



Exploring how experienced and unexperienced professionals use a privacy threat modeling methodology

Andrey Rodrigues  [Federal University of Amazonas | andrey.rodrigues@ufam.edu.br]

Maria Lúcia Villela  [Federal University of Viçosa | maria.villela@ufv.br]

Eduardo Feitosa  [Federal University of Amazonas | efeitosa@icomp.ufam.edu.br]

Abstract

Online Social Networks (OSNs) have become one of the principal technological phenomena of the Web, gaining an eminent popularity among its users. With the growing worldwide expansion of OSN services, people have devoted time and effort to maintaining and manipulating their online identity on these systems. However, the processing of personal data through these networks has exposed users to various privacy threats. Consequently, new solutions need to be developed for addressing the threat scenarios to which a user is potentially exposed. In this sense, this paper proposes PTMOL (Privacy Threat Modeling Language), an approach for modeling privacy threats in OSN domain. The proposed language aims to support the capture, organization and analysis of specific privacy threats that a user is exposed to when sharing assets in a social application, also enabling the definition of countermeasures to prevent or mitigate the effects of threat scenarios. The first language version has undergone a preliminary empirical study that identified its validity as a modeling language. The results indicate that the use of the language is potentially useful for identifying real privacy threats due to its exploratory and reflexive nature. We expect to contribute to support designers in making more preemptive decisions about user privacy risk, helping them to introduce privacy early in the development cycle of social applications.

Keywords: *Threat Modeling, Privacy Threat, Online Social Network, Empirical Study.*

1 Introduction

Online Social Networks (OSNs) have exploded in popularity over the past few years. Currently, these systems provide a variety of features and services that allow its users to share information with large and diverse audiences. They can analyze data and correlate user preferences to provide advanced and personalized services. Thus, they can recommend friends or common interests based on information extracted from users' profiles and activities, such as shopping preferences, daily navigation, among others [Oukemeni et al., 2019].

With the growing worldwide popularity of OSN services, people have spent time and effort to maintain and manipulate their online identity on these systems. However, the processing of personal data by these networks has exposed users to various privacy threats [Rathore et al., 2017; Siddula et al., 2018; Ali et al., 2018]. A privacy threat is a potential or real undesirable event that can cause harm to a user in the form of exposure and manipulation of data [Joyee De and Imine, 2019; Laorden et al., 2010]. Its consequence is a privacy breach by which personal data is disclosed to unauthorized individuals or entities for malicious purposes [Abawajy et al., 2016]. The Facebook - Cambridge Analytica incident is a prominent example of a breach in which the personal data of a large number of users was disclosed and most of the users had neither control nor knowledge of this disclosure [Solon, 2018].

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 [Ouke-

meni et al., 2019]. 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 crimes such as fraud or identity theft.

As a result, OSNs have attracted the attention of privacy researchers in both the industry and in academic fields. There are many researchers that have presented their own solutions to protect users against privacy threats and breaches [Zeng et al., 2015; Abid et al., 2018; Wen et al., 2018; Al-Asmari and Saleh, 2019] and, in general, these approaches are directed at addressing privacy issues related to the operation 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.

In this sense, one strategy for addressing the issues mentioned is to anticipate concerns about privacy threats to the stages prior to the development of OSN systems. This promising privacy strategy is known as privacy by design [Cavoukian et al., 2009], and its concept was introduced in the 1990s by a privacy expert named Ann Cavoukian. The central idea of the approach is to incorporate privacy and the protection of personal data in the early stages of the system development life cycle, rather than addressing them at later points in time. There are different techniques that support system design, such as creation of personas, task modeling,

interaction modeling and construction of mockups [Preece et al., 1994; Lazar and Barbosa, 2017]. However, these generalist solutions lack specific features for addressing privacy threats. A widely used technique that can support privacy anticipation in the early stages of system development is the threat modeling methodology [Shostack, 2008].

The threat modeling methodology was initially introduced by Microsoft, and its proposal was that it be inserted in the security design stage, with the aim of making the applications developed by the company more secure [Shostack, 2008]. Overall, threat modeling is a systematic and structured process that aims to identify potential threats and vulnerabilities in order to reduce the risks to IT resources. Although there are existing threat modeling techniques for certain domains [Uceda Velez and Morana, 2015; Potteiger et al., 2016; Wuyts et al., 2018], many of them were developed to model the most common threat categories related to the functioning and architecture of general systems. Moreover, they have characteristics that make their application difficult or are not sufficient for modeling specific privacy threats in the OSN domain.

Thus, we believe is possible to propose new solutions for addressing this gap, since, to the best of our knowledge, we have not identified any proposals for user-centric privacy threat modeling that would enable its use in the OSN. In this sense, this paper presents 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. This language was developed from evidence gathered in the literature and was empirically evaluated through experimental study.

Identifying privacy threats through a modeling approach can promote the following benefits: (i) the anticipation, still in design stage, of threat scenarios to which a user is potentially exposed; (ii) the prioritization of privacy efforts; (iii) the justification for making informed decisions about user's privacy risk; (iv) greater assertiveness in the implementation of privacy mechanisms, since the identified threats come from a perspective directly linked to the user; and (v) support designers in considering privacy threats at the time of design. These are considered important since modeling potential threats that a user is exposed to can be an important support that enables better design of the current and next generation of OSNs. 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.

2 Background

There are some important questions to answer in order to understand what privacy threats are in the context of OSNs.

First, what is privacy? Next, what is a privacy threat? Last, but not least, what is a privacy breach? Next, the concepts involved in this paper's background are presented, exemplified and related, which inspire relevant reflections for modeling privacy threats in OSN systems.

