Interconexão

No mundo interconectado atual, as organizações horizontais desafiam o pressuposto de que a segurança depende de uma cadeia clara de comando. A ausência de hierarquia formal pode se transformar em um ativo estratégico ao dificultar ataques centralizados e ao permitir uma reconfiguração da gestão da confiança, promovendo a resiliência organizacional [19]. Em sistemas de confiança distribuída, como os utilizados em organizações baseadas em blockchain, a segurança é promovida por mecanismos colaborativos que substituem líderes formais por processos participativos e soluções orientadas à transparência e consenso [15].

Metodologias tradicionais de análise de ameaças, tais como Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE) e árvores de ataque, fornecem fundamentos valiosos, mas enfrentam limitações em ambientes descentralizados, destacando a necessidade de abordagens mais adequadas às especificidades de estruturas horizontais [7]. Contextos menos hierárquicos requerem abordagens adaptadas que compreendam a complexidade da confiança horizontal e dos potenciais riscos associados.

Nesse sentido, tecnologias como a criptografia colaborativa [4, 1] e abordagens de modelagem de ameaças que adotam a perspectiva do adversário podem promover um entendimento mais realista da segurança em estruturas descentralizadas. A horizontalidade, frequentemente vista como um desafio, deve ser explorada como um ativo estratégico capaz de diluir pontos únicos de falha e fortalecer a resiliência organizacional.

1.3 Protocolo de Segurança para Organizações Não-Hierárquicas

Esta pesquisa propõe um protocolo de segurança que integra a horizontalidade como elemento estratégico, indo além da simples adaptação de metodologias tradicionais. Em vez disso, busca demonstrar como a descentralização, quando bem estruturada, reforça a resiliência frente a ameaças complexas, mitigando pontos únicos de falha.

A proposta preenche uma lacuna na literatura sobre segurança em estruturas horizontalizadas, abordando desafios apontados em estudos como o uso limitado de metodologias tradicionais em contextos descentralizados [7] e a necessidade de criptografia adaptada [4]. Considere organizações descentralizadas que gerenciam ativos digitais sensíveis. A pergunta central é como garantir proteção contra fraudes internas e ataques externos, preservando a governança horizontal.

O protocolo proposto oferecerá mecanismos de consenso, transparência e uma modelagem de ameaças adaptada, como a inclusão de abordagens colaborativas e participativas descritas em [4] e [1], fornecendo soluções pragmáticas para tais desafios.

1.4 Delimitando o Escopo da Pesquisa

A variedade de arranjos horizontais é ampla, e analisar todos em um único estudo seria pouco produtivo. Para permitir uma análise detalhada e alinhada com os objetivos da pesquisa, este trabalho concentra-se em estruturas plenamente horizontais que exemplifiquem confiança distribuída, governança democrática e mecanismos colaborativos para a tomada de decisão [4]. Ambientes híbridos ou parcialmente horizontalizados, onde a governança é compartilhada entre níveis hierárquicos e horizontais, ficam fora do escopo, permitindo avaliar com maior precisão a eficácia do protocolo em um cenário idealizado e mais controlado.

Futuras investigações poderão expandir este protocolo, adaptando suas diretrizes a contextos organizacionais híbridos ou altamente dinâmicos, como redes sociais e plataformas cooperativas digitais [9, 6]. A escolha por cooperativas de trabalhadores e redes comunitárias também reflete a relevância prática dessas estruturas em demonstrar a viabilidade de governança descentralizada e segurança distribuída [8, 19].

1.5 Contribuições Esperadas

Esta pesquisa busca avançar a compreensão teórica da segurança em estruturas horizontais, abordando lacunas relacionadas à aplicabilidade de metodologias tradicionais em contextos descentralizados, como a falta de adaptação às dinâmicas de governança horizontal identificadas em [12] e [21]. O objetivo é superar adaptações limitadas de metodologias existentes, desenvolvendo um protocolo que não apenas respeite os valores de participação coletiva, transparência e confiança distribuída, mas também aproveitem a horizontalidade como ativo estratégico, conforme sugerido em [4].

