

## RESEARCH ARTICLE

# Privacy Threat MOdeling Language

ANDREY RODRIGUES<sup>1</sup>, MARIA LÚCIA BENTO VILLELA<sup>2</sup>,  
AND EDUARDO LUZEIRO FEITOSA<sup>1</sup>, (Member, IEEE)

<sup>1</sup>Institute of Computing, Federal University of Amazonas, Manaus, Amazonas 69080-900, Brazil

<sup>2</sup>IT Department, Federal University of Viçosa, Viçosa, Minas Gerais 36570-900, Brazil

Corresponding author: Andrey Rodrigues (andrey@icomp.ufam.edu.br)

This work was supported by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior-Brasil (CAPES) under Grant 001.

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by the Ethics and Research Committee of the Federal University of Amazonas under Application No. CAAE-63572122.0.0000.5020.

**ABSTRACT** Online Social Networks (OSNs) are becoming pervasive in today's world. Millions of people worldwide are involved in different forms of online networking. However, this ease of use of OSNs comes with a cost in terms of privacy. Users of OSNs become victims of identity theft, cyberstalking, and information leakage, which are real threats to privacy. Consequently, new solutions need to be developed for addressing the threat scenarios to which a user is potentially exposed. In this sense, this paper presents PTMOL (Privacy Threat MOdeling Language) as an approach for modeling privacy threats in an OSN domain. The proposed language is related to the attempt to mitigate privacy threats at the design level, thus promoting concern about threats in the stages preceding the development of OSNs. Two studies were conducted to evaluate the use of PTMOL at the design stages, which provided insights into the correctness, completeness, ease of use, usefulness, user satisfaction, and feasibility of the proposal. The results indicated that PTMOL can be incorporated into software development during the design phase. Via the language, we expect to support designers in making more pre-emptive decisions about user privacy risk, and help them to introduce privacy early in the development cycle of OSNs.

**INDEX TERMS** Empirical study, online social network, privacy threat, threat modeling.

## I. INTRODUCTION

Online Social Networks (OSNs) have become one of the principal technological phenomena of the Web, and have gained eminent popularity among its users [1], [2], [3]. OSNs offer various functionalities and services that attract a large number of users. These services combine user-created profiles with a communication mechanism that allows users to establish a virtual connection between people with common interests and backgrounds [4].

With the worldwide expansion of OSN services, people have devoted time and effort to maintaining and manipulating their online identity on these systems. However, the collection of data from OSNs and its subsequent processing is not always transparent or controllable by users. Generally, by agreeing to be part of a particular OSN, users give their

full consent to the providers through their terms of use to store and analyze their data and sometimes sell it to third parties for advertising and marketing purposes [5]. In addition, the service providers also control the databases in which user information is stored. In this sense, the large amount of personal data shared in these systems makes users desirable targets for attackers. An attacker can easily find relevant information about users, such as their identity or location and, with this data, he or she can commit identity theft, cyberstalking, and inference, which are real privacy threats.

A privacy threat is an undesirable event that can cause harm to a user through exposure and manipulation of data [6], [7]. The consequence is a breach of privacy that occurs when there is disclosure of personal information to unauthorized individuals or entities that use them for malicious purposes [2]. The Facebook – Cambridge Analytica incident is a prominent example of a privacy breach. In this case, Facebook shared personal data with Cambridge Analytica who used these data

The associate editor coordinating the review of this manuscript and approving it for publication was Shovan Barma<sup>1</sup>.

in political campaigns to influence public opinion without users having neither control nor knowledge of this disclosure [8]. This incident only reinforces the need to protect user privacy in OSNs, which are highlighted as the main channel for exploiting or executing privacy threats [9], [10].

As such, OSNs have attracted the attention of privacy researchers in both industry and in academic fields. There are many researchers that have presented their own solutions to protect users against privacy threats and breaches [11], [12], [13], [14] and, in general, these approaches are directed at mitigating threats and vulnerabilities and reducing the risks related to the functioning and architecture of these systems. However, there is still a lack of solutions that address privacy threat scenarios with a focus on the user. Even though mechanisms are implemented to allow users to protect their personal data by applying privacy settings defined by the OSN, these controls are not effective in preventing privacy threats. This could be related to the fact that there are still gaps in the prevention of privacy threats in the steps leading up to the development of OSNs.

Anticipating privacy concerns in the stages prior to the development of OSNs is a promising strategy for addressing personal data protection. This interest increases the credibility of using threat modeling methodologies and brings opportunities for developing new solutions that address this issue. Recently, we proposed PTMOL (Privacy Threat Modeling Language), a language that allows you to represent in a structured way all threat scenarios that affect user privacy on an OSN, as well as define countermeasures to prevent or mitigate the effects of threats [15]. This language was developed from evidence gathered in the literature and was empirically evaluated through experimental study. The first version of PTMOL was presented in Rodrigues et al. [15]. In the first paper, we presented a preliminary study of the language, but without detailing any improvements and refinements to it.

In this paper, we present a complete and updated version of the structure of PTMOL, and show the improvements implemented in the language. To investigate whether and to what extent the adoption of PTMOL enables designers to model privacy threats, this paper also presents a feasibility study conducted in order to analyze the acceptance of PTMOL from the point of view of novice designers. We also evaluated the correctness and completeness of PTMOL. In addition, an observational study was also carried out with the purpose of further consolidating the PTMOL modeling process. The results of both studies indicated that PTMOL can be incorporated into software development during the design phase. Via the language, we expect to support designers in making more pre-emptive decisions about user privacy risk, and help them to introduce privacy early in the development cycle of OSNs.

The following sections include the theoretical foundations in which the language is based and the related works to this research. Subsequently, the proposed language is described. Then, the experimental studies and their results are shown. Finally, conclusions and future perspectives for this research are presented.

## II. 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. Much of this content consists of personal information, and the online availability of which may pose a serious risk to user privacy. There are some questions to be answered in order to understand privacy threats in OSNs. First, what is privacy? Second, what is a privacy threat? Last, but not least, what is a privacy breach? In this section, we describe these concepts since they are extremely important in the context of this work.

### A. PRIVACY

According to the privacy regulation theory presented by Altman [16], privacy is defined as the individual's ability to control what information is disclosed, to whom, when, and under what circumstances. In this theory, privacy was conceived as a boundary regulation process in which individuals control the amount of information about themselves that can be disclosed to others. Privacy is therefore the individual's right to control his or her personal information and to know or restrict how it is collected, transferred, stored, and used.

Based on Altman's [16] theory, maintaining adequate privacy levels to protect personal information in a communication and social interaction environment is essential in order to preserve privacy. However, controlling data disclosure levels in OSNs can be difficult due to the peculiar characteristics of these systems, such as mass content sharing and transmission of information [17], [18].

### B. 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 [6], [7]. 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 [19]. 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.

### C. PRIVACY BREACH

A privacy breach occurs when private and confidential information is disclosed to unauthorized individuals [2], [20] and can be classified into four types [21], [22]: (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 [23]. In addition, commercial and government entities may also violate users' privacy for different purposes, such as targeted marketing, health screening, or political monitoring [24].

#### D. 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 [25]. 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 [26]. 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. Therefore, modeling potential threats during the design phase is an essential step in order to save significant resources that may be required for (re)design [27], [28].

The threat modeling process is composed of assets that are compromised by threats; threats that exploit vulnerabilities, which, when misused, result in breaches, and which represent a potential risk. Finally, countermeasures mitigate the harm caused by these threats; countermeasures that aim to protect the assets.

#### III. 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.

##### A. 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 [29]. 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 [30].

Using the STRIDE methodology, the general threat-modeling process comprises six steps. In summary, the first step aims at identifying the system assets that need to be protected. These assets can be, for example, web pages or the application's database server, among others. Following this, an overall system architecture should be created. The decomposition step seeks a more in-depth view of the system through the use of a DFD (data flow diagram), which helps visualize the functionalities and communication between the system components. A DFD uses the following four standard components: (i) external entity; (ii) data storage; (iii) process; and (iv) data flow. In the threat identification step, the STRIDE threat categorization scheme should be used and associated with each component of the DFD. Subsequently, in the threat documentation step, STRIDE provides a document for recording the identified threats. Finally, the last step recommends using a risk-assessment model to classify the threats by using a severity scale.

In a similar vein, Wuyts et al. [31] 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.

The second step of the methodology uses a custom table to map threats corresponding to the elements of the DFD created in the previous step. Each 'X' displayed in the mapping table is examined to determine if it represents a threat to the system. For this analysis, LINDDUN provides a set of privacy threat trees. These trees represent the most common attack paths for a LINDDUN threat category associated with a DFD element type. Finally, LINDDUN provides an extensive list of technologies that can be used to manage and mitigate elicited threats. The second step of the methodology uses a custom table to map the threats corresponding to the elements of the DFD that was created in the previous step. Each 'X' displayed in the mapping table is examined to determine whether it represents a threat to the system. For this analysis, LINDDUN provides a set of privacy-threat trees. These trees represent the most common attack paths for a LINDDUN threat category associated with a DFD element type. Finally, LINDDUN provides an extensive list of technologies that can be used to manage and mitigate elicited 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 [27] 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. [32] 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) [33]. 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.

## B. 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. [34] 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 [35] 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 analyzed, 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. [34] and by Wang and Nepali [35] 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. [9] 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



**TABLE 1.** Characteristics of the main methodologies for threat modeling.

Methodologies	Focus	System	Context
STRIDE [29]	Attack/Prevention	Generic	Security
LINDDUN [31]	Attack/Threat	Generic	Privacy
PASTA [27]	Risk	Generic	Security
hTMM [32]	Attack/Prevention	Generic	Security
Threat Model [34]	Attack/Prevention	OSN	Security
Framework [35]	Attack/Prevention	OSN	Security
Attack/Defense tree [9]	Attack/Prevention	OSN	Security
PTMOL [15]	Threat	OSN	Privacy

good knowledge of cybersecurity and, therefore, it does not provide guidelines to support professionals who have little knowledge in threat modeling.

Table 1 compares the methodologies presented during the related work section in terms of focus of interest, type of system and context for which the proposals are intended.

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.

#### IV. LITERATURE REVIEW

To address privacy threats in OSNs and integrate them into the PTMOL modeling process, we sought to identify and characterize them more comprehensively. For this, a thorough literature review was carried out. There are many privacy threats in OSNs that put user's data at risk. However, previous works do not investigate in detail the existing privacy threats in the OSN domain.

In order to identify and report the existing privacy threats in OSNs, a thorough analysis in several papers found in the literature was performed, noting how these threats were cited or described by the authors of the papers. Each paper was analyzed and the threats addressed in them were extracted.

After this analysis, a privacy threat diagnostic was created, which contained more than 30 threats. When analyzing this diagnosis, it was observed that many threats were described

**TABLE 2.** List of top privacy threats identified in literature review.

Threats	Synonyms	References
<b>Cyberstalking</b>	Stalking	[36] [37] [38]
	Digital stalking	[39]
<b>Information disclosure</b>	Dissemination	
	Content Disclosure	[40] [37] [11]
	Identity Disclosure Misuse data	[41] [42]
<b>Profile cloning</b>	Fake profile	[40] [12] [37]
	Cloned profile	[43] [44]
<b>Inference or Tracking</b>	Information extraction	
	Activity tracking	[7] [45] [35]
	Data mining Profiling	[12] [22]
<b>Reputation threat</b>	Discrimination	
	Embarrassment	[40] [37]
	Sybil attacks Data manipulation	
<b>Face recognition</b>	Image retrieval	
	Photo tagging	[7] [46] [47]
<b>Surveillance</b>	Corporate espionage	
	Monitoring	[37]
<b>Unauthorized recording</b>	Video call risk	
	Group video calls	[40] [48]
<b>Identity Theft</b>	Phishing	[36] [14] [49]
	Account Hacking	[50]
	Attribute Discovery	

with different nomenclature, but had the same meaning. To better understand the set of threats and arrive at a more accurate list, the main threats (those most cited or considered crucial in papers) were separated and joined up with their synonyms (those threats with different names, but with the same meaning). This analysis can be seen in Table 2.

