Journal on Interactive Systems, 2025, 16:1, doi: 10.5753/jis.2025.5610

Evaluating privacy threats in deployed OSNs: A case study on PTMOL

Andrey Rodrigues [**Federal University of Amazonas** | ***andrey.rodrigues@ufam.edu.br***]
Maria Lúcia Villela [**Federal University of Viçosa** | ***maria.villela@ufv.br***]
Eduardo Feitosa [**Federal University of Amazonas** | ***efeitosa@icomp.ufam.edu.br***]

Institute of Exact and Technological Sciences, Federal University of Amazonas, Av. Nossa Senhora do Rosário, 3863, Tiradentes, Itacoatiara, AM, 69103-128, Brazil.

Received: 25 February 2025 • **Accepted:** 01 October 2025 • **Published:** 15 October 2025

Abstract: *Background:* The growth of Online Social Networks (OSNs) has significantly expanded opportunities for interaction and information sharing, while also introducing increasing challenges to user privacy protection. The exposure of sensitive data and the misuse of shared information on these platforms highlight the need for effective methodologies to identify and mitigate privacy threats. *Purpose and Methods:* In this context, this study investigates the application of the PTMOL methodology to identify and describe privacy threats in already deployed OSNs, aiming to demonstrate its versatility in threat modeling. *Results:* The results indicate that PTMOL is well-suited for structuring the identification of privacy threats, providing a detailed view of the vulnerabilities present in the analyzed platform. The comparison between modeled threats and documented incidents further reinforces PTMOL's ability to anticipate real-world risks. *Conclusion:* As a contribution, this study validates PTMOL's applicability as a valuable approach for assessing threats in deployed OSNs, extending its use beyond the design phase. The impact of this research extends to strengthening privacy protection strategies and assisting researchers, developers, and policymakers in adopting more effective measures to ensure safer and more transparent digital environments.

Keywords: Online Social Networks, Privacy Threats, Threat Modeling, Case Study

1 Introduction

Online Social Networks (OSNs) have become one of the most significant technological phenomena of the Web, redefining how people connect, communicate, and share information [Singh *et al*., 2024]. These platforms are designed to facilitate the creation and dissemination of user-generated content, fostering social interactions in a digital environment. Additionally, they enable individuals to build networks of connections, express opinions, share photos and videos, engage with third-party content, and participate in virtual communities. With their dynamic and collaborative nature, OSNs have established themselves as an essential element of modern communication, influencing various aspects of society, including business, education, and politics [Sathya and Prabhavathi, 2024].

The popularity of OSNs is evident in the growing number of users worldwide, who interact with these platforms daily for entertainment, information, and socialization. The ease of access and interactivity of these platforms encourage the sharing of personal information, often without proper consideration of the associated risks. Consequently, privacy threats have emerged as a critical concern, compromising the security of user data [Jain *et al*., 2021; Alkhamees *et al*., 2021]. A privacy threat is a potential or actual undesirable event that can lead to the disclosure, exposure, or misuse of a user's private data [Rodrigues *et al*., 2023]. The consequences of these threats range from minor inconveniences, such as receiving unwanted targeted advertisements, to severe impacts, including identity theft, financial fraud, and online harassment.

The collection and processing of data through OSNs are not always transparent or controllable by users. Typically, by agreeing to a platform's terms of service, users grant providers permission to store, analyze, and, in some cases, sell their personal information to third parties, primarily for advertising and marketing purposes [Infante and Mardikaningsih, 2022]. Furthermore, service providers maintain control over the databases where this information is stored, increasing the risk of data leaks and unauthorized access. As a result, users become potential targets for attackers seeking to exploit their data for illicit activities [Jain *et al*., 2021]. Attackers can obtain sensitive information, such as users' identities and locations, facilitating crimes like identity theft, financial fraud, and cyberstalking.

With the increasing number of privacy threats arising from personal data sharing on OSNs, various approaches have been proposed to mitigate risks and enhance user security. Among them, PTMOL stands out as a language specifically designed for modeling privacy threats in OSNs [Rodrigues *et al*., 2023]. PTMOL provides a structured framework for identifying and anticipating potential threats. Unlike traditional methods, it focuses exclusively on privacy-related risks, offering a detailed understanding of how user data may be exploited by malicious actors.

In this context, this study explores the following research question: Can PTMOL effectively identify and describe privacy threats in a manner consistent with real incidents on existing social networking platforms? This investigation is crucial for evaluating PTMOL's utility in threat modeling and its applicability to analyzing deployed OSNs.

Thus, this study aims to evaluate PTMOL as a tool for identifying and analyzing privacy threats in deployed OSNs, showcasing its versatility in threat modeling. To this end, a case study was conducted, applying PTMOL to an OSN to assess the alignment between the modeling results and real-world privacy issues. The findings indicate that PTMOL effectively identified documented threats, reinforcing its validity as a privacy evaluation approach for OSNs.

This paper extends the original work by presenting a detailed practical application of the PTMOL methodology in a real case study focused on analyzing privacy threats in already implemented online social networks. Unlike the prior papers, this study explores the methodology's versatility through modeling in a real-world context, comparing the results with documented incidents and validating its effectiveness as a practical assessment tool. It also deepens the discussion regarding the experts' experience and the limitations identified.

The study contributes to a deeper understanding of privacy in digital interactions and addresses a pressing contemporary issue: privacy threats in social media, providing valuable insights for both researchers and practitioners in the field of interactive systems. It advances the understanding of privacy threat modeling in social platforms by providing empirical evidence of PTMOL's applicability. Moreover, its findings can help developers and service providers enhance user privacy protection by integrating PTMOL for threat detection and evaluation.

The remainder of this paper is structured as follows: Section 2 presents the fundamental concepts. Section 3 details the PTMOL methodology. Section 4 presents the case study conducted. Section 5 discusses the study's findings and contributions. Finally, Section 6 presents the conclusions and suggestions for future research.

2 Background

The increasing use of OSNs has given rise to a large volume of user-generated content, most of which is free and publicly available. A significant portion of this content includes personal information, whose online exposure can pose serious risks to user privacy. To better understand privacy threats in OSNs, three key questions must be addressed: What is privacy? What constitutes a privacy threat? And what defines a privacy breach? This section explores these concepts, as they are fundamental to the context of this study..

2.1 Privacy

According to Altman's privacy regulation theory Altman [1975], privacy is defined as an individual's ability to control what information is disclosed, to whom, when, and under what circumstances. In this framework, privacy is viewed as a boundary regulation process, where individuals manage the extent to which their personal information is shared with others. Thus, privacy encompasses an individual's right to control their personal data, including how it is collected, transferred, stored, and used.

2.2 Privacy Threat

A privacy threat is a potential or real undesirable event that can cause harm to user in the form of disclosure, exposure, and manipulation of data [Joyee De and Imine, 2019; Laorden *et al*., 2010]. Threats can occur in applications that are not necessarily malicious, but that collect or store more personal information than necessary. Privacy threats can arise from inside or outside the system, from network users themselves, or from malicious users who disguise themselves as legitimate system users or find ways to circumvent privacy controls.

In systems like OSNs, sharing personal data can be a desirable focus for attackers (malicious agents). Location disclosure, for example, can result in tracking threats, which seek to analyze users' general behavior [Singh *et al*., 2024]. Furthermore, through location data, an attacker can also collect information to gain clues about various types of private user data, such as lifestyle, time and purpose of movements in different locations.

