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

MASTER IN COMPUTER SCIENCE AND ENGINEERING

NOVA University Lisbon

Draft: *September 27, 2025*

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
Associate Professor, NOVA University Lisbon

MASTER IN COMPUTER SCIENCE AND ENGINEERING

NOVA University Lisbon
Draft: *September 27, 2025*

Abstract

This thesis presents and validates a novel threat modeling protocol specifically designed to address the security challenges of non-hierarchical organizations. While traditional structures assume top-down control, this protocol is based on the premise that horizontality and democratic participation can be leveraged as strategic assets for building resilience. It translates abstract security concepts into an accessible and collaborative process that integrates principles from established methodologies, such as STRIDE and PASTA, with the realities of distributed governance.

The protocol was tested in real-world workshops with two non-hierarchical organizations, and its effectiveness was compared with the STRIDE framework. The results confirm that the proposed protocol excels at identifying critical sociotechnical and governance threats—such as insider risks, process failures, and quorum manipulation—that traditional methods miss. Consequently, it produces more relevant and actionable mitigations that empower organizations to improve their security posture through changes to their own collective processes. This work provides a tangible tool for decentralized groups to take collective ownership of their digital security, effectively bridging the gap between democratic principles and robust cybersecurity practices.

Keywords: threat modeling, horizontal organizations, distributed governance, collaborative security, decentralized trust

Resumo

Esta tese apresenta e valida um novo protocolo de modelação de ameaças especificamente concebido para abordar os desafios de segurança das organizações não hierárquicas. Enquanto as estruturas tradicionais pressupõem o controlo de cima para baixo, este protocolo assenta na premissa de que a horizontalidade e a participação democrática podem ser alavancadas como ativos estratégicos para a construção de resiliência. A pesquisa traduz conceitos abstratos de segurança num processo acessível e colaborativo que integra princípios de metodologias estabelecidas, como o STRIDE e o PASTA, com as realidades da governação distribuída.

O protocolo foi testado em workshops reais com duas organizações não hierarquizadas e a sua eficácia foi comparada com o modelo STRIDE. Os resultados confirmam que o protocolo proposto se destaca na identificação de ameaças sociotécnicas e de governação críticas como riscos internos, falhas de processo e manipulação de quórum que os métodos tradicionais ignoram. Consequentemente, produz mitigações mais relevantes e acionáveis que capacitam as organizações para melhorar a sua postura de segurança através de mudanças nos seus próprios processos coletivos. Este trabalho fornece uma ferramenta tangível para os grupos descentralizados assumirem a propriedade coletiva da sua segurança digital, eliminando efetivamente o fosso entre os princípios democráticos e as práticas robustas de cibersegurança.

Palavras-chave: modelagem de ameaças, organizações horizontais, governança distribuída, segurança colaborativa, confiança descentralizada

Contents

Acronyms **vi**

1 Introduction **1**
- 1.1 Threat Modeling: Relevance and Challenges . . . 1
- 1.2 Horizontal Security in Times of Interconnection . . . 2
- 1.3 Organizational Governance: A Historical Perspective . . . 2
- 1.4 Security Protocol for Non-Hierarchical Organizations . . . 3
- 1.5 Defining the Scope of Research . . . 3
- 1.6 Expected Contributions . . . 4
- 1.7 Structure of the Thesis . . . 4

2 Background **6**
- 2.1 Foundations of Threat Modeling . . . 6
  - 2.1.1 Conceptual Definitions . . . 6
  - 2.1.2 Main Methodologies . . . 7
- 2.2 Taxonomy of Organizational Structures . . . 7
  - 2.2.1 Traditional Hierarchical Structures . . . 7
  - 2.2.2 Horizontal Organizations . . . 8
  - 2.2.3 Leaderless Organizational Models . . . 9
- 2.3 Democratic Centralism . . . 10
  - 2.3.1 Fundamental Principles and Theoretical Origins . . . 10
  - 2.3.2 Contemporary Models of Application . . . 10
  - 2.3.3 Implications and Potentials for Governance . . . 10

3 Related Work **12**
- 3.1 Traditional Approaches to Threat Modeling . . . 12
  - 3.1.1 STRIDE . . . 12
  - 3.1.2 Attack Trees . . . 14
- 3.2 Emerging Methodologies . . . 14
  - 3.2.1 PASTA . . . 14

3.2.2 Security Cards . . . 15
3.2.3 Personae Non Grata . . . 16
3.3 Hybrid and Collaborative Approaches . . . 17
3.4 Decentralized Trust and Cryptographic Frameworks . . . 17
3.4.1 COLBAC . . . 17
3.4.2 ABCcrypto . . . 18
3.4.3 PGP and the Web of Trust . . . 19
3.5 Comparative Perspectives . . . 20
3.5.1 Evaluation Criteria . . . 20
3.5.2 Applicability in Non-Hierarchical Organizations . . . 20

4 Solution **23**
4.1 Threat Modeling Protocol for Horizontal Organizations . . . 23
4.1.1 Key Design Principles . . . 23
4.1.2 Target Audience . . . 24
4.2 Threat Modeling Process Overview . . . 24
4.2.1 Step 1: Establish Context and Goals . . . 24
4.2.2 Step 2: Map Systems and Trust Boundaries . . . 25
4.2.3 Step 3: Profile Adversaries . . . 26
4.2.4 Step 4: Identify Threats Collaboratively . . . 27
4.2.5 Step 5: Analyze Attack Scenarios . . . 29
4.2.6 Step 6: Prioritize Risks Together . . . 30
4.2.7 Step 7: Mitigations and Governance Decisions . . . 31
4.2.8 Participation Tips . . . 32

5 Evaluation **33**
5.1 Experimental Design . . . 33
5.2 Evaluation Metrics . . . 33
5.2.1 Threat Volume and Diversity . . . 33
5.2.2 Relevance to Critical Assets . . . 34
5.2.3 Actionability of Outcomes . . . 34
5.3 Participant Experience and Usability . . . 35
5.3.1 Ethics and Protection of Organizations . . . 35
5.4 Results . . . 35
5.4.1 Threat Volume and Diversity . . . 35
5.4.2 Relevance to Critical Assets . . . 36
5.4.3 Actionability of Outcomes . . . 37
5.4.4 Participant Experience and Usability . . . 37

6 Conclusion **39**
6.1 Summary of Findings . . . 39
6.2 Discussion and Implications . . . 39

6.3 Limitations of the Research 40
6.4 Future Work 41

Bibliography **42**

Annexes

I Workshop results **48**

Acronyms

ABC Asset-Based Cryptocurrency *(pp. 18–21)*

COLBAC Collective based access control system *(pp. 8, 10, 17, 18, 20, 21)*
CoReTM Collaborative and Remote Threat Modeling *(p. 17)*

DAC Discretionary Access Control *(p. 17)*
DFD Diagrama de Fluxo de Dados *(pp. 26, 37)*
DFDs Diagramas de Fluxo de Dados *(pp. 12, 21)*
DREAD Damage, Reproducibility, Exploitability, Affected users, Discoverability *(p. 13)*

hTMM Hybrid Threat Modeling Method *(p. 17)*

MAC Mandatory Access Control *(p. 17)*

PASTA Process for Attack Simulation and Threat Analysis *(pp. 1, 2, 13–15, 20)*
PGP Pretty Good Privacy *(pp. 19, 20)*
PnGs Personae Non Gratae *(p. 16)*
PTM Participatory Threat Modeling *(p. 17)*

RBAC Role-Based Access Control *(p. 17)*

STRIDE Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege *(pp. 1, 2, 7, 8, 12–14, 16, 18, 20, 22, 28, 33–38)*

WoT Web of Trust *(pp. 19, 20)*

1

Introduction

1.1 Threat Modeling: Relevance and Challenges

Threat modeling is an essential discipline in information security, whose main function is to identify, classify and mitigate vulnerabilities in technological systems before they can be exploited by adversaries [38, 51]. In a context where systems become increasingly complex and integrated, threat modeling stands out as a critical tool for anticipating risks and establishing effective security measures [45, 36].

Traditional models such as Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE), attack trees, and iterative methodologies such as Process for Attack Simulation and Threat Analysis (PASTA) have been widely applied in hierarchical contexts [34, 35, 47]. These approaches focus on linear, hierarchical data flows, but face significant challenges when applied to horizontal organizations, where the distribution of power and responsibilities fundamentally alters risk dynamics [40, 9].

Horizontal organizational structures, characterized by the absence of a formal hierarchy, face particular challenges in threat modeling [9]. The lack of centralization can make it difficult to implement role based access controls (RBAC) and other systems that rely on hierarchical structures [9]. Furthermore, the temporary centralization of organizational secrets, such as passwords or encryption keys, often leads to conflicts known as "password wars" during leadership transitions [19].

Additionally, digital tools often promote implicit centralization of power, creating the phenomenon of the "digital vanguard", where individuals control critical resources such as communication platforms [10]. This is exacerbated by attacks specific to horizontal systems, such as identity spoofing (Sybil attacks) and quorum manipulation, which exploit the dependency on participatory processes [46, 7].

The challenges highlighted indicate the need for adaptations in threat modeling methods for horizontal contexts [9]. In addition to technical limitations, such as the difficulty of integrating collaborative cryptography [1], the need for participatory tools that respect democratic dynamics and promote resilience is also highlighted [6].

1.2 Horizontal Security in Times of Interconnection

In today's interconnected world, horizontal organizations challenge the assumption that security depends on a clear chain of command [11, 42]. The absence of a formal hierarchy can become a strategic asset by preventing centralized attacks and enabling a reconfiguration of trust management, promoting organizational resilience [42, 9]. In distributed trust systems, such as those used in blockchain based organizations, security is promoted by collaborative mechanisms that replace formal leaders with participatory processes and solutions oriented towards transparency and consensus [33, 1].

Traditional threat analysis methodologies such as STRIDE and PASTA provide valuable insights but face limitations in decentralized environments, highlighting the need for approaches better suited to the specificities of horizontal structures [14, 36]. Less hierarchical contexts require adapted approaches that understand the complexity of horizontal trust and the potential associated risks [9].

In this sense, technologies such as collaborative cryptography [9, 1] and threat modeling approaches that adopt the global perspective of the organization can promote a more realistic understanding of security in decentralized structures. Horizontality, often seen as a challenge, should be explored as a strategic asset capable of diluting single points of failure and strengthening organizational resilience [42].

1.3 Organizational Governance: A Historical Perspective

Organizational governance reflects the social, economic, and technological structures of each era. From the earliest human groups to the complex organizations of contemporary times, the ways of organizing power and decision making have been shaped to respond to specific contexts [11]. The hierarchical model, widely adopted, emerged as a solution to demands for control and efficiency. However, history also records experiments that challenged this logic, suggesting the possibility of new approaches to the management and coordination of activities [15, 50].

Even in systems considered pioneers in horizontality, such as Athenian democracy, governance faced significant limitations related to inclusion and practical applicability, highlighting weaknesses in the operationalization of equal participation [2]. As the Industrial Revolution progressed, hierarchical centralization intensified to cope with organizational growth and complexity [50]. Additionally, experiences such as cooperatives and the 19th century labor movement outlined alternatives to absolute centralization, while modern technologies offer decentralized structures that challenge traditional paradigms of control [15, 42].

Innovations such as the internet open up new possibilities for decentralization, yet face challenges in equitable distribution of power and resources, as evidenced by the concentration of miners on public networks [17].

These historical and technological evolutions not only shape governance structures, but also introduce unique challenges in threat modeling [49, 41]. Critical analysis of these attempts allows us to identify vulnerabilities and strengths that underpin the construction of security protocols in horizontal organizations [9].

1.4 Security Protocol for Non-Hierarchical Organizations

This research proposes a security protocol that integrates horizontality as a strategic element, going beyond the simple adaptation of traditional methodologies [9]. The main objective is to demonstrate how decentralization, when structured in a way that is coherent with organizational principles, can strengthen resilience against complex threats, mitigating single points of failure and distributing responsibilities equitably [38]. The protocol aims to balance operational efficiency and democratic participation, ensuring that security measures do not compromise decision making agility or the inclusion of members in critical processes [33]. To this end, it relies on collaborative approaches, such as cryptography adapted to horizontal contexts [9], and on threat modeling methodologies that consider participatory dynamics [43].

The integration between security and governance is addressed through guidelines that harmonize technical requirements with organizational principles [43]. The protocol will apply transparent and auditable consensus mechanisms, inspired by distributed reputation models [33], to validate access policies and mitigate risks such as Sybil attacks [46]. In addition, it incorporates modular structures that allow adaptation to different levels of horizontality, from fully decentralized networks to organizations with more hierarchical structures [9]. This flexibility is essential to respond to dynamic threats without compromising the autonomy of members and to cover the largest number of organizations.

To strengthen resilience, the protocol combines technical and social layers: cryptographic techniques protect against external threats, while radical transparency structures and periodic reviews by rotating committees prevent internal fraud [42]. The traceability of decisions via immutable records ensures that vulnerabilities are identified and corrected collaboratively, in line with studies on failures in distributed systems [33].

1.5 Defining the Scope of Research

The diversity of horizontal organizations ranges from informal collectives to complex digital networks, each with its own dynamics [42]. To ensure analytical focus, this study is limited to structures that operate under strict principles of horizontality, characterized by: (1) absence of formal hierarchies or permanent centralization of power; (2) decision making processes based on consensus or broad participation; and (3) explicit mechanisms for distributing responsibilities and resources [9]. This delimitation excludes hybrid or partially decentralized models, where the coexistence of hierarchical and horizontal

structures introduces additional variables that make it difficult to evaluate the proposed protocol in isolation [11].