2.1 Privacy

According to the privacy regulation theory presented by Altman [1975], 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 [1975] 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 [Derlega and Chaikin, 1977; Petronio, 2002].

2.2 Privacy Threat

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

In systems like OSNs, sharing personal data can be a desirable focus for attackers (malicious agents). Location disclosure, for example, can result in tracking threats, which seek to analyze users' general behavior [Xu et al., 2005]. Furthermore, through location data, an attacker can also collect information to gain clues about various types of private user data, such as lifestyle, time and purpose of movements in different locations.

2.3 Privacy Breach

A privacy breach occurs when private and confidential information is disclosed to unauthorized individuals [Zheleva and Getoor, 2011; Abawajy et al., 2016] and can be classified into four types [Vu et al., 2019; Dong and Zhou, 2016]: (i) identity disclosure, when an individual's identity is revealed; (ii) attribute disclosure, when the value of some sensitive attributes associated with an individual is compromised; (iii) relationship disclosure, when a sensitive relationship between two people is disclosed; and (iv) disclosure of affiliation relationship, when a person's membership of a particular group or community is disclosed.

Overall, a privacy breach is a consequence of a threat execution, and this can cause harm to users in the form of harassment, financial loss, and even identity theft. They can also make users vulnerable to unwanted ads, scams and crimes, which can damage their social reputation or economic situation and cause them to be them victims of blackmail or physical violence [Shokri et al., 2012]. In addition, commercial and government entities may also violate users' privacy for different purposes, such as targeted marketing, health screening, or political monitoring [Zheleva and Getoor, 2009].

2.4 Threat Modeling

Threat modeling is a structured approach for identifying and prioritizing potential threats to a system and thus determine countermeasures to prevent or mitigate the effects of those threats [Shostack, 2014]. The methodology was proposed so that developers, designers, and system analysts could include threat modeling in their software development cycle. The process allows one to generate a threat model and determine what types of mitigation are needed during an early development stage of a new system, application, or feature. 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 [UcedaVelez and Morana, 2015; Xiong and Lagerström, 2019].

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. Below, some definitions for these terms found in various threat modeling papers are provided [Laorden et al., 2010; Xiong and Lagerström, 2019; Shi et al., 2021]:

- **Asset** - entity of value to the business or enterprise, be it a computer processor, disk, network link, program, data or user.
- **Threat** - any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service
- **Vulnerability** - weakness in system that could be exploited to violate system policy; the possibility of an exploit or exposure to a threat that is specific to a given platform.
- **Exposure** - proximity and/or contact with a source of a disease agent or computer virus in such a manner that effective transmission of the harmful effects of the agent/virus may occur.
- **Risk** - expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
- **Countermeasure** - any action, device, procedure, technique, or other measure that reduces the vulnerability of a threat to a system.
- **Attack** - the act of trying to bypass security or privacy controls on a system. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures.

An analysis of elements that make up the threat modeling

methodology was performed, so as to verify its suitability for the privacy context in OSNs. For this purpose, the elements were contrasted with some specific privacy characteristics of OSNs and were the subject of three strategic decisions: exclusion, adaptation or insertion of a new element. Our analysis made it possible to generate a new threat modeling process that is introduced in section 4.

3 Related Works

In this section, the main works related to our research are presented. As privacy threat modeling is still incipient, some existing solutions for threat modeling that focus on generalist systems are presented.

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

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

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 map-

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

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

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

garding countermeasures that OSNs should implement to prevent targeted attacks on the system.

In a similar vein, Wang and Nepali [2015] proposed a framework for modeling threats in OSNs from a conceptual perspective. The authors' proposal presents some relevant steps for the modeling context. In the first step, four components of the system must be characterized, which are understood as fundamental elements for threat modeling, such as (i) OSN sites, (ii) OSN providers, (iii) users of OSNs, and (iv) malicious users. Given the characterization of these components, it is recommended that the different objectives that malicious users intend to accomplish are identified. After that, system's vulnerabilities should be identified and 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. [2010] and by Wang and Nepali [2015] present conceptual approaches for modeling threats in the context of OSNs and highlight the importance of using this methodology as a solution to security issues in these systems. However, the approaches presented in these works appreciate a conceptual perspective, which can serve as input and basis for proposing a more complete methodology applicable to the context of OSNs. Furthermore, the proposals do not provide methodological guidance to assist designers and other IT professionals who want to incorporate privacy threat modeling into OSNs at the design level.

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

4 Privacy Threat Modeling Language

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

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

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

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

According to Lowson [2005], the difference between the current situation and a desired situation is the main motivation for designing and synthesizing an intervention. In other words, an intervention is called a solution, as it answers the

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

4.2 Catalog of Privacy Threats

PTMOL's threat modeling process is supported by catalog of privacy threats for the context of OSNs, which describes the most critical threats to user privacy. These threats were discovered via a thorough investigation of the literature. This threat set is a very valuable resource as it helps the designer to think through which threat scenarios a user is potentially exposed to. 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 [De and Imine, 2018b; Aktypi et al., 2017; Fogues et al., 2015; Sramka, 2012].
- **Information Disclosure** - Information disclosure refers to the detection and extraction of information that was unintentionally disclosed [Ali et al., 2019]. This disclosure can directly expose an enormous amount of the users' confidential information, such as their home address, health-related data, recent activities, and so on. The sharing of such sensitive and private information may have negative implications for OSN users, and this can compromise their privacy [Rathore et al., 2017; Aktypi et al., 2017; Zeng et al., 2015; Bioglio et al., 2019; Casas et al., 2015].
- **Profile cloning.** A malicious user can use the shared data in OSNs to duplicate a user's profile. This threat is known as profile cloning, which is when a fake identity is created to make friends believe in the new "fake" profile. The attacker collects confidential private information about the user's friends to make social links, and capture data of the victim that is not shared in their public profiles [Rathore et al., 2017; Abid et al., 2018; Aktypi et al., 2017; Mahmood, 2012; Jaafar and Birregah, 2015].
- **Data Inference or Tracking** - Data inference is a type of threat applied to discover personal information of the user's that is not directly shared in their profiles on OSNs, but can be predicted using different computational techniques. In addition, OSN providers track and analyze the user's routine activities (such as daily browsing and shopping preferences, for example) through various machine-learning techniques. As a result, OSNs build complete user profiles for the purpose of sell-