2.3 Privacy Breach

A privacy breach occurs when private and confidential information is disclosed to unauthorized individuals [Abawajy *et al*., 2016] and can be classified into four types [Vu *et al*., 2019; Dong and Zhou, 2016]: (i) *identity disclosure*, when an individual's identity is revealed; (ii) *attribute disclosure*, when the value of some sensitive attributes associated with an individual is compromised; (iii) *relationship disclosure*, when a sensitive relationship between two people is disclosed; and (iv) *disclosure of affiliation relationship*, when a person's membership of a particular group or community is disclosed. Overall, a privacy breach is a consequence of a threat execution, and this can cause harm to users in the form of harassment, financial loss, and even identity theft. They can also make users vulnerable to unwanted ads, scams and crimes, which can damage their social reputation or economic situation and cause them to be them victims of blackmail or physical violence [Shokri *et al*., 2012]. In addition, commercial and government entities may also violate users' privacy for different purposes, such as targeted marketing, health screening, or political monitoring [Zheleva and Getoor, 2009].

2.4 Threat Modeling

The threat modeling process was initially introduced by Microsoft, and its proposal was that it be inserted in the security design stage, with the aim of making the applications developed by the company more secure [Shostack, 2008]. Overall, threat modeling is a structured approach for identifying and prioritizing potential threats to a system and thus determine countermeasures to prevent or mitigate the effects of those threats [Shostack, 2014]. The methodology was proposed so that developers, designers, and system analysts could include threat modeling in their software development cycle. The process allows one to generate a threat model and determine what types of mitigation are needed during an early development stage of a new system, application, or feature.

3 Related Works

In this section, the main related works to our research are presented. For a better understanding, this section was divided into two subsections: subsection III-A presents the general context of threat modeling, showing the main methodologies proposed for other contexts that are not OSNs and subsection III-B presents the current context of threat modeling in the OSN domain.

3.1 Generalist Threat-modeling Methodologies

In the 1990s, Loren Kohnfelder and Praerit Garg proposed the STRIDE methodology, which includes systematic management of various security threats from the design stage of all Microsoft products [Khan *et al*., 2017]. The STRIDE acronym is formed by the initials of the following threat categories: spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege. Currently, STRIDE is the most refined threat-modeling method used in the context of security design [Kim *et al*., 2021].

In a similar vein, Wuyts *et al*. [2018] developed a methodology for threat modeling with a focus on privacy. LINDDUN provides structured support that guides software analysts and architects in eliciting and mitigating threats in general systems. Like STRIDE, the method's name is an acronym: Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance. The LINDDUN methodology encompasses three main steps: (i) modeling the system, (ii) identifying threats and (iii) managing threats. Similarly to STRIDE, in the first step, LINDDUN uses a data flow diagram (DFD) to understand how the system functions and, subsequently, perform a privacy analysis. After the system is described, each element of the DFD is systematically analyzed for potential privacy threats.

Although the methodologies STRIDE and LINDDUN are an interesting guide to the threat-modeling process, they are not fully suited to the context of OSNs. Both were proposed to mitigate the risk of threats to the functioning and architecture of general systems, in other words, they were designed to deal with threats related to this particular context. This implies that the concern for user data protection is not the central focus of the methodologies. For example, the categorization model used in the LINDDUN threat identification phase may not include categories of relevant threats that could breach user privacy and which are present in the current context of OSNs.

From another perspective, UcedaVelez and Morana [UcedaVelez and Morana, 2015] proposed a method for attack simulation and threat analysis, which is called PASTA (Process for Attack Simulation and Threat Analysis). The main goal of the method is to provide a dynamic process for identifying, enumerating, and scoring threats to a given system. The PASTA methodology involves seven steps that support the threat modeling process: (i) define the objectives; (ii) define the scope; (iii) decompose the application; (iv) analyze the system threats; (v) analyze the system vulnerabilities and weaknesses; (vi) model the attacks; and (vii) analyze the risk impact. One of the main steps of the methodology is the detailed analysis of the identified threats. This analysis allows you to determine the appropriate controls and mechanisms to be implemented in the system, as well as possible countermeasures.

Overall, PASTA is a methodology that is recommended for organizations that want to align their business strategies with product safety. To this end, it considers threats to be a business problem. In other words, the method focuses on factors such as the software architecture, the business context and the system's usage profile, but it is not concerned with protecting user data. Furthermore, as well as the STRIDE and LINDDUN methodologies, the PASTA methodology faces similar issues regarding its adaptation to the context of OSNs for the same reasons mentioned previously.

Different from the aforementioned threat-modeling methodologies, Mead *et al*. [2018] developed the hTMM (Hybrid Threat-Modeling Method), a method for modeling hybrid threats. The proposal consists of an association of activities from other methods, such as SQUARE (Security Quality Requirements Engineering Method), Security Cards, and Persona non Grata (PnG) [Denning *et al*., 2013]. In general terms, hTMM uses the requirements engineering proposed by SQUARE to elicit, categorize and prioritize security requirements. It then uses the PnG technique to discover ways in which a system can be breached to serve an attacker's goals. Finally, it applies the Security Cards technique to eliminate any PnGs that are considered unlikely to appear, summarizes the results and formally assesses the risk of a threat occurring. Although it presents a threat-modeling process that involves several software engineering and systems design activities, hTMM does not address privacy aspects in OSNs. In addition, like the other methods previously mentioned, the main focus of hTMM threat modeling is the security of system components, and no attention is given to the protection of user privacy.

3.2 Methodologies for Threat Modeling in the Context of OSNs

In the context of OSNs, few studies focus on threat modeling. The work by Sanz *et al*. [2010] describes a methodology for modeling threats, with a focus on security aspects of OSNs. The methodology proposed by the authors suggests some key steps to integrate into a modeling context, such as an analysis of the system's assets, an analysis of the threats and attacks on the system, and recommendations regarding countermeasures that OSNs should implement to prevent targeted attacks on the system.

In a similar vein, Wang and Nepali [2015] proposed a framework for modeling threats in OSNs from a conceptual perspective. The authors' proposal presents some relevant steps for the modeling context. In the first step, four components of the system must be characterized, which are understood as fundamental elements for threat modeling, such as (i) OSN sites, (ii) OSN providers, (iii) users of OSNs, and (iv) malicious users. Given the characterization of these components, it is recommended that the different objectives that malicious users intend to accomplish are identified. After that, system's vulnerabilities should be identified and ana-

lyzed, based on six security aspects, such as hardware, operating systems, OSNs privacy policies, user privacy settings, user relations and user data. Then, an analysis of possible threats to and attacks on the system and their associated risk must be carried out. Risks must be analyzed and prioritized through two aspects: probability and impact.

The works proposed by [Sanz *et al*., 2010] and [Wang and Nepali, 2015] present conceptual approaches for modeling threats in the context of OSNs and highlight the importance of using this methodology as a solution to security issues in these systems. However, the approaches presented in these works appreciate a conceptual perspective, which can serve as input and basis for proposing a more complete methodology applicable to the context of OSNs. Furthermore, the proposals do not provide methodological guidance to assist designers and other IT professionals who want to incorporate privacy threat modeling into OSNs at the design level.

The work proposed by Du *et al*. [2018] uses the concept of attack trees to create an attack and defense tree model. The main objective of the model is to represent, evaluate and prevent security and privacy threats in large-scale OSNs. The solution adopts a hierarchical structure that describes an attack process and the corresponding countermeasures. The root node of the tree is the target of the attack. The leaf nodes (atomic attack) are the steps to complete the objective of the attack, that is, what is necessary in order to reveal the privacy of users.

Attack trees are easy to understand and adopt, and they are useful for modeling threats related to the security context. Furthermore, the method assumes that analysts have a very good knowledge of cybersecurity and, therefore, it does not provide guidelines to support professionals who have little knowledge in threat modeling.