Based on this threat diagnosis, our catalog indicating the most critical existing privacy threats in OSNs cited in the literature was created. This catalog was generated from the analysis performed on the papers identified in the literature. These threats can heavily impact user privacy in the form of disclosure, manipulation or misuse of private data. It should be noted that before arriving at the final catalog of threats, several revisions and refinements were carried out by the authors of the research, in order to consolidate the final artifact. Later, this catalog was integrated into PTMOL's threat modeling process. The next section describes in detail each threat identified in the literature review and how they can be used in PTMOL threat modeling.

#### V. PRIVACY THREAT MODELING LANGUAGE (PTMOL)

PTMOL is a privacy threat modeling solution focused on protecting user data [15]. 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.

Based on the PTMOL vocabulary, a set of elements was created that determine the language syntax. These elements are illustrated in Figure 1, and grouped according to their zone: sharing zone, risk zone, and leakage zone. They can be used at the end of the process to generate the threat model resulting from the modeling.

#### A. 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 [51]: (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 to Lowson [51], 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.

#### B. 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. In addition, this resource also enables the designer to think about actions that a potential attacker would carry out to exploit threats and put the user's assets at risk. 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 [36], [37], [38], [39].
- **Information Disclosure** - Information disclosure refers to the detection and extraction of information that was unintentionally disclosed [52]. 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 [11], [37], [40], [41], [42].
- **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 [12], [37], [40], [43], [44].
- **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 [7], [12], [22], [35], [45].
- **Threat to Reputation** - Sharing personal or sensitive information can make OSN users victims of a threat to

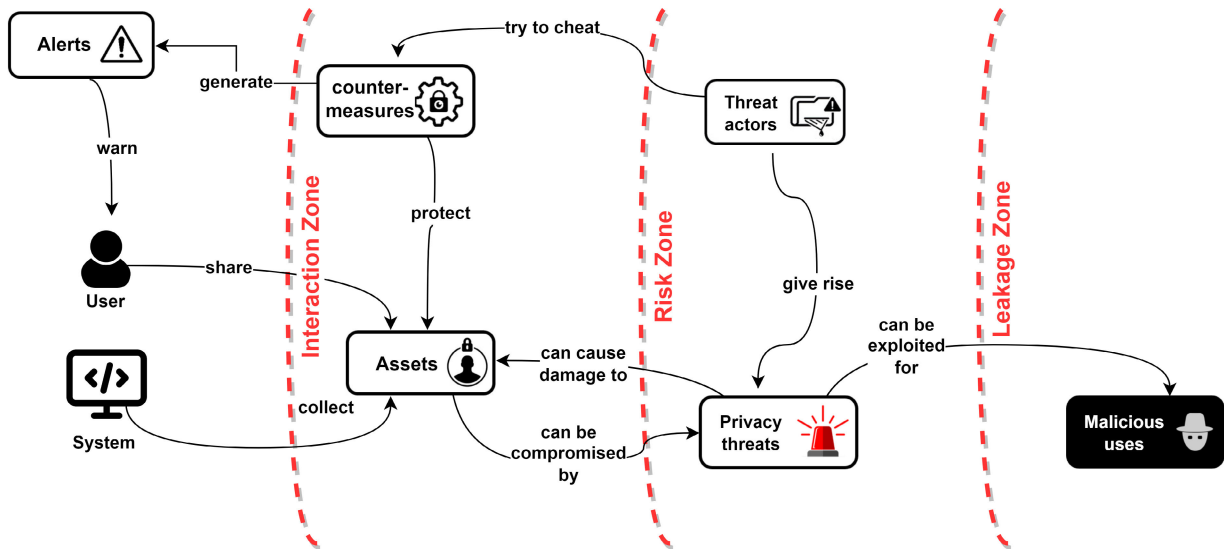


FIGURE 1. Overview on the relationships between PTMOL elements.

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 [12], [35], [40], [46]. 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 [7], [46], [47], [48].
- **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 [37].
- **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 [40], [48].
- **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 [14], [36], [49], [50].

### C. 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 [53], [54] and serve as a contribution to assist in formulating preventative countermeasures to address the threats identified with the language. Designers have the possibility to build mitigation strategies, which can be provided later to the development team, so they can consider them during the construction of the application. 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. In other words, 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

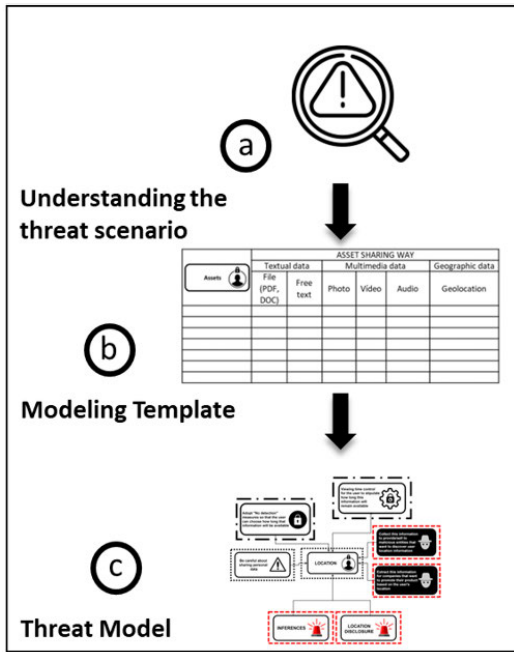


FIGURE 2. PTMOL methodology steps to be applied during a design phase.

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

**D. APPLICATION PROCESS**

Figure 2 illustrates how the PTMOL application process works. The language allows the designer to represent and consequently elaborate and refine their design in layers, i.e., bit by bit. Initially, the designer (Figure 2 element a) 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 (Figure 2 element b) 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

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 3. Template for asset identification and classification.

information has been analyzed, the designer must produce the threat model (Figure 2 element c) 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.

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 3 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.

There are assets that are not directly shared by users, but are collected or generated by the system itself. In general, OSN






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 4. Template for classifying assets collected by the system.





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 5. Template for identifying threats, malicious uses and threat actors.

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 4. 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.

### 2) IDENTIFYING THREATS, MALICIOUS USES AND THREAT ACTORS

The second step can be considered to be the main one in the PTMOL threat modeling process. At this stage, the designer must consult the language-integrated threat catalog and identify, based on a pre-defined set of threats, which of them may occur in relation to the asset under analysis. For each asset listed, one or more privacy threats must be identified. After that, the designer must indicate the threat agents, which can be inside or outside the system and breach the user's privacy. Threat actors can assume four values: (i) malicious member; (ii) provider; (iii); third-party app; and (iv) external sources. After associating the threat to the asset and indicating the threat agents, the designer must foresee the malicious uses, whose filling has free value. Figure 5 presents the template for identifying threats, malicious uses and threat actors.

### 3) IDENTIFYING MITIGATION STRATEGIES

Finally, in the last step, the designer will have to make strategic decisions that guarantee greater assertiveness in the


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 6. Template for identifying violated privacy properties.





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 7. Template for identifying mitigation strategies.

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 6.

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 7 presents the template for identifying mitigation strategies.

### 4) THREAT MODEL GENERATION

Figure 8 illustrates a diagram modeled with the elements of PTMOL. The illustration shows the result of a modeling process applied to the asset location. It can be observed that for the shared asset, two potential threats could occur: Inferences and Information Disclosure. Based on these threats, the

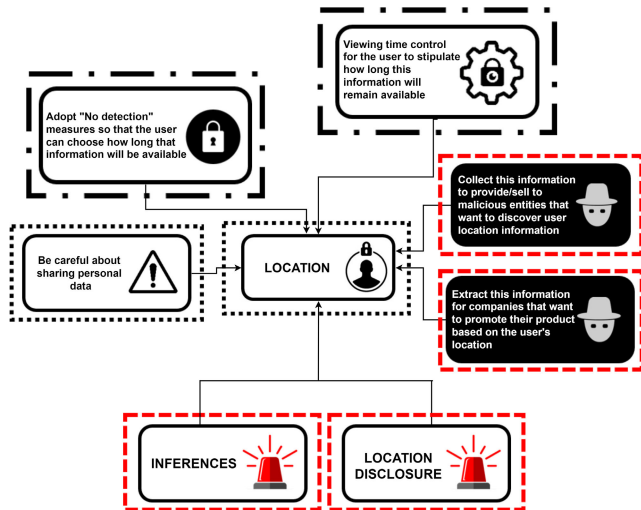


FIGURE 8. Diagram modeled with elements of PTMOL.

designer could establish actions that the attacker could carry out against the shared asset.

Regarding the inference threat, it can be seen that the model describes, as an malicious uses, the possibility of them disclosing the asset to a location-based place recommendation system. Many companies collect data to build complete profiles with the intention of selling products and recording user behavior. This behavioral analysis is usually done without the user's knowledge, with relevant implications for their privacy. Another threat highlighted in the diagram is the improper collection of this asset for malicious purposes, such as its disclosure to entities that want to manipulate these data to discover more information about the owner of the asset (user). As a prevention strategy, the designer establishes an alert to warn the user about the consequences of this disclosure. The designer also indicates a triggerable privacy feature and also a countermeasure to mitigate the threat and reduce the risk to an acceptable level.

## VI. CONSTRUCTION AND EVOLUTION OF PTMOL VIA EXPERIMENTAL STUDIES

Experimentation is the scientific process core and provides a systematic, disciplined, computable and controlled way of evaluating human activity [55]. According to Shull et al. [56], besides providing validation for different proposals, the use of experimental studies can also help in identifying problems present in them.

### A. FIRST STUDY: VALIDATION STUDY

The first study aimed to evaluate the initial version of PTMOL and understand its use in modeling privacy threats in OSNs. The results of this study are published in Rodrigues et al [15].

### B. IMPROVEMENTS IN PTMOL

The qualitative analyses of the first study led to a new version of the PTMOL. The description of some language elements

has been modified in order to make their definition clearer and eliminate redundancies. Another point that was reviewed was the "Control" and "Countermeasures" elements, for which some participants reported that these elements basically had the same meaning. In reviewing these PTMOL components, it was noted that the control element is also a form of countermeasure to prevent a threat. Therefore, the purpose of the element is strongly linked to that of the countermeasure. With that, it was decided to remove the "control" element from the language notation and leave the "prevention alert" and "countermeasures" elements as a mitigation strategy.

Another element that was modified was the "Attacker's Actions", which allows the designer to create a rationale on the possible actions that a malicious agent could perform when in possession of the assets. To make the element's purpose clearer, the name of the element was changed to "Malicious Uses", which tries to predict what malicious behavior the attacker might present when gaining access to the user's private data. After the improvements made to PTMOL, the second study was carried out with the purpose of testing its feasibility. The planning, execution and results of the second experimental study will be detailed in the next sections.

## VII. FEASIBILITY STUDY

Experimental studies should be conducted and repeated in order to improve the quality of the proposal that is being developed [55]. The knowledge used in the execution of the experiment should be made public to other researchers, thus enabling a better understanding and analysis of the proposal. In order to obtain data to improve the context of the use of PTMOL, a feasibility study was conducted.

Within the context of conducting experimental studies, the feasibility study is one of the first studies to be conducted to evaluate a newly created solution and verify its viability by means of the proposed objective [55], [56]. A feasibility study does not aim to obtain a concrete and definitive answer, but to capture data that can be used to refine the solution being tested and generate hypotheses about its use. In this sense, the purpose of this feasibility study was to answer the following question: "Is PTMOL effective in relation to the number of threats encountered"? This study evaluates the feasibility of PTMOL as a language for modeling privacy threats at design stage. The study analyzes the results of the application of PTMOL by a group of participants from a Computer Science course. The experimental design used in the PTMOL studies is based on the [31] and [57] protocols. The planning, execution, and results achieved in the study will be presented below.