The choice to analyze organizations such as worker cooperatives and community networks is justified by their empirical relevance: these models have robust documentation on operational challenges [15], in addition to explicitly adopting principles of self management and radical transparency [42]. These characteristics allow testing the protocol in contexts where security depends directly on collective coordination, without intermediaries or central authorities [38].

Although digital platforms and decentralized social networks [18] represent equally relevant cases, their dynamic nature and dependence on heterogeneous technical infrastructures would require methodological adaptations beyond the current scope. Future studies could explore these variations, using the protocol developed here as a basis for comparative analyses in less controlled environments.

1.6 Expected Contributions

The research will deliver a threat modeling protocol specific to horizontal organizations, integrating the principles of distributed governance, collective participation, and transparency. This protocol will be designed to identify, understand and mitigate threats in decentralized structures, providing practical guidelines adapted to the particularities of these organizations. In addition, it will be accompanied by an evaluation method to validate its effectiveness and its application in real cases.

The protocol is expected to demonstrate how horizontality can be a strategic asset, reinforcing organizational security and resilience in the face of complex threats. In addition to contributing to theoretical advancement on security in decentralized structures, the research seeks to offer a practical solution that strengthens autonomy and promotes the integration between security and democratic governance.

1.7 Structure of the Thesis

After the introduction, the Background chapter presents the fundamentals of threat modeling and security in horizontal structures. The Related Work chapter analyzes previous studies, identifying relevant gaps and opportunities.

The first chapter presented the context that support this research, identifying challenges faced by non-hierarchical organizations in the area of digital security and threat modeling. The structural particularities of these organizations were described, highlighting the need for specific methods for risk analysis and mitigation. Having defined the objectives, intended contributions and structure of this research, Chapter 2 will address the essential

concepts that underpin the study, including threat modeling, the conceptual differences between horizontal organizations and organizations without explicit leadership, and the role of democratic centralism as an organizational principle.

2

Background

2.1 Foundations of Threat Modeling

Threat modeling is a central component of cybersecurity as it allows the identification of valuable assets, analysis of potential attack vectors and establishment of controls capable of mitigating risks. This practice goes beyond technical factors incorporating organizational and human elements that shape security in diverse contexts, especially in horizontal structures, where internal processes and trust relationships become even more critical due to the absence of formal hierarchies [9]. In a scenario of rapid technological evolution and constant diversification of threats, a broad and flexible approach gains relevance, meeting the particularities of changing contexts [38].

Studies such as [28], [29], and [45] demonstrate the need for structured, yet adaptable, methods to keep up with changing environments. Adopting the adversary perspective [25] is crucial to anticipate complex scenarios and strengthen resilience in decentralized environments, where the multiplicity of actors and the distribution of power require a holistic analysis of threats. In this type of context, threat modeling needs to reflect the distribution of power and the multiplicity of actors, including potential internal, external and hybrid threats [36].

In addition, Microsoft's experience, documented in [37], emphasizes the importance of involving diverse stakeholders and applying collaborative tools. These elements become crucial when decision making is democratic or decentralized, since identifying and mitigating risks requires collective engagement and strategic flexibility, connecting the threat modeling exercise to organizational dynamics [43].

2.1.1 Conceptual Definitions

Threat modeling can be understood as a systematic protection effort that considers both technical vulnerabilities and social and organizational factors. By adopting a holistic view, as suggested by [28] and [29], security analysis is not restricted to infrastructure, but incorporates internal practices, information flows, and the organization's culture. In non-hierarchical contexts, the absence of clear lines of authority and the participatory

nature make an analysis that considers the distribution of responsibilities and the reliance on collective mitigation mechanisms essential [9].

In turn, [45] emphasizes that there is no single solution for threat modeling. In this sense, threat modeling becomes an iterative process, adapting to structural changes and incorporating innovations such as participatory decision making tools and collaborative security practices [43].

2.1.2 Main Methodologies

Widely discussed methodologies such as Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE), attack trees, and scenario based frameworks [40] provide a tested starting point, but they often fail to capture the complexity of horizontal structures.

The documentation [36] provides an overview of existing methods, cautioning that the effectiveness of each approach depends on the context. For example, STRIDE and attack trees are useful for identifying straightforward attack vectors, but the lack of formal hierarchies intensifies the need to explore complex scenarios such as insider threats coupled with external attacks, as well as flaws in distributed authentication, consensus, and governance mechanisms, as suggested in [9, 35, 20].

Integrating diverse approaches, such as collaborative cryptography practices [1] and hybrid approaches [48], enables horizontal organizations to identify less obvious risk patterns and strengthen their collective resilience. This integration becomes crucial in distributed structures for reaching maximum cohesiveness.

2.2 Taxonomy of Organizational Structures

Understanding the relationship between organizational form and security is essential to adjust threat modeling to the reality of each institution [11]. While hierarchical structures rely on central decision points for control and coordination, these same points can become critical vulnerabilities [38]. Horizontal organizations can disperse vulnerabilities and increase resilience through decentralized governance, although they can also create multiple entry points that require collaborative control [9]. Analysis of this taxonomy, as [15, 21], provides a basis for identifying how the distribution of power in different organizational forms affects the effectiveness of security measures, including the ability to respond to internal and external threats.

2.2.1 Traditional Hierarchical Structures

Hierarchical organizations have clear lines of authority, which facilitates control but can concentrate vulnerabilities in critical areas [34]. These organizations are characterized by a well defined chain of command, where decisions flow from the top down. Classic examples include large multinational corporations, where the board of directors establishes policies

that are implemented by layers of managers, supervisors, and employees. On the other hand, in small businesses, such as family offices, the hierarchy may be less formal but still based on a clear, centralized command structure [15].

In large organizations, such as banks or automotive manufacturers, hierarchy allows for efficient allocation of resources and tight control over operations. For example, IT departments in these environments often use security frameworks such as STRIDE for threat modeling, focusing on protecting critical assets and centralized access management [34, 51]. Centralization facilitates rapid incident response, but it also creates single points of failure, such as vulnerabilities in key servers or administrative credentials [49, 27].

In contrast, small businesses face different challenges. In these contexts, lack of resources may lead to fewer hierarchical layers, but decisions are still centered on a single owner or manager [50]. This reduces organizational complexity but increases reliance on specific individuals, making them prime targets for attacks [15]. Furthermore, the lack of dedicated security teams can limit the ability to implement sophisticated frameworks such as STRIDE, requiring more streamlined solutions.

The difference between large and small organizations also impacts threat modeling [15, 36]. In larger organizations, hierarchical structures allow for detailed segmentations to identify and mitigate risks at specific levels of the organization. However, this segmentation can lead to communication gaps between departments, making it difficult to implement integrated solutions [51]. On the other hand, smaller organizations have greater flexibility to quickly adapt their security strategies, although they often lack the resources to implement robust solutions [50].

Therefore, while hierarchical organizations offer advantages in terms of control and clarity, they also introduce specific challenges for threat modeling. These challenges vary significantly with the size and complexity of the organization, requiring adaptations to traditional frameworks to meet the specific needs of each type of hierarchy.

2.2.2 Horizontal Organizations

Horizontal organizations are distinguished by their rejection of traditional hierarchies, prioritizing distributed decision making processes and equitable participation of all members. This model contrasts directly with hierarchical structures, which centralize power at higher levels, perpetuating inequalities in access to information and organizational control [11].

Horizontality is both a tool and an objective in itself [9]. In Argentine social movements, as analyzed by Marina Sitrin, horizontality has emerged as an essential mechanism for establishing relationships based on trust and consensus, overcoming traditional forms of organization. Neighborhood assemblies and collectives of unemployed workers exemplify how horizontality can be applied to self management and collective planning [42].

In the field of cybernetics, the Collective based access control system (COLBAC) protocol demonstrates the relevance of horizontality in digital security systems, promoting

collaborative access control that reduces the centralization of power. This model avoids the vulnerabilities created by the dependence on single owners of passwords or permissions, reinforcing the coherence between organizational practices and technological tools [9].

In addition, historical examples, such as Athenian democracy, illustrate that horizontal structures can be complemented by temporary centralization mechanisms in times of crisis, ensuring flexibility and efficiency without compromising the basic principles of distributed governance [2].

Despite the challenges, such as the risk of domination by more influential voices or the management of conflicts in collective spaces, horizontal organizations demonstrate that, with adequate mechanisms, it is possible to promote autonomy, inclusive participation and efficiency in decentralized structures [10].

2.2.3 Leaderless Organizational Models

Leaderless organizations hides an additional complexity, where the absence of a formal hierarchy does not necessarily imply genuine horizontality [10]. Critical studies highlight how these organizations often replicate veiled power dynamics and informal centralizations [10, 42].

Marina Sitrin, in her analysis of horizontal movements in Argentina, points out that although horizontality is declared as an objective, many movements face significant challenges in sustaining truly participatory practices. The lack of formal hierarchy often leads to informal power structures, where dominant voices assume leadership roles without oversight or clear collective responsibility [42].

In the digital context, movements such as Occupy Wall Street demonstrate that the absence of recognizable leadership does not eliminate internal conflicts [10]. Studies of social media teams in these movements reveal that account management, as on Twitter, was often marked by struggles for control, illustrating how power and influence can consolidate even in supposedly horizontal structures [10].

Furthermore, research on worker cooperatives in the United States indicates that these organizations, although often seen as non-hierarchical alternatives, tend to develop informal leaders who influence decisions in significant ways, challenging the narrative of absolute horizontality [50].

Technologies used by these organizations also carry political implications [49, 41]. Langdon Winner argues that technical artifacts can perpetuate existing power structures, even when employed in decentralized contexts [49]. For example, digital platforms, often designed for individual use, create challenges in building effective collective governance, exacerbating latent inequalities [49, 27].

These examples highlight that while the idea of formal leadershiplessness is appealing, its practical execution often results in informal forms of hierarchy [42, 10]. Thus, the success of these organizations depends on the ability to identify and mitigate hidden power dynamics, promoting clear mechanisms of collective governance and mutual

accountability that truly sustain the desired horizontality [9].

2.3 Democratic Centralism

In the midst of increasingly challenging scenarios in terms of organizational coordination, whether in the management of large corporations or in the maintenance of decentralized networks such as blockchain, the need arises to reconcile efficiency in decision making with the active participation of all those involved [49]. Democratic centralism, formulated to meet the demands of revolutionary movements, maintains its relevance by proposing a dynamic balance between collective deliberation and centralized execution [31]. This approach has proven to be relevant both in political and social contexts and in contemporary technological scenarios [9].

2.3.1 Fundamental Principles and Theoretical Origins

Democratic centralism is based on the idea that opinion gathering and deliberation (democracy) must be harmonized with the ability to implement decisions in a unified manner (centralism) [44]. This system was originally conceived as a response to the need for organization in contexts of high structural complexity [52].

Its initial formulation, associated with the Communist Party of the Soviet Union, inspired the adoption of the model by different groups around the world [52]. In China, for example, the practices of democratic centralism demonstrate remarkable resilience, being reconfigured as political and social situations change [44].

2.3.2 Contemporary Models of Application

The transposition of the precepts of democratic centralism to modern contexts has been observed in different organizational and technological structures [49, 9]. One example is the COLBAC protocol, which adapts the bases of democratic centralism to a collaborative access control environment, enabling participatory decisions combined with cohesive implementation [9].

Trade unions and social organizations have also integrated principles of democratic centralism [8].

2.3.3 Implications and Potentials for Governance

The influence of democratic centralism transcends the limits of political parties and can be extended to diverse scenarios that require both broad participation and efficient execution [44, 5]. Horizontal or distributed organizations can use this model to reconcile the voice of their members with the need to make centralized decisions at critical moments [52, 44].

In this sense, the application of elements of democratic centralism in digital platforms highlights how historical concepts can be reappropriated to meet contemporary governance demands [9].

Chapter 2 presented the theoretical foundations related to threat modeling, addressing structured and flexible methods needed to deal with decentralized organizational contexts. Approaches that incorporate adversarial perspectives were discussed and emphasized the importance of considering social and organizational factors, in addition to technical vulnerabilities, highlighting especially the relevance of collaboration between different actors in the process. Building on these fundamental concepts, Chapter 3 will analyze related works, describing in detail traditional threat modeling approaches, such as STRIDE, and exploring their applications and limitations in decentralized and collaborative environments.

3

Related Work

The references discussed in this chapter were chosen based on an initial selection suggested by the advisor of this work, Professor Kevin Gallagher. As a starting point, the professor provided three fundamental articles related to his research area: COLBAC, ABCcrypto and PGP's Web of Trust. In particular, the work on COLBAC is directly linked to Professor Gallagher's academic production, offering a solid and highly relevant basis for the development of this research. Based on these initial references, traditional and emerging methods for threat modeling were explored, aiming to establish a comprehensive overview that would allow a critical analysis of the applicability of these methods to the specific context of non-hierarchical organizations.

3.1 Traditional Approaches to Threat Modeling

3.1.1 STRIDE

Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE), developed by Microsoft, is a systematic threat modeling methodology designed to identify potential vulnerabilities in software systems [34]. The acronym STRIDE stands for six main categories of threats [38]. Each of these categories reflects a specific violation of desired security properties such as authenticity, integrity, non-repudiation, confidentiality, availability, and authorization [34].

Applying STRIDE begins with the creation of Diagramas de Fluxo de Dados (DFDs) to map the movement of information within the system [12]. DFDs help identify elements such as external entities, processes, data flows, and data stores. For each element in the diagram, the six STRIDE threat categories are analyzed to identify potential vulnerabilities [38].