Overall, the related works show that methodologies for threat modeling are emerging, but do not fully meet privacy expectations in OSNs. In other words, some fail by not providing sufficient methodological guidance for a threat design process, others fail by assigning the main focus only on the security of system components, disregarding potential attention to the protection of data of users of OSNs. To fill this gap, we developed PTMOL. Unlike existing works, PTMOL is a solution for modeling privacy threats with a focus on protecting user data. PTMOL guarantees greater assertiveness in the implementation of privacy mechanisms, since the threats that can be identified with PTMOL are directly linked to the user, and are based on an action of a potential attacker. In addition, it provides methodological guidance to enable support for professionals with little experience in privacy, and helps them to introduce privacy early on the OSN development cycle. Furthermore, threat modeling tends to be increasingly in demand, as its result can improve users' confidence in systems and ensure compliance with laws for the protection of personal data. Therefore, PTMOL's threat modeling process is an important support that enables better design of the next generation of OSNs.

4 Privacy Threat MOdeling Language (PTMOL)

PTMOL is a privacy threat modeling solution focused on protecting user data [Rodrigues *et al*., 2023]. PTMOL allows designers to identify potential privacy threats, their consequences, and how they can be neutralized. To accomplish this support, PTMOL has features for threat design and a threat model that can be generated by the designer as part of the design. The language consists of the following components: (a) vocabulary; (b) syntax; and (c) semantics. The vocabulary is the collection of all words that can be used by the designer. The syntax is the set of elements that determines the format of words by defining how they can be represented in the model generated by the designer. Finally, semantics refers to the meaning associated with the language elements. As for its vocabulary, PTMOL has the following terms:

- **Assets**. Something related to the target (user) that has a personal value.
- **Threat**. A situation that can endanger the user's assets.
- **Threat Actors**. A malicious agent that operates inside or outside the system to breach user privacy.
- **Malicious Uses**. Describes the anticipated malicious uses that may affect the user's privacy.
- **Prevent Alert**. System alert to inform users of any action that can cause major breaches to their privacy.
- **Countermeasure**. System actions to mitigate privacy threats exploited by threat actors.
- **Sharing Zone**. Represents the user sharing zone.
- **Risk Zone**. Represents the system zone where attacker's actions may occur.
- **Leakage Zone**. Zone that refers to data leakage for malicious uses.

4.1 Types of services and point of the design process in which PTMOL can be used

PTMOL was developed to be applied in OSN systems. Therefore, all its vocabulary, syntax and semantics are associated with this context. It is generic to the point that it can be applied to many types of systems that have characteristics of social networks, such as relationship, entertainment or professional networks, where assets are shared and may be susceptible to privacy threats.

In general terms, the activities of the design process can be characterized as [Lowson, 2005]: (i) analysis of the current situation or problem, whereby the designer must seek to study and interpret a good way to improve one or more characteristics of the situation current system; (ii) synthesis of an intervention, whereby an intervention must be planned and executed in the current situation; and (iii) assessment of a new situation, for which the previously analyzed situation must be compared with the new situation reached after the intervention.

According Lowson [2005], the difference between the current situation and a desired situation is the main motivation for designing and synthesizing an intervention. In other words, an intervention is called a solution, as it answers the question that defines a problem to be solved: "How can this

situation be improved?". From this perspective, PTMOL can be applied in the design process, both in an analysis activity, to previously identify all the threats that may compromise the user's privacy, and in the intervention synthesis activity, in order to select mitigation strategies that can reduce the effects of threats by executing an intervention in the current situation.

4.2 Catalog of Privacy Threats

PTMOL's threat modeling process is supported by catalog of privacy threats for the context of OSNs, which describes the most critical threats to user privacy. These threats were discovered via a thorough investigation of the literature. This threat set is a very valuable resource as it helps the designer to think through which threat scenarios a user is potentially exposed to. The threats considered by the language are:

- **Cyberstalking**. A threat in which the attackers harass an individual or group through the OSNs. Many times, users frequently reveal their personal information on their profiles. malicious user can gather their information by content-based retrieval methods and, at a later stage, they can misuse it for cyberstalking [De and Imine, 2018b; Aktypi *et al*., 2017; Fogues *et al*., 2015].
- **Information Disclosure** - Information disclosure refers to the detection and extraction of information that was unintentionally disclosed [Ali *et al*., 2019]. This disclosure can directly expose an enormous amount of the users' confidential information, such as their home address, health-related data, recent activities, and so on. The sharing of such sensitive and private information may have negative implications for OSN users, and this can compromise their privacy [Rathore *et al*., 2017; Aktypi *et al*., 2017; Zeng *et al*., 2015; Bioglio *et al*., 2019; Casas *et al*., 2015].
- **Profile cloning**. A malicious user can use the shared data in OSNs to duplicate a user's profile. This threat is known as profile cloning, which is when a fake identity is created to make friends believe in the new "fake" profile. The attacker collects confidential private information about the user's friends to make social links, and capture data of the victim that is not shared in their public profiles [Rathore *et al*., 2017; Abid *et al*., 2018; Aktypi *et al*., 2017; Mahmood, 2012; Jaafor and Birregah, 2015].
- **Data Inference or Tracking** - Data inference is a type of threat applied to discover personal information of the user's that is not directly shared in their profiles on OSNs, but can be predicted using different computational techniques. In addition, OSN providers track and analyze the user's routine activities (such as daily browsing and shopping preferences, for example) through various machine-learning techniques. As a result, OSNs build complete user profiles for the purpose of selling products or tracking their behavior [Laorden *et al*., 2010; Watanabe *et al*., 2011; Wang and Nepali, 2015; Abid *et al*., 2018; Dong and Zhou, 2016].
- **Threat to Reputation** - Sharing personal or sensitive information can make OSN users victims of a threat to reputation. A malicious user or an online entity can create multiple false profiles to gain access to sensitive private information and exploit them to harm the reputation of the OSN user [Abid *et al*., 2018; Rathore *et al*., 2017; Kumar *et al*., 2017; Wang and Nepali, 2015]. Moreover, users could become victims of manipulation and distortion of data. Currently, there are several tools available to distort diverse data. Using these tools, a malicious user can alter the personal images of legitimate users, for example, in order to harm or damage their reputation.
- **Facial Recognition**. Face recognition algorithms are capable of identifying or verifying a person from a digital image or a video source. Identifying a person's face from a photo or video and cross-referencing it with other datasets might be used to expose personal information about the individual [Kagan *et al*., 2024; Laorden *et al*., 2010; Kumar *et al*., 2017; Kavianpour *et al*., 2011].
- **Surveillance**. Surveillance is a new type of monitoring that allows, in real-time, the collection and processing of various activities of users of OSNs by using their profiles and relationships with others [Aktypi *et al*., 2017].
- **Unauthorized Recording** - Nowadays, many OSNs support both chat and video conferencing services since video conferencing can provide more interaction between users. However, with this, more information can be disclosed. One of the participants of the video conference can easily record the conference in order to blackmail the other participant (victim) or to distort the conference data and display it accordingly [Rathore *et al*., 2017; Kagan *et al*., 2024].
- **Identity theft** - Identity theft is a type of threat where a malicious user attempts to collect personal information from OSN users (victims) so that he/she can impersonate them in order to gain some benefit or harm the victim [De and Imine, 2018b; Al-Asmari and Saleh, 2019; De and Imine, 2018a; Tucker *et al*., 2015].