### A. PLANNING

The study, which involved training and an evaluation of the application of PTMOL, was executed over a period of two days. On the first day, the participants received training on the language. On the second day, the participants applied PTMOL to a threat scenario. The detailed planning of the experimental study is reported below.

## B. PARTICIPANTS

Twelve participants from the Computer Science course of a higher education institution were selected. These participants attended the Computer Systems Security classes and were chosen by convenience criteria.

In order to ensure the voluntary consent of the participants in the study and respect ethical aspects, they authorized their participation in the research through an informed consent form (ICF). The participants were informed that they had full freedom to withdraw their consent at any stage of the research, without any penalty. Additionally, participants were required to complete a characterization form to identify their experience in systems modeling and privacy. The prior knowledge of the participants regarding systems modeling was classified as: (i) yes; if the participants had already performed modeling activities in undergraduate classes, in research or in software companies; and (ii) no; if the participants had never performed modeling activities. With respect to the participants' experience regarding privacy, this was categorized as follows:

- High level of experience (H): participants who had participated in more than five privacy projects in the industry;
- Medium-level experience (M): participants who had participated in between 1 and 4 privacy projects in the industry;
- Low level of experience (L): participants who had participated in at least one classroom privacy project.
- No experience (N): participants who had no knowledge about privacy or who knew only some privacy concepts (acquired in readings/lectures), but with no practical experience.

According to Fernandez et al. [58], students may have similar skills to less experienced professionals. In addition, these students are people trained in computing; therefore, they master the use of technologies and develop them. Thus, the students can be characterized as novice designers who are learning about threat modeling. By doing so, our study has the potential to show how these designers, who did not have previous knowledge of PTMOL, made sense of it and used it in a privacy threat design context.

After the application of PTMOL by the participants, they answered a post-study questionnaire to report their experiences during the modeling activities with the language. After the data collection, the participants were informed that they could still request the exclusion of the content provided in the questionnaires, in whole or in part.

## C. SCENARIO

The scenario used in the context of this study described a potential interaction of a user connecting in a content sharing social network for the first time. In general terms, the scenario demonstrated a user forming a profile with some personal information that would become publicly available. In addition, the user also provided a photo in his profile and posted a video with a caption that informed that he was going

on a trip. In the video, the user also disclosed his current location. Finally, the user made a purchase via the system and provided some data from his card. In this scenario, the privacy threats that could occur were not described since the objective was to observe whether the PTMOL methodology would lead the participants to detect the privacy threats present in the scenario.

## D. INSTRUMENTS

Several instruments were defined to support the study, such as (i) Informed Consent Form (ICF); (ii) participant profile characterization form; (iii) threat scenario; (iv) task script; (v) support material for the application of the PTMOL; and (vi) post-study questionnaire.

## E. TASKS

Participants were invited to employ PTMOL for the scenario provided, and perform the following tasks: (i) identify the assets; (ii) identify the threats; (iii) identify the malicious uses and threat actors; (iv) identify mitigation strategies; and (v) generate the threat model.

## F. HYPOTHESIS

Based on the research question of this study, the following null hypotheses (H01, H02 and H03) and corresponding alternative hypotheses (HA1, HA2 and HA3) were formulated:

### 1) CORRECTNESS

The first set of hypotheses refers to correctness, which defines how correctly the language employs its elements according to the established syntax. Instead of using the total number of errors made by the participants, correctness was measured through precision. In this sense, the null and alternative hypotheses were formulated as described below:

- H01: There is no difference between the number of correctly identified threats (true positives) versus the number of incorrect threats (false positives).

- HA1: The number of correctly identified threats (true positives) is greater than the number of incorrect threats (false positives).

### 2) COMPLETENESS

The second set of hypotheses refers to completeness, which defines how well the language presents the necessary information according to the modeling purpose. As in the first study, completeness was measured by means of recall. The null and alternative hypothesis are described below:

- H02: There is no difference between the number of correctly identified threats (true positives) versus the number of undetected threats (false negatives).

- HA2: The number of correctly identified threats (true positives) is greater than the number of undetected threats (false negatives).

### 3) PRODUCTIVITY

The third set of hypotheses refers to productivity, which evaluates how many valid threats are identified by the participants

in a given period of time. Productivity is defined as the number of correct threats (TP) per hour. The null and alternative hypothesis are described below:

- H03: The productivity of the threat modeling process that applies PTMOL is greater than or equal to one threat per hour.

- HA3: The productivity of the threat modeling process that applies PTMOL is less than one threat per hour.

### G. PARTICIPANT PREPARATION

The study was executed over two days. On the first day, participants received language training and, on the second day, they performed the application of PTMOL to the threat scenario provided. The training with the participants was divided into two stages lasting 1 hour each. During the first stage, general concepts about threats and privacy breaches in OSNs were introduced and a specified presentation of PTMOL was given. In the second stage, a threat scenario was demonstrated to the participants in order to illustrate the PTMOL modeling procedure. The scenario chosen as an example was different from the one chosen for the study, thus ruling out any bias. Upon completion of the training, the lead researcher provided general guidelines on the study protocol. These orientations included the participants' right to opt out of the study without any penalty.

### H. STUDY CONDUCT

The study was conducted in a research laboratory and provided computers for use by the participants. The lead researcher acted as a supervisor during the study, and was primarily responsible for assisting in the case of doubts regarding the process of applying PTMOL, taking due precaution not to influence the threat modeling activity.

Each participant received the artifacts of the study, as described in subsection VII-D, and performed the modeling activities individually. All artifacts were made available via Google Drive. Participants were required to describe the entire modeling process (and its logic) in a spreadsheet provided in the study. At the end of the study, all participants handed in the spreadsheet containing all the threats identified for each asset extracted from the scenario, the predicted malicious uses and the associated countermeasures, thus fulfilling all the anticipated tasks. The threats appear in the spreadsheet according to their order of discovery. In addition, the participants also delivered the generated threat model and annotated the total time spent modeling. After that, they answered the post-study questionnaire. It is worth noting that, during the modeling activity, the students did not receive any help from the researchers involved in the study. The study lasted approximately four hours.

## VIII. RESULTS

The documents completed by the participants were evaluated by two experts (the lead researcher and an assistant professor). The experts analyzed the assumptions contained in the templates and determined whether each of the identified threats was applicable to the scenario under analysis. More

**TABLE 3.** Reference solution showing type and number of threats per category.

Privacy threats	Number of threats
Profile cloning	6
Reputation damage	2
Cyberstalking	2
Disclosure of information	6
Surveillance	3
Face recognition	2
Identity theft	1
Tracking/Inference	2
Unauthorized recording	0
<b>Total</b>	<b>24</b>

specifically, the experts determined the number of correct threats (true positives) and incorrect threats (false positives) based on the definitions provided in Section VII. Correct threats were those that were a) relevant, privacy-related in the context of the provided scenario, and sound with respect to the assumptions documented by the participants; b) compatible with the PTMOL threat catalog; and c) documented with sufficient detail and reasoning. In addition, undetected threats (false negatives) were also accounted for.

### A. ORACLE

An oracle (reference solution) was created by two experts (the lead researcher and an assistant professor). This oracle provides a rough estimate of how many privacy threats could be found in the scenario under analysis. The experts applied

PTMOL to the scenario, which resulted in 24 threats as presented in Table 3. Although the oracle is the benchmark for the quantitative analysis of the study, the participants could make assumptions that differ from the oracle. Thus, the reference solution is used only as a guide for the researchers, who carefully examined the template with the assumptions made by each participant.

Information disclosure and profile cloning threats are the most prevalent threats in the threat landscape provided. Because the impact of information disclosure varies depending on how a particular asset is shared (for example, textual data, multimedia data, and usage data), the number of threats in this category tends to grow easily. The threat of profile cloning is also frequent in the landscape, as publicly disclosed personal data can be used to create a fake profile of the victim for the purpose of deceiving followers and for capturing private information.

### B. QUANTITATIVE RESULTS

Table 4 consolidates the results of the study conducted and presents a general synthesis of the threat modeling performed by each participant in the study. The first column (P) represents the code of each participant (denoted by P01, P02...). The second column (PE) indicates the participants' privacy experience. The third column (ME) indicates the participants' experience in system modeling. The fourth column (PT) represents the number of possible threats identified per participant. The fifth column (TP) presents the number of



**TABLE 4.** Summary of threat modeling result per participant.

P	PE	ME	PT	TP	FP	FN	TS	Pre.	Rec.
P01	N	Yes	17	14	3	10	3.45	82.35%	58.33%
P02	N	Yes	18	17	1	7	3.10	94.44%	70.83%
P03	N	Yes	19	12	7	12	3.55	63.16%	50.00%
P04	N	Yes	18	17	1	7	3.17	94.44%	70.83%
P05	N	Yes	17	16	1	8	3.35	94.12%	66.67%
P06	N	Yes	18	18	0	6	3.49	100.00%	75.00%
P07	N	Yes	16	15	1	9	3.25	93.75%	62.50%
P08	N	Yes	16	16	0	8	2.55	100.00%	66.67%
P09	N	Yes	20	20	0	4	2.45	100.00%	83.33%
P10	N	Yes	19	19	0	5	3.32	100.00%	79.17%
P11	N	Yes	19	18	1	6	3.13	94.74%	75.00%
P12	N	Yes	21	17	4	7	3.53	80.95%	70.83%

true positives, i.e., the number of threats identified correctly. The sixth column (FP) indicates the number of false positives identified, which are not threats. The seventh column (FN) reveals the number of false negatives, i.e., the number of undetected threats. The eighth column (TS) indicates the time (in hours) each participant spent to perform the threat-modeling process. The ninth column (Pre.) indicates the precision per participant, and the last column (Rec.) indicates the recall for each participant.

Based on the data provided in Table 4, it can be observed that all the participants reported having knowledge of systems modeling. This prior knowledge removes some threats to the validity of the study, for example, those related to not understanding the protocol of the study or a steep learning curve. On the other hand, all participants reported having no experience in privacy; they knew only some privacy concepts acquired from reading/lectures, but had no practical experience. Even though the participants indicated no experience regarding privacy, they stated that was with respect to research about privacy in OSNs, not about the importance of taking care of shared information and its possible threats. Furthermore, the fact that participants have no practical knowledge regarding privacy, but have experience in system modeling, is an important result in terms of the profile of the professional who will use PTMOL. That said, this study continues to look at the participants as novice designers who are learning about privacy and who have the potential to show how they (as designers who do not know PTMOL) made sense of it and used it in a threat-modeling context.

Overall, all the participants were able to detect privacy threats in the scenario provided with the aid of PTMOL. A low number of false positives was found. Regarding the number of true positives, in most cases, it is noted that the threats pointed out by the participants were correct. This higher number of true positives can be explained by two factors: a) previous training, which allowed the clarification of specific doubts regarding the process of applying PTMOL and also allowed a comprehensive discussion about the language elements; and b) experience of the participants, who had already attended an introduction to information security class in the first semester of the course and were attending a System Security class in a later semester, besides

their experience in software modeling. Therefore, it can be observed that the factor of PTMOL training and knowledge may be more important than the factor of privacy experience. This is clear when examining the data provided in Table 4, since all participants were able to map threat scenarios, even if they were not security and privacy experts. This indicates that PTMOL can aid software designers in threat modeling without requiring a high level of expertise in the area of privacy.

Most of the possible threats listed by the participants were true positives, i.e. they were identified correctly. Participants P06, P08, P09 and P10 detected the highest number of threats in the scenario and all were correct, which indicates 100% precision in their threat diagnoses. However, participant P03 obtained the lowest precision (63.16%) and also had the highest number of false positives in the threat modeling. Furthermore, although PTMOL enabled the identification of correct threats, not all threats present in the scenario were detected. This justifies the number of false negatives and relatively low recall per participant.