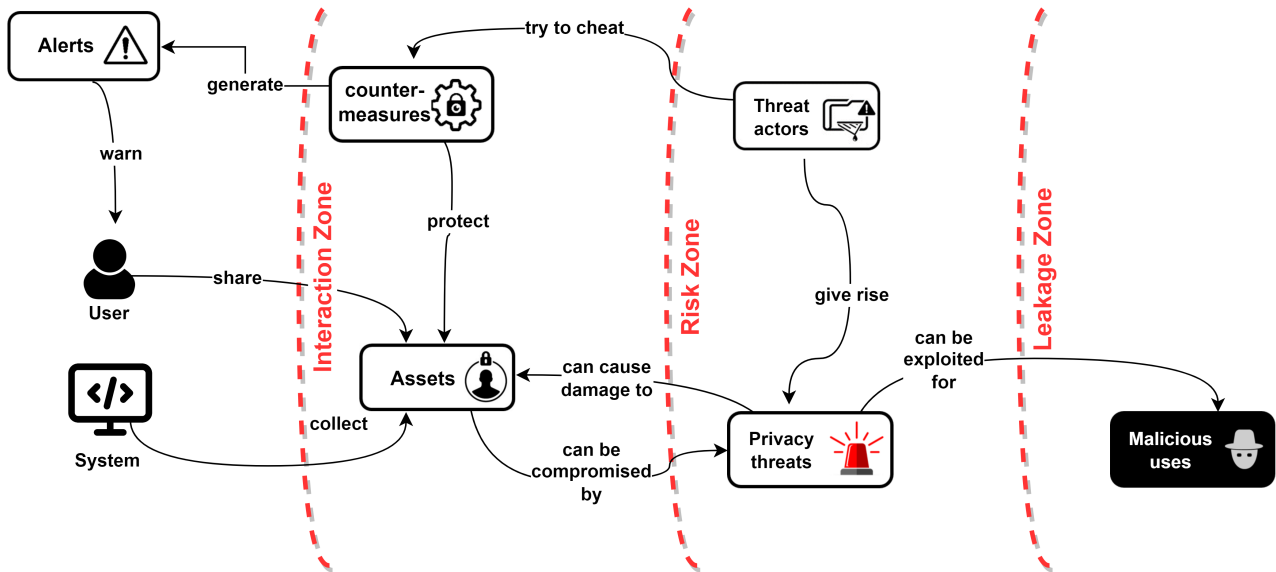


Figure 1. Overview on the relationships between PTMOL elements

ing products or tracking their behavior [Laorden et al., 2010; Watanabe et al., 2011; Wang and Nepali, 2015; Abid et al., 2018; Dong and Zhou, 2016].

- **Threat to Reputation** - Sharing personal or sensitive information can make OSN users victims of a threat to reputation. A malicious user or an online entity can create multiple false profiles to gain access to sensitive private information and exploit them to harm the reputation of the OSN user [Abid et al., 2018; Rathore et al., 2017; Kumar et al., 2017; Wang and Nepali, 2015]. Moreover, users could become victims of manipulation and distortion of data. Currently, there are several tools available to distort diverse data. Using these tools, a malicious user can alter the personal images of legitimate users, for example, in order to harm or damage their reputation.
- **Facial Recognition**. Face recognition algorithms are capable of identifying or verifying a person from a digital image or a video source. Identifying a person's face from a photo or video and cross-referencing it with other datasets might be used to expose personal information about the individual [Kagan et al., 2020; Laorden et al., 2010; Kumar et al., 2017; Kavianpour et al., 2011].
- **Surveillance**. Surveillance is a new type of monitoring that allows, in real-time, the collection and processing of various activities of users of OSNs by using their profiles and relationships with others [Aktypi et al., 2017].
- **Unauthorized Recording** - Nowadays, many OSNs support both chat and video conferencing services since video conferencing can provide more interaction between users. However, with this, more information can be disclosed. One of the participants of the video conference can easily record the conference in order to blackmail the other participant (victim) or to distort the conference data and display it accordingly [Rathore et al., 2017; Kagan et al., 2020].
- **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 imperson-

ate them in order to gain some benefit or harm the victim [De and Imine, 2018b; Al-Asmari and Saleh, 2019; De and Imine, 2018a; Tucker et al., 2015].

4.3 Mitigation Strategies

A second resource, which is envisioned to aid the PTMOL modeling process, is that of generalist mitigation strategies, which can be used as a basis for creating preventative countermeasures. These strategies have been adapted from a set of privacy threat properties proposed by Pfitzmann and Hansen [2010] and Rannenberg [2011] 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 users are aware of the collection of their personal data and that only the necessary information should be used to allow the performance of the systems' functions.
- **Transparency.** This requires that any system that stores user data informs the owner of the data about the system's privacy policy and allows the owner of the data to specify their consent in compliance with the legislation, before users access the system

4.4 Application Process

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.