4.3 Mitigation Strategies

A second resource, which is envisioned to aid the PTMOL modeling process, is that of generalist mitigation strategies, which can be used as a basis for creating preventative countermeasures. These strategies have been adapted from a set of privacy threat properties [Pfitzmann and Hansen, 2010] and serve as a contribution to assist in formulating preventative countermeasures to address the threats identified with the language. The mitigation strategies adopted are:

- **Unlinkability**. Refers to the ability to hide the link (relationship) between two or more user actions, identities, or information. The malicious actor may not be able to identify whether two items are related.
- **Anonymity and Pseudonymity**. The attacker may not be able to identify an individual within a pool of anonymous individuals. A pseudonym is an identifier of an individual other than one of their real names.
- **Plausible deniability**. This refers to the ability to deny having performed an action that other parties can neither confirm nor contradict. A malicious actor cannot

prove that a user knows, did or said something. For example, if the user makes a report, they will want to deny sending a certain message to protect their privacy.
- **Non-detection**. This refers to hiding user activities. For example, an attacker may not have the ability to accurately distinguish whether someone or no one is in a given location.
- **Confidentiality**. Refers to concealment of user data contents or controlled release of such contents. In general, confidentiality means preserving restrictions on the access and disclosure of information.
- **Awareness**. With the emergence of OSNs, users tend to provide a large amount of information to service providers and lose control over their personal data. Thus, the awareness property has the purpose of ensuring that users are aware of the collection of their personal data and that only the necessary information should be used to allow the performance of the systems' functions.
- **Transparency**. This requires that any system that stores user data informs the owner of the data about the system's privacy policy and allows the owner of the data to specify their consent in compliance with the legislation, before users access the system.

4.4 Application Process

The language allows the designer to represent and consequently elaborate and refine their design in layers, i.e., bit by bit. Initially, the designer must understand the domain of the OSN they want to solve. A description of the features that allow the user to share information in the system or of an eventual interaction scenario where the user will share assets in the system is required.

After understanding a possible threat scenario that a user may be exposed to, PTMOL enables the designer to define portions of their threat modeling from patterns, or templates integrated into the language, so that their understanding of the problem and possible solutions broadens. The modeling template serves as a support for representing all the information that affects the user's privacy in a structured way. In addition, the template allows all the attacker's actions to also be documented so that future changes to the system settings, threat landscape and sharing environment can be quickly evaluated. The template performs yet another valuable function: it helps the designer to understand the design logic underlying the proposed language. After all this information has been analyzed, the designer must produce the threat model resulting from the design.

The execution of PTMOL allows splitting a complex process into smaller tasks, and makes it easier to identify the entire threat landscape. Thus, to start threat modeling via the template, the designer will have to follow a set of activities in order to identify: (i) what needs to be protected from the user (assets), (ii) what undesirable events (threats) may occur and can put the user's assets at risk, (iii) what malicious uses can carry out in order to breach the user's privacy, and (iv) what strategies to adopt (countermeasures) to prevent or mitigate the effects of threats to the user's data. For some steps of PTMOL, there is a pre-defined set of values to fill in in the modeling template, where the designer can indicate a value from the set as suggested by the syntax of the language. In other stages, the designer can freely fill in the modeling template, and is able to indicate values based on their reasoning or by taking into account decisions made by the design team. The PTMOL modeling steps are described in detail below.

4.4.1 Identifying Assets

In this step, the designer must identify the assets to be protected. An asset is something related to the target (user) that has a personal value. As such, the designer needs to understand what must be protected, before they can start figuring out what threats might occur. The designer needs to have a clear understanding of the assets, because the next modeling steps will be directed to them. Depending on how the asset has been shared in the system, different threats can occur. By this look, three values were defined:

- **Textual data**: files or free text;
- **Multimedia data**: photos, audios or videos;
- **Geographic data**: geolocation

Figure 1 presents the template for the classification of the asset with its filling rules. The template allows the designer to list all the assets extracted from the threat scenario and classify their sharing type based on the predefined set of values. Depending on how asset was shared in the OSN, different threats may arise. For example, location described in textual form is different from geolocation.

Assets	TYPE OF ASSET SHARED					
	Textual data		Multimedia data			Geographic data
	File (PDF, DOC)	Free text	Photo	Video	Audio	Geolocation
Asset 1						
Asset 2						
Asset 3						
...						
Asset n						
<List all assets>	<Mark with "X" the type of asset shared>					

Figure 1. Template for asset identification and classification

There are assets that are not directly shared by users, but are collected or generated by the system itself. In general, OSN providers track and analyze user activities and build complete profiles for the purpose of selling products and tracking user behavior. In this sense, two forms of collection were defined, as illustrated in Figure 2. The assets collected by the platform itself can assume two values:

- **Usage data**: activities, preferences or user behavior on OSN;
- **Relationship data**: user's links and relationships with others.

4.4.2 Identifying Threats, Malicious Uses and Threat Actors

The second step is considered the core of the PTMOL threat modeling process. After listing all the system's assets, the designer must consult the PTMOL privacy threat catalog.

Assets	ASSETS COLLECTED BY THE SYSTEM	
	USAGE DATA	RELATIONSHIP DATA
Asset 1		
Asset 2		
Asset 3		
...		
Asset n		
<List all assets>	<Mark with "X" if the asset belongs to this category>	<Mark with "X" if the asset belongs to this category>

Figure 2. Template for classifying assets collected by the system

For each asset identified, the designer should associate at least one potential privacy threat, reflecting on how that asset might be vulnerable. Although this association is open-ended, the catalog is designed to be reflective, encouraging the designer to critically consider how each listed threat might compromise a specific asset.

Once threats are mapped to assets, the next step is to identify the threat actors, those who might be responsible for exploiting the vulnerability. PTMOL defines four possible categories of threat agents: (i) malicious member, (ii) platform provider, (iii) third-party application, and (iv) external entities. The designer must evaluate, based on the system context, which of these actors is most likely to execute the threat.

Finally, the designer should describe the possible malicious uses associated with each threat–asset pair. This step involves considering realistic abuse scenarios and how the identified threats could be exploited in practice. For example, in a social network where users' connections with others are visible through mutual friends, the "social link" asset could be vulnerable to a cyberstalking threat. In this case, the threat might be executed by a malicious member (e.g., someone exploiting the network to track user relationships), with the malicious use involving invasive monitoring of a user's personal network to infer private details or movements. Figure 3 illustrates the template used for mapping threats, malicious uses, and threat actors.

Assets	Asset classification	Privacy Threats	Threat Actors	Malicious uses
What must be protected?	Asset collected or shared?	What situations can put the user's assets at risk?	Who are the threat actors?	What are the malicious uses that can affect the user's privacy?
Asset 1	Pre-defined value	Pre-defined value	Pre-defined value	Free value
Asset 2				
Asset 3				
...				
Asset n				
<List all assets>	<Classify Asset>	<Associate threat [from catalog] to asset>	<Indicate threat actors>	<Predict malicious uses>

Figure 3. Template for identifying threats, malicious uses and threat actors

4.4.3 Identifying Mitigation Strategies

Finally, in the last step, the designer will have to make strategic decisions that guarantee greater assertiveness in the implementation of alerts and appropriate countermeasures to protect the assets. After listing the set of threats and their consequences for the user's privacy, the designer should consult the implemented taxonomy with privacy properties. With this, the designer must indicate, through a selection mark "X", which properties were violated, as shown in Figure 4.

Privacy Threats	Which privacy property can be violated?						
	Unlikability	Anonymity	Plausible deniability	Non-detection	confidentiality	Awareness	Transparency
Threat 1	X					X	
Threat 2		X					
Threat 3			X				X
...				X		X	
Threat n		X			X		

Figure 4. Template for identifying violated privacy properties

For each property indicated as possibly being violated, it is necessary to transform it later into a countermeasure, so that it can reduce or hinder the foreseen malicious uses. Furthermore, the designer also has the option of issuing alerts to inform users about any action that may cause serious breaches to their privacy. With this, the designer will be able to think of appropriate countermeasures for the system, allowing the anticipation, still in the design phase, of strategic decisions for the protection of user data. Figure 5 presents the template for identifying mitigation strategies.