### C. DESCRIPTIVE STATISTICS

In order to analyze the quantitative results more specifically, statistical analyses were performed using the Shapiro-Wilk normality test. The normality test tests the hypothesis that the data present a normal distribution. In the case of smaller samples (<30 cases), the Shapiro-Wilk test is the most appropriate [59]. In these tests, if the significance of the normality test is less than 0.05, then the sample distribution is not normal. If it is greater than 0.05, it can be said that the sample distribution is normal [59]. The normality test showed that the feasibility study data do not have normal distribution ( $p=0.001$ ).

According to Lazar et al. [59], when a sample does not follow a normal distribution, a non-parametric test should be used. For this, the Wilcoxon test was selected. In general, the Wilcoxon test is a hypothesis test for comparing the difference between two measures of the same sample, i.e., when the participants' results are measured under two different conditions. To perform the comparison, the data are ranked according to the difference between the two paired measures. At the end, the Wilcoxon test will give a hypothesis result, in which one should reject the null hypothesis when  $p<0.05$  and accept that there is a difference between the compared measures. To represent a summary of the results of these analyses, the boxplot graph was used. The analyses were performed using the statistical tool SPSS V. 23, considering an alpha (significance level) of less than 0.05 to refute the null hypothesis.

#### 1) CORRECTNESS

The first set of hypotheses refers to correctness, as described in subsection VII-F. In this sense, the Wilcoxon test was applied to determine whether there was a statistical difference between the number of true positives in relation to the number

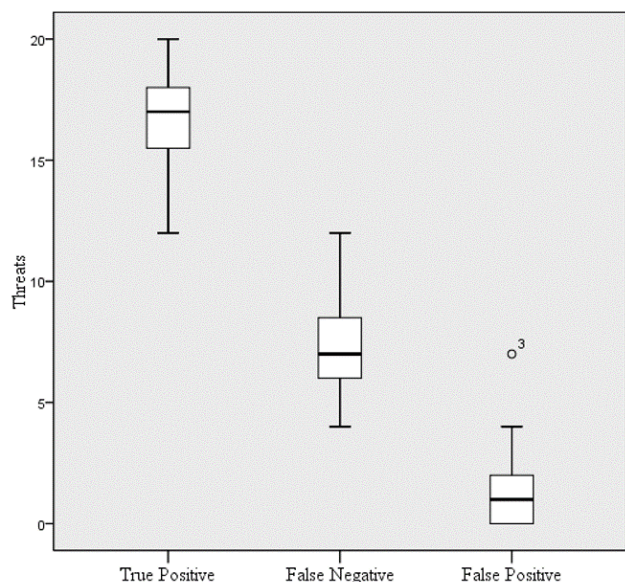


FIGURE 9. Boxplot comparing the true positives, false negatives and false positives.

of false positives. Thus, as a hypothesis for the statistical test, we had the lack of difference between the means of the measurements.

Figure 9 presents the boxplot comparing the true positives (correct threats), false negatives (undetected threats) and false positives (incorrect threats). Based on the graphical representation in Figure 9, it can be observed that the number of false positives is much lower when compared to the true positives. The mean for the number of true positives is 16.58 (with a standard deviation of 2.193) with a 95% confidence interval (one-sample Wilcoxon test). On average, only 1.58 false negatives (standard deviation is 2.109) were found, with a 95% confidence interval. As such, the Wilcoxon test confirmed that the number of true positives was significantly higher than the number of false positives ( $p=0.002$ ). Therefore, there is evidence to reject the null hypothesis H01. In summary, these results show that PTMOL identifies a higher number of correct threats than incorrect threats, and evidences a good level of correctness.

## 2) COMPLETENESS

The second set of hypotheses refers to completeness, as described in subsection VII-F. In the context of completeness, the Wilcoxon test was applied to determine whether there was a statistical difference between the number of true positives in relation to the number of false negatives. Based on this, the hypothesis for the statistical test was that there was no difference between the means of these measures.

As illustrated previously in Figure 9, it can be observed that the number of false negatives (threats not detected or not perceived in the scenario) is lower than the number of true positives. When relating the two measures using the

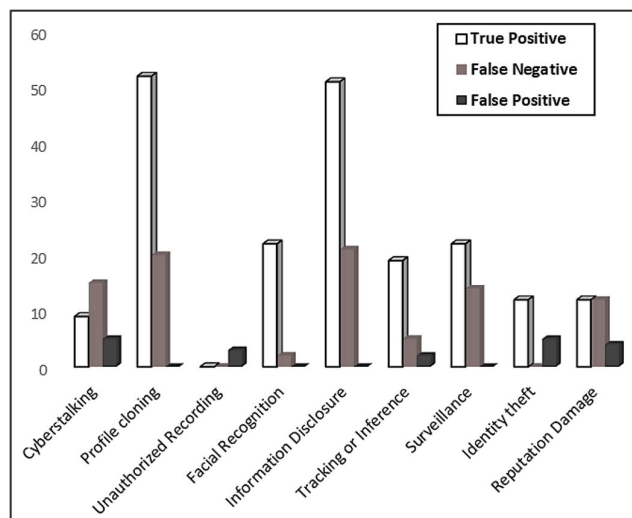
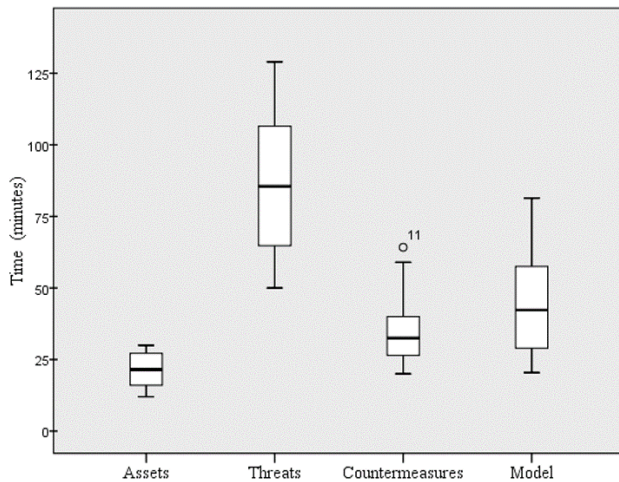


FIGURE 10. Average number of true positives, false negatives, and false positives for each threat.

non-parametric Wilcoxon test, a statistical difference was also identified ( $p=0.003$ ). The results of the statistical test support the alternative hypothesis HA2 - “The number of correctly identified threats (true positives) is greater than the number of undetected threats (false negatives)” and, therefore, rejects the null hypothesis H02.

Figure 10 presents the average number of true positives (white bars), false negatives (gray bars), and false positives (black bars) for each threat. Similar to the oracle, information disclosure and profile cloning were the threats most often pointed out by participants. Cyberstalking and identity theft are the ones that obtained the highest number of false positives. This can be explained by the fact that the threats of profile cloning and identity theft have relatively similar semantics, which may have led to some confusion during some points of the modeling. Such an issue indicates that the description of these threats should be refined in order to avoid confusing the concepts. The threat of unauthorized recording does not apply to the scenario provided in the study. Overall, all participants were able to detect most of the threats present in the evaluation scenario. This indicates that PTMOL was able to assist in detecting a considerable number of correct threats, thus evidencing its practical viability as a privacy threat modeling language.

The data provided in Figure 10 shows that the participants were able to detect most privacy threats, but some threats were not detected or perceived in the modeling scenario, which resulted in cases of false negatives. Although the threats of profile cloning and information disclosure obtained the highest number of correct diagnoses (true positives), at certain points in the modeling, neither were detected or perceived as threats, which also resulted in them presenting the highest proportion of false negatives. The facial recognition and inference/tracking were the threats that obtained the lowest number of false negatives.



**FIGURE 11.** Boxplots for the amount of effort devoted (time spent) by participants to each step of the PTMOL modeling process.

### 3) PRODUCTIVITY

In addition to the set of hypotheses formulated for completeness and correctness, a hypothesis for productivity was also formulated, as described in subsection VII-F. Figure 11 presents the boxplots that summarize the amount of effort devoted (time spent) by participants to each step of the PTMOL modeling process. The asset identification step took an average of 4.33 hours (asset boxplot). The threat and attacker action identification step lasted an average of 17.39 hours (boxplot threats). The countermeasure selection step had an average of 7.2 hours spent (boxplot countermeasures). Finally, the threat model generation step took an average of 8.91 hours (boxplot model). Therefore, participants spent an average of 37 hours on the PTMOL stages, most of which was devoted to the threat identification stage, as expected.

To calculate productivity, the amount of effort was used as a parameter for comparison with the actual effort made. Since productivity is interested only in correct results, we considered only the number of correctly identified threats (true positives) per the total time spent (real effort), as formulated in the hypothesis. On average, the productivity of the participants was 5.26 threats per hour. This means that productivity is much higher than expected and the null hypothesis HOP can be rejected.

#### D. ANALYSIS OF PARTICIPANTS' PERCEPTIONS

The participants indicated their degree of acceptance of PTMOL via a post-study questionnaire. This questionnaire was designed based on the indicators of the TAM (Technology Acceptance Model) model [60]. From the theoretical foundation provided by TAM, three main indicators were chosen:

- **Perceived ease of use:** Defines the degree to which the participant believes that using PTMOL to model privacy threats in OSNs would be effortless.

**TABLE 5.** Participants' perception regarding the ease of use of PTMOL.

N°	Variables	DA(%)	DD(%)
F1	PTMOL is easy to learn	91.67%	8.33%
F2	It was easy to use PTMOL to model privacy threats	83.33%	16.67%
F3	The elements of PTMOL are clear and easy to understand	75.00%	25.00%
F4	PTMOL is easy to use	91.67%	8.33%

DA = Degree of agreement, DD = Degree of disagreement.

- **Perceived usefulness:** Defines the degree to which the participant believes that PTMOL could improve their performance in modeling privacy threats in OSNs.
- **Perceived satisfaction:** Defines the degree to which using PTMOL to model privacy threats in OSNs is perceived as pleasurable, over and above any performance consequences of use.

For each indicator, a set of variables was created with a scale consisting of six points. The scale used is ordinal in nature, ranging from 6 (strongly agree) to 1 (strongly disagree). The degree of agreement grows in accordance with the greater the number of points. As suggested by Laitenberger and Drayer [61], the neutral point (neither agree nor disagree) was not used in the ordinal scale, since it does not allow us to identify the inclination (positive or negative) of the participants. In addition, not using the neutral point helps to avoid the bias of central tendency in ratings, thus forcing participants to judge the result as adequate or inadequate.

#### 1) PERCEIVED EASE OF USE

Table 5 presents the results of the participants' perception regarding the ease of use of PTMOL for modeling privacy threats. Overall, the data presented in Table 5 indicate positive results for all variables of the indicator in question. However, there were also disagreements involving some variables. Some quotes from the participants indicate factors that may have influenced this result:

"Although there are only a few elements in the annotation, some were not clear to me" - P12.

"It is easy to learn the language, but the process of modeling is difficult. It requires time and a lot of attention" - P07.

"I found it easy to use, although it demands a certain level of attention to detail in the modeling scenario" - P03.

"The language is simple; however, using it for the first time seems a bit complicated due to the amount of information, but it wouldn't be hard to make it a habit" - P01.

The quotes made by the participants indicate that, overall, the PTMOL language is easy to learn and use. However, the language requires an inherent effort regarding the application process. Because it is a solution that is proposed to be applied at the design level, the results produced by the participants need to be detailed enough to ensure a quality interpretation of the threat scenario to which a user may be exposed. Therefore, one can observe that PTMOL has a relevant degree of ease of use, but requires a peculiar effort in terms of time spent.