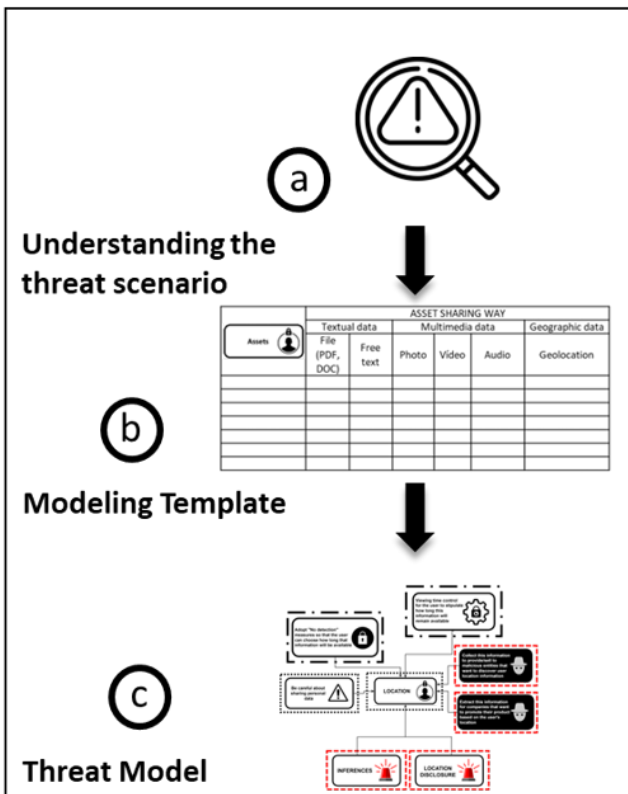


Figure 2. PTMOL methodology steps to be applied during a design phase

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 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.

4.4.1 Identifying Assets

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

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

Figure 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.

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

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




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

4.4.2 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.





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

4.4.3 Identifying Mitigation Strategies

Finally, in the last step, the designer will have to make strategic decisions that guarantee greater assertiveness in the implementation of alerts and appropriate countermeasures to

protect the assets. After listing the set of threats and their consequences for the user’s privacy, the designer should consult the implemented taxonomy with privacy properties. With this, the designer must indicate, through a selection mark “X”, which properties were violated, as shown in Figure 6.


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

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.





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

4.4.4 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 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

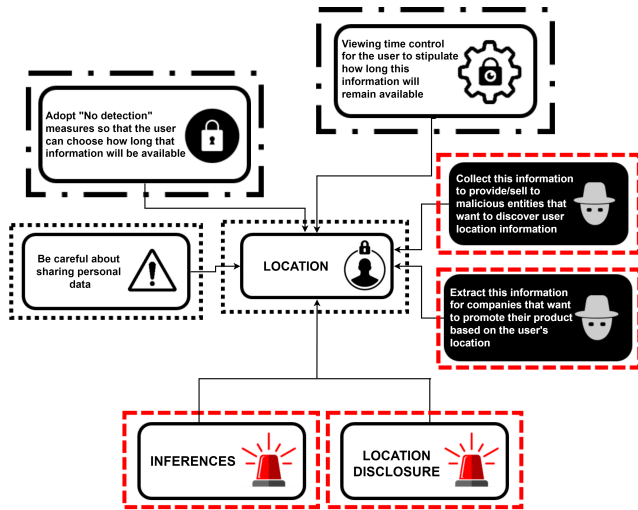


Figure 8. Diagram modeled with elements of PTMOL

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.

5 Experimental Study

Experimentation is the scientific process core and provides a systematic, disciplined, computable and controlled way of evaluating human activity [Basili, 1996]. According to Shull et al. [2001], besides providing validation for different proposals, the use of experimental studies can also help in identifying problems present in them. The experimental design used in the PTMOL studies is based on the Wuyts et al. [2018] and Scandariato et al. [2015] protocols.

5.1 Methodological Procedures

The first study aimed to evaluate the initial version of PTMOL and understand its use in modeling privacy threats in OSNs. In addition, the study was also conducted to carry out the validity and reliability procedures of the language and acquire opportunities for its refinement. The study protocol was approved by the Ethics and Research Committee of the Federal University of Amazonas (CAAE-63572122.0.0000.5020).

5.1.1 Study Planning

For study planning, six research questions were formulated, which are described below:

- **QP1 - Correctness.** On average, how many threats discovered by the participants are correct (true positives vs. false positives)?

- **QP2 - Completeness.** How many threats are not detected by the participants (false negatives)?
- **QP3 - Productivity.** How many valid threats are identified by the participants in a given period of time?
- **QP4 - Ease of use.** Did the participants perceive the language as being easy to learn and apply?
- **QP5 - Usefulness.** Do the participants believe the language would improve their performance in threat modeling?
- **QP6 - Intention to use.** Would the participants use the language in future projects?

Table 1 presents an overview of the terms adopted for the quantitative evaluation. Based on the aforementioned research questions, null and alternative hypotheses were formulated, as shown below.

Table 1. Terminology adopted for quantitative evaluation

Terms	Meaning
True Positive (TP)	Correct Threat
False Negative (FN)	Overlooked Threat
False Positive (FP)	Incorrect Threat
Precision (Prec)	$TP/(TP+FP)$
Recall (Rec)	$TP/(TP+FN)$
Productivity (Prod)	$TP/time$
Average (μ)	Population mean

Correctness. This defines to what extent the language employs the elements and relationships according to the syntax. Instead of using the total number of mistakes made by the participants, correctness is measured by means of precision (see Table 1), which scales the number of correctly identified threats (true positives) with respect to the errors (false positives). Our null-hypothesis is represented below. Our alternative hypothesis (i.e., expectation of a 'good' result) is that precision will be at least 80%, or greater.

$$H_0 : \mu \{ \text{Prec} = \frac{VP_{participant}}{VP_{participant} + FP_{participant}} \} < 0.80$$