Each threat in STRIDE has a clear definition and practical examples to aid in identification and mitigation. For example:

1. **Spoofing:** Threats that involve falsification of the identity of users or processes, compromising authenticity.

2. **Tampering:** Manipulation of data in transit, in storage, or in memory, affecting integrity.
3. **Repudiation:** Scenarios where users deny actions performed, often due to the lack of adequate logging mechanisms.
4. **Information Disclosure:** Exposure of sensitive information to unauthorized parties, compromising confidentiality.
5. **Denial of Service:** Attacks that overload system resources, impairing availability.
6. **Elevation of Privilege:** Cases where a malicious actor obtains privileges above those authorized, compromising authorization.

The STRIDE methodology can be adapted to different contexts. For example, in cyber-physical systems, it is possible to assess threats related to hardware and software components, such as failures in synchronization or communication [20]. In addition, variants such as STRIDE-per-Element and STRIDE-per-Interaction offer more focused approaches to identify threats in specific elements or in interactions between components [38].

Although widely used, STRIDE has limitations. It relies heavily on analyst experience and may not capture emerging threats in decentralized systems or dynamic environments [13]. Therefore, it is often complemented with other frameworks, such as Damage, Reproducibility, Exploitability, Affected users, Discoverability (DREAD), to prioritize threats based on impact and probability [22].

In summary, STRIDE provides a solid foundation for threat identification, but its effective application requires integration with other methodologies and adaptations to meet the specific needs of modern, decentralized systems [12].

3.1.1.1 STRIDE Complementary Models

Several complementary models have been derived from or used in conjunction with STRIDE to improve its effectiveness and adaptability in different contexts [32]. Notable among these is the DREAD model, which complements STRIDE by providing a quantitative approach to threat prioritization [22]. DREAD uses five main categories: Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability, allowing analysts to assign values and create scores to rank threats according to their severity [32, 22].

The combined use of STRIDE and DREAD can improve risk assessment in more complex systems. However, the inherent subjectivity in assigning values in DREAD can compromise the consistency of [22] analyses. To mitigate these limitations, some organizations have integrated STRIDE with more comprehensive frameworks, such as Process for Attack Simulation and Threat Analysis (PASTA), which takes an iterative approach to identifying and prioritizing threats [32].

Additionally, the use of attack trees has proven effective in complementing STRIDE, allowing teams to visually represent complex threat scenarios and identify multiple attack paths [24]. This integration is particularly useful in horizontal organizations, where the lack of centralization increases the need for collaborative threat mapping [38].

3.1.2 Attack Trees

Attack trees, introduced by Bruce Schneier [35], provide a hierarchical framework for threat modeling, where the attack objective is represented by the root node, and the sub objectives and steps required to achieve it are arranged in child nodes. Each node can be detailed with logical operators such as AND and OR, representing conditions that must be met either together or alternatively [24].

A key advantage of attack trees is their ability to decompose complex threats into smaller, more manageable components, enabling systematic analysis [17]. This methodology makes it easier to identify multiple attack paths, allowing organizations to prioritize countermeasures based on metrics such as cost, impact, and likelihood [16].

Practical applications of attack trees include their use in wireless sensor networks to assess location privacy risks [16], as well as in energy theft detection in advanced metering infrastructures such as smart grids [17]. In both cases, the approach enables organizations to map specific threat scenarios and design effective countermeasures.

In addition, studies such as [24] highlight the reuse of subtrees to increase efficiency in complex systems. This practice allows shared elements across different scenarios to be modeled once and incorporated into future analyses, saving time and resources.

Although broadly applicable, attack trees present challenges related to the effort required for their initial construction and the complexity in large scale systems [35, 17]. Collaboration between stakeholders, including technical and operational experts, is essential to ensure that threat representation is accurate and comprehensive [17].

Attack trees also stand out as complementary tools to methodologies such as STRIDE and can be used both to identify threats and to organize those already discovered [24, 51]. Furthermore, reusing existing trees, such as those focused on fraud or elections, saves time and provides a solid foundation for analysis [24]. Despite their versatility, effective use of trees depends on clear representations of AND/OR nodes and continuous evaluation to avoid oversights or gaps [38].

3.2 Emerging Methodologies

3.2.1 PASTA

PASTA is a risk centric threat modeling methodology designed to integrate security throughout the software development lifecycle. Proposed by Tony UcedaVelez and Marco M. Morana [47], the framework consists of seven sequential stages that allow for in depth and iterative analysis of threats and vulnerabilities.

The main goal of PASTA is to align security concerns with business objectives, ensuring that mitigation measures address both technical risks and organizational impacts [47]. The methodology promotes a risk oriented approach by integrating attack simulations to evaluate the effectiveness of proposed countermeasures [47].

1. **Definition of the Objectives (DO):** In this initial stage, the security requirements, risk profile, and potential business impacts are defined.

2. **Definition of the Technical Scope (DTS):** This stage details the technical aspects, such as users, software components, third party infrastructure, and external dependencies.

3. **Application Decomposition and Analysis (ADA):** The application is broken down into basic functional elements to identify data flows, user types, and existing security controls.

4. **Threat Analysis (TA):** Identification of potential threats based on the analyzed elements and assets, considering the most likely attack vectors.

5. **Weakness and Vulnerability Analysis (WVA):** At this stage, threats are associated with specific vulnerabilities, evaluating the effectiveness of existing controls and identifying weaknesses.

6. **Attack Modeling and Simulation (AMS):** Performing simulations to determine the most likely attack paths, using attack trees and other models to explore risk scenarios.

7. **Risk Analysis and Management (RAM):** Identifying technical and business impacts, proposing measures to mitigate priority risks [47].

PASTA stands out for its flexibility and analytical depth, making it particularly effective in dynamic and distributed environments [51]. The methodology encourages collaboration between stakeholders from different areas, promoting a unified understanding of risks and organizational priorities [43]. In addition, the integration of attack simulations allows organizations to test the effectiveness of their security strategies under realistic conditions, improving their resilience against emerging threats [47].

One of the most relevant aspects of PASTA is its compatibility with horizontal organizations. The collaborative approach of the methodology is aligned with the principles of distributed governance [9]. In non-hierarchical structures, PASTA offers a structured framework to identify and mitigate risks in a participatory and efficient way.

3.2.2 Security Cards

Security Cards are a tool designed to facilitate brainstorming of security threats, using a deck of cards that address different aspects of potential attacks [6]. Created by Tamara

Denning, Batya Friedman, and Tadayoshi Kohno, the cards cover four main dimensions: adversary motivations, adversary capabilities, adversary methods, and human impact [4]. This approach aims to foster creativity and collaboration among stakeholders, encouraging a more holistic and comprehensive analysis of threats [39].

Each card provides examples and scenarios related to its dimension, helping teams explore vulnerabilities that might otherwise be missed by traditional methods [6]. For example, in the "Human Impact" dimension, cards can highlight how security breaches can affect privacy, emotional or financial well being, providing a more user centric perspective [4].

Security Cards have been used in a variety of applications, such as protecting biometric systems against presentation attacks [23, 4]. Their flexible structure allows them to be adapted to different organizational contexts, including decentralized environments [43]. In horizontal organizations, Security Cards facilitate the participation of multiple stakeholders, promoting distributed governance and reinforcing collaboration [39].

Despite their potential, the methodology can generate a high number of false positives, which requires additional effort to filter relevant threats [4]. However, their emphasis on creativity and inclusion of multiple perspectives makes Security Cards a valuable tool for exploring emerging threats and strengthening organizational resilience [39].

3.2.3 Personae Non Grata

Personae Non Gratae (PnGs) represent an innovative approach to threat modeling, notable for their focus on malicious users and undesirable behaviors [3]. Inspired by traditional user experience design personas, PnGs help anticipate how adversaries might exploit vulnerabilities in a system, providing a detailed adversarial perspective [26].

PnGs are created through techniques such as crowd sourcing, allowing different stakeholders to contribute insights to threat identification [26]. This collaborative approach increases the breadth and diversity of attacker profiles considered, allowing for more robust modeling that is adapted to different contexts [3].

One of the main advantages of PnGs is their ability to capture specific attacker motivations, capabilities, and behaviors [26]. For example, a PnG might describe an adversary who uses phishing to obtain credentials or exploits security flaws in financial transactions [3]. This level of detail helps in prioritizing countermeasures and allocating security resources [26].

In addition, PnGs are particularly effective in contexts where internal and external threats overlap [3]. In flat organizations, where governance is distributed and responsibility is shared, PnGs help map potential risks that may arise from internal actors, such as employees, or external actors, such as competitors [3].

Despite its benefits, implementing PnGs requires significant effort to ensure that profiles are accurate and relevant [26]. However, when integrated with other methodologies such as attack trees or STRIDE, PnGs provide an additional layer of analysis, making

them an indispensable tool for organizations seeking to comprehensively understand and mitigate threats [26].

3.3 Hybrid and Collaborative Approaches

Hybrid and collaborative approaches seek to integrate different methodologies to create adaptable and effective frameworks in different contexts [25, 48]. Among these, Hybrid Threat Modeling Method (hTMM) stands out, combining elements of different frameworks for a comprehensive risk analysis. It is particularly useful in scenarios involving multiple stakeholders and requiring alignment between security objectives and business priorities [25].

Another example is Collaborative and Remote Threat Modeling (CoReTM), designed to facilitate threat modeling in distributed or remote teams. Using collaborative tools, such as shared annotation platforms, CoReTM makes the process more accessible and inclusive [48].

Finally, Participatory Threat Modeling (PTM) promotes the inclusion of a wide range of stakeholders in the threat modeling process [43]. This approach values the diversity of perspectives, being especially relevant in decentralized contexts where transparency and collective participation are essential [43]. These methodologies reinforce distributed governance and strengthen organizational resilience, complementing the work developed by more traditional frameworks [9].

3.4 Decentralized Trust and Cryptographic Frameworks

3.4.1 COLBAC

Collective based access control system (COLBAC) is an access control model designed to address the specificities of horizontal organizations, promoting a democratic and participatory approach to access authorization. Its proposal seeks to overcome the challenges imposed by traditional access control models, such as Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-Based Access Control (RBAC), which often reinforce hierarchical dynamics that are inadequate for horizontalized structures [9].

One of the most striking features of COLBAC is its ability to align access control with horizontal governance practices, allowing decisions to be made collectively through democratic processes [43]. The model organizes resources and processes into three main spheres: the Collective Sphere, which concentrates critical resources subject to collective approval; the User Sphere, which encompasses individually managed resources based on traditional controls; and the Immutable Sphere, responsible for storing logs and records in an unalterable manner, ensuring transparency and traceability [9].

In the context of COLBAC, interactions with the Collective Sphere follow a process structured in three phases: in the Draft Phase, the user creates a token that specifies the

permissions and objectives of the action; in the Petition Phase, the token is submitted to a vote by the members of the organization; in the Authorization Phase, the results of the vote determine the approval or rejection of the action, with all records being stored in the Immutable Sphere [9]. This structure offers flexibility by allowing the adaptation of the level of horizontality according to the needs of the organization, including in crisis situations that may require temporary centralizations [9].

Despite its advantages, COLBAC faces challenges inherent to its democratic approach [9]. Frequent voting processes can result in user fatigue, especially in larger organizations [9, 42]. In addition, democratic attacks, such as quorum manipulation or the abuse of emergency tokens, pose significant risks. Such issues can be mitigated by implementing independent audits, dynamic adjustments to quorum criteria, and mechanisms that limit the use of emergency tokens [9]. Another important issue is the learning curve associated with the model, which requires familiarity with democratic practices and an understanding of how tokens work [9].

COLBAC offers an innovative solution for organizations that want to align their horizontal governance with robust digital security practices [9]. Its transparency, flexibility, and commitment to democratic participation position it as a strategic tool to overcome security challenges in decentralized structures, transforming potential vulnerabilities into opportunities to strengthen collective autonomy [9, 42].

3.4.2 ABCcrypto

Asset-Based Cryptocurrency (ABC) is a threat modeling framework specifically developed to address the peculiarities of cryptocurrencies and blockchain based systems. In contrast to generalist frameworks such as STRIDE, ABC is designed to address the unique security challenges presented by distributed and permissionless systems, where actors distrust each other and economic incentives play a central role [1].

The main differentiator of ABC is the introduction of collusion matrices, which allow the analysis of threat scenarios involving collaborations between different malicious actors. This systematic approach reduces the complexity of the modeling process by eliminating irrelevant cases and grouping scenarios with similar effects [1]. Furthermore, the framework uses threat categories specific to cryptocurrencies, considering not only tangible assets, such as blockchains and tokens, but also abstract assets, such as privacy and reputation [1].

A key feature of ABC is its ability to tailor threat categories to the objectives and assets of each [1] system. The process begins with a detailed characterization of the system model, identifying participants, assets, and financial motivations. Threat categories are then derived based on potential violations of the security properties of the assets, such as service corruption, payment theft, and blockchain inconsistencies. Finally, concrete attack scenarios are enumerated and analyzed using the collusion matrix, which considers all possible combinations of attackers and [1] targets.

ABC also highlights the importance of incorporating economic analysis and financial incentives into the risk mitigation process. For example, “detect and punish” mechanisms can be implemented to discourage dishonest behavior by making it financially unviable. This use of game theory and economic modeling is particularly effective for addressing threats that cannot be neutralized by cryptographic means alone [1].

The effectiveness of ABC has been demonstrated in case studies involving real systems such as Bitcoin, Filecoin, and CacheCash. In the case of Filecoin, the framework revealed significant gaps in the public design, particularly in collusion scenarios that had not previously been considered. In CacheCash, ABC was used from the early design stages to identify 525 cases of collusion and implement incentive based countermeasures [1].