Do ponto de vista prático, espera-se oferecer diretrizes que demonstrem como a segurança pode ser integrada à governança democrática, promovendo decisões participativas e protegendo ativos organizacionais de forma descentralizada, conforme discutido em [6]. Ao fazê-lo, o protocolo busca demonstrar que a horizontalidade pode ser uma vantagem estratégica, transformando a segurança em um catalisador para autonomia e resiliência organizacional frente a ameaças complexas, como enfatizado em [15] e [1].

1.6 Estrutura da Tese

Após esta introdução, o capítulo de Background explorará conceitos fundamentais, como modelagem de ameaças, segurança em estruturas horizontais e confiança distribuída, oferecendo um quadro analítico robusto que sustentará o desenvolvimento do protocolo. Em seguida, o capítulo de related work analisará estudos anteriores que investigam a segurança em organizações descentralizadas, situando a proposta no debate acadêmico e identificando lacunas que o protocolo visa abordar.

O capítulo de design detalhará o protocolo proposto, destacando seus componentes técnicos, metodológicos e os critérios utilizados para avaliar sua eficácia em estruturas horizontais. Por fim, as conclusões sintetizarão os achados, discutindo as limitações, propondo direções futuras e destacando como a horizontalidade pode ser integrada à segurança em um mundo interconectado.

2

Background

2.1 Fundamentos da Modelagem de Ameaças

A modelagem de ameaças é um componente central da cibersegurança, pois permite identificar ativos valiosos, analisar potenciais vetores de ataque e estabelecer controles capazes de mitigar riscos. Essa prática vai além de fatores técnicos, incorporando elementos organizacionais e humanos que moldam a segurança em contextos diversos, especialmente em estruturas horizontais, onde processos internos e relações de confiança se tornam ainda mais críticos devido à ausência de hierarquias formais. Em um cenário de rápida evolução tecnológica e diversificação constante das ameaças, uma abordagem ampla e flexível ganha relevância, atendendo às particularidades de contextos em transformação, incluindo estruturas não-hierárquicas.

Estudos como [12], [13] e [21] demonstram a necessidade de métodos estruturados, porém adaptáveis, para acompanhar ambientes em mutação. A adoção da perspectiva do adversário [11] é crucial para antecipar cenários complexos e fortalecer a resiliência em ambientes descentralizados, onde a multiplicidade de atores e a distribuição de poder requerem uma análise holística das ameaças. Esse ponto é especialmente relevante quando se consideram organizações horizontais, nas quais não há um ponto central de comando. Nesse tipo de contexto, a modelagem de ameaças precisa refletir a distribuição de poder e a multiplicidade de atores, incluindo as possíveis ameaças internas, externas e híbridas.

Além disso, a experiência da Microsoft, documentada em [17], enfatiza a importância de envolver stakeholders diversos e de aplicar ferramentas colaborativas. Esses elementos tornam-se cruciais quando a tomada de decisão é democrática ou descentralizada, pois a identificação e mitigação de riscos demandam engajamento coletivo e flexibilidade estratégica, conectando o exercício de modelagem de ameaças às dinâmicas organizacionais.

2.1.1 Definições Conceituais

A modelagem de ameaças pode ser entendida como um esforço sistemático de proteção que considera tanto vulnerabilidades técnicas quanto fatores sociais e organizacionais. Ao adotar uma visão holística, conforme sugerem [12] e [13], a análise de segurança não fica

restrita à infraestrutura, mas incorpora práticas internas, fluxos de informação e a cultura da organização. Em contextos não-hierárquicos, a ausência de linhas claras de autoridade e o caráter participativo tornam essencial uma análise que considere a distribuição de responsabilidades e a dependência de mecanismos coletivos de mitigação [4].