Completeness. This defines to what extent the language presents the necessary information according to the modeling purpose. This metric is related to the language's semantics. Completeness is measured by means of recall (see Table 1), which scales the number of correctly identified threats (true positives) with respect to missing threats (false negatives). Our null-hypothesis is described below. As before, our hope (alternative hypothesis) is that recall is at least 80%.

$$H_0 : \mu \{ \text{Rec} = \frac{VP_{participant}}{VP_{participant} + FN_{participant}} \} < 0.80$$

Productivity. Productivity is defined as the number of correct threats (TP) per hour. Our null-hypothesis is described below. In a related study on threat modeling Scandariato et al. [2015], an average productivity of one threat per hour was observed. Therefore, our expectation is that PTMOL performs either comparably or better.

$$H_0 : \mu \{ \text{Prod} = \frac{VP_{participant}}{time} \} < \text{threat/hour}$$

A post-study questionnaire was used to answer the remaining research questions. This questionnaire was designed based on the TAM model indicators (Technology Acceptance Model), which has been widely adopted in a number of studies to assess why users accept or reject a given solution [Davies, 2015; Marangunić and Granić, 2015]. The indicators used to answer the research questions were as follows:

- **Perceived ease of use.** Defines the degree to which a person considers that using PTMOL would be effortless.
- **Perceived usefulness.** Defines the degree to which a person considers that using PTMOL would improve their performance in modeling activities.
- **Self-predicted future usage.** Defines the degree to which a person predicts that they would use PTMOL in the future.

5.1.2 Participants

As the study participants, eight undergraduate students were selected from the Computer Science course of a Federal Public Institution. They were attending Systems Security classes and were chosen by convenience criteria. This convenience sampling represented a greater operational ease and low sampling cost.

Participants were required to sign an informed consent form (ICF) and complete a characterization form, so as to identify their experience with system modeling and privacy. According to Fernandez et al. [2012], 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.

5.1.3 Scenario

The scenario used in the study described a potential interaction, via chat, between two OSN users. Overall, the scenario showed a user searching for OSN profiles that offered quick and easy home repair services. The user finds a profile and sends a message, via chat, to find out more information about services provided by the profile owner. However, this page is managed by a malicious agent, who tries to find out the victim's personal data. The scenario did not describe privacy threats that might occur, as the goal was to observe whether the PTMOL elements would direct participants to model privacy threats present in the scenario.

5.1.4 Tasks

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

5.2 Study Execution

The study execution was divided into three stages: preparation, application, and evaluation. These stages are described in detail below.

5.2.1 Preparation

In this step, participants received the pertinent information regarding the execution of the privacy threat modeling. A tutorial was presented to the participants, which contained a brief introduction to the main privacy concepts in OSNs and a detailed explanation on practical application of PTMOL in a possible threat scenario. This tutorial lasted for about an hour.

5.2.2 Application

After preparation, participants applied PTMOL to model privacy threats according to the scenario provided. At the beginning of this step, the informed consent form was signed and the participant profile form was filled in. Then, the task script and the supporting material were provided, which explained what each artifact contained. The task script explicitly described the different language steps that participants were to perform. As support material, they received a language application tutorial and the threat modeling template.

One of the study's researchers acted as the moderator during the evaluation, and was responsible for assisting in cases of doubts regarding the modeling process. The researcher took precautions not to influence the execution of tasks. The researcher also informed the participants that, after completing the tasks, they should answer a questionnaire on their experience with the application of PTMOL. No time limit was set for the completion of the tasks.

5.2.3 Evaluation

Finally, participants were asked to provide feedback via a post-study questionnaire about their experience using PTMOL. Though this, the idea was to collect quantitative indicators and qualitative reflections in order to gain new insights regarding the practical application of PTMOL. Via this evaluation, it was hoped to gain indicators about the possibilities and/or difficulties in understanding what it is to model privacy threats in the context of OSNs, as well as to gain opportunities for language refinement.

5.3 Results

After the execution of the study, the artifacts generated by the participants (threat modeling templates and models) were analyzed, as well as the data collected in the post-evaluation questionnaires. In this section, the quantitative and qualitative results obtained are presented.

5.3.1 Quantitative Results

The scenario provided contained six assets that were shared by the victim via chat, namely: name, phone number, e-mail address, photos, videos, and home address. Depending on

how the asset was shared, different privacy threats could occur. The reports generated by the participants were evaluated by experts (model authors). Each threat reported in the modeling template was evaluated as correct (true positive) or incorrect (false positive). Correct results are threats that are considered: a) relevant to the context/scenario provided; b) compatible with threats considered by PTMOL; and c) documented with sufficient detail of the reasoning.

It should be highlighted that, prior to running the study, a modeling task was performed with PTMOL using the scenario provided in the study. Therefore, an oracle (reference solution) was created containing all the possible threats that an ideal modeling with PTMOL would produce. This oracle was used to check whether the participants disregarded or did not identify some threats (false negatives) present in the proposed scenario. In total, sixteen privacy threats could occur depending on the way assets are shared. This value was the reference for the completeness and correctness analysis. the completeness and correctness analysis.

Table 2 presents an overview of the quantitative results obtained from the individual analysis on modeling performed by the participants. The label 'P', followed by a number, indicates each participant, for example, P1 identifies participant 1 and so on.