While ABC has clear benefits, it is not without its challenges [1]. Creating collusion matrices and analyzing threat categories in detail can be resource intensive, especially in systems with multiple participants and complex assets. However, these efforts are rewarded by the identification of critical threats and the robustness of the proposed solutions [1].

ABC offers an advanced and adaptable approach to cryptocurrency threat modeling, demonstrating that specialized frameworks can significantly improve the security and resilience of distributed systems [1].

3.4.3 PGP and the Web of Trust

Pretty Good Privacy (PGP), developed by Philip Zimmermann, is a cryptographic system that combines privacy, authentication, and convenience to protect messages and files [30]. PGP uses public key cryptography to enable secure communication between individuals, even without prior trust or key exchange over secure channels [30].

In the PGP operating model, each individual has a pair of keys — a public key, which is widely disseminated, and a private key, which is kept secret. The public key is used to encrypt messages, while the private key is used to decrypt them. This scheme not only ensures the privacy of messages, but also allows authentication through digital signatures, ensuring the integrity and origin of a content [30].

A central feature of PGP is the Web of Trust (WoT) model, which adopts a decentralized approach to identity validation. Unlike centralized hierarchies of Certificate Authorities, WoT allows any user to digitally sign another’s public key, certifying its authenticity. These signatures create a distributed trust network, in which the validation of a public key depends on the accumulated trust of the signatures of other trusted users [30].

In PGP, each user can assign different levels of trust to other individuals to act as "trusted introducers". This mechanism allows the trust network to be built organically, reflecting natural social relationships. For example, a user may fully trust another to certify keys, or only marginally, depending on their perception of the introducer’s competence and integrity [30].

In addition to promoting decentralization, WoT also provides resilience against [30] attacks. Rather than relying on a single point of failure, as is the case in centralized systems, WoT allows users to validate public keys based on multiple signatures, reducing the impact of individual compromises. However, this approach also presents challenges, such as the difficulty of managing large key rings and the subjectivity in assigning trust levels [30].

The relevance of PGP and WoT to horizontal organizations is evident. Non-hierarchical structures can take advantage of the decentralized nature of WoT to create security systems aligned with the principles of collective autonomy and distributed governance . By allowing each participant to build their own web of trust, PGP strengthens security without compromising the horizontality of these organizations [42, 9].

3.5 Comparative Perspectives

3.5.1 Evaluation Criteria

The evaluation of threat modeling frameworks requires objective criteria to compare their effectiveness, applicability, and suitability to different organizational contexts [40]. Key criteria include the ability to identify specific threats, adaptability to changes in the operational environment, implementation costs and the integration of social, economic, and technical dimensions into the modeling process [51]. In addition, scalability and the ability to handle complex organizational structures are critical factors [1].

STRIDE, for example, is widely used for its simplicity and applicability in traditional software systems [38]. However, it faces limitations in decentralized environments due to its reliance on predefined threat categories [20]. In contrast, frameworks such as ABC offer a specialized approach, using collusion matrices, while PASTA focuses on iterative risk assessment for dynamic systems [1, 47].

3.5.2 Applicability in Non-Hierarchical Organizations

The applicability of threat modeling frameworks to non-hierarchical organizations depends on their ability to address specific dynamics of these structures [9, 51]. Horizontal organizations operate on the basis of distributed governance, equitable participation, and the absence of formal centralization, requiring approaches that respect and reinforce these principles [42].

Frameworks such as COLBAC and PASTA demonstrate strong compatibility with horizontal organizations due to their emphasis on collaborative processes and adaptability to decentralized contexts. COLBAC uses collective authorization tokens to align security and democratic governance. PASTA, with its iterative and participatory approach, facilitates the involvement of stakeholders at all levels, ensuring that diverse perspectives are considered in the threat modeling process.

Table 3.1: Comparison of Threat Modeling Methods

Method	Threat categories considered	Scope	Key Features	Limitations
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege	Software and application security (design phase threat analysis)	Six category mnemonic covers major attack types (acts as a checklist). Applied to DFDs to systematically identify threats per component. Simple and widely adopted; easy for teams new to threat modeling.	Focused on technical threats, may miss threats outside its six categories (e.g., collusion or social attacks). No built in risk ranking, so a long list of threats may need additional prioritization. Considered less detailed for complex, business specific threats.
Attack Trees	No fixed set, any threat goal can be modeled (e.g., malware attack, insider abuse, social engineering) as the root, with sub goals as attack steps.	Broadly applicable (software, cyber-physical systems, critical infrastructure) for visualizing attack paths.	Graphical tree diagrams map out attacker goals and all possible paths (leaf nodes are specific attack methods). Can capture complex multi step attacks (including technical exploits or human tactics) by branching logic. Often used in combination with other methods (e.g., STRIDE or risk scoring) for comprehensive analysis.	Time consuming to create for large or complex systems (trees can become very large). No inherent risk scoring, requires supplemental analysis (like CVSS) to prioritize threats. Maintenance can be difficult as systems evolve (manual updates needed for tree changes).
PASTA	Not predefined by categories, addresses all threat types identified through its stages, from technical vulnerabilities to misuse and fraud (prioritized by business impact).	Enterprise and critical systems where business impact and risk alignment are key (e.g., fintech, large applications). Integrates with SDLC and organizational risk management.	Seven stage, risk centric methodology (from defining scope to attack simulation) providing in depth analysis. Aligns threats with business objectives, focuses on likely attacks that matter most to the organization's mission. Emphasizes risk prioritization: analyzes likelihood/impact of each threat to guide resource allocation.	Complex and resource intensive, the 7 step process is lengthy and requires cross functional expertise. Not widely used compared to simpler models; has a steep learning curve and longer implementation time. Geared toward comprehensive analysis, which may be overkill for small projects or early phase designs.
Trike	Doesn't use classic threat categories, focuses on unauthorized actions on assets. Threats are modeled as any action (Create, Read, Update, Delete) by any actor that violates assigned permissions (e.g., an insider modifying data they shouldn't, or an outsider gaining illicit access).	Primarily for security audit and risk management in software systems. Suitable for organizations wanting to set and verify acceptable risk levels for each asset/user role.	Risk based audit approach, assigns a risk score to each asset's threat scenarios, ensuring risk is acceptable to stakeholders. Uses a unique actor-asset matrix (CRUD matrix) to identify where an actor's permitted actions differ from potential malicious actions. Provides a structured way to involve stakeholders in deciding which risks to mitigate vs. accept (tying into governance).	Can be too granular/complex in large IT environments, requires detailed mapping of all assets, roles, and permissions. Less mainstream and fewer tooling options and community support compared to STRIDE/PASTA. Focuses on internal policy violations; may require augmentation to cover threats like external social engineering or collusion not captured by role permission analysis.
ABC	Collusion based threats (multiple actors cooperating maliciously) and financial attacks specific to crypto systems. Derives custom threat categories for new blockchain assets (e.g., double spend fraud, consensus manipulation) beyond traditional threat lists.	Blockchain and decentralized systems (cryptocurrencies, decentralized organizations). Tailored for systems with economic incentives and distributed trust, but also applied to other large scale distributed systems (e.g., cloud native architectures).	Introduces collusion matrices, a novel tool to systematically enumerate complex collusion scenarios among actors (forcing analysis of combinations of insider/outsider attacks). Asset centric: identifies unique assets (crypto tokens, consensus, smart contracts) and derives system specific threat categories incorporating financial impact.	Specialized scope, designed for cryptocurrency and blockchain context, so it may require adaptation to use in other domains. Complexity: Collusion analysis can become intricate (though the matrix approach manages complexity, it still demands detailed domain knowledge).

The choice of a framework for horizontal organizations must balance technical effectiveness with transparency and collective engagement. Solutions such as ABC and COLBAC excel at integrating social and economic dimensions, demonstrating that security can be strengthened through collaborative practices and inclusive governance [1, 9].

Chapter 3 analyzed traditional threat modeling approaches, highlighting established methodologies such as STRIDE, as well as their applications and limitations in decentralized and collaborative environments. The fundamental categories used in vulnerability identification were described and the necessary adaptations for non-hierarchical contexts were discussed. Based on these analyses, Chapter 4 presents the preliminary design of a protocol specifically adapted for horizontal organizations, describing the fundamental security and governance requirements necessary to maintain organizational resilience and ensure democratic participation in threat analysis and mitigation processes.

4

Solution

4.1 Threat Modeling Protocol for Horizontal Organizations

4.1.1 Key Design Principles

- **Transparency**: Security activities like decisions, configurations and incidents should be visible to members. Open logs and auditable records ensure nothing happens behind closed doors, building trust and accountability among the group.
- **Decentralization**: No single person should have unchecked power over systems or data. Access and control are distributed. This prevents a single admin from being a weak link and avoids creating a digital vanguard where a tech savvy few hold all the keys.
- **Democratic Participation**: All members can participate in identifying and addressing threats. Security decisions are made through inclusive discussions or votes, so measures are collective. This keeps the process aligned with the cooperative's democratic governance.
- **Traceability**: Every important action like granting access or making a change leaves an immutable trail. For example, changes can be logged on tamper proof ledgers and digitally signed by those who approved them. This way, if something goes wrong, the cooperative can trace what happened and who was involved, without relying on memory or hearsay.
- **Resilience**: The protocol aims to strengthen the cooperative's ability to withstand and recover from threats. By eliminating single failure points and planning for crises with backup plans and rapid response mechanisms, the organization stays resilient even under attack.

These principles ensure that improving security will not undermine the organization nature of the group. Instead, security measures will reinforce collaboration, shared responsibility, and trust. What follows is a step by step threat modeling process designed

with these values in mind. Each step includes guidance and checklists for participatory activities, and the protocol can be scaled or adapted for organizations of different sizes and structures.

While this protocol is inspired by established frameworks like PASTA, it does not use the formal seven stage PASTA terminology. Instead, it presents an equivalent logic in a more accessible format focusing on horizontal scenarios.

4.1.2 Target Audience

The protocol is designed for members of horizontal organizations without specialized cybersecurity expertise. Unlike traditional expert oriented models, our protocol emphasizes simplicity and accessibility. It supports members involved in decision making, operational activities, conflict resolution, and coordination tasks, as well as informal community groups, by providing clear guidance and intuitive methods for effectively dealing with security threats.

4.2 Threat Modeling Process Overview

The threat modeling process is broken into eight collaborative steps. In a small cooperative, most steps can be taken in all hands meetings or workshops with everyone. In larger groups, you might delegate initial work to working groups, but every member should have a chance to review and contribute at each stage. The process is iterative and modular, so you can adjust the depth or format of each step based on your organization's size and needs. For each step below we describe the process and its activities.

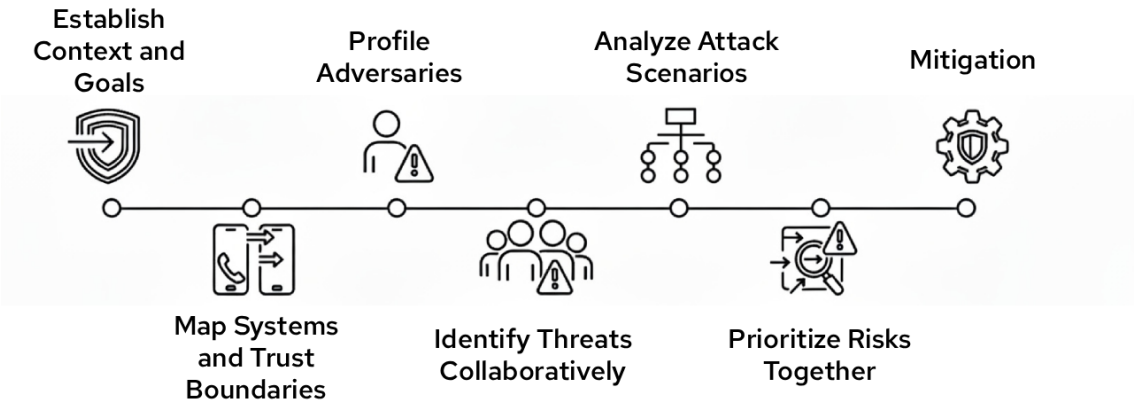

Figure 4.1: Process overview.

4.2.1 Step 1: Establish Context and Goals

What Are We Protecting?

4.2.1.1 Purpose

Set the stage by agreeing on what assets and operations you need to protect, and what your security objectives are. This ensures everyone is on the same page about why you are doing threat modeling and what success looks like.

4.2.1.2 Activities

- **Identify Critical Assets**: In a group, list out what is most valuable to your organization. This can include digital assets as member data, documents, the website, chat platforms or physical assets as office space, devices, servers or intangible assets as the organization's reputation, member trust. Ask yourselves what would hurt the most if it were stolen, destroyed, or made public.
- **Outline Key Operations/Workflows**: Describe in simple terms what the organization does everyday. For example, "We coordinate orders through an online platform", or "We have weekly meetings to make decisions", or "We run a community space with an entry badge system". Understanding these workflows helps identify where disruptions would be most damaging.
- **State Security Objectives and Requirements**: Discuss what security means for your organization. Do you need to keep member data private? Ensure your service is always available? Meet any legal regulations like GDPR? Also consider organization statutes or policies about confidentiality and data handling. For instance, if your statutes say all financial info must be accessible to members, that influences how you balance transparency with confidentiality.
- **Define the Scope and Boundaries**: Decide what will and won't be covered in this threat modeling exercise. Maybe you want to focus on a particular system and not on unrelated areas. Or include only digital systems but not physical office security or vice versa. Clearly defining scope prevents the discussion from going off track. It is okay to start with a narrow scope and expand later if needed.
- **Agree on Terminology**: Ensure everyone understands basic terms you will use. For example, define what you mean by asset, threat, vulnerability, etc., in plain language. A quick glossary on a whiteboard can help.