**TABLE 6. Participants’ perception of usefulness of PTMOL.**

N°	Variables	DA(%)	DD(%)
U1	Using a language like PTMOL, I would be able to model privacy threats more quickly	91.67%	8.33%
U2	Using PTMOL would improve my performance in modeling privacy threats (I believe I would identify a greater number of threats in a shorter time than it would take without using this approach)	100.00%	0.00%
U3	Using PTMOL for modeling privacy threats would increase my productivity	100.00%	0.00%
U4	I find PTMOL useful for modeling privacy threats	100.00%	0.00%

DA = Degree of agreement, DD = Degree of disagreement.

### 2) PERCEIVED USEFULNESS

Table 6 presents the results of the perception of usefulness of PTMOL for modeling privacy threats. The usefulness indicator usually indicates a subjective probability perceived by the user that the proposed solution can improve the performance regarding the object of use. In this sense, analyzing the participants’ perception regarding the usefulness of PTMOL, it is possible to note positive results for variables U2, U3 and U4. Some of the quotes justify the results:

- “It is quite interesting to model threats with PTMOL” - P01.
- “I found it very useful to model threats with the language because it has a simple, brief and self-explanatory procedure” - P10.
- “A very important approach and definitely made me think about privacy in a way I hadn’t thought about it before” - P11.
- “It allows us to perform a well-made and valid assessment, besides raising questions that address important privacy issues” - P05.

### 3) PERCEIVED SATISFACTION

Regarding the perceived satisfaction with PTMOL for threat modeling, positive results were obtained for all statements according to the participants’ opinions. There were no disagreements, as shown in Table 7, in relation to the variables of the indicator in question, thus indicating that PTMOL, although it has an inherent effort in relation to its context of use, it provides a good user experience during its application. However, some participants indicated the profile of the professional who will use PTMOL as a factor that may influence the user experience:

- “I believe that the person has to have practice and experience in privacy and security, if the person does not have this, it can impact on the application and make the modeling process tedious” - P03.
- “PTMOL is good for those who already have knowledge” - P02.

## IX. DISCUSSION

The quantitative results of the experimental study showed good correctness (above 80%) and completeness (above 60%)

**TABLE 7. Participants’ perceived satisfaction of PTMOL.**

N°	Variables	DA(%)	DD(%)
S1	Using PTMOL can be enjoyable	100.00%	0.00%
S2	The current process of using PTMOL is pleasurable	100.00%	0.00%
S3	I had fun using PTMOL	100.00%	0.00%

DA = Degree of agreement, DD = Degree of disagreement.

in relation to the purpose of the language. The perception of usefulness, ease-of-use and satisfaction was generally positive, although some participants disagreed with the ease-of-use aspect. From these analyses, it was possible to understand some points that caused some difficulty in applying the PTMOL modeling process. This could be an indicator that some elements of PTMOL may not be clear and understandable. This question corroborates the assumption made in the analysis of the TAM, in which there was disagreement about the ease of use of the language. Although two participants indicated disagreement with the statements that assessed clarity and comprehension, overall, PTMOL was perceived as useful.

The comments made by the participants highlight a factor that should be observed regarding the methodology of PTMOL, i.e., the need for prior knowledge in security and privacy of systems. In principle, PTMOL was proposed to be applied by software designers without necessarily requiring technical knowledge from them. All the participants in the study were students with a certain degree of academic knowledge in software modeling and system security and privacy, but who had no technical knowledge regarding the background topic. Students are less experienced professionals, nonetheless they are novice designers.

In this sense, the results indicate that the technical knowledge factor is not considered relevant for applying PTMOL, since all the participants, who were not experts, were able to execute the entire language application process and produce satisfactory results. The self-explanatory features and procedures of PTMOL serve as a guide to assist in modeling and ensure an effective privacy threat design. Therefore, it can be concluded that the security and privacy expertise factor should not be seen as a prerequisite for running PTMOL. The next section describes the planning, execution and results of a new study with PTMOL.

## X. OBSERVATIONAL STUDY

Once the results obtained with the previous studies had indicated the validity and viability of PTMOL, a new study was then carried out with the purpose of further consolidating the PTMOL modeling process. Thus, an observational study [56] was carried out in order to better understand the process used by designers when applying PTMOL during a modeling of privacy threats, and also identify the situations in which the difficulties in using PTMOL may occur. According to Shull et al. [56] in an observational study, data can be collected in either an observational or in an inquisitive way.



**TABLE 8.** Characterization of the participants in the observational study with PTMOL.

Participants	Group 01	Group 02	Group 03	Group 04
Female gender	2	0	3	2
Male gender	2	4	3	3
<b>Total</b>	<b>4</b>	<b>4</b>	<b>6</b>	<b>5</b>

Observational data can be collected during the use of a solution, without the interference of the researcher, while inquisitive data is usually collected after finishing an evaluation, where the researcher asks participants about usage aspects related to the solution.

For the context of this study, both observational and inquisitive techniques were applied. For the collection of observational data, the design rationale [62] technique was used as a basis to record the improvement decisions for PTMOL. For the collection of inquisitive data, the focus group technique [63] was used.

### A. PLANNING

The study participants were nineteen undergraduate students of Computer Science and Software Engineering courses at a local university. Participants were informed the reason for the research and how the data obtained through it would be used, so that they could make their decision fairly and without embarrassment. Only after signing an informed consent form was the research initiated. Participants were required to form groups consisting of four to six members. Unlike previous studies, in which each participant performed their threat modeling individually, for the context of this study, the participants were to perform the modeling activities in groups. The total number of groups formed by the participants was four. Table 8 presents the characterization of the participants in the observational study with PTMOL.

### B. EXECUTION OF THE OBSERVATIONAL STUDY

The study was planned to be executed over three days. On the first day, participants received a general training on the PTMOL application process and tested the threat-modeling steps for the scenario provided. The scenario used was the same as in the previous study. This training lasted approximately two hours. The scenario used as an example during the training was different from the one chosen for the study, thus ruling out any possibility of bias. This first stage also functioned as a pre-test and allowed any possible doubts about the process to be cleared up. After the training was completed, the researcher provided the main information about the study protocol.

On the second day of the study, in groups, the participants carried out threat modeling for the provided scenario, and each team applied the following tasks: (i) identify assets; (ii) identify privacy threats; (iii) prevent malicious uses; and (iv) identify countermeasures.

At the end of the second study day, the teams delivered the modeling templates containing all the threats identified in

the scenario, the anticipated malicious uses, and the associated countermeasures. This step lasted for approximately two hours. Finally, on the third and final study day, data collection on the PTMOL usage experience took place, which will be detailed in the next subsection.

### C. DATA COLLECTION

After completing the second step of the study, for data collection purposes, the students were asked to report their experiences and perceptions when performing the PTMOL modeling activities. In order to obtain these qualitative reflections and gain new insights regarding the PTMOL application process, two techniques were used for data collection, focus group and design rationale. Next, we describe how each technique was applied.

#### 1) FOCUS GROUP

The first part of data collection with the participants was carried out through a focus group, a technique that allows data to be obtained from group meetings and enables the understanding of the population under analysis. It can be used to understand different perceptions and attitudes about a solution [63]. The script used to apply this technique was based on the work of De França et al. [64]. During the focus group session, participants discussed the main positive and negative aspects related to the usefulness, ease of use and ease of learning of PTMOL. To encourage discussions and provoke the teams to expose their different perceptions, the dynamics of lovers x haters [64] were used in the focus group. During this dynamic, the participants given the role of lovers presented arguments in favor of PTMOL, while the haters opposed the team with arguments critical of the language.

From this, two teams were created to apply the focus group and each participant was allocated to a specific team. The choice of roles for each member of the teams (lover or hater) was defined by drawing lots. There was a greater number of members for the haters team, since the objective of the focus group was to obtain relevant insights about PTMOL's application process and collect opportunities for increments. To conduct the discussion with the lovers x haters dynamic, a board was used with three topics to be debated, each referring to the usefulness, ease of use and ease of learning of PTMOL (Figure 12). Teams had 10 minutes to internally discuss two arguments on each topic at hand. After this internal discussion about the topics shown in Figure 12, they recorded each argument in post-its and attached them to the board according to the specific topic. Afterwards, the focus group session was initiated and, in the following order, discussed: (i) usefulness of PTMOL; (ii) ease of use of PTMOL and ease of learning of PTMOL. Teams were encouraged to read their arguments and argue about them against each other. After the first argument, an opposing team continued the discussion by rebutting the previous argument. This flow was followed until all teams had presented their arguments.

Using PTMOL to model privacy threats in OSNs					
LOVERS 😊			HATERS 😡		
It is useful because...	It is easy to use because...	It is easy to learn because...	It is not useful because...	It is difficult to use because...	It is difficult to learn because...

FIGURE 12. Focus group board.

Two researchers were involved in conducting the focus group. One played the role of mediator and led the discussions to keep the teams focused, and encouraged the participants to expose their arguments for or against the aforementioned topics and discuss their opinions, according to their defined roles. At the same time, the other researcher wrote down the observations regarding the dynamics used. All audio from the focus group session was recorded for later analysis. The arguments provided in the post-its and the notes taken by the researcher during the observation study were also used for data analysis.

## 2) DESIGN RATIONALE

To collect suggestions for improvements and refinement opportunities on the use of PTMOL, after the end of the data collection session via the focus group, the teams were reunited to record the decisions and suggestions for improvement through a template based on design rationale (DR). In general terms, the DR technique can be applied with the purpose of registering the reasons and justifications regarding a decision, alternatives that were considered or discarded, or the arguments that led to the final design decisions.

Decisions to be recorded could be mainly related to doubts regarding the application phases of the PTMOL modeling process, doubts about some element and association between them, or general doubts about any PTMOL application resource. Figure 13 illustrates an example of a design decision record provided to teams.

## D. DATA ANALYSIS PROCEDURE

The data collected during the observation study were transcribed and subsequently imported and analyzed using Atlas.ti<sup>1</sup> software. Data were analyzed using Grounded Theory (GT) procedures. Grounded Theory is a qualitative research method that uses a set of systematic data collection and analysis procedures to generate, elaborate and validate substantive theories about essentially social phenomena [65]. GT is based on the idea of coding, which is the process of analyzing data. During coding, concepts (or codes) and categories are identified. A code indicates a phenomenon of interest that has meaning for the researcher [66]. Categories are

<sup>1</sup><https://atlasti.com/>

FIGURE 13. Document for recording the design rationale decision provided to the teams.

groupings of code put together at a higher level of abstraction. Of the GT procedures, open coding and axial coding were used, but not selective coding. Open coding involves sharing, analyzing, comparing, conceptualizing, and categorizing data. Axial coding examines relationships between identified categories. Selective coding refines this entire process by identifying a core category to which all other categories are related.

Initially, open coding was performed (first phase) to associate codes with quotes from transcripts. Then, the codes were grouped according to their properties, thus forming concepts that represent more abstract categories. Open coding procedures encourage the constant creation of new codes and their merging with existing codes as new evidence and interpretation data emerge. Finally, the codes were related to each other – axial coding (second phase). Once prepared, the codes and networks identified in the categories were reviewed and analyzed by other researchers. The identified codes and categories underwent successive revisions, and, in the end, 37 codes were produced, which were associated with 3 categories: PTMOL Structure, Difficulty in using PTMOL and Perception of PTMOL.

The GT procedures permitted an in-depth analysis of PTMOL, comparing and analyzing the relationship between the codes and the categories produced. Since the intention of this study is not to create a theory, selective coding (third phase of the GT method) was not performed. The open and axial coding phases were sufficient to understand the positive and negative aspects related to the usefulness, ease and difficulties involved in PTMOL’s application process. In addition, it was possible to obtain the answer to the research question of the study after the execution of the open and axial coding phases.