Table 2. Overview of the quantitative results performed by the participants

Terms	P1	P2	P3	P4	P5	P6	P7	P8
TF	12	9	16	10	11	10	11	8
TP	9	9	11	10	8	9	9	7
FP	3	0	5	0	3	1	2	1
FN	7	7	5	6	8	7	7	9
TS	2,21	1,04	1,22	1,46	1,38	1,58	1,35	1,32
PC	75%	100%	69%	100%	73%	90%	82%	88%
RC	56%	56%	69%	63%	50%	56%	56%	44%
PR	4	9	9	7	6	6	7	5

*TF - Threats found, TP - True positive, FP - False positive, FN - False negative, TS - Time spent, PC - Precision, RC - Recall, PR - Productivity

Completeness and Correctness (QP1-QP2). Completeness was measured by means of precision, which scales the number of correctly identified threats (true positives) with respect to the errors (false positives). On the other hand, completeness was measured by means of recall, which scales the number of correctly identified threats (true positives) with respect to missing threats (false negatives). Table 3 presents the quantitative results for correctness and completeness indicators.

An average over 0.80 for correctness was obtained, which suggests a positive result for this indicator and retains the null hypothesis (H0P). This result demonstrates that PTMOL has a good correctness and helps to identify valid threats in OSN privacy design. Regarding completeness, it can be noted that the recall degree was 0.562, which is below what was expected. Such a result supports the null hypothesis (0.80 in H0R).

This indicates that difficulties may have occurred in representing some PTMOL elements or some participants did not correctly understand the semantic language. This justifi-

Table 3. Quantitative results of correctness and completeness

#P	Correctness(%)	Completeness(%)
P1	75,00%	56,25%
P2	100,00%	56,25%
P3	68,75%	68,75%
P4	100,00%	62,50%
P5	72,73%	50,00%
P6	90,00%	56,25%
P7	81,82%	56,25%
P8	87,50%	43,75%
Average	84,47%	56,25%

cation explains the incidence of false negatives (see Table 2), since some threats present in the provided scenario were not detected or perceived. This analysis validates the language correctness and shows what improvements need to be made in order to refine its completeness.

Productivity (QP3). Participants spent a total of 11 hours applying PTMOL in the given scenario, which resulted in a productivity of 1.33 threats per hour. Our expectation would be that PTMOL would have a productivity that was equivalent to or greater than one correctly identified threat per hour. Thus, it can be observed that the language obtained a good productivity in its execution, thus rejecting the null hypothesis.

5.3.2 Qualitative Results

The participants' perceptions were collected regarding the threat modeling language through a post-evaluation questionnaire. This questionnaire contained a six-point ordinal scale ranging from (6) totally agree; (5) strongly agree; (4) partially agree; (3) partially disagree; (2) strongly disagree; and (1) totally disagree. As suggested by Laitenberger and Dreyer [1998], the neutral point (neither agree nor disagree) was not used in the ordinal scale since it does not allow identifying the slope (positive or negative) of the participants' responses.

Perceived Ease of Use of PTMOL (QP4). This defines the degree to which a person considers that using PTMOL would be free of effort. To collect this indicator, the following questions were defined: (F1) Learning to model privacy threats with this language was easy for me; (F2) I would find it easy to use this language (the language elements are clear and understandable); (F3) I understood what was happening while using this language; and (F4) I found this language easy to use. Figure 9 presents a graphical representation of the participants' perceptions regarding the ease of use indicator.

By analyzing the data provided in Figure 9, it can be observed that participants P2 and P3 partially disagreed regarding statement F2 "I would find this language easy to use (the language elements are clear and understandable)". This degree of disagreement may be an indicator that the language is not yet fully clear and understandable. Moreover, this data can also justify the completeness degree presented in Table 2, which indicates that PTMOL could improve its semantics to present more complete information according to the modeling purpose.

Regarding the statement (F1) "Learning to model privacy threats with this language was easy for me", it is noted that there were no incidences of disagreements. Such responses

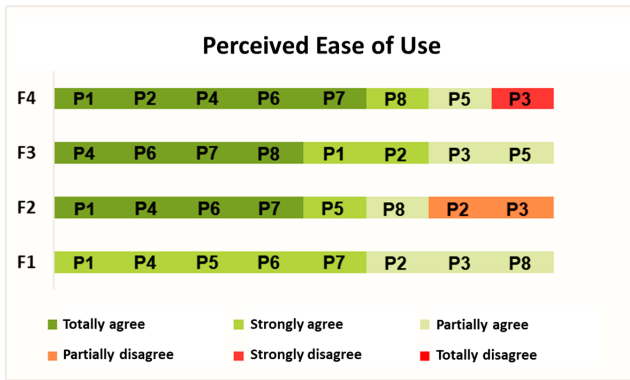


Figure 9. Perceived ease of use of PTMOL

indicate a positive result for PTMOL, thus demonstrating that the language is easy to learn. Another relevant result that can be highlighted is the non-occurrence of disagreement regarding statement F3 "I understood what was happening while using this language". This result suggests that the understanding of the PTMOL threat modeling process has inherent ease.

Perceived Usefulness (QP5). This defines the degree to which a person considers that using PTMOL would improve performance in modeling activities. To collect perceived usefulness, the following statements were defined: (U1) Using this language enables me to model privacy threats in OSNs quickly; (U2) Using this language makes my performance better in modeling privacy threats in OSNs; (U3) Using this language could improve my productivity in modeling privacy threats in OSNs, as I believe I would identify a greater number of threats in a shorter time than I would without using it; and (U4) I consider this language to be useful for supporting the process of modeling privacy threats in OSNs. Figure 10 details the perceived usefulness results.