4.2.2 Step 2: Map Systems and Trust Boundaries

How Do We Work?

4.2.2.1 Purpose

Create a shared understanding of how information and processes flow in your organization, and where important trust boundaries are. Essentially, draw a map of your organization's

sociotechnical system including people, tech, and their interactions. In threat modeling, this is similar to diagramming your system architecture and identifying entry points. For a cooperative, it also means noting social trust assumptions like who or what we trust and in what ways.

4.2.2.2 Activities

Diagram the workflow sketching on a Diagrama de Fluxo de Dados (DFD) how components interact. Use rectangles for entities, circles for actions/processes, and cylinders for storage. Draw arrows to represent data flow or interactions (e.g., members log into the chat platform, the website communicates with a payment processor, emails are sent, files shared, money transferred). Mark external services clearly since they are only partially under your control.

Identify trust boundaries, the points in the system where the level of trust changes. For instance: between an external user and your internal system like a public website and your internal database; between a regular member and personal data; social trust boundaries for example the trust members will not to leak info from private discussions.

On your diagram, draw a dotted line where these boundaries are. Essentially ask: At what points do we assume things are safe on one side and potentially risky on the other?

Document Who Has Access to What: Alongside the map, list which roles or people have access to which assets. E.g., "Only tech team members can access the server", or "All members can post in the forum", or "Treasurer has the bank account login". This helps spotlight any concentrations of access and areas where trust is placed in individuals. Write down services or partners you rely on and mark them on the diagram for example, your website host, email service, or any software provider.

4.2.3 Step 3: Profile Adversaries

Who Might Attack Us?

4.2.3.1 Purpose

Humanize the threats by creating adversary personas that represent fictional characters that represent types of attackers or sources of threats. This helps the group to think from an attacker's perspective and ensures you consider the motivations and capabilities behind the threats. In this step we focus on personas for intentional actors. Developing these profiles makes later analysis more concrete and relatable.

4.2.3.2 Activities

- **Identify Key Threat Actors**: Ask yourselves, "Who would carry out these actions?". You will find a few recurring personas. For example: a hacker or vandal with no connection to the organization, motivated by profit or entertainment; a state or

corporate actor who opposes the organization's mission; a disgruntled or former member with inside knowledge and intent to cause harm; or a careless insider who, even without bad intentions, may introduce risks through mistakes or negligence. It is also important to distinguish between adversaries with technical skills, such as a mid level hacker and those who act in a non technical manner, such as an insider who manipulates rules or processes to his or her own advantage.

- **For each type of actor**, it is recommended to create a brief profile that includes their name and role, for example: "Cristie, the Malicious Insider" or "Zé, the Unaware member", as well as describing their motivations such as profit, revenge, or simply wanting to harm the organization and their capabilities or resources, from intrusion techniques to privileged insider knowledge. In addition, it is important to indicate what methods this actor might use for example: phishing, vulnerability exploitation, manipulation of legitimate credentials. And relate each persona to specific scenarios from the threat list, highlighting how their actions fit into the group dynamics.

- **Include at Least One Insider Persona**: Cooperatives thrive on trust, yet history shows sometimes insiders can cause harm (intentionally or not). By creating, say, "Insider Agatha" who is well meaning but prone to bypassing rules. Make it clear this is hypothetical to improve security for everyone.

- **Use Personas in Discussion**: Once you have personas, you can use them in future steps. For example, when thinking about mitigations, you might ask "Would this stop Maria?" or "How would we detect Henrique's actions?". Personas help ground these discussions.

4.2.4 Step 4: Identify Threats Collaboratively

What Could Go Wrong?

4.2.4.1 Purpose

Brainstorm all the potential threats and bad things that could happen to the assets and processes you identified. The goal is a comprehensive list of threat scenarios, covering both technical attacks and governance risks. At this stage, quantity is more important than quality. We want to surface as many ideas as possible, without judging them yet. This step groups the different perspectives in your organization: digitally skilled members might think of hacking scenarios, whereas others might point out process failures or insider issues that a pure tech focus could miss.

4.2.4.2 Activities

- **Brainstorm in a Safe Environment**:

Gather a group of members, ideally representing different roles or viewpoints, for a threat brainstorming session. Set some ground rules: no idea is too small and everyone's input is valued. It's important people feel comfortable mentioning even unpleasant hypotheticals.

- **Introduce Creative Tools**: Present the classic Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE) (see section 3.1.1) structure as a checklist for generating questions adapted to horizontal dynamics: Can disputes arise over actions recorded in collaborative tools, allowing for rejection? Are there vulnerabilities that allow unauthorized escalation of privileges in shared administrative workflows?

  If there is time, extend this analysis with Security Cards (see section 3.2.2) to further explore adversarial motivations, methods, and impacts allowing all members to contribute.

- **Write Down Concrete Scenarios**: For each idea, capture it as a short scenario description. For example:

  - **Sybil Attack on decision making:** An attacker creates multiple fake member accounts to gain extra votes in an online poll, influencing the group decision illicitly.
  - **Insider data leak:** A discontented member with access to sensitive data decides to leak member emails and addresses to the public.
  - **Ransomware on shared drive:** Malware infects a member's computer and encrypts the shared cloud drive files, making them inaccessible until a ransom is paid.
  - **Lost credentials:** A member who manages the Twitter account leaves suddenly, and no one else has the password so the group loses control of its own social media.
  - **Miscoordination outage:** In a crisis, no one is designated to respond, because everyone thinks someone else will, and a small issue like a certificate expiry escalates, taking the website offline for days.
  - **Service provider failure:** The third party platform goes down or is compromised, affecting the organization's operations.

  Aim for a broad list, covering cyber attacks, human mistakes, physical events like the office gets robbed or a server gets wet, and governance failures. Don't worry at this stage if some scenarios seem very unlikely. List them as if someone is concerned about it.

- **Ensure Social/Process Threats are Included**: Cooperatives might face threats like quorum manipulation, abuse of emergency powers (someone invoking a crisis to

grab authority), or "digital vanguard" accumulation (one person quietly gaining control of many digital assets). Include these in your brainstorming. For example, "Member X holds all the keys and if they quit or go rogue, we're locked out" is a valid threat scenario to record (it's an internal risk).

4.2.5 Step 5: Analyze Attack Scenarios

How Could Attacks Happen?

4.2.5.1 Purpose

Now, use your list of threats and personas to explore in detail how attacks might happen step by step. This deeper analysis helps you understand exactly where your vulnerabilities are. By turning abstract threats into clear scenarios or stories, you can clearly see what needs to be defended against and how severe the consequences will be.

4.2.5.2 Activities

- **Build Attack Trees**: Choose a primary threat scenario, such as "unauthorized access to the member list." Place it at the root of your tree and explore the possible paths: an attacker could exploit software vulnerabilities to gain administrator access, or an attacker could misuse legitimate access, or someone could trick a member into sharing credentials. At each step, clearly identify what defenses already exist, whether they are effective, and what improvements are needed. Keep the tree clear and easy to understand.

- **Conduct Simulations**: Organize simulation exercises for more complex scenarios. Assign someone to represent the adversary, while others act as defenders or observers. For example, simulate a Sybil attack scenario: "Maria secretly created false identities before a vote and uses them to influence the results." Go through the steps, discussing whether current procedures would detect the attack. This exercise helps reveal weaknesses in a safe, low pressure environment rather than during an actual incident. This kind of storytelling helps highlight if your current processes have detection or not.

- **Identify Vulnerabilities at Each Step**: For each scenario, explicitly identify the weaknesses that make the attack possible including both technical issues like outdated software or no data backups and organizational issues as no membership verification or one person controls critical knowledge. Identify your current controls and assess whether they actually prevent the attack or if they can be circumvented. Clearly document these vulnerabilities for each scenario, which helps directly inform your mitigation efforts.

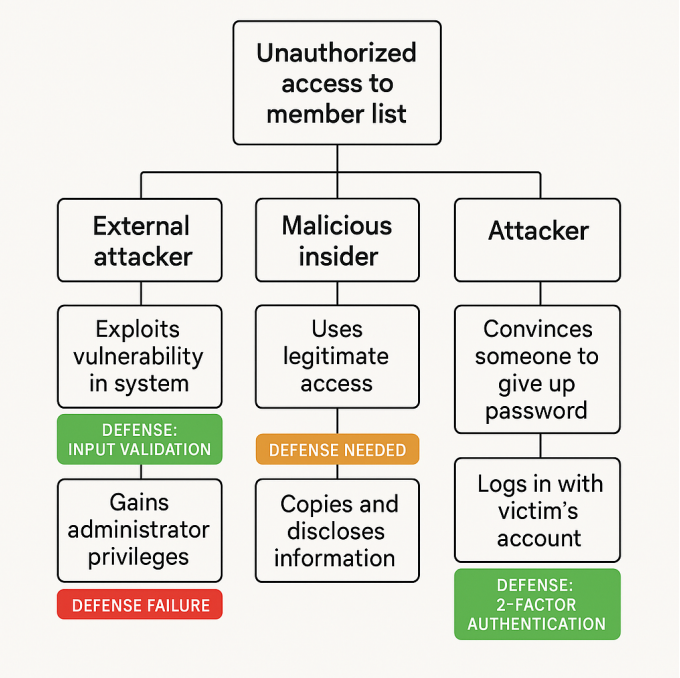

Figure 4.2: Attack Tree Example

- **Leverage Past Incidents**: Incorporate experiences from previous incidents or near misses to make scenarios more concrete. Ask questions like: Could this happen again, perhaps in a more damaging way? or We temporarily lost control of our Twitter account before, what if the attackers post harmful content next time? Using real world examples helps everyone to understand the severity of the threats and the importance of preventive measures.

4.2.6 Step 6: Prioritize Risks Together

Which Problems Matter Most?

4.2.6.1 Purpose

This step consists essentially of risk analysis and ranking. Risk is usually judged by two factors: how severe the impact would be and how likely the threat is to occur. By scoring or discussing these, the group can focus on the most critical issues. Importantly, this is done participatorily, everyone's perspective on what is important is considered, keeping the process democratic. The output will be a clear list of top risks that the organization will invest effort in mitigating.

4.2.6.2 Activities

- **Define Impact and Likelihood**: First, agree on clear definitions for impact and likelihood: high impact risks threaten the organization's survival, break laws, or

deeply harm member trust; medium impacts create noticeable but manageable problems; low impacts result in minor inconveniences. High likelihood means there's strong evidence a risk can easily happen, medium is conditional, and low likelihood means it's rare or requires sophisticated effort.

- **Evaluate Each Threat Scenario**: Review your scenarios from Step 3 to 5 one by one, asking two questions: If this happens, how bad is it? (Impact) and How likely is it? (Likelihood). Different perspectives matter, for example, tech members might know a threat is difficult to execute (low likelihood), while governance experts could emphasize the severe impact on trust.

- **Check Against Goals**: Revisit Step 1's initial assets and objectives. Ensure the prioritized risks align with your core mission and values. If important assets lack high ranked threats, double check if something was overlooked or truly low risk.

4.2.7 Step 7: Mitigations and Governance Decisions

How Do We Fix or Prevent Issues?

4.2.7.1 Purpose

For each of the top priority threats, figure out what security measures to implement and how to approve and enforce them democratically. This step is where you turn analysis into concrete changes: technical fixes, new or improved policies, training, etc. It is also where you make sure that implementing these fixes doesn't accidentally centralize power or violate cooperative principles.

4.2.7.2 Activities

- **Brainstorm Mitigation Options:** These might include technical solutions (software updates, two factor authentication, encryption), workflow improvements (clear onboarding/offboarding processes, regular backups, peer reviews for critical tasks), training and education (phishing awareness, password management sessions), and governance policies (emergency decision protocols, member identity verification). Discuss how difficult or costly they are, if external resources are required, if they introduce significant workflow friction, and if they align with organizational values.

- **Assign Responsibilities Clearly:** Define clear responsibilities for each mitigation task, distributing them among relevant members or working groups. Technical tasks should include tech skilled members paired with others for transparency. Assign policy drafting and educational roles to suitable teams or individuals.

- **Integrate into Governance Documents:** Codify agreed upon mitigations and emergency protocols into the organization's official documentation. Update handbooks

or wikis to institutionalize these practices, ensuring new members receive proper orientation.

4.2.8 Participation Tips

Successful threat modeling requires that everyone in the organization feels comfortable and motivated to contribute. In small groups, completing activities in a single meeting is effective, fostering unity and avoiding repeat sessions. For larger groups, use brief questionnaires or small group discussions, consolidating ideas later in plenary to ensure that everyone can contribute.

It is important that members with technical expertise do not dominate the conversation. Encourage more reserved participants by asking them directly for their opinions on specific threats or solutions.

Keep a relaxed and creative environment when role playing scenarios or developing adversarial personas and document decisions transparently, explaining the reasons clearly, allowing for future review and improvements.

This chapter has presented the core contribution of this research: a threat modeling protocol designed from the ground up for horizontal organizations. It is not merely a set of instructions, but a process rooted in the core principles of horizontality: transparency, decentralization, and democratic participation. Through a series of collaborative steps, the protocol guides organizations on a journey from defining what is most valuable to them, to humanizing their adversaries through personas, and finally to developing mitigations that are not just technically sound, but democratically legitimate. It is designed to be a tangible tool, translating abstract security concepts into an accessible, collective practice. In essence, the protocol provides a pathway for horizontal organizations to take ownership of their security in a way that strengthens, rather than subverts, their fundamental values.