Por sua vez, [21] enfatiza que não existe uma solução única para modelagem de ameaças, especialmente em cenários onde a descentralização exige abordagens diversificadas e adaptáveis. Nesse sentido, a modelagem de ameaças torna-se um processo iterativo, adaptando-se a alterações estruturais e incorporando inovações como ferramentas de tomada de decisão participativa e práticas de segurança colaborativa, fundamentais para ambientes horizontais.

2.1.2 Principais Metodologias

Metodologias amplamente discutidas, como o Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE), as árvores de ataque e frameworks baseados em cenários [18], fornecem um ponto de partida testado, mas frequentemente não capturam a complexidade de estruturas horizontais. A participação ativa de stakeholders, como destacado em [20], é essencial em organizações descentralizadas, onde a responsabilidade coletiva pela segurança exige o envolvimento de todos os membros para identificar riscos e implementar contramedidas.

A documentação [16] apresenta um panorama de métodos existentes, alertando que a eficácia de cada abordagem depende do contexto. Por exemplo, STRIDE e árvores de ataque são úteis para identificar vetores de ataque diretos, mas a ausência de hierarquias formais intensifica a necessidade de explorar cenários complexos, como ameaças internas associadas a ataques externos, bem como falhas em mecanismos distribuídos de autenticação, consenso e governança, como sugerido em [4].

A integração de métodos diversos, como práticas de criptografia colaborativa [1] e abordagens híbridas [22], permite que organizações horizontais identifiquem padrões de risco menos óbvios e fortaleçam sua resiliência coletiva. Essa integração se torna crucial em estruturas distribuídas, onde a ausência de um 'centro' transforma a segurança em um esforço coletivo, e a resiliência emerge da interação contínua entre membros, sistemas e mecanismos de governança descentralizada.

2.2 Taxonomia de Estruturas Organizacionais

Entender a relação entre forma organizacional e segurança é essencial para ajustar a modelagem de ameaças à realidade de cada instituição. Enquanto estruturas hierárquicas confiam em pontos centrais de decisão para controle e coordenação, esses mesmos pontos podem se tornar vulnerabilidades críticas. Organizações horizontais, cooperativas ou sem liderança podem dispersar vulnerabilidades e aumentar a resiliência por meio da governança descentralizada, embora também possam criar múltiplos pontos de entrada

que exigem controle colaborativo. A análise desta taxonomia, conforme [8, 10], oferece uma base para identificar como a distribuição de poder em diferentes formas organizacionais afeta a eficácia de medidas de segurança, incluindo a capacidade de resposta a ameaças internas e externas.

2.2.1 Estruturas Tradicionais Hierárquicas

Organizações hierárquicas apresentam linhas claras de autoridade, o que facilita o controle, mas pode concentrar vulnerabilidades em pontos críticos. Essas organizações são caracterizadas por uma cadeia de comando bem definida, onde as decisões fluem do topo para a base. Exemplos clássicos incluem grandes corporações multinacionais, onde a diretoria estabelece políticas que são implementadas por camadas de gerentes, supervisores e funcionários. Por outro lado, em pequenas empresas, como escritórios familiares, a hierarquia pode ser menos formal, mas ainda assim baseada em uma estrutura de comando clara e centralizada [8].

Em grandes organizações, como bancos ou indústrias automotivas, a hierarquia permite uma alocação eficiente de recursos e um controle rigoroso sobre as operações. Por exemplo, as divisões de TI desses ambientes frequentemente utilizam frameworks de segurança como o STRIDE para modelagem de ameaças, focando na proteção de ativos críticos e no gerenciamento de acessos centralizados [25]. A centralização facilita a resposta rápida a incidentes, mas também cria pontos únicos de falha, como vulnerabilidades em servidores principais ou credenciais administrativas [23].