## E. RESULTS OF THE OBSERVATIONAL STUDY

### 1) RESULTS OF THE FOCUS GROUP

The codes identified in the transcripts were grouped according to their properties, thus forming concepts that represent categories. Together with other researchers, these categories

were analyzed with the aim of providing greater clarity about the phenomenon of interest.

Figure 14 presents the coding result for the PTMOL structure category. This category shows the codes derived from the participants' comments regarding the organization of PTMOL's application process. The codes are presented followed by two numbers that represent, respectively, the degree of grounding (groundedness) and the theoretical density (density). The degree of substantiation indicates the number of citations with which the code is associated. The degree of theoretical density indicates the number of relationships of the code with other codes. In addition, there is dimensional variation, which explains the causes and effects for a given category.

According to Glaser [67], the relationships between the codes, known as connectors, can be defined by the researcher. To observe the dimensional variation, two connectors were proposed: "it is evidence of ease" and "it is evidence of usefulness". "It is evidence of ease" shows a positive variation for the PTMOL structure, where the language application process is cited as being easy to use and learn. "It is evidence of usefulness" also presents a positive variation for the PTMOL structure, showing the language elements and resources considered appropriate and useful for threat modeling.

Based on the illustration represented in Figure 14, in relation to the structure of PTMOL, some important evidence can be noted that point to the ease of use of the language. An example of this evidence can be seen in the code "has an easy-to-understand structure for filling in", a code related to five comments (degree of reasoning of the code is equal to five). In addition, several other comments indicate evidence regarding the usefulness of PTMOL's elements and resources. One of the main comments highlighted by the participants refers mainly to the self-explanatory capacity of the language's modeling steps. The codes "it has elements that explain what they refer to well", "it is self-explanatory" and "the categories of threats are highly explanatory and give valid examples" are demonstrations of this. Other codes indicate to the relevance of PTMOL's resources for diagnosing privacy threats in OSNs, such as "it has a wide threat-classification catalog", "it allows the capture of threats" and "all the most common cases of violations have already been cataloged".

Figure 15 presents the relationships between the codes in the category "difficulty of using PTMOL". To observe the dimensional variation, only one connector was proposed: "it is evidence of", which links codes related to aspects that the participants considered as difficulties in the application of the language. Based on the codes represented in Figure 15, it is possible to observe that there is evidence of difficulties in relation to PTMOL's catalog of threats, which was captured through the codes "it is necessary to reread the catalog of threats several times" and "it is a little hard to remember what the threat addresses just by name." In fact, the threat catalog can or needs to be consulted several times during

the threat identification stage, especially when a designer is not familiar with some concepts about them. However, this issue should not be considered as a problem, but rather as an effort inherent in the application procedure, which, as it is a conceptual modeling at the design level, requires greater effort on the part of the person applying it.

It can also be observed, through the degree of reasoning equal to three, that the codes "too much information to be filled in" and "the application process is very laborious" also indicate the need for a greater effort to apply PTMOL. This shows that there is time and cost involved in the process of applying the language, but that they are fundamental to guarantee an effective and complete modeling of privacy threats in OSNs. The codes "it is not very intuitive" is refuted by the code "the categorization of assets and threats is intuitive".

Another code, "prior training is required to use the methodology", can be seen as a potential difficulty, but not as a limitation of the proposal, since the entire methodological procedure requires prior training when applied for the first time. Although it is known that the authors of PTMOL will not be present to conduct training at the time of use, the objective of the proposal is to effectively make the application process self-explanatory, so that future users of the language can understand it without prior training. The previous category, PTMOL structure, indicated relevant evidence about the self-explanatory capacity of the language.

Finally, Figure 16 presents the relationships between the codes in the "Perception of PTMOL" category. To observe the dimensional variation, the original GT connector, "is a", was used, which connects codes related to the participants' perceptions of general aspects, whether positive or negative, of PTMOL's elements and resources. Some codes highlight that PTMOL's application process can be complex and generic; "it has a complex process" and "it can have a very generic process". However, both codes have a low degree of justification, with only 1 degree. Other codes, such as "there are many classifications and details", "there are many steps in the asset and threat collection/analysis process", "each step has a lot of concepts" and "it is an extensive technique", were not perceived as problems or obstacles related to PTMOL's methodological process, but rather as important points that demonstrate that the language produces detailed and complete guidance for effective modeling of privacy threats at the design level.

Codes such as "in an agile development cycle it would be impracticable to maintain the documentation" and "if many assets were identified, the documentation expands quickly" bring an interesting argument about phases of software development into which PTMOL cannot be incorporated. In its design, PTMOL is intended to be applied in order to anticipate the diagnosis and prevention of privacy threats at the design level of OSNs. In fact, in an agile development cycle, it would be unfeasible to use it, since one of the agile values, working software is better than comprehensive documentation, is distinguished from the central purpose of PTMOL, which has extensive documentation to

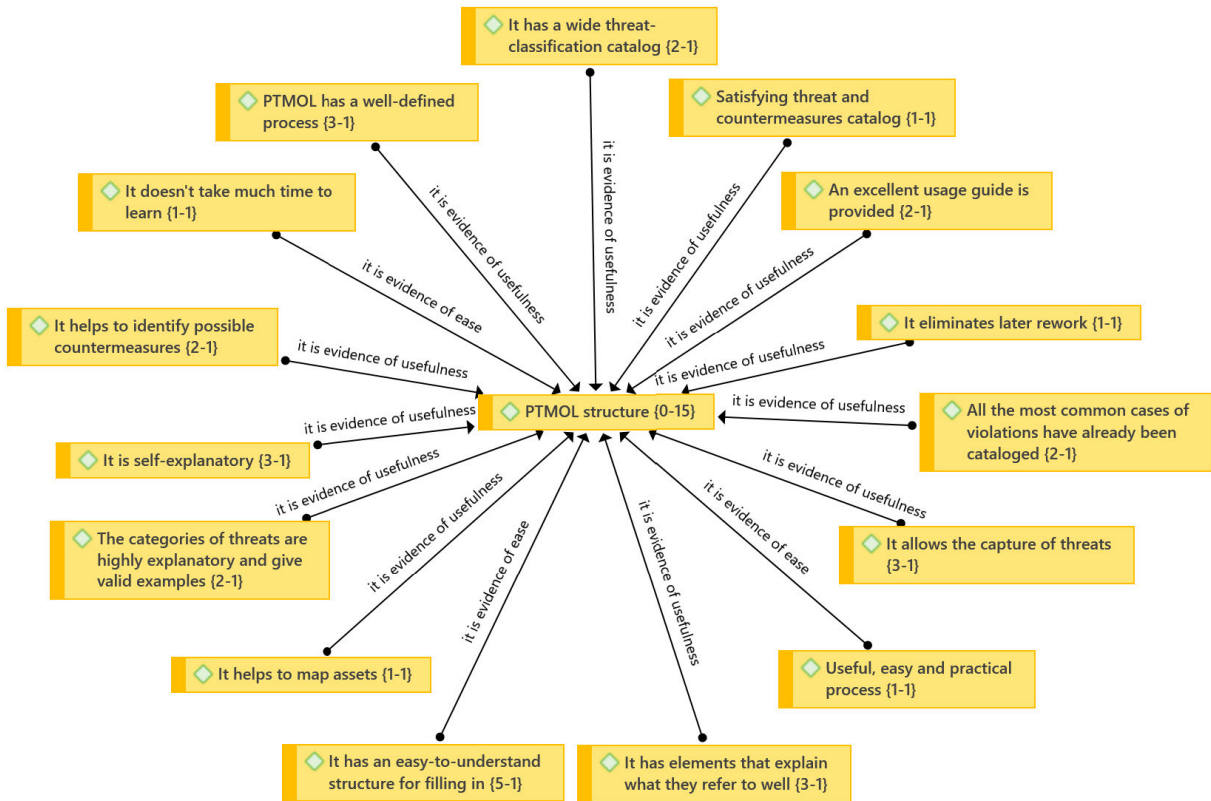


FIGURE 14. Codes related to the teams' perception of the PTMOL structure.

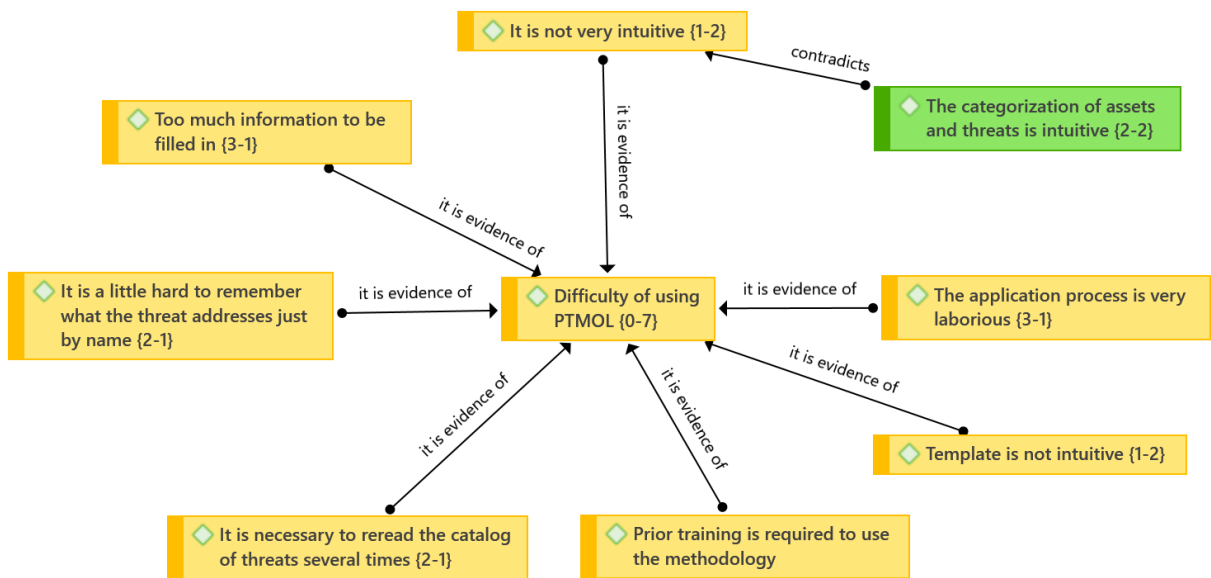


FIGURE 15. Codes related to the teams' perception of difficulty of using the PTMOL.

map all threat scenarios that a user could potentially be exposed to. Finally, codes such as “it takes time” again emphasize the time and effort dedicated to the application of PTMOL.