5

Evaluation

To validate the effectiveness, usability, and unique contributions of the threat modeling protocol developed in this research (see Chapter 4), a structured evaluation with the objective to empirically assess whether the protocol achieves better results in identifying a broader range of threats relevant to non-hierarchical organizations compared to Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE).

The evaluation is structured around a real world workshop and uses a combination of quantitative output metrics to provide a holistic assessment.

5.1 Experimental Design

The evaluation will be conducted as a two session workshop with members of multiple horizontal organizations. To ensure a fair comparison, the experiment will alternate the order of methodologies between sessions. Participants will be randomly divided into two groups, one for each session.

If there are not enough people to fill two groups, the same group will use both methodologies in different sessions. In this case, the order of methodologies will be randomized within different organizations to avoid bias.

5.2 Evaluation Metrics

The outputs from the sessions using the proposed protocol and STRIDE will be compared using a set of objective metrics.

5.2.1 Threat Volume and Diversity

This metric assesses the breadth and scope of the threats identified by each methodology. The goal is to determine if the proposed protocol successfully guides participants to consider risks beyond the purely technical domain.

- **Measurement:** After each session, the complete list of unique threats will be categorized. A predefined set of categories will be used for consistency:

  - **Technical:** Threats related to software flaws, network vulnerabilities, data breaches, or malware.
  - **Governance/Process:** Threats related to decision making failures, loss of critical credentials due to poor process, single points of human failure, or flawed onboarding/offboarding.
  - **Social/Human:** Threats originating from human actors, such as malicious insiders, social engineering, member conflict impacting operations, or unintentional errors.
  - **Third Party:** Threats originating from the failure or compromise of an external service provider.

- **Analysis:** The total number of threats in each category will be counted and compared for both methodologies. It is hypothesized that STRIDE will produce a high volume of threats in the "Technical" category, whereas the proposed protocol will show a more balanced distribution across all categories, particularly highlighting "Governance/Process" and "Social/Human" threats.

5.2.2 Relevance to Critical Assets

This dimension evaluates whether the identified threats are significant and pertinent to the organization, moving the focus from quantity to severity. Using the list of critical assets defined in Step 1 of the protocol, we will count the number of these assets that have at least one valid threat identified against them by each method. This metric measures how well each methodology focused the discussion on what the organization explicitly defined as most valuable.

5.2.3 Actionability of Outcomes

An effective threat modeling process must lead to concrete, implementable security improvements. This metric quantifies the practical value of the mitigations proposed.

We will count the number of proposed mitigations from each session that are specific, measurable, and assignable. An actionable mitigation is one that can be converted directly into a task (e.g., "Enable two factor authentication for all member accounts") rather than a vague goal (e.g., "Improve login security"). This metric provides a direct measure of the protocol's ability to translate analysis into action.

5.3 Participant Experience and Usability

Given that the proposed protocol is designed for democratic and inclusive participation, the subjective experience of the users is a primary criteria for success.

We will evaluate the experience through careful observation during the workshops. We will watch for specific things like who is speaking? Is it only the members with technical skills, or is everyone contributing ideas? Do people seem interested and focused? Are they building on each other's ideas?

At the end of each session, we will have a short, informal conversation. We will ask what felt useful, what was difficult, and how the process could be better. This direct feedback is more valuable than numbers on a scale. It helps us see if the protocol truly serves the collective.

5.3.1 Ethics and Protection of Organizations

A principle of this study is the protection and confidentiality of the organizations that agree to participate. The workshops involves the disclosure of sensitive information, including existing vulnerabilities, internal processes, and strategic challenges, creating a significant responsibility to safeguard this data from any potential harm.

To honor this responsibility, a strict ethical framework was followed. All information gathered during the evaluation is treated with confidentiality. Any specific findings, examples, or details about the participating organizations are included in this thesis only after receiving their explicit and informed authorization. This ensures that the collaboration and the data shared are used responsibly and do not expose the organizations to risk.

5.4 Results

The proposed protocol was evaluated in practical workshops with two non-hierarchical organizations: ComuniDária, a non-profit immigrant association, and Frente Anti-Racista, a political activist collective. Each organization participated in two separate sessions, one using the proposed protocol and another using the traditional STRIDE methodology. The following sections present the results of these workshops, analyzed according to the evaluation metrics defined in section 5.2.

5.4.1 Threat Volume and Diversity

As we hypothesized in the evaluation design, the results show a big difference in the types of threats identified by each methodology. The numbers themselves tell a story. In total, the proposed protocol found more threats across the two workshops—16 in total, compared to the 11 found by STRIDE.

Table 5.1: Quantitative Comparison of Threat Modeling Methodologies

Evaluation Metric	STRIDE	Proposed Protocol
Threat Volume		
Total Threats Identified	11	16
Threat Diversity (% of Total Threats)		
Technical	45% (5 threats)	31.25% (5 threats)
Governance/Process	0% (0 threats)	18% (3 threats)
Social/Human	36% (4 threats)	37% (6 threats)
Third Party	18% (2 threats)	12% (2 threats)
Actionability of Outcomes		
Total Actionable Mitigations Proposed	2	12

The STRIDE sessions, for both ComuniDária and Frente Anti-Racista, gave us a list of threats that were very technical or about external things. We saw things like "Phishing", "lack of backup", and "mobile device security failure". Important, yes. But these are problems any organization could have. And most critically, across both workshops, STRIDE identified exactly zero threats in the Governance/Process category. It is a blind spot.

Then we look at our protocol. The picture is completely different. The distribution of threats is much more balanced. For Frente Anti-Racista, it uncovered critical governance threats like "a person pretending to be a member to vote in an assembly" and the risk of "not complying with bureaucracy and losing state funding." For ComuniDária, it found the risk of "misconduct for personal gain." These are the deep, internal, structural risks that can really damage a non-hierarchical group. These are threats STRIDE cannot see.

Also, our protocol found more Social/Human threats (6 versus 4), and they were more specific to the context of these organizations. Not just a generic "user error," but the very real danger of "a new member joining just to infiltrate and leak information." This shows that the protocol guides the conversation to the risks that are most real and dangerous for these specific groups, moving beyond the purely technical view into the socio-technical reality of their work.

5.4.2 Relevance to Critical Assets

Beyond just the number of threats, it is the quality and relevance that showed the biggest difference. A threat modeling process must protect what is most important.

Our protocol's process starts by asking a simple question: What are your critical assets? And the groups did not just list technical things. ComuniDária identified intangibles like credibility (reputation) and member trust. Frente Anti-Racista listed their operationality of the nucleo and the very safety of their members.

Because of this, the threats we found were naturally tied to these assets. It is simple logic. When Frente Anti-Racista prioritized an extremist physically attacking a member using leaked data or an infiltrator leaking internal communications, these are direct attacks on their most valued assets. They are existential threats.

The STRIDE methodology is different. Its asset model is the system's data flow diagram. So it finds threats against a process, like the flow of information in a messaging app, but not explicitly against the assets the organization itself said were most valuable. While it identified important technical weaknesses, the priorities were different, like potential for data interception on WhatsApp. This is important, yes, but it does not capture the same level of organizational risk. It is a technical vulnerability, not a threat to the soul of the organization.

This created a disconnect. STRIDE was looking at the machine, but our protocol was looking at the mission. And for these groups, that is where the real risk lives.

5.4.3 Actionability of Outcomes

A threat modeling process must lead to action. Real change. Without this, it is only talk. The workshops showed a very clear difference here.

The proposed protocol guided the organizations to create their own internal, process-based mitigations. These are solutions they can build themselves. For example, in response to the "infiltrator" threat, Frente Anti-Racista did not propose a new software; they proposed to create "a screening process for new members." This is not a technical fix. It is a change in their collective governance. ComuniDária proposed to "register which member has access to each page or file." These are actions they can take, together, to make themselves stronger from the inside. They are empowered.

The mitigations from the STRIDE sessions were different. Across both organizations, the number of actionable mitigations proposed was zero. Nothing. But even if there were mitigations, the threats STRIDE found point to a different kind of solution. The threats were technical, so the fixes would be technical—"enable two-factor authentication"—or they would point to a dependency on others. On a big company. "Depender da segurança da Google" (to depend on Google's security). This suggests the proposed protocol is much more effective at helping organizations improve their security through changes in their own collective processes, which is a core goal for non-hierarchical structures. It gives them the power.

5.4.4 Participant Experience and Usability

The evaluation of the participant experience was not done with surveys, but through direct observation of the workshops.

A clear challenge emerged, and it was common to both methodologies: the initial step of creating a visual map of the system. Whether it was the formal Diagrama de Fluxo de Dados (DFD) for STRIDE or the system and trust map in our protocol, this was the most difficult part for the participants. It is an abstract exercise, and it requires a kind of thinking that can be a barrier before the real discussion begins.

But it is what happened after this step that the difference became profound. During the STRIDE sessions, the conversation became the property of the few members with

more technical knowledge. The vocabulary of STRIDE—spoofing, tampering, repudiation—created a wall. Many participants became quiet observers.

With the proposed protocol, this wall did not exist. The change was immediate. The room came alive with discussion. Both ComuniDária and Frente Anti-Racista interacted much, much more. The reason is simple. Our protocol speaks a human language. When the discussion is about creating a persona for "the malicious insider" or protecting an asset like "reputation," everyone is an expert. It is not a technical debate anymore; it is a collective conversation about their own organization.

This chapter detailed the structured evaluation conducted to validate the proposed threat modeling protocol. Through comparative workshops with two non-hierarchical organizations, the protocol was tested against the standard STRIDE methodology. Across all metrics the proposed protocol demonstrated a clear superiority for this context. It did not just find more threats, it surfaced the right threats. The governance and social vulnerabilities that STRIDE is blind to. Furthermore, the evaluation confirmed a significantly more inclusive and empowering experience for the participants, transforming a technical exercise into a collective, strategic conversation.

6

Conclusion

6.1 Summary of Findings

This research examined an important gap in cybersecurity: the absence of threat modeling methodologies made to the distinct socio technical challenges of non-hierarchical organizations. In response, we proposed a participatory context driven protocol designed explicitly to align with the core principles of democratic governance, decentralization, and transparency. It was a new construction made from tools and practices that share the commitment to inclusivity and collaboration.

The effectiveness of the protocol was not merely theorized but validated through a series of comparative workshops engaging two distinct organizations. The results confirmed a clear superiority when compared to the industry standard STRIDE methodology. Our protocol enabled participants to identify a broader and more relevant range of threats. Most notably those rooted in social, governance, and political domains where traditional approaches demonstrated a significant blindness.

Furthermore, the investigation revealed that the protocol did not just produce a longer list of risks. It fundamentally guided organizations toward the development of actionable, internal mitigations. These were solutions that reinforced their horizontal principles, effectively empowering the collectives to strengthen their security from within.

6.2 Discussion and Implications

The findings of this study have significant implications for cybersecurity theory and its practice. Theoretically, they present a direct challenge to the presumed universality of conventional threat modeling frameworks. Such established methods operate on the presupposition of a command chain that, in these contexts is simply not there, causing them to fail when faced with the realities of decentralized collectives. Security is not, and cannot be, a one size fits all discipline; it must be a reflection of the organizational structure and the specific values it aims to protect. This work makes clear that for non-hierarchical organizations, horizontality is not a vulnerability to be mitigated but an essential design

principle for building any meaningful security.

Practically, this thesis delivers something tangible. A protocol that can be immediately adopted by cooperatives, activist collectives, and other groups. It answers a real need by translating the often blurred concepts of security into a accessible process, the protocol empowers members even those without any specialized expertise to take ownership of their digital protection. This is not a tool to be imposed by an outside expert, but a framework to be inhabited and shaped by the collective itself, and this distinction is crucial for bypassing the common danger of creating a "digital vanguard" where technical knowledge becomes a new, unelected form of centralized power.

This enables a truly democratic security practice. It's importance goes far beyond the technical domain. For any organization that is founded on deep principles of equity and shared power, the act of employing an authoritarian, top-down security model introduces a profound contradiction between its values and its necessary practices. Our protocol offers a pathway. A way to build resilience that is congruent with their core beliefs in democratic participation and shared responsibility, ensuring that the very methods used to protect the organization do not, in the end, corrupt its soul.

6.3 Limitations of the Research

Despite the encouraging outcomes this study had several clear limitations. First, the evaluation was conducted with only two organizations since the disponibility of members from these organizations was limited. While they represented different sectors from community service and activism, the findings may not possess universal generalizability to all forms of non-hierarchical organizations, such as large-scale worker cooperatives. The specific contexts are different. The pressures are different.

Second, the evaluation consisted of single session workshops. These provided a valuable snapshot in time but could not capture the long term dynamics of security practice and efficacy of the protocol. Whether the proposed mitigations are successfully implemented, maintained, and adapted over time was consequently not assessed. This remains an open question.

A third limitation arises from the modest size of the workshop groups. The protocol is designed to leverage the power of broad participation and diverse viewpoints; it is conceivable that with a larger, more varied set of participants, the deliberative process would have yielded even richer outcomes and uncovered subtler, more complex threats.

Finally, as the primary researcher facilitated all workshop sessions, an element of facilitator bias may have influenced the discussions and outcomes, despite conscious efforts to maintain neutrality. The hand that guides the process inevitably leaves a faint impression upon the result.

6.4 Future Work

The limitations of this study do not close a door; instead, they point toward several compelling paths for future inquiry.