Em contrapartida, pequenas empresas enfrentam desafios diferentes. Nesses contextos, a falta de recursos pode levar a menos camadas hierárquicas, mas as decisões ainda se concentram em um único proprietário ou gerente. Isso reduz a complexidade organizacional, mas aumenta a dependência de indivíduos específicos, tornando-os alvos prioritários em ataques [8]. Ademais, a ausência de equipes dedicadas de segurança pode limitar a capacidade de implementar frameworks sofisticados, como STRIDE, exigindo soluções mais simplificadas.

A diferença entre organizações grandes e pequenas também reflete no impacto sobre a modelagem de ameaças. Em empresas maiores, as estruturas hierárquicas permitem segmentações detalhadas para identificar e mitigar riscos em níveis específicos da organização. No entanto, essa segmentação pode levar a lacunas de comunicação entre departamentos, dificultando a implementação de soluções integradas [25]. Por outro lado, organizações menores têm maior flexibilidade para adaptar rapidamente suas estratégias de segurança, embora frequentemente careçam de recursos para implementar soluções robustas [24].

Portanto, enquanto organizações hierárquicas oferecem vantagens em termos de controle e clareza, elas também introduzem desafios específicos para a modelagem de ameaças. Esses desafios variam significativamente com o tamanho e a complexidade da organização, exigindo adaptações nos frameworks tradicionais para atender às necessidades específicas

de cada tipo de hierarquia.

2.2.2 Organizações Horizontais

Organizações horizontais se distinguem pela rejeição de hierarquias tradicionais, priorizando processos decisórios distribuídos e participação equitativa de todos os membros. Este modelo contrasta diretamente com estruturas hierárquicas, que centralizam o poder em níveis superiores, perpetuando desigualdades no acesso à informação e controle organizacional [6, 14].

A horizontalidade é tanto uma ferramenta quanto um objetivo em si. Nos movimentos sociais argentinos, como analisado por Marina Sitrin, a horizontalidade emergiu como um mecanismo essencial para estabelecer relações baseadas na confiança e no consenso, superando formas tradicionais de organização. Assembleias de bairro e coletivos de trabalhadores desempregados exemplificam como a horizontalidade pode ser aplicada para autogestão e planejamento coletivo [19].

No campo da cibernética, o protocolo COLBAC demonstra a relevância da horizontalidade em sistemas de segurança digital, promovendo um controle de acesso colaborativo que reduz a centralização de poder. Este modelo evita as vulnerabilidades criadas pela dependência de proprietários únicos de senhas ou permissões, reforçando a coerência entre práticas organizacionais e ferramentas tecnológicas [4].

Adicionalmente, exemplos históricos, como a democracia ateniense, ilustram que estruturas horizontais podem ser complementadas por mecanismos temporários de centralização em momentos de crise, garantindo flexibilidade e eficiência sem comprometer os princípios básicos da governança distribuída [2].

Apesar dos desafios, como o risco de dominação por vozes mais influentes ou a gestão de conflitos em espaços coletivos, as organizações horizontais demonstram que, com mecanismos adequados, é possível promover autonomia, participação inclusiva e eficiência em estruturas descentralizadas [5].

2.2.3 Modelos Organizacionais Sem Liderança

O discurso de organizações sem liderança esconde uma complexidade adicional, onde a ausência de uma hierarquia formal não implica necessariamente uma horizontalidade genuína. Estudos críticos destacam como essas organizações frequentemente replicam dinâmicas de poder veladas e centralizações informais.

Marina Sitrin, em sua análise sobre movimentos horizontais na Argentina, aponta que, embora a horizontalidade seja declarada como objetivo, muitos movimentos enfrentam desafios significativos para sustentar práticas realmente participativas. A falta de hierarquia formal frequentemente leva a estruturas de poder informais, onde vozes dominantes assumem papéis de liderança sem supervisão ou responsabilidade coletiva clara [19].