Assets	Privacy Threats	Violated privacy property	Countermeasures	Prevention alert
What must be protected?	What situations can put the user's assets at risk?	What privacy properties were violated?	What strategy to adopt to mitigate the threats?	What alert could be issued to inform the user of consequences for their privacy?
Asset 1	Pre-defined value	Pre-defined value	Free value	Free value
Asset 2				
Asset 3				
...				
Asset n				
<List all assets>	<List all threats>	<Indicate the violated property>	<Predict countermeasures>	<Generate an alert in serious situations>

Figure 5. Template for identifying mitigation strategies

5 Case Study with PTMOL

While privacy concerns in online social networks have been widely studied, there remains a gap in applying structured methodologies for threat modeling in already deployed platforms. Our study extends PTMOL's scope by validating its applicability in evaluating privacy threats within a real-world scenario.

In this context, this study aimed to evaluate PTMOL as a tool for identifying and analyzing privacy threats in existing OSNs, demonstrating its versatility in threat modeling. The adopted approach allowed us to assess whether PTMOL was useful in analyzing the current state of privacy in platforms in use, comparing its results with previously documented real incidents. This comparison enabled us to test PTMOL not only as a predictive tool for design-level application but also for evaluating operational OSNs. In this context, the research question guiding this study was: Can PTMOL effectively

identify and describe privacy threats in a manner consistent with real incidents on existing social networking platforms?

The study was based on the analysis of previously recorded privacy incidents, covering documented cases that directly impacted users of these platforms. These incidents ranged from personal data exposure to the misuse of information for malicious purposes. By applying PTMOL to these systems, the study demonstrated its ability to identify and detail privacy threats, providing a risk assessment for current OSNs.

5.1 Study Planning

The study was carefully structured to ensure a detailed analysis of privacy threats, aiming not only to identify these threats but also to validate PTMOL in real-world scenarios. The methodological steps adopted are described in detail below.

5.1.1 Platform Selection

The social network X (formerly Twitter) was chosen for analysis due to several reasons that justify its relevance to this study. First, X has a globally extensive user base, making it a relevant case study for investigating privacy threats in large-scale platforms. Additionally, the platform has been the target of numerous widely documented privacy incidents in academic literature and reputable journalistic sources. The availability of detailed information on these events allowed for a comparison between PTMOL's modeling results and real incidents, providing a well-founded analysis.

5.1.2 Interaction Scenario

At the beginning of the PTMOL modeling process, the designer must develop a clear understanding of the social network's domain, identifying the features that enable user information sharing. In this context, an interaction scenario was designed to reflect the typical use of X, emphasizing the most common functionalities among users. This scenario focused on describing how users share assets while considering aspects that could lead to privacy threats. The representation included different types of interactions, such as login validation, post creation, and engagement with other users' content. The formulated scenario is described below:

> *A user named Carlos creates an account on platform X, providing his email address and phone number for account verification. He also sets a username and adds a profile picture. After configuring his profile, he posts his first tweet containing text about a local event, attaching an image of the event poster. Later, he decides to share his location while commenting on a restaurant he visited. Additionally, Carlos uses the platform's "circles" feature to share a personal thought exclusively with a restricted group of friends. While browsing, he interacts with other users' posts, liking and commenting on various pieces of content. Unknowingly, his activity generates a behavioral profile that the platform uses to suggest new content and personalized advertisements.*

5.1.3 Real Privacy Incidents

To compare with PTMOL's modeling results, two real privacy incidents with significant impact on X were selected. The selection of these incidents was based on two criteria to ensure their relevance and representativeness:

- **Relevance:** Incidents were chosen based on extensive documentation in both academic literature and reputable journalistic sources. This ensured that the selected cases represented actual threats with a tangible impact on user privacy.
- **Representativeness:** The chosen incidents reflected situations commonly encountered in the daily use of X, ensuring that the analysis aligned with real user behavior on the platform. These cases were examined to identify recurring threats such as data breaches and the misuse of personal information.

Based on these criteria, the selected incidents provided a representative scenario for evaluating PTMOL's applicability in detecting privacy threats that have actually materialized. The incidents analyzed occurred at two different points in time:

- **Twitter Data Breach Affecting 5.4 Million Accounts**[1] **(August 2022):** Due to a platform vulnerability, data such as users' phone numbers and email addresses were exposed and later put up for sale on online forums. This incident demonstrated how account-linked information can be compromised and used for malicious purposes.
- **Exposure of Private Tweets**[2] **(May 2023):** A system error resulted in the unintended disclosure of private tweets, making public the content that users intended to keep restricted. This incident raised concerns about the reliability of the platform's privacy settings.

5.2 Study Execution

5.2.1 Participation of Experts

The application of PTMOL was conducted by three specialists with prior experience in threat modeling and privacy analysis in interactive systems. The selection process was asynchronous and involved targeted invitations to researchers and professionals affiliated with privacy and information security projects with whom the authors had previously collaborated. The recruitment aimed to ensure diversity in background and practical expertise with modeling methodologies.

Two of the specialists had previously contributed to the development and early validation of PTMOL, providing deep technical knowledge of the method. The third participant had a background in software engineering and specialized in requirements analysis and threat modeling using other approaches, which allowed for a complementary and critical perspective.

[1] https://www.bleepingcomputer.com/news/security/54-million-twitter-users-stolen-data-leaked-online-more-shared-privately/. Access on 02 October 2025.

[2] https://techcrunch.com/2023/05/05/twitter-confirms-circle-tweets-temporarily-were-not-private/. Access on 02 October 2025.

The modeling process itself was divided into two phases. In the first phase, each participant independently performed the modeling task asynchronously, based on the provided materials (i.e., the interaction scenario and the documented real-world privacy incidents). Importantly, none of the specialists had any prior involvement in preparing these materials. In the second phase, the participants convened to review and consolidate their findings collaboratively. These discussions were moderated by one of the authors, who ensured that all methodological steps were followed consistently and that consensus was reached without external influence or bias.

All specialists who participated in the study signed an Informed Consent Form (ICF) prior to their involvement. No personal data was collected from the participants during the study. They were only required to carry out the modeling tasks and participate in the group discussion. All data generated during the study referred exclusively to the outcomes of the modeling activity.

5.2.2 Ethical Considerations

This study was reviewed and approved by the Research Ethics Committee of the Federal University of Amazonas (UFAM), under the protocol CAAE: 63572122.0.0000.5020. All procedures adhered to ethical research standards, including transparency, informed consent, and privacy protection.

Participation was entirely voluntary, and all specialists signed an Informed Consent Form before contributing to the study. No sensitive or personal information was collected from the participants; their involvement was limited to performing the threat modeling activities and contributing to discussions. All data analyzed were derived from the modeling outcomes and not from any individual characteristics of the participants.

6 Results

This section presents the results obtained from applying PTMOL to the selected scenarios. The analysis includes identifying the assets of the evaluated social networking platform (SNP), as well as the associated threats, leakage sources, and malicious uses. Additionally, a comparison is made between the identified threats and documented real-world incidents.

6.1 Asset Identification

This process was conducted based on a previously developed interaction scenario, enabling a targeted analysis of potential threat scenarios that may occur within the selected platform. Tables 1, 2 and 3 present the consolidated results obtained from the PTMOL modeling. These data represent a compilation of the individual analyses performed by each of the expert participants in the study. Initially, each participant conducted the modeling independently based on the provided interaction scenario and following the methodology guidelines. Subsequently, the results were compared and discussed in a joint meeting, where discrepancies were carefully analyzed and resolved through technical argumentation and consensus among the experts. Table 1 presents the classification of identified assets in the interaction scenario. For this analysis, assets were categorized according to PTMOL's classification:

- **Textual data:** Information shared in text format, such as tweets and comments.
- **Multimedia data:** Image, audio, or video files posted by the user.
- **Geographic data:** Location information explicitly shared by the user.
- **Usage data:** Behavioral patterns, interactions, and preferences captured by the platform.
- **Relationship data:** The user's connections and interactions with other profiles within the social network.