The most crucial next step is to observe the protocol's effects over a much longer stretch of time. A study that follows a group of organizations not for a single session, but through seasons of change, for a year or more. This would be crucial. Only then could we see if the new practices truly take root and survive the pressures of real-world operation. That is the ultimate test of its worth.

We must also take this protocol into new environments. Testing it across a large worker cooperatives, would challenge its assumptions in necessary ways. It would reveal its breaking points. Every new context is a chance to learn, to harden the protocol, to make it better.

Furthermore, a clear opportunity exists to build a 'playbook' or a digital toolkit. A guide to accompany the process. This would reduce the influence of any single facilitator and make the work radically more accessible, empowering groups to take this process into their own hands, on their own terms.

Finally, future work could explore a hybrid construction, one that carefully integrates the narrative, human-centered strengths of this process with the systematic technical sharpness of older frameworks. This might be an optional 'deep dive' module. A special addition for organizations needing a greater level of technical detail, creating a tool that is both simple at its core and profound in its potential depth.

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. 1, 2, 7, 18–21).

[2] C. W. Blackwell. "Athenian Democracy: An Overview". In: *Dēmos: Classical Athenian Democracy*. Ed. by 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. 2, 9).

[3] J. Cleland-Huang. "How Well Do You Know Your Personae Non Gratae?" In: *IEEE Software* 31.4 (2014), pp. 28–31. DOI: 10.1109/MS.2014.85 (cit. on p. 16).

[4] J. Cleland-Huang et al. "Keeping Ahead of Our Adversaries". In: *IEEE Software* 33.3 (2016), pp. 24–28. DOI: 10.1109/MS.2016.75 (cit. on p. 16).

[5] N. Couldry and U. A. Mejias. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford, California: Stanford University Press, 2019. ISBN: 9781503609754. URL: https://lccn.loc.gov/2019010213 (cit. on p. 10).

[6] T. Denning, B. Friedman, and T. Kohno. *The Security Cards: A Security Threat Brainstorming Toolkit*. Accessed: 2024-12-09. 2013. URL: http://securitycards.cs.washington.edu/assets/security-cards-information-sheet.pdf (cit. on pp. 1, 15, 16).

[7] J. R. Douceur. "The Sybil Attack". In: *Peer-to-Peer Systems*. Ed. by P. Druschel, F. Kaashoek, and A. Rowstron. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 251–260. ISBN: 978-3-540-45748-0 (cit. on p. 1).

[8] *Estatutos da Confederação Geral dos Trabalhadores Portugueses – Intersindical Nacional: Declaração de Princípios e Objectivos Programáticos*. Accessed: 2024-12-08. Confederação Geral dos Trabalhadores Portugueses (CGTP), 2020. URL: https://www.cgtp.pt/images/images/2020/02/ESTATUTOSCGTP.pdf (cit. on p. 10).

[9] 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. 1–3, 6–11, 15, 17, 18, 20, 21).

[10] 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. 1, 9).

[11] 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. 2, 4, 7, 8).

[12] S. Hernan et al. *Uncover Security Design Flaws Using The STRIDE Approach*. Accessed: 2024-Dec-09. 2006-11. URL: https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach (cit. on pp. 12, 13).

[13] M. Howard and S. Lipner. *The Security Development Lifecycle: SDL, a Process for Developing Demonstrably More Secure Software*. Secure software development series. Microsoft Press, 2006. ISBN: 978-07356-2214-2 (cit. on p. 13).

[14] 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).

[15] 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. 2, 4, 7, 8).

[16] R. Jiang, J. Luo, and X. Wang. "An Attack Tree Based Risk Assessment for Location Privacy in Wireless Sensor Networks". In: *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*. 2012, pp. 1–4. DOI: 10.1109/WiCOM.2012.6478402 (cit. on p. 14).

[17] R. Jiang et al. "Energy-theft detection issues for advanced metering infrastructure in smart grid". In: *Tsinghua Science and Technology* 19.2 (2014), pp. 105–120. DOI: 10.1109/TST.2014.6787363 (cit. on pp. 2, 14).

[18] 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. 4).

[19] A. Kavada and T. Poell. "From Counterpublics to Contentious Publicness: Tracing the Temporal, Spatial, and Material Articulations of Popular Protest Through Social Media". In: *Communication Theory* 31.2 (2020-10), pp. 190–208. ISSN: 1050-3293. DOI: 10.1093/ct/qtaa025. eprint: https://academic.oup.com/ct/article-pdf/31/2/190/37900340/qtaa025.pdf. URL: https://doi.org/10.1093/ct/qtaa025 (cit. on p. 1).

[20] R. Khan et al. "STRIDE-based threat modeling for cyber-physical systems". In: *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. 2017, pp. 1–6. DOI: 10.1109/ISGTEurope.2017.8260283 (cit. on pp. 7, 13, 20).

[21] 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).

[22] D. LeBlanc. *DREADful*. Accessed: 2024-Dec-09. 2007-08. URL: https://learn.microsoft.com/en-us/archive/blogs/david_leblanc/dreadful (cit. on p. 13).

[23] E. Marasco et al. "Attack Trees for Protecting Biometric Systems Against Evolving Presentation Attacks". In: *16th Annual IEEE International Conference on Technologies for Homeland Security (HST) 2017*. 2017 (cit. on p. 16).

[24] S. Mauw and M. Oostdijk. "Foundations of Attack Trees". In: *Information Security and Cryptology - ICISC 2005*. Ed. by D. H. Won and S. Kim. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 186–198. ISBN: 978-3-540-33355-5 (cit. on p. 14).

[25] N. Mead and F. Shull. *The Hybrid Threat Modeling Method*. Carnegie Mellon University, Software Engineering Institute's Insights (blog). Accessed: 2025-Feb-11. 2018-04. URL: https://insights.sei.cmu.edu/blog/the-hybrid-threat-modeling-method/ (cit. on pp. 6, 17).

[26] N. Mead et al. "Crowd Sourcing the Creation of Personae Non Gratae for Requirements-Phase Threat Modeling". In: *2017 IEEE 25th International Requirements Engineering Conference (RE)*. 2017, pp. 412–417. DOI: 10.1109/RE.2017.63 (cit. on pp. 16, 17).

[27] E. Morozov. *Big Tech: A Ascensão dos Dados e a Morte da Política*. Ed. by R. Lemos. São Paulo: Ubu Editora, 2018. ISBN: 978-85-7126-012-2 (cit. on pp. 8, 9).

[28] S. Myagmar, A. J. Lee, and W. Yurcik. "Threat modeling as a basis for security requirements". In: (2005) (cit. on p. 6).

[29] P. Nancy R. Mead. *Advanced Threat Modeling (ATM)*. Tech. rep. Pittsburgh, PA 15213: Software Engineering Institute, Carnegie Mellon University, 2017. URL: https://apps.dtic.mil/sti/trecms/pdf/AD1089727.pdf (cit. on p. 6).

[30] P. Zimmermann. *PGP User's Guide, Volume I: Essential Topics*. Revised Edition. PGP Version 2.6.2. Massachusetts Institute of Technology: Phil's Pretty Good Software, 1994. URL: https://web.pa.msu.edu/reference/pgpdoc1.html (cit. on pp. 19, 20).

[31] P. C. Português. *Programa e Estatutos do PCP*. Revisão tipográfica: Edições «Avante!». Lisboa, Portugal, 2013. URL: https://www.pcp.pt/estatutos-do-pcp (cit. on p. 10).

[32] B. Potteiger, G. Martins, and X. Koutsoukos. "Software and attack centric integrated threat modeling for quantitative risk assessment". In: *Proceedings of the Symposium and Bootcamp on the Science of Security*. HotSos '16. Pittsburgh, Pennsylvania: Association for Computing Machinery, 2016, pp. 99–108. ISBN: 9781450342773. DOI: 10.1145/2898375.2898390. URL: https://doi.org/10.1145/2898375.2898390 (cit. on p. 13).

[33] 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).

[34] R. Scandariato, K. Wuyts, and W. Joosen. "A Descriptive Study of Microsoft's Threat Modeling Technique". In: *Requirements Engineering* 20.2 (2015-06), pp. 163–180. ISSN: 1432-010X. DOI: 10.1007/s00766-013-0195-2. URL: https://doi.org/10.1007/s00766-013-0195-2 (cit. on pp. 1, 7, 8, 12).

[35] B. Schneier. *Attack Trees*. Tech. rep. 12. 1999. URL: https://tnlandforms.us/cs594-cns96/attacktrees.pdf (cit. on pp. 1, 7, 14).

[36] 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. 1, 2, 6–8).

[37] A. Shostack. "Experiences Threat Modeling at Microsoft". In: *MODSEC@ MoDELS* (2008) (cit. on p. 6).

[38] A. Shostack. *Threat Modeling: Designing for Security*. Available in print and electronic formats. Indianapolis, Indiana: John Wiley & Sons, Inc., 2014. ISBN: 978-1-118-80999-0 (cit. on pp. 1, 3, 4, 6, 7, 12–14, 20).

[39] F. Shull and N. Mead. *Cyber Threat Modeling: An Evaluation of Three Methods*. Carnegie Mellon University, Software Engineering Institute's Insights (blog). Accessed: 2024-Dec-9. 2016-11. URL: https://insights.sei.cmu.edu/blog/cyber-threat-modeling-an-evaluation-of-three-methods/ (cit. on p. 16).

[40] F. Shull et al. *Evaluation of Threat Modeling Methodologies*. Tech. rep. Carnegie Mellon University, Software Engineering Institute, 2016-10. URL: https://insights.sei.cmu.edu/documents/4027/2016_017_001_474200.pdf (cit. on pp. 1, 7, 20).

[41] S. A. da Silveira. *Democracia e os códigos invisíveis: como os algoritmos estão modulando comportamentos e escolhas políticas*. São Paulo: Edições Sesc São Paulo, 2019. ISBN: 978-85-9493-180-1 (cit. on pp. 3, 9).

[42] M. A. Sitrin. *Everyday Revolutions: Horizontalism and Autonomy in Argentina*. London, UK; New York, USA: Zed Books Ltd, 2012. ISBN: 9781780320502 (cit. on pp. 2–4, 8, 9, 18, 20).

[43] 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. 3, 6, 7, 15–17).

[44] P. M. Thornton. "Of Constitutions, Campaigns and Commissions: A Century of Democratic Centralism under the CCP". In: *The China Quarterly* 248.S1 (2021), pp. 52–72. DOI: 10.1017/S0305741021000758 (cit. on p. 10).

[45] P. Torr. "Demystifying the threat modeling process". In: 3.5 (2005), pp. 66–70. DOI: 10.1109/MSP.2005.119 (cit. on pp. 1, 6, 7).

[46] Z. Trifa and M. Khemakhem. "Sybil Nodes as a Mitigation Strategy Against Sybil Attack". In: *Procedia Computer Science* 32 (2014). The 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), the 4th International Conference on Sustainable Energy Information Technology (SEIT-2014), pp. 1135–1140. ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2014.05.544. URL: https://www.sciencedirect.com/science/article/pii/S1877050914007443 (cit. on pp. 1, 3).

[47] T. UcedaVelez and M. M. Morana. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. John Wiley & Sons, 2015-05, p. 696. ISBN: 978-0-470-50096-5 (cit. on pp. 1, 14, 15, 20).

[48] 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. 7, 17).

[49] 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. 3, 8–10).

[50] C. Wright. *Worker Cooperatives and Revolution: History and Possibilities in the United States*. Bradenton, Florida, USA: BookLocker.com, Inc., 2014. ISBN: 978-1-63263-432-0 (cit. on pp. 2, 8, 9).

[51] 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, 8, 14, 15, 20).

[52] 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).