## 2) RESULTS OF DESIGN RATIONALE

After the end of the data collection session via the focus group, the participants met again with their teams to record decisions about the PTMOL modeling process as well as



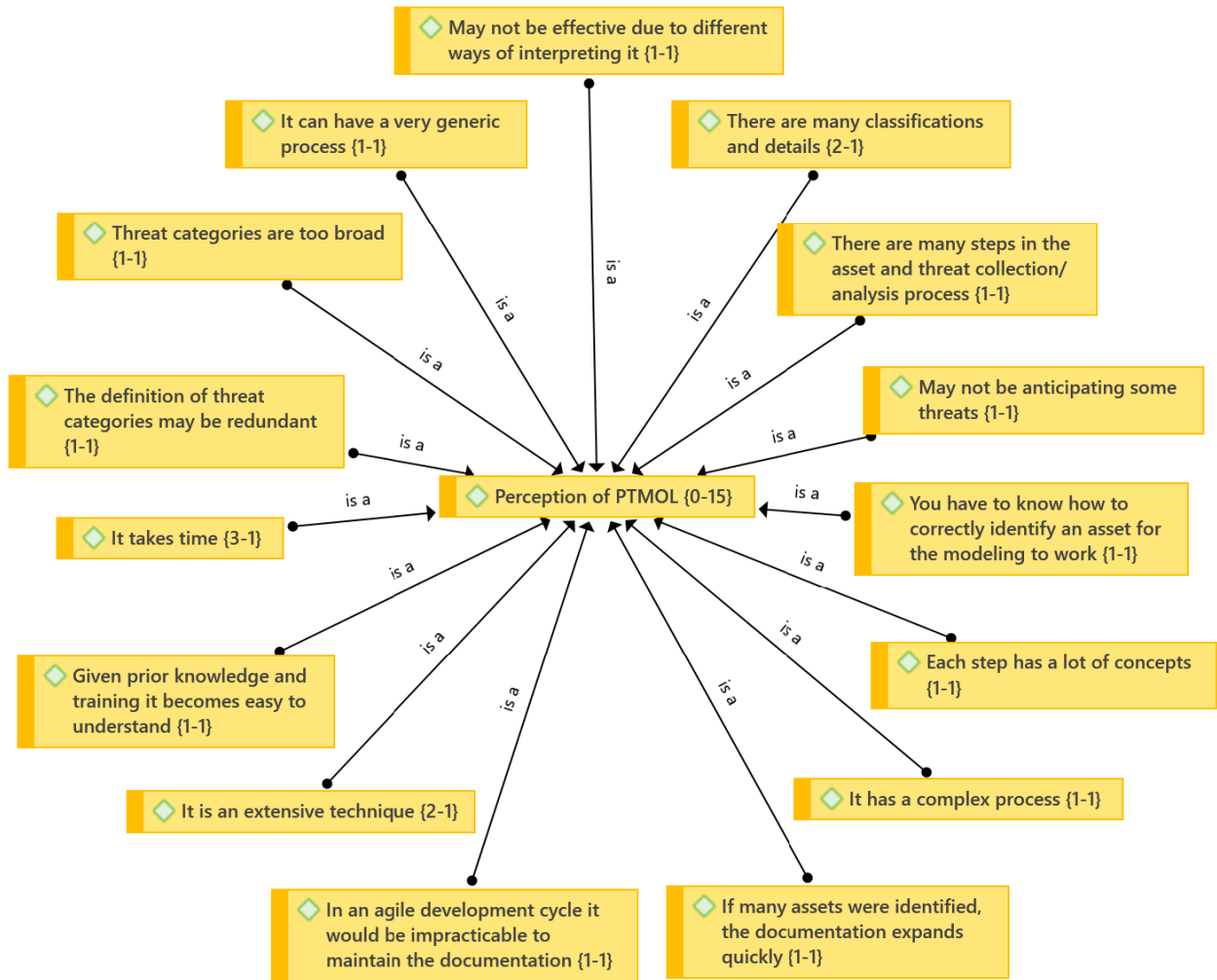


FIGURE 16. Codes related to the teams' perception of PTMOL.

suggestions for improvements through the *design rationale*. The data analyzed were the reports provided by the participants, which contained the RD records. The reports were examined for three main purposes: (i) to identify common problems in threat modeling with PTMOL; (ii) analyze the participants' arguments about the problems pointed out; and (iii) identify suggestions for improvement. Table 9 summarizes the main issues provided by the teams, as well as possibilities for improvement.

Based on the information presented in Table 9, it is noted that it was possible to elicit specific problems on threat modeling with PTMOL, which highlights the need for improvements that could be implemented with the possible solutions indicated. The problems described and their possible solutions aim to help professionals who use PTMOL to clarify doubts and minimize difficulties arising from the use of the language. It is worth noting that all arguments were suggested based on the participants' experience during the observational study, which reinforces their applicability. Each need for

improvement was analyzed and the feasibility of implementing it was verified with a second researcher.

#### F. IMPROVEMENTS IN PTMOL AFTER THE EXECUTION OF THE OBSERVATIONAL STUDY

The qualitative data analysis provided relevant insights to improve the ease of use of PTMOL, since both the data collected in the focus group and the records provided through the design rationale indicated specific problems regarding the language. These problems were analyzed and viable improvements were implemented, which generated a new version of PTMOL, as shown in Section V. Initially, the codes that were considered evidence of difficulties in applying the PTMOL threat modeling process were analyzed. After the analysis carried out by the specialist researchers, some adaptations were made in order to make the language elements clearer. All the improvements mentioned above were incorporated into the new version of PTMOL, which is presented in Section V. The main changes implemented include:

**TABLE 9. Problems and possible solutions identified in the design rationale.**

Question/Problem	Possible solution	Source
Leak source options are quite generic and it can be difficult to tie them to a specific threat	New elements could be added, such as attributes that further detail leak sources so you can effectively differentiate between them	Team 1
PTMOL does not clarify the standards for the filling in of the modeling templates	PTMOL could describe the rules for filling in of the templates so as not to cause doubts when modeling	Team 2
It does not have its own threat modeling tool	Development of a support tool for PTMOL that validates the language syntax and allows for more automated modeling	Team 3
The association of the countermeasure with the threat may not be effectively clear	it could indicate for each threat listed in the modeling template which countermeasure was violated, so it is clearer to think about mitigation strategies	Team 4

- The definitions of some threats in the catalog were updated in order to make them clearer and more concise and eliminate possible redundancies.
- Creation of filling in rule for modeling templates.
- Elimination of confusing information.
- More detailed description of leak sources

### G. CONCLUSION OF THE OBSERVATIONAL STUDY

Shull et al. [56] state that through an observational study it is possible collect data on how a given solution is applied. In this way, when witnessing potential difficulties that participants may present, researchers can acquire a refined understanding of the solution under analysis. Therefore, this section presented an observational study with the objective of understanding the way in which possible system designers would apply the PTMOL threat-modeling process.

The results of the study were positive, since they provided relevant insights to improve the quality of PTMOL. After the analysis carried out by the specialist researchers, some updates and modifications were carried out in order to make the elements and resources of the language clearer. Although the results of a single experiment cannot be generalized to other contexts, it is believed that the qualitative results of this observational study can contribute to a better understanding of the behavior of novice designers in threat modeling.

### XI. LIMITATIONS

Every study has limitations and they need to be reported. Among the limitations of the studies, we highlight two main ones. The first is related to the fact that the participants were undergraduate students and the study was conducted in an academic environment. However, something that could be seen as a limitation by some, in fact is not if one considers Fernandez et al. [58] who state that students who do not have experience in the industry may, however, have similar

skills to less experienced professionals. Therefore, despite the limitation imposed by the participation of students and not professionals in the study, it is believed that the results found should not be considered invalid. Another limitation may be related to the generalization of the results obtained. The number of participants involved in the study cannot be considered representative, but we sought to mitigate this threat by obtaining and collecting important data on the language application process.

### XII. CONCLUDING REMARKS AND FUTURE WORK

The use of OSNs has exploded, with millions of people using their services around the world. This increase in social networking use has led to user anxiety related to the unauthorized exposure of personal information. The problem of privacy threats in OSNs can severely affect the social activities in which users engage while online.

Anticipating privacy concerns in the stages prior to the development of OSNs is a promising strategy for addressing personal data protection. This interest increases the credibility of using threat modeling methodologies and brings opportunities for developing new solutions that address this issue. In this paper, we presented PTMOL (Privacy Threat Modeling Language), a privacy threat modeling solution focused on protecting user data. The paper also reports a feasibility study conducted in order to analyze the PTMOL acceptance from the point of view of novice designers. We also evaluated the PTMOL correctness and completeness.

PTMOL proved to be applicable even by non-expert threat modeling professionals, since all participants were able to map threat scenarios, even if they were not security and privacy experts. This indicates that PTMOL can be incorporated into software development during the design phase and can aid software designers in threat modeling without requiring a high level of expertise in the area of privacy.

Through qualitative analysis, improvements to be made in PTMOL were identified, such as the need to include and adapt elements of the notation to allow the effective representation of aspects of threat modeling. All improvements have now been implemented. As future works, we highlight the continuity of new studies to evaluate the language in a more comprehensive way. Consequently, new points that may arise regarding the language application should be observed in order to further develop it. For this evolution process, we also intend to execute exploratory studies, such as interviews or focus groups, mainly seeking to explore and explain qualitative data that can enrich the language use context.

### ACKNOWLEDGMENT

The authors would like to thank the undergraduate students who participated in the study.

### REFERENCES

- [1] Y. Shao, J. Liu, S. Shi, Y. Zhang, and B. Cui, "Fast de-anonymization of social networks with structural information," *Data Sci. Eng.*, vol. 4, no. 1, pp. 76–92, Mar. 2019.