The classification presented highlights the diversity of assets involved in platform X, which may be subject to privacy threats. Textual data is strongly present, both in public posts and in content restricted to specific groups, such as tweets within "Circles". Additionally, the collection of sensitive information, such as email and phone numbers, poses an extra risk, as these data points can be exploited in attacks like phishing and social engineering. Another relevant aspect is the interconnection between usage and relationship data, which allows the platform to construct detailed user behavior profiles.

6.2 Identification of Privacy Threats, Threat Actors, and Malicious Uses

The second stage of threat modeling with PTMOL involves identifying threats that could compromise user privacy on the platform. This phase is crucial for understanding the risks involved in information sharing and the potential malicious uses that could arise. To conduct this analysis, each asset identified in the previous stage was linked to one or more threats from the PTMOL catalog. In addition to identifying threats, potential threat actors were also recognized—specifically, the possible agents responsible for violating user privacy. Finally, for each identified threat, potential malicious uses were described, outlining how attackers might exploit the obtained information. Table 2 presents the categorization of threats associated with the assets identified in the interaction scenario.

The analysis reveals that the assets shared or collected on the platform may be exposed to multiple privacy threats. These threats include surveillance, cyberstalking, identity theft, facial recognition, profile cloning, information disclosure, and tracking, highlighting that the collection and misuse of data pose significant risks to users.

It is noted that platform providers can play a central role as leak sources, either through excessive data collection or through security and privacy failures that expose user data. Additionally, malicious members may exploit vulnerabilities to conduct targeted attacks, such as profile cloning, espionage, and reputation threats. Finally, the identified malicious uses indicate that if a data leak occurs, these assets could be exploited for fraud, social engineering attacks, unauthorized surveillance, and content manipulation.

Table 1. Identified assets in the interaction scenario

Asset List	Textual Data	Multimedia Data	Geographic Data	Usage Data	Relationship Data
Username	X				
Profile Picture		X			
Public Tweet	X				
Comment on a Post	X				
Photo Attached to a Tweet		X			
Location			X		
Registered Email	X				
Phone Number	X				
Private Tweets (“Circles”)	X				X
Likes and Interactions with Posts				X	X
Personalized Content Suggestions				X	
Relationships and Connections with Other Profiles					X

Table 2. Threats, threat actors, and predicted malicious Uses

Asset	Asset Type	Threats	Threat Actors	Malicious Uses
Username	Text Data	Profile cloning, identity theft	Malicious member, provider	Creation of fake profiles for fraud and scams
Profile picture	Multimedia Data	Facial recognition, cyberstalking	Malicious member, provider	Use in deepfakes or identity tracking
Tweets (public and private)	Text Data	Information disclosure, surveillance, threat to reputation	Provider, third-party app	Exposure of private opinions, leak of conversations
Comments, likes, and interactions	Usage Data	Data inference or tracking, surveillance	Provider, third-party app	Behavioral profiling used for content manipulation and targeted ads
Photo attached to a tweet	Multimedia Data	Information disclosure, facial recognition, cyberstalking	Provider, malicious member	Identification of user’s location, misuse in deepfakes or tracking
Location	Geographical Data	Data inference or tracking	External source, provider	Tracking user’s routine for malicious purposes
Registered email	Text Data	Information disclosure, profile cloning, identity theft	Provider, external source	Phishing emails, social engineering for scams
Phone number	Text Data	Information disclosure, identity theft	Provider, external source	Banking fraud, WhatsApp account cloning
Personalized content suggestions	Usage Data	Data inference or tracking, surveillance	Provider, third-party app	Algorithmic manipulation to influence preferences and behaviors
Relationships and connections with other profiles	Relationship Data	Surveillance, cyberstalking	Malicious member, provider	Monitoring social connections for social engineering

6.3 Comparison with Real Privacy Incidents

The comparative analysis was conducted by examining the assets identified during the modeling process and checking which ones were actually breached in the analyzed leaks. Table 3 provides a detailed mapping between the assets identified in the modeling process, the associated threats for each asset, and the threats that materialized in the incidents. Additionally, the mapping in Table 3 shows whether PTMOL successfully anticipated significant risks and which predicted threats did not occur in the analyzed incidents.

The analysis results show that PTMOL was effective in predicting threats that actually occurred in the real incidents analyzed. The assets of private tweets and contact data (email and phone), which were compromised in the 2022 and 2023 leaks, had already been classified in the modeling process as vulnerable to threats such as information disclosure and tracking. This suggests that the PTMOL modeling process can help identify threats before they materialize.

In addition to the threats that materialized in the analyzed incidents, the modeling also identified other potential risks, such as profile cloning and cyberstalking. Although these threats were not observed in these specific cases, they still represent plausible vulnerabilities within the platform’s context. This highlights PTMOL’s ability not only to predict known threats but also to identify risk scenarios that can be proactively mitigated.

6.4 Analysis of PTMOL Coverage in Real Incidents

The comparative analysis conducted in the previous section allowed for the evaluation of PTMOL’s ability to predict threats that actually occurred in real incidents. This enabled the identification of gaps in the modeling and suggested improvements to enhance its application. To deepen this assessment, a threat coverage matrix was created, as shown in Table 4. This matrix compares the threats predicted by PTMOL

Table 3. Comparison between PTMOL modeling and real incidents

Asset	Present in PTMOL Modeling?	Breached in Real Incident?	Threats Predicted by PTMOL	Threats Observed in Incident
Username	Yes	No	Profile cloning, reputation threat, identity theft	Not observed
Profile picture	Yes	No	Facial recognition, cyberstalking	Not observed
Tweets (public and private)	Yes	Yes (May 2023)	Information disclosure, espionage, tracking, reputation threat	Information disclosure, tracking, reputation threat
Comments, likes, and interactions	Yes	No	Espionage, tracking	Not observed
Photo attached to a tweet	Yes	No	Facial recognition, espionage	Not observed
Location	Yes	No	Inference or tracking, espionage	Not observed
Registered email	Yes	Yes (August 2022)	Information disclosure, profile cloning, identity theft	Information disclosure, identity theft
Phone number	Yes	Yes (August 2022)	Information disclosure, profile cloning, identity theft	Information disclosure, identity theft
Personalized content suggestions	Yes	No	Inference or tracking, espionage	Not observed
Relationships and connections with other profiles	Yes	No	Espionage, cyberstalking	Not observed

with those that actually occurred in the analyzed incidents, categorizing them as covered (when predicted and occurred), false positives (when predicted but did not occur), and gaps (when occurred but were not predicted in the model).

The results from the coverage matrix indicate that PTMOL demonstrated strong predictive capability, successfully anticipating threats that materialized in the real incidents analyzed. Notably, the threats of information disclosure, inference or tracking, and identity theft were accurately predicted, reinforcing the tool's value in forecasting real privacy risks. Additionally, the reputation threat, evidenced by the exposure of private tweets, was also correctly identified in the model, showing that PTMOL is applicable in scenarios involving social networks and improper content exposure.

However, some predicted threats, such as cyberstalking, profile cloning, facial recognition, and unauthorized recording, were not observed in the analyzed incidents. This may indicate the presence of false positives in the model, or simply that these threats did not materialize in these specific cases. It is important to note that this does not invalidate these threats but rather suggests that their occurrence depends on the context. No threat analyzed in the real incidents was completely absent from the model, meaning there were no significant gaps in PTMOL for the cases considered.

7 Discussion

The results obtained in this study demonstrate the effectiveness of PTMOL in identifying privacy threats in existing Social Networking Services (SNS), highlighting its applicability in both anticipating threats and evaluating past incidents. The alignment between the modeling findings and the documented issues in practice reinforces the validity of the methodology, suggesting that PTMOL can also serve as a reliable tool for evaluating threats on social platforms.