I

Workshop results

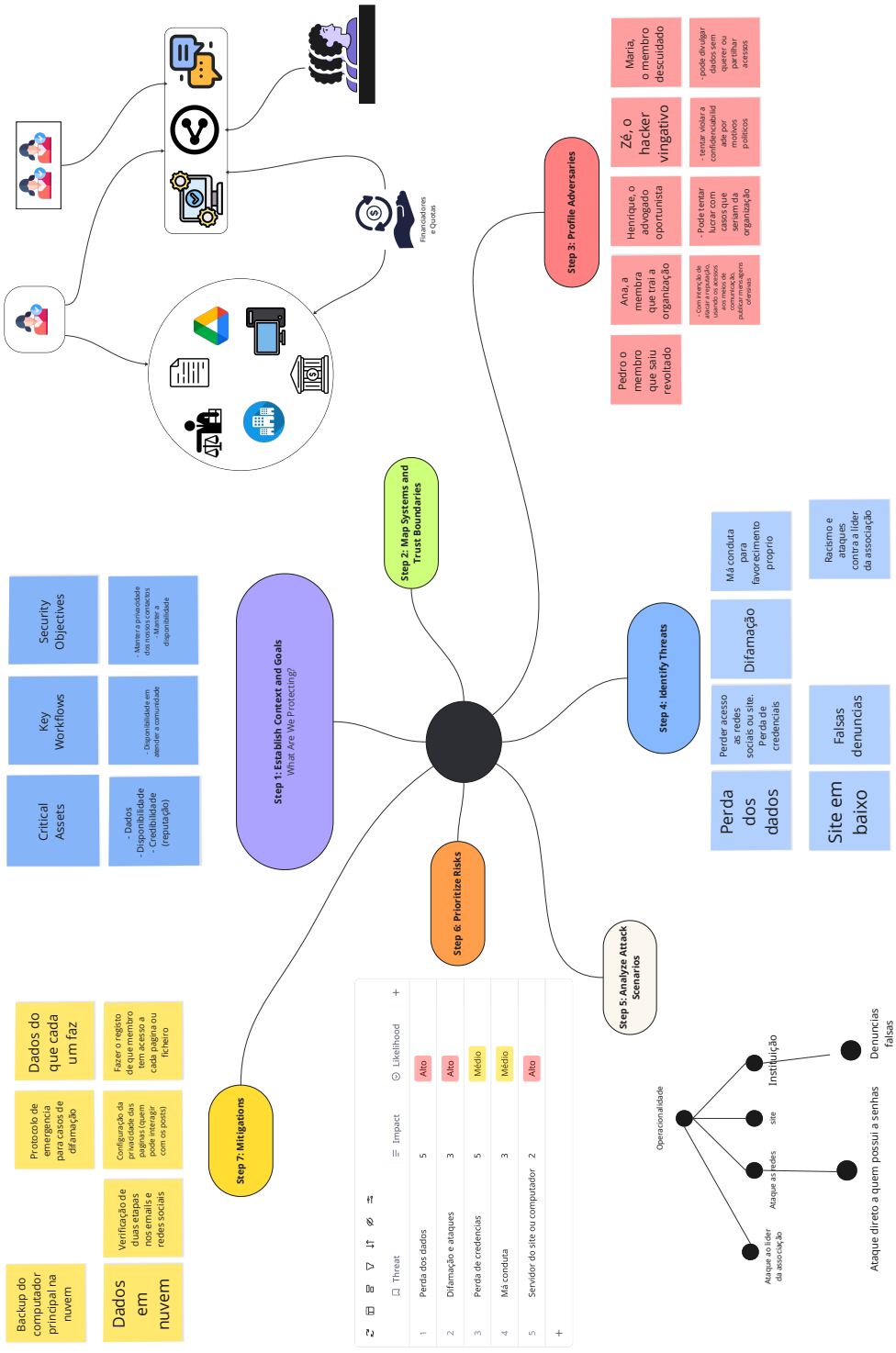

Figure I.1: Proposed protocol result from the first workshop.

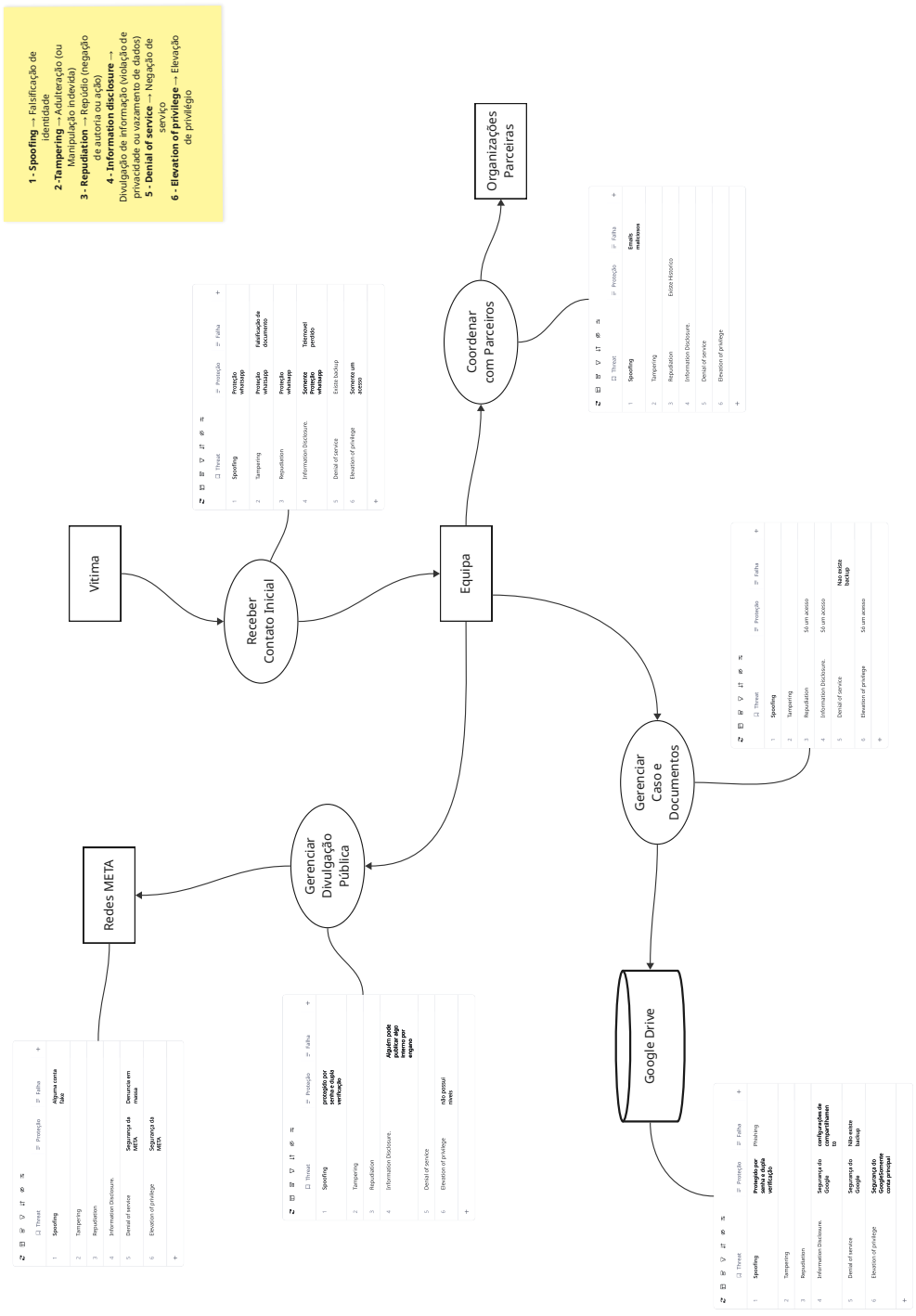

Figure I.2: STRIDE result from the first workshop.

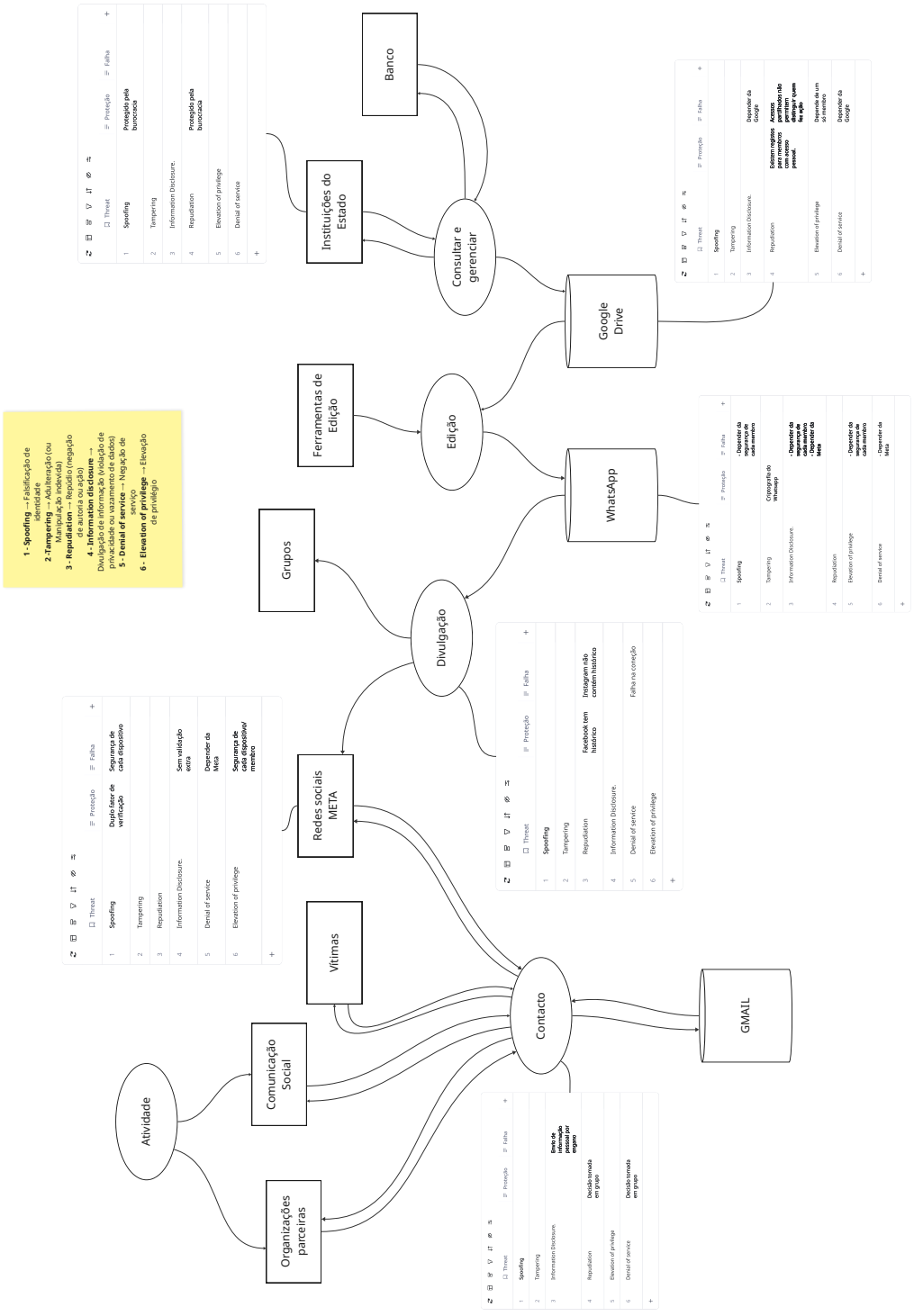

Figure I.3: STRIDE result from the second workshop.

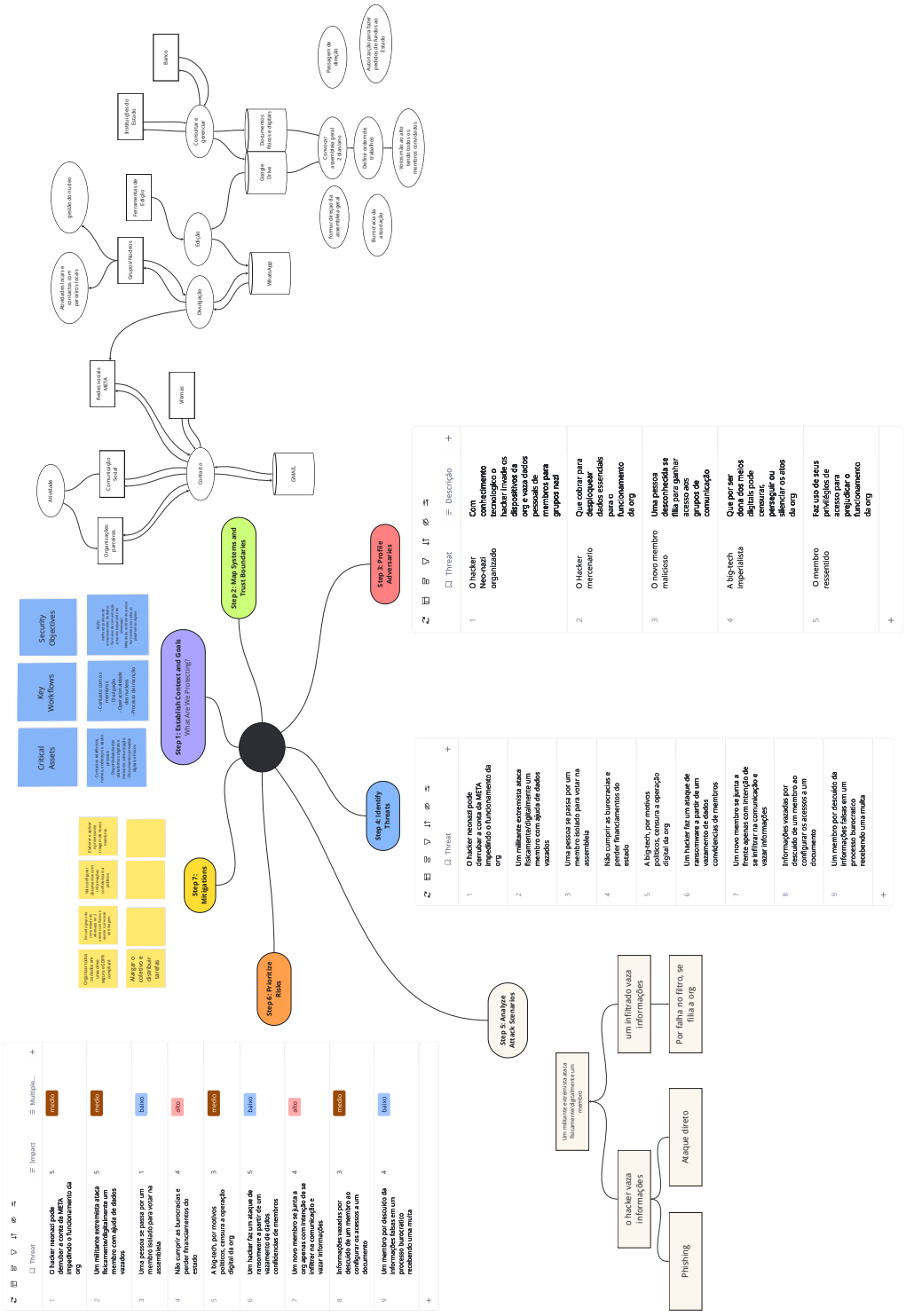

Figure I.4: Proposed protocol result from the second workshop.