No contexto digital, movimentos como Occupy Wall Street demonstram que a ausência de uma liderança reconhecível não elimina conflitos internos. Estudos sobre as equipes de

mídia social desses movimentos revelam que a administração de contas, como no Twitter, foi frequentemente marcada por disputas de controle, ilustrando como poder e influência podem se consolidar mesmo em estruturas supostamente horizontais [5].

Além disso, pesquisas sobre cooperativas de trabalhadores nos Estados Unidos indicam que essas organizações, embora frequentemente vistas como alternativas não hierárquicas, tendem a desenvolver líderes informais que influenciam decisões de maneira significativa, questionando a narrativa de horizontalidade absoluta [24].

Tecnologias utilizadas por essas organizações também carregam implicações políticas. Langdon Winner argumenta que artefatos técnicos podem perpetuar estruturas de poder existentes, mesmo quando empregados em contextos descentralizados. Por exemplo, plataformas digitais, muitas vezes projetadas para usos individuais, criam desafios na construção de governança coletiva efetiva, exacerbando desigualdades latentes [23].

Esses exemplos destacam que, embora a ideia de ausência de liderança formal seja atraente, sua execução prática frequentemente resulta em formas informais de hierarquia. Assim, o sucesso dessas organizações depende da capacidade de identificar e mitigar as dinâmicas de poder ocultas, promovendo mecanismos claros de governança coletiva e responsabilidade mútua que realmente sustentem a horizontalidade desejada.

2.3 Centralismo Democrático

O centralismo democrático é um modelo organizacional que harmoniza a participação coletiva com a eficiência na execução de decisões. Originalmente associado a contextos políticos, o conceito evoluiu para incorporar aplicações contemporâneas, incluindo algoritmos de governança digital e frameworks colaborativos.

2.3.1 Princípios Fundamentais e Origens Teóricas

O centralismo democrático é baseado em dois pilares complementares: a democracia, que assegura o direito ao debate e participação de todos os membros, e o centralismo, que garante a implementação unificada das decisões. Esse modelo foi desenvolvido como uma resposta à necessidade de aliar eficiência e participação coletiva, especialmente em organizações complexas [14].

Historicamente, o centralismo democrático destacou-se como um método de organização que equilibrava a autonomia local e a coordenação centralizada, permitindo que decisões coletivas fossem transformadas em ações coesas sem comprometer a diversidade de opiniões [3].

2.3.2 Modelos Contemporâneos de Aplicação

Atualmente, o centralismo democrático encontra novas aplicações em contextos organizacionais e tecnológicos. Protocolos como o Collective based access control system (COLBAC)

exemplificam a tradução dos princípios de centralismo democrático em sistemas de controle de acesso colaborativos. Nesse modelo, decisões são tomadas de forma participativa e implementadas com centralização temporária, garantindo eficiência e adaptabilidade [4].

No campo das mídias sociais, equipes de administração de contas coletivas em movimentos como o Occupy Wall Street demonstraram a viabilidade prática desse modelo. A coordenação centralizada de mensagens e campanhas foi possível graças a uma base democrática de decisão, mostrando como o centralismo democrático pode emergir naturalmente em estruturas horizontais [5].

Além disso, o centralismo democrático foi explorado como um componente essencial em sistemas políticos contemporâneos, como no modelo chinês, que utiliza princípios de centralização e participação para promover estabilidade e adaptabilidade na governança nacional [26].

2.3.3 Implicações e Potenciais para Governança

As implicações do centralismo democrático vão além de sua aplicação política, oferecendo soluções para desafios em governança organizacional e tecnológica. Em sistemas distribuídos, o modelo pode ser implementado como um algoritmo de governança, onde inputs democráticos (decisões coletivas) são transformados em outputs centralizados (ações coordenadas), promovendo tanto participação quanto eficiência [23].

Esse modelo também se alinha com estruturas sindicais e cooperativas, como demonstrado nos estatutos da Confederação Geral dos Trabalhadores Portugueses (CGTP). A possibilidade de coordenação entre diferentes níveis de governança e a flexibilidade na tomada de decisões destacam o centralismo democrático como uma ferramenta robusta para gerenciar organizações complexas [3].