- [2] J. H. Abawajy, M. I. H. Ninggal, and T. Herawan, "Privacy preserving social network data publication," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1974–1997, 3rd Quart., 2016.
- [3] J. Alemany, E. Del Val, J. M. Alberola, and A. Garcia-Fornes, "Metrics for privacy assessment when sharing information in online social networks," *IEEE Access*, vol. 7, pp. 143631–143645, 2019.
- [4] N. C. Rathore and S. Tripathy, "A trust-based collaborative access control model with policy aggregation for online social networks," *Social Netw. Anal. Mining*, vol. 7, no. 1, pp. 1–13, Dec. 2017.
- [5] S. Oukemeni, H. Rifa-Pous, and J. M. M. Puig, "Privacy analysis on microblogging online social networks: A survey," *ACM Comput. Surv.*, vol. 52, no. 3, pp. 1–36, 2019.
- [6] S. Joyee De and A. Imine, "On consent in online social networks: Privacy impacts and research directions," in *Proc. 13th Int. Conf. Risks Secur. Internet Syst.*, 2019, pp. 128–135.
- [7] C. Laorden, B. Sanz, G. Alvarez, and P. G. Bringas, "A threat model approach to threats and vulnerabilities in on-line social networks," in *Computational Intelligence in Security for Information Systems*. Berlin, Germany: Springer, 2010, pp. 135–142.
- [8] O. Solon, "Facebook says Cambridge analytica may have gained 37M more users' data," *The Guardian*, London, U.K., 2018, vol. 4.
- [9] S. Du, X. Li, J. Zhong, L. Zhou, M. Xue, H. Zhu, and L. Sun, "Modeling privacy leakage risks in large-scale social networks," *IEEE Access*, vol. 6, pp. 17653–17665, 2018.
- [10] R. G. Pensa and L. Bioglio, "Your privacy, my privacy? On leakage risk assessment in online social networks," in *Proc. 1st Int. Workshop Pers. Anal. Privacy*, 2017, pp. 3–9.
- [11] Y. Zeng, Y. Sun, L. Xing, and V. Vokkarane, "A study of online social network privacy via the TAPE framework," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1270–1284, Oct. 2015.
- [12] Y. Abid, A. Imine, and M. Rusinowitch, "Online testing of user profile resilience against inference attacks in social networks," in *Proc. Eur. Conf. Adv. Databases Inf. Syst.* Berlin, Germany: Springer, 2018, pp. 105–117.
- [13] G. Wen, H. Liu, J. Yan, and Z. Wu, "A privacy analysis method to anonymous graph based on Bayes rule in social networks," in *Proc. 14th Int. Conf. Comput. Intell. Secur. (CIS)*, Nov. 2018, pp. 469–472.
- [14] H. A. Al-Asmari and M. S. Saleh, "A conceptual framework for measuring personal privacy risks in Facebook online social network," in *Proc. Int. Conf. Comput. Inf. Sci. (ICCCIS)*, Apr. 2019, pp. 1–6.
- [15] A. Rodrigues, M. L. Villela, and E. Feitosa, "PTMOL: A suitable approach for modeling privacy threats in online social networks," in *Proc. 21st Brazilian Symp. Hum. Factors Comput. Syst.*, 2022, pp. 1–12.
- [16] I. Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey, CA, USA: Brooks/Cole Publishing Company, 1975.
- [17] V. J. Derlega and A. L. Chaikin, "Privacy and self-disclosure in social relationships," *J. Social Issues*, vol. 33, no. 3, pp. 102–115, Jul. 1977.
- [18] S. Petronio, *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY, USA: Suny Press, 2002.
- [19] H. Xu, H.-H. Teo, and B. Tan, "Predicting the adoption of location-based services: The role of trust and perceived privacy risk," in *Proc. 26th Int. Conf. Inf. Syst.*, 2005, pp. 897–910.
- [20] E. Zheleva and L. Getoor, "Privacy in social networks: A survey," in *Social Network Data Analytics*. Berlin, Germany: Springer, 2011, pp. 277–306.
- [21] H. Q. Vu, R. Law, and G. Li, "Breach of traveller privacy in location-based social media," *Current Issues Tourism*, vol. 22, no. 15, pp. 1825–1840, Sep. 2019.
- [22] C. Dong and B. Zhou, "Privacy inference analysis on event-based social networks," in *Proc. 8th Int. Conf. Social Inform. (SocInfo)*, 2016, pp. 421–438.
- [23] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, "Protecting location privacy: Optimal strategy against localization attacks," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2012, pp. 617–627.
- [24] E. Zheleva and L. Getoor, "To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles," in *Proc. 18th Int. Conf. World Wide Web*, 2009, pp. 531–540.
- [25] A. Shostack, "Experiences threat modeling at Microsoft," in *Proc. MOD-SEC@ MoDELS*, 2008, p. 35.
- [26] A. Shostack, *Threat Modeling: Designing for Security*. Hoboken, NJ, USA: Wiley, 2014.
- [27] T. UcedaVelez and M. M. Morana, *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. Hoboken, NJ, USA: Wiley, 2015.
- [28] W. Xiong and R. Lagerström, "Threat modeling—A systematic literature review," *Comput. Secur.*, vol. 84, pp. 53–69, Jul. 2019.
- [29] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. Eur. (ISGT-Europe)*, Sep. 2017, pp. 1–6.
- [30] K. H. Kim, K. Kim, and H. K. Kim, "STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery," *ETRI J.*, vol. 44, no. 6, pp. 991–1003, 2021.
- [31] K. Wuys, D. Van Landuyt, A. Hovsepian, and W. Joosen, "Effective and efficient privacy threat modeling through domain refinements," in *Proc. 33rd Annu. ACM Symp. Appl. Comput.*, Apr. 2018, pp. 1175–1178.
- [32] N. R. Mead, F. Shull, K. Vemuru, and O. Villadsen, "A hybrid threat modeling method," *Softw. Eng. Inst., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-2018-TN-002*, 2018.
- [33] T. Denning, B. Friedman, and T. Kohno, *The Security Cards: A Security Threat Brainstorming Toolkit*. Seattle, WA, USA: Univ. Washington, 2013.
- [34] B. Sanz, C. Laorden, G. Alvarez, and P. G. Bringas, "A threat model approach to attacks and countermeasures in on-line social networks," in *Proc. 11th Reunion Espanola de Criptografia y Seguridad de la Informacion*, 2010, pp. 343–348.
- [35] Y. Wang and R. K. Nepali, "Privacy threat modeling framework for online social networks," in *Proc. Int. Conf. Collaboration Technol. Syst. (CTS)*, Jun. 2015, pp. 358–363.
- [36] S. De and A. Imine, "To reveal or not to reveal: Balancing user-centric social benefit and privacy in online social networks," in *Proc. 33rd Annu. ACM Symp. Appl. Comput.*, 2018, pp. 1157–1164.
- [37] A. Aktypi, J. Nurse, and M. Goldsmith, "Unwinding Ariadne's identity thread: Privacy risks with fitness trackers and online social networks," in *Proc. Workshop Multimedia Privacy Secur.*, 2017, pp. 1–11.
- [38] R. Fogues, J. M. Such, A. Espinosa, and A. Garcia-Fornes, "Open challenges in relationship-based privacy mechanisms for social network services," *Int. J. Hum.-Comput. Interact.*, vol. 31, no. 5, pp. 350–370, 2015.
- [39] M. Sramka, "Privacy scores: Assessing privacy risks beyond social networks," *Infocommun. J.*, vol. 4, no. 4, pp. 36–41, 2012.
- [40] S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, "Social network security: Issues, challenges, threats, and solutions," *Inf. Sci.*, vol. 421, pp. 43–69, Dec. 2017.
- [41] L. Bioglio, S. Capecchi, F. Peiretti, D. Sayed, A. Torasso, and R. G. Pensa, "A social network simulation game to raise awareness of privacy among school children," *IEEE Trans. Learn. Technol.*, vol. 12, no. 4, pp. 456–469, Oct. 2019.
- [42] I. Casas, J. Hurtado, and X. Zhu, "Social network privacy: Issues and measurement," in *Proc. 16th Int. Conf. Web Inf. Syst. Eng.*, 2015, pp. 488–502.
- [43] S. Mahmood, "New privacy threats for Facebook and Twitter users," in *Proc. 7th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput.*, Nov. 2012, pp. 164–169.
- [44] O. Jaafar and B. Birreghah, "Multi-layered graph-based model for social engineering vulnerability assessment," in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining*, Aug. 2015, pp. 1480–1488.
- [45] C. Watanabe, T. Amagasa, and L. Liu, "Privacy risks and countermeasures in publishing and mining social network data," in *Proc. 7th Int. Conf. Collaborative Computing: Netw., Appl. Worksharing*, 2011, pp. 55–66.
- [46] H. Kumar, S. Jain, and R. Srivastava, "Risk analysis of online social networks," in *Proc. Int. Conf. Comput., Commun. Autom. (ICCCA)*, Apr. 2016, pp. 846–851.
- [47] S. Kavianpour, Z. Ismail, and A. Mohtasebi, "Effectiveness of using integrated algorithm in preserving privacy of social network sites users," *Commun. Comput. Inf. Sci.*, vol. 167, no. 2, pp. 237–249, 2011.
- [48] D. Kagan, G. Fuhrmann Alpert, and M. Fire, "Zooming into video conferencing privacy and security threats," 2020, *arXiv:2007.01059*.
- [49] S. De and A. Imine, "Privacy scoring of social network user profiles through risk analysis," in *Proc. 12th Int. Conf. Risks Secur. Internet Syst.*, 2018, pp. 227–243.
- [50] R. Tucker, C. Tucker, and J. Zheng, "Privacy pal: Improving permission safety awareness of third party applications in online social networks," in *Proc. IEEE 17th Int. Conf. High Perform. Comput. Commun. 7th Int. Symp. Cyberspace Saf. Secur., IEEE 12th Int. Conf. Embedded Softw. Syst.*, Aug. 2015, pp. 1268–1273.

- [51] B. Lowson, "How designers think," in *The Design Process Demystified*. Tehran, Iran: Univ. Shahid-Beheshti, 2005.
- [52] S. Ali, A. Rauf, N. Islam, and H. Farman, "A framework for secure and privacy protected collaborative contents sharing using public OSN," *Cluster Comput.*, vol. 22, no. S3, pp. 7275–7286, May 2019.
- [53] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," Dresden, Germany, Tech. Rep., 2010. [Online]. Available: [http://www.maroki.de/pub/dphistory/2010\\_Anon\\_Terminology\\_v0.34.pdf](http://www.maroki.de/pub/dphistory/2010_Anon_Terminology_v0.34.pdf)
- [54] K. Rannenberg, "ISO/IEC standardization of identity management and privacy technologies," *Datenschutz und Datensicherheit-DuD*, vol. 35, no. 1, pp. 27–29, Jan. 2011.
- [55] V. R. Basili, "The role of experimentation in software engineering: Past, current, and future," in *Proc. IEEE 18th Int. Conf. Softw. Eng.*, 1996, pp. 442–449.
- [56] F. Shull, J. Carver, and G. H. Travassos, "An empirical methodology for introducing software processes," *ACM SIGSOFT Softw. Eng. Notes*, vol. 26, no. 5, pp. 288–296, Sep. 2001.
- [57] R. Scandariato, K. Wuyts, and W. Joosen, "A descriptive study of Microsoft's threat modeling technique," *Requirements Eng.*, vol. 20, no. 2, pp. 163–180, 2015.
- [58] A. Fernandez, S. Abrahão, E. Insfran, and M. Matera, "Further analysis on the validation of a usability inspection method for model-driven web development," in *Proc. ACM-IEEE Int. Symp. Empirical Softw. Eng. Meas.*, Sep. 2012, pp. 153–156.
- [59] J. Lazar, J. H. Feng, and H. Hochheiser, *Research Methods in Human-Computer Interaction*. San Mateo, CA, USA: Morgan & Kaufmann, 2017.
- [60] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quart.*, vol. 13, no. 3, pp. 319–340, 1989.
- [61] O. Laitenberger and H. M. Dreyer, "Evaluating the usefulness and the ease of use of a web-based inspection data collection tool," in *Proc. 5th Int. Softw. Metrics Symp. Metrics*, 1998, pp. 122–132.
- [62] J. Lee, "Design rationale systems: Understanding the issues," *IEEE Expert*, vol. 12, no. 3, pp. 78–85, May 1997.
- [63] M. C. F. Pelicioni, "A utilização do grupo focal como metodologia qualitativa Na promoção da saúde," *Revista da Escola de Enfermagem da USP*, vol. 35, pp. 115–121, May 2001.
- [64] B. B. N. de França, T. V. Ribeiro, P. S. M. dos Santos, and G. H. Travassos, "Using focus group in software engineering: Lessons learned on characterizing software technologies in academia and industry," in *Proc. CibSE*, 2015, p. 351.
- [65] B. G. Glaser, A. L. Strauss, and E. Strutzel, "The discovery of grounded theory; strategies for qualitative research," *Nursing Res.*, vol. 17, no. 4, p. 364, Jul. 1968.
- [66] J. Corbin and A. Strauss, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Newbury Park, CA, USA: Sage, 2014.
- [67] B. G. Glaser, *Basics of Grounded Theory Analysis: Emergence vs Forcing*. Mill Valley, CA, USA: Sociology Press, 1992.



**ANDREY RODRIGUES** received the bachelor's degree in information systems and the master's degree in informatics from the Federal University of Amazonas (UFAM), in 2016 and 2019, respectively, where he is currently pursuing the Ph.D. degree in informatics with PPGI. He is an Assistant Professor I with the Estácio Amazonas Higher Education Society. He also works as a Researcher/Collaborator with the Emerging Technologies and Systems Security (ETSS) Research Group. He has experience in the area of computer science, with an emphasis on security and privacy of systems, structured programming, and human-computer interaction (HCI). His research interests include detection of threats and attacks in systems, modeling and prevention techniques privacy, machine learning algorithms for system security and privacy, and the design and evaluation of interfaces.



**MARIA LÚCIA BENTO VILLELA** received the degree in computer science from the Federal University of Viçosa (UFV) and the M.Sc. and Ph.D. degrees in computer science from the Federal University of Minas Gerais (UFMG). She is currently an Adjunct Professor with the Department of Informatics, UFV. She participates in the Graduate Program in Education (PPGED), Federal University of Vales do Jequitinhonha and Mucuri (UFVJM). She works in human-computer interaction, emphasizing user interface design and evaluation and semiotic engineering. She also works in the software engineering field, mainly in software development processes and requirements engineering, and in the computer education field, specifically in computational thinking.



**EDUARDO LUZEIRO FEITOSA** (Member, IEEE) received the degree in data processing from the Federal University of Amazonas (UFAM), in 1998, the master's degree in computer science from the Federal University of Rio Grande do Sul (UFRGS), in 2001, and the Ph.D. degree in computer science from the Federal University of Pernambuco (UFPE). He is currently an Associate Professor with the Institute of Computing (IComp), UFAM. He is also a Researcher and a Leader with the Emerging Technologies and System Security (ETSS) Research Group. He holds a position as a Research Fellow with the Networking and Emerging Technologies Research Group.

...