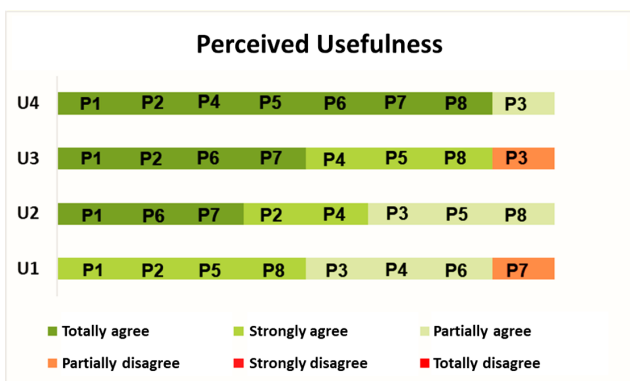


Figure 10. Perceived usefulness of PTMOL

Based on Figure 10, it is seen that most participants agreed with the statements regarding usefulness, thus indicating that they believe PTMOL would improve performance and increase productivity in modeling privacy threats in OSNs. In other words, they agreed that with language support it was possible to identify a greater number of threats in a shorter time than they would identify if they were not using it. Therefore, in the context of this study, PTMOL obtained a positive result regarding its usefulness.

Self-predicted Future Usage (QP6). This defines the degree to which a person predicts they would use PTMOL in the future. To collect this indicator, the following statements

were used: (I1) Assuming that I have enough time to model privacy threats in OSNs, I would use this language; (I2) Taking into account that I have the domain to choose any support for modeling privacy threats in OSNs, I predict that I will use this language; and (I3) I intend to use this language at other times. Figure 11 presents the participants' responses about their intention to use PTMOL in the future.

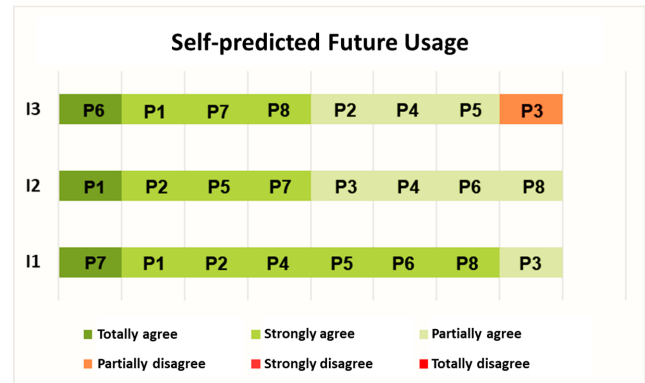


Figure 11. Predicted future usage of PTMOL

Positive results were obtained regarding this indicator. The fact that the participants have academic experience with other analysis and design models strengthens the result of statement I2, which highlights the preference to use PTMOL. These results suggest that the participants would to use PTMOL in future privacy modeling activities.

5.3.3 Comments on difficulties when using PTMOL

A specific analysis of the participants' comments (qualitative data) obtained through open-ended questions contained in the post-evaluation questionnaire was carried out. Some difficulties regarding PTMOL were identified based on the answers provided by the participants. The main difficulties collected were the following: a downside of PTMOL is that it's a bit cumbersome (see quote from P4); some PTMOL elements have the same concept (see quote from P1 below); one difficulty was noticing the difference between some elements (see quote from P8); some threats in the catalog need to be re-concepted (see quote from P3).

"I think it's a good technique that allows you to think about threats, but it takes a little more time and creativity for the malicious uses" (Participant 4).

"The control and countermeasure elements tend to cause conceptual confusion at first, indicating a lack of clarity between the concepts" (Participant 1).

"I didn't quite understand the difference between control and countermeasure – the way it is described, they seem to be the same thing" (Participant 8).

"I think it would be interesting for the authors to review some concepts of the threats in the catalog because some may be getting mixed up, or even make it clearer for the person that will apply them."

From these analyses, it was possible to understand some points that caused some difficulty in applying the PTMOL modeling process. One of the points to be highlighted can be seen in the report of participant P1 who reported: "The control and countermeasure elements tend to cause concep-

tual confusion at first, indicating a lack of clarity between the concepts". 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. Note that the relationship between some elements needs to be revised in order to reduce redundancies.

5.4 Improvements in PTMOL

This section provides an overview of the improvements implemented in the PTMOL modeling process. Based on the analyses performed in the post-study questionnaires, it was possible to understand some points that caused certain difficulties during the application of the language. These points generated the impression that some elements of PTMOL were not clear and easily understandable. For each of the difficulties collected, a change in PTMOL's methodological process was suggested. These evidence-based improvements are discussed in the following sections.

5.4.1 Elements with similar definitions

Comments made by the study participants indicated that the relationship between some PTMOL elements needed to be modified in order to make their definition clearer and eliminate redundancies. Among the elements mentioned were 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. As a result, it was decided to remove the "control" element from the language notation and leave the "prevention alert" and "countermeasures" elements as a mitigation strategy.

5.4.2 Confusing features and elements

During the study, there were several doubts related to some features and elements of PTMOL, because, in general, some were confusing or difficult to understand. This situation indicated opportunities for refinement and inspired some changes that were implemented to improve understanding and navigability between language components.

The element "Attacker's Actions", which allows the designer to create a rationale regarding the possible actions that a malicious agent could perform when in possession of the assets, was renamed. To make the purpose of the element 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.

Another point observed in relation to PTMOL's methodological procedure refers to the asset identification stage. In this step, the designer must identify the assets to be protected, before starting to discover what threats may occur. Depending on how the asset was shared in the system, three sharing ways and their respective variants are defined in order to enable an asset classification. However, it was observed

that the template for classifying assets is only intended for assets shared by the user in the system. This template did not foresee the classification of assets collected and processed by the system, which are not necessarily shared by the user, but which are collected and combined to generate other personal information. These assets refer to: (i) usage data; and (ii) relationship data. With that, a second template was created to also enable the classification of assets collected by the system.