Considerações Finais

Este capítulo apresentou os fundamentos da modelagem de ameaças e suas interseções com diferentes estruturas organizacionais, destacando desafios e soluções em contextos hierárquicos e horizontais. Em estruturas horizontais, a ausência de hierarquias formais exige mecanismos claros de segurança coletiva, enquanto o centralismo democrático oferece um modelo para combinar participação e execução eficiente, aplicável em contextos contemporâneos, como algoritmos e protocolos colaborativos [4, 14].

A integração de metodologias como STRIDE, árvores de ataque e práticas colaborativas demonstra que a segurança é um esforço tanto técnico quanto social, sendo essencial adaptar abordagens a diferentes dinâmicas organizacionais. Assim, este capítulo reafirma a importância de combinar inovação e estratégia para fortalecer a resiliência em organizações complexas e descentralizadas.

3

Related Work

3.1 Traditional Threat Modeling Approaches

3.1.1 STRIDE

3.1.2 Attack Trees

3.2 Emerging Methodologies

3.2.1 PASTA

3.2.2 Security Cards

3.2.3 Personae Non Grata

3.3 Hybrid and Collaborative Approaches

3.3.1 Hybrid Threat Modeling Method (hTMM)

3.3.2 Collaborative and Remote Threat Modeling (CoReTM)

3.3.3 Participatory Threat Modeling (PTM)

3.4 Decentralized Trust and Cryptographic Frameworks

3.4.1 PGP and the Web of Trust

3.4.2 COLBAC

3.4.3 ABCcrypto

3.5 Comparative Perspectives

3.5.1 Criteria for Evaluation

3.5.2 Applicability in Non-Hierarchical Organizations

4

Design

4.1 Preliminary Protocol Concept

4.2 Security and Governance Requirements

4.3 Evaluation Strategy

4.4 Experimental Design

4.5 Research Questions

5

Conclusion

6

Work Plan

6.1 Tasks and Milestones

6.2 Timeline and Scheduling

6.3 Resource Allocation and Dependencies

6.4 Risk Assessment and Contingencies

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, 3, 6).

[2] C. W. Blackwell. "Athenian Democracy: An Overview". In: *Dēmos: Classical Athenian Democracy*. Ed. by C. W. Blackwell. © 2003, C.W. Blackwell. www.stoa.org: The Stoa: A Consortium for Electronic Publication in the Humanities, 2003. URL: http://www.stoa.org (cit. on pp. 1, 8).

[3] *Estatutos da Confederação Geral dos Trabalhadores Portugueses – Intersindical Nacional: Declaração de Princípios e Objectivos Programáticos*. Acesso em: 08 dez. 2024. Confederação Geral dos Trabalhadores Portugueses (CGTP), 2020. URL: https://www.cgtp.pt/images/images/2020/02/ESTATUTOSCGTP.pdf (cit. on pp. 9, 10).

[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. URL: https://doi.org/10.1145/3498891.3498903 (cit. on pp. 2, 3, 6, 8, 10).

[5] P. Gerbaudo. "Social media teams as digital vanguards: The question of leadership in the management of key Facebook and Twitter accounts of Occupy Wall Street, Indignados and UK Uncut". In: *Information, Communication & Society* 20.2 (2017), pp. 185–202. DOI: 10.1080/1369118X.2016.1161817. URL: https://doi.org/10.1080/1369118X.2016.1161817 (cit. on pp. 8–10).

[6] P. Herbst. "Non-Hierarchical Forms of Organization". In: *Acta Sociologica* 19.1 (1976), pp. 65–75. DOI: 10.1177/000169937601900106. URL: https://doi.org/10.1177/000169937601900106 (cit. on pp. 3, 8).

[7] 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 p. 2).