The modeling process identified threat scenarios that were consistent with previously recorded real incidents, suggesting that PTMOL not only predicts potential threats but also reflects the impact these threats have on users. This alignment is an important indicator that the PTMOL-based approach can be used both by designers and developers during the design phase of social interaction systems, as well as by analysts and researchers aiming to diagnose vulnerabilities in already implemented platforms.

Another key point concerns the breadth of the modeling process. The analysis of assets and leakage sources allowed the identification of threats that, although not explicitly mentioned in the documented incidents, posed a high potential risk. This suggests that PTMOL can not only map known threats but also uncover potential privacy issues that might otherwise go unnoticed. Moreover, the use of a structured modeling process, guided by experts in the technique, ensured greater accuracy in identifying and categorizing threats. The convergence of individual assessments further reinforces the reliability of the methodology, minimizing subjectivity and making the analysis more systematic. This factor is crucial for PTMOL to be applied in different contexts, enabling replicability and adaptability to various platforms.

Another notable aspect is PTMOL's ability to describe threats in sufficient detail to aid decision-making. The modeling process not only allowed for the identification of potential risks in the analyzed OSN but also provided context for these risks within the platform's actual functioning, making the results more actionable for mitigating issues. This sets the approach apart from more generic analyses, which often

Table 4. Coverage matrix

Threat (PTMOL)	Predicted by PTMOL?	Occurred in 2022 Leak?	Occurred in 2023 Leak?	Coverage
Cyberstalking	Yes	No	No	False Positive
Information Disclosure	Yes	Yes	Yes	Covered
Profile Cloning	Yes	No	No	False Positive
Inference or Tracking	Yes	No	Yes	Covered
Reputation Threat	Yes	No	Yes	Covered
Facial Recognition	Yes	No	No	False Positive
Espionage	Yes	No	No	Covered
Identity Theft	Yes	Yes	No	Covered
Unauthorized Recording	Yes	No	No	False Positive

lack specificity when identifying privacy violations.

Overall, the findings of this study consolidate PTMOL as an effective approach for evaluating privacy threats in deployed OSN, demonstrating its capacity to capture threats and audit already launched platforms. The degree of compatibility between the modeling results and the real incidents analyzed further reinforces its validity as a privacy evaluation method, with the potential to be integrated into both development processes and privacy audits of OSN systems. As a result, PTMOL could become a tool for digital security teams, assisting in compliance with regulations such as the GDPR.

8 Threats to Validity

Like any empirical study, this research has certain limitations that may impact the validity of its results. Below, we discuss the main threats to validity and the strategies adopted to mitigate them.

Internal validity refers to the extent to which the results accurately reflect the relationships investigated in the study. A significant threat was the potential subjectivity in identifying assets and threats. To mitigate this risk, the identification process was conducted systematically, following predefined PTMOL guidelines, and reviewed by experts in the field.

External validity concerns the generalization of the results to other contexts. One limitation of this study is that the analysis was conducted on a single social media platform, which may limit the applicability of the findings to other online services. To address this issue, we selected a widely used platform whose core functionalities are similar to those of other popular social networks.

Additionally, the selection of scenarios may not encompass all potential threats users face. To minimize this limitation, the scenario was defined based on previous studies, ensuring it represented realistic threats.

9 Conclusion

The rise of online social networks (OSNs) has expanded opportunities for interaction and information sharing while also intensifying challenges related to user privacy. In this context, adopting methodologies that enable the systematic identification and evaluation of threat scenarios in these systems is essential. This study aimed to evaluate the use of PTMOL in describing privacy threats in already deployed OSNs, demonstrating its versatility in threat modeling.

The results indicate that PTMOL effectively facilitates the structured identification of digital assets and associated threats, allowing for a detailed analysis of the risks present in the evaluated platform. The methodology not only helped identify patterns of sensitive data exposure but also enabled the comparison of modeled threats with documented incidents, reinforcing PTMOL's ability to anticipate real risks. Additionally, the categorization of assets highlighted the interdependence between different data types and how their combination can be exploited for malicious purposes, underscoring the importance of threat mitigation strategies.

The findings suggest that PTMOL extends beyond its use as a design methodology and can also serve as a valuable tool for evaluating privacy threats, providing valuable insights for both researchers and practitioners in the field of interactive systems. Future research could expand this approach to other OSNs and explore the integration of PTMOL with automated threat detection mechanisms.

Given the growing complexity of the digital ecosystem, it is essential for researchers, developers, and policymakers to adopt proactive strategies to safeguard user privacy. The application of PTMOL represents an important step in this direction, contributing to more precise threat modeling and the development of solutions that enhance the privacy and transparency of social plataforms.

Acknowledgements

We thank the Brazilian Symposium on Human Factors in Computer Systems for the invitation to submit an extended version of the paper "*PTMOL: A Privacy Threat Modeling Language for Online Social Networks*" to compose a special issue of the JIS-SBC Journal on Interactive Systems. ChatGPT was used to review and improve the text of this paper.

References

Abawajy, J. H., Ninggal, M. I. H., and Herawan, T. (2016). Privacy preserving social network data publication. *IEEE communications surveys and tutorials*, 18(3):1974–1997. DOI: https://doi.org/10.1109/COMST.2016.2533668.

Abid, Y., Imine, A., and Rusinowitch, M. (2018). Online testing of user profile resilience against inference attacks in social networks. In *European Conference on Advances in Databases and Information Systems*, pages 105–117. Springer. DOI: https://doi.org/10.1007/978-3-030-00063-9_12.

Aktypi, A., Nurse, J., and Goldsmith, M. (2017). Unwinding ariadne's identity thread: Privacy risks with fitness trackers and online social networks. In *Proceedings of the 2017 on Multimedia Privacy and Security*, page 1–11, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/3137616.3137617.

Al-Asmari, H. and Saleh, M. (2019). A conceptual framework for measuring personal privacy risks in facebook online social network. In *Proc. International Conference on Computer and Information Sciences*, pages 1–6. DOI: https://doi.org/10.1109/ICCISci.2019.8716477.

Ali, S., Rauf, A., Islam, N., and Farman, H. (2019). A framework for secure and privacy protected collaborative contents sharing using public osn. *Cluster Computing*, 22:7275–7286. DOI: https://doi.org/10.1007/s10586-017-1236-2.

Alkhamees, M., Alsaleem, S., Al-Qurishi, M., Al-Rubaian, M., and Hussain, A. (2021). User trustworthiness in online social networks: A systematic review. *Applied Soft Computing*, 103:107159. DOI: https://doi.org/10.1016/j.asoc.2021.107159.

Altman, I. (1975). The environment and social behavior: Privacy, personal space, territory, and crowding.

Bioglio, L., Capecchi, S., Peiretti, F., Sayed, D., Torasso, A., and Pensa, R. (2019). A social network simulation game to raise awareness of privacy among school children. *IEEE Transactions on Learning Technologies*, 12(4):456–469. DOI: https://doi.org/10.1109/TLT.2018.2881193.

Casas, I., Hurtado, J., and Zhu, X. (2015). Social network privacy: Issues and measurement. In *Proc. 16th International Conference Web Information Systems Engineering*, pages 488–502. DOI: https://doi.org/10.1007/978-3-319-26187-4_44.

De, S. and Imine, A. (2018a). Privacy scoring of social network user profiles through risk analysis. In *Proc. 12th International Conference on Risks and Security of Internet and Systems*, pages 227–243. DOI: https://doi.org/10.1007/978-3-319-76687-4_16.

De, S. and Imine, A. (2018b). To reveal or not to reveal: Balancing user-centric social benefit and privacy in online social networks. In *Proc. ACM Symposium on Applied Computing*, pages 1157–1164. DOI: https://doi.org/10.1145/3167132.316725.

Denning, T., Friedman, B., and Kohno, T. (2013). The security cards: A security threat brainstorming toolkit. *Univ. of Washington*.