[8] R. Jackall and H. M. Levin, eds. *Worker Cooperatives in America*. Berkeley and Los Angeles, California: University of California Press, 1984. ISBN: 0-520-05117-3 (cit. on pp. 1, 3, 7).

[9] A. Kavada. "Creating the collective: social media, the Occupy Movement and its constitution as a collective actor". In: *Information, Communication & Society* 18.8 (2015), pp. 872–886. DOI: 10.1080/1369118X.2015.1043318. eprint: https://doi.org/10.1080/1369118X.2015.1043318. URL: https://doi.org/10.1080/1369118X.2015.1043318 (cit. on p. 3).

[10] J. W. Kuyper and J. S. Dryzek. "Real, not nominal, global democracy: A reply to Robert Keohane". In: *International Journal of Constitutional Law* 14.4 (2017-01), pp. 930–937. ISSN: 1474-2640. DOI: 10.1093/icon/mow063. eprint: https://academic.oup.com/icon/article-pdf/14/4/930/9607155/mow063.pdf. URL: https://doi.org/10.1093/icon/mow063 (cit. on p. 7).

[11] 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 p. 5).

[12] S. Myagmar, A. J. Lee, and W. Yurcik. "Threat modeling as a basis for security requirements". In: (2005) (cit. on pp. 3, 5).

[13] P. Nancy R. Mead. *Advanced Threat Modeling (ATM)*. Tech. rep. This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. Pittsburgh, PA 15213: Carnegie Mellon University, 2017. URL: permission@sei.cmu.edu (cit. on p. 5).

[14] P. C. Português. *Programa e Estatutos do PCP*. Revisão tipográfica: Edições «Avante!». Impressão: Papelmunde — SMG, Lda. Lisboa, Portugal, 2013. URL: https://www.pcp.pt/estatutos-do-pcp (cit. on pp. 8–10).

[15] Y. Saito and J. A. Rose. "Reputation-based Decentralized Autonomous Organization for the Non-Profit Sector: Leveraging Blockchain to Enhance Good Governance". In: *Frontiers in Blockchain* 5 (2023). ISSN: 2624-7852. DOI: 10.3389/fbloc.2022.1083647. URL: https://www.frontiersin.org/articles/10.3389/fbloc.2022.1083647 (cit. on pp. 2, 3).

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

[17] A. Shostack. "Experiences Threat Modeling at Microsoft". In: *MODSEC@ MoDELS* (2008) (cit. on p. 5).

[18] 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 p. 6).

[19] M. A. Sitrin. *Everyday Revolutions: Horizontalism and Autonomy in Argentina*. London, UK; New York, USA: Zed Books Ltd, 2012. ISBN: 9781780320502 (cit. on pp. 1–3, 8).

[20] 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 p. 6).

[21] P. Torr. "Demystifying the threat modeling process". In: 3.5 (2005), pp. 66–70. DOI: 10.1109/MSP.2005.119 (cit. on pp. 3, 5, 6).

[22] 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 p. 6).

[23] L. Winner. "Do Artifacts Have Politics?" In: *Daedalus* 109.1 (1980), pp. 121–136. ISSN: 00115266. URL: http://www.jstor.org/stable/20024652 (visited on 2024-12-08) (cit. on pp. 1, 7, 9, 10).

[24] C. Wright. *Worker Cooperatives and Revolution: History and Possibilities in the United States*. First Edition. Copyright © 2014 Chris Wright. All rights reserved. No part of this publication may be reproduced without prior written permission. Bradenton, Florida, USA: BookLocker.com, Inc., 2014. ISBN: 978-1-63263-432-0 (cit. on pp. 1, 7, 9).

[25] 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 p. 7).

[26] G. Yang. "Still a Century of the Chinese Model? Exploring Dimensions of Democratic Centralism". In: *Chinese Political Science Review* 1.1 (2016), pp. 171–189. DOI: 10.1007/s41111-016-0005-3. URL: https://doi.org/10.1007/s41111-016-0005-3 (cit. on p. 10).