Dong, C. and Zhou, B. (2016). Privacy inference analysis on event-based social networks. In *Proc. 8th International Conference SocInfo*, pages 421–438. DOI: https://doi.org/10.1007/978-3-319-47874-6_29.

Du, S., Li, X., Zhong, J., Zhou, L., Xue, M., Zhu, H., and Sun, L. (2018). Modeling privacy leakage risks in large-scale social networks. *IEEE Access*, 6:17653–17665. DOI: https://doi.org/10.1109/ACCESS.2018.2818116.

Fogues, R., Such, J., Espinosa, A., and Garcia-Fornes, A. (2015). Open challenges in relationship-based privacy mechanisms for social network services. *International Journal of Human-Computer Interaction*, 31(5):350–370. DOI: https://doi.org/10.1080/10447318.2014.1001300.

Infante, A. and Mardikaningsih, R. (2022). The potential of social media as a means of online business promotion. *Journal of Social Science Studies*, 2(2):45–48.

Jaafor, O. and Birregah, B. (2015). Multi-layered graph-based model for social engineering vulnerability assessment. In *Proc. International Conference on Advances in Social Networks Analysis and Mining*, pages 1480–1488. DOI: https://doi.org/10.1145/2808797.2808899.

Jain, A. K., Sahoo, S. R., and Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, 7(5):2157–2177. DOI: https://doi.org/10.1007/s40747-021-00409-7.

Joyee De, S. and Imine, A. (2019). On consent in online social networks: Privacy impacts and research directions. In *Proc. 13th International Conference Risks and Security of Internet and Systems*, pages 128–135. DOI: https://doi.org/10.1007/978-3-030-12143-3_11.

Kagan, D., Alpert, G. F., and Fire, M. (2024). Zooming into video conferencing privacy and security threats. *IEEE Transactions on Computational Social Systems*, 11(1):933–944. DOI: https://doi.org/10.1109/TCSS.2022.3231987.

Kavianpour, S., Ismail, Z., and Mohtasebi, A. (2011). Effectiveness of using integrated algorithm in preserving privacy of social network sites users. *Communications in Computer and Information Science*, 167(2):237–249. DOI: https://doi.org/10.1007/978-3-642-22027-2_20.

Khan, R., McLaughlin, K., Laverty, D., and Sezer, S. (2017). Stride-based threat modeling for cyber-physical systems. In *Proc. Innovative Smart Grid Technologies Conference Europe*, pages 1–6. DOI: https://doi.org/10.1109/ISGTEurope.2017.8260283.

Kim, K. H., Kim, K., and Kim, H. K. (2021). Stride-based threat modeling and dread evaluation for the distributed control system in the oil refinery. *ETRI Journal*, 44(6):991–1003. DOI: https://doi.org/10.4218/etrij.2021-0181.

Kumar, H., Jain, S., and Srivastava, R. (2017). Risk analysis of online social networks. In *Proc. International Conference on Computing, Communication and Automation*, pages 846–851. DOI: https://doi.org/10.1109/CCAA.2016.7813833.

Laorden, C., Sanz, B., Alvarez, G., and Bringas, P. G. (2010). A threat model approach to threats and vulnerabilities in on-line social networks. In *Proc. Computational Intelligence in Security for Information Systems 2010*, pages 135–142. DOI: https://doi.org/10.1007/978-3-642-16626-6_15.

Lowson, B. (2005). How designers think. the design process demystified. *Tehran: University of Shahid-Beheshti*.

Mahmood, S. (2012). New privacy threats for facebook and twitter users. In *Proc. 7th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, pages 164–169. DOI: https://doi.org/10.1109/3PGCIC.2012.46.

Mead, N. R., Shull, F., Vemuru, K., and Villadsen, O. (2018). A hybrid threat modeling method. *Carnegie Mellon University-Software Engineering Institute-Technical Report-CMU/SEI-2018-TN-002*.

Pfitzmann, A. and Hansen, M. (2010). *A terminol-*

ogy for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, pages 1–9. Springer Berlin Heidelberg, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-44702-4_1.

Rathore, S., Sharma, P., Loia, V., Jeong, Y.-S., and Park, J. (2017). Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, 421:43–69. DOI: https://doi.org/10.1016/j.ins.2017.08.063.

Rodrigues, A., Villela, M. L. B., and Feitosa, E. L. (2023). Privacy threat modeling language. *IEEE Access*, 11:24448–24471. DOI: https://doi.org/10.1109/ACCESS.2023.3255548.

Sanz, B., Laorden, C., Alvarez, G., and Bringas, P. G. (2010). A threat model approach to attacks and countermeasures in on-line social networks. In *Proc. 11th Reunion Espanola de Criptografia y Seguridad de la Información*, pages 343–348.

Sathya, N. and Prabhavathi, C. (2024). The influence of social media on investment decision-making: examining behavioral biases, risk perception, and mediation effects. *International Journal of System Assurance Engineering and Management*, 15(3):957–963. DOI: https://doi.org/10.1007/s13198-023-02182-x.

Shokri, R., Theodorakopoulos, G., Troncoso, C., Hubaux, J.-P., and Le Boudec, J.-Y. (2012). Protecting location privacy: optimal strategy against localization attacks. In *Proc. ACM conference on Computer and communications security*, pages 617–627. DOI: https://doi.org/10.1145/2382196.2382261.

Shostack, A. (2008). Experiences threat modeling at microsoft. *MODSEC@ MoDELS*, 2008:35.

Shostack, A. (2014). *Threat modeling: Designing for security*. John Wiley & Sons.

Singh, S. S., Muhuri, S., Mishra, S., Srivastava, D., Shakya, H. K., and Kumar, N. (2024). Social network analysis: A survey on process, tools, and application. *ACM Computing Surveys*, 56(8):1–39. DOI: https://doi.org/10.1145/3648470.

Tucker, R., Tucker, C., and Zheng, J. (2015). Privacy pal: Improving permission safety awareness of third party applications in online social networks. In *Proc. 17th International Conference on High Performance Computing and Communications*, pages 1268–1273. DOI: https://doi.org/10.1109/HPCC-CSS-ICESS.2015.83.

UcedaVelez, T. and Morana, M. M. (2015). *Risk Centric Threat Modeling: process for attack simulation and threat analysis*. John Wiley & Sons.

Vu, H., Law, R., and Li, G. (2019). Breach of traveller privacy in location-based social media. *Current Issues in Tourism*, 22(15):1825–1840. DOI: https://doi.org/10.1080/13683500.2018.1553151.

Wang, Y. and Nepali, R. (2015). Privacy threat modeling framework for online social networks. In *Proc. International Conference on Collaboration Technologies and Systems*, pages 358–363. DOI: https://doi.org/10.1109/CTS.2015.7210449.

Watanabe, C., Amagasa, T., and Liu, L. (2011). Privacy risks and countermeasures in publishing and mining social network data. In *Proc. 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pages 55–66. DOI: https://doi.org/10.4108/icst.collaboratecom.2011.247177.

Wuyts, K., Van Landuyt, D., Hovsepyan, A., and Joosen, W. (2018). Effective and efficient privacy threat modeling through domain refinements. In *Proc. 33rd Annual ACM Symposium on Applied Computing*, pages 1175–1178. DOI: https://doi.org/10.1145/3167132.3167414.

Zeng, Y., Sun, Y., Xing, L., and Vokkarane, V. (2015). A study of online social network privacy via the tape framework. *Journal on Selected Topics in Signal Processing*, 9(7):1270–1284. DOI: https://doi.org/10.1109/JSTSP.2015.2427774.

Zheleva, E. and Getoor, L. (2009). To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In *Proc. 18th international conference on World wide web*, pages 531–540. DOI: https://doi.org/10.1145/1526709.1526781.