5.4.3 Low completeness rate

The results of the experimental study showed a relatively low level in regards to the completeness metric. When examining the questions asked by the participants during the research, as well as some comments collected in the post-study questionnaire, it was noted that some elements of PTMOL were confused with others and others were absent, for example, the table for classifying assets collected by the system. Such components are an important aid for achieving completeness. This implies that the lack of important features in the methodological procedure of PTMOL affected its completeness in the experimental study. However, as previously shown, changes and additions have been made in order to enable a more complete modeling of privacy threats in the context of OSNs.

5.5 Discussion

The quantitative results of the experimental study indicated that improvements were needed in the PTMOL completeness indicator. Participants also pointed out doubts in using the language notation and understanding the language's semantics, a fact that possibly led to the occurrence of incompleteness.

On the other hand, the qualitative results indicate that PTMOL was perceived as useful and relatively easy to apply. Nonetheless, the qualitative results indicate that PTMOL was perceived as useful and relatively easy to apply. Although two participants indicated disagreement with the statements that assessed clarity and comprehension, overall, PTMOL was considered easy to learn and apply.

Our analyses enabled us to identify improvements to be made in PTMOL, such as the need to insert or adapt elements to make the threat modeling process effectively clearer. Based on the results obtained during the study, PTMOL was refined to meet the identified needs for improvement and a new version was designed in order to define its elements more clearly, as shown in Section 5.

5.6 Threats to Validity

Every study has threats that may affect the validity of its results [Wohlin et al., 2012]. 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 by Fernandez et al. [2012], 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. This study is rather small in terms of number of participants. Therefore, no strong statistical significance is expected and the quantitative results are to be considered as exploratory. Nevertheless, we put quite some effort on gathering qualitative observations and received rich and varied feedback from the participants.

6 A case study comparing PTMOL to an ad hoc technique

The previous study focused entirely on characterizing PTMOL, e.g., by analyzing the results of applying the language via a set of participants who represented potential users of the language. That study provided both quantitative and qualitative evidence with respect to PTMOL's threat modeling process, and showed how the language would perform once it is in the hands of potential designers. We carried out a new study with a different focus, since the purpose was to examine the reliability of the results produced by the modeling process proposed by PTMOL. There is a possibility that the catalog of threats implemented by PTMOL is limited and, consequently, does not anticipate important privacy threats. To check this hypothesis, we asked seven privacy experts to perform a threat analysis on an OSN modeled by a class diagram. The study protocol was approved by the Ethics and Research Committee of the Federal University of Amazonas (CAAE- 63572122.0.0000.5020). The execution and the results of the study are described below.

6.1 Characterization of the study object

To apply PTMOL in OSN threat modeling at the design level, it is necessary to have a general description of the features that allow the user to share data in the system or the features that inform how their data will be collected by the OSN. Therefore, the team of designers can use several design artifacts to help PTMOL threat modeling such as task and interaction models, personas, scenarios, or any other representation of the system by which it is possible to understand how the OSN carries out the sharing, the collection and the processing of user assets.

For the context of this study, a class diagram representing the modeling of an OSN for content sharing (general purpose) was used as an artifact. This choice, unlike the previous study, in which threat scenarios were applied, was also made to evaluate the level of application of PTMOL in another type of system representation, in this case a class diagram.

6.2 Privacy experts

Seven privacy experts were invited to participate in the study. Participants were given the class diagram and asked to identify as many privacy threats as possible for this scenario. Experts could consult the researchers to ask specific questions

about the scenario. To facilitate a uniform comparison, the experts were asked to document the threats in a template (Figure 12), which exemplified the level of detail expected of them in the threat analysis. Each specialist worked individually, i.e., without any contact with the others, and used their own knowledge (ad hoc technique) to perform the task. It is important to highlight that none of the participants knew PTMOL, thus ruling out any possibility of bias.

Assets	Privacy Threats	Threat Actors	Malicious uses
What must be protected?	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			
Asset 2			
Asset 3			
...			
Asset n			
<List all assets>	<Associate threat to asset>	<Indicate threat actors>	<Predict malicious uses>

Figure 12. Template provided to privacy experts for threat identification (ad hoc technique)

At the end of the analysis, which lasted about a week, the results were collected by the lead researcher. Each of the experts had to deliver a report that listed all threats identified in the scenario in question, which were documented using the template provided. In addition, they also individually discussed their results with the lead researcher in order to correct any ambiguities in their reports. Table 4 presents the characterization of the participants in this study; each participant has an ID, and the table shows their level of education and profession.

Table 4. Characterization of privacy experts

ID	Education	Profession
P1	Master	Teacher
P2	Master	Cybersecurity manager
P3	Specialist	IT Analyst
P4	Master	Teacher
P5	Master	IT Analyst
P6	Specialist	Teacher
P7	PhD	Cybersecurity manager

6.3 PTMOL experts

Three individuals are experts in the use of PTMOL: one is the first author and the others are PhD researchers, one in the field of security and privacy, the other in the field of HCI and privacy. The three PTMOL experts had to apply the PTMOL threat modeling process to the same class diagram provided to the privacy experts. Only the first and second steps - identification of assets and threats - of PTMOL were carried out, since the objective of the study was to compare the results produced with PTMOL modeling in relation to an ad hoc threat analysis. The first expert carried out his modeling and presented the results to his coauthors, who reviewed it. After a joint discussion to clarify any disagreements, the PTMOL experts documented the identified threats in a consolidated report.

6.4 Hypotheses

For the context of this study, we sought to investigate the reliability of PTMOL and assess whether the language did not consider any important threat that, ad hoc, could be discovered or pointed out by privacy experts. From this, the study was conducted to answer the following research question: Does PTMOL identify fewer privacy threats than privacy experts identify using an ad hoc technique (their own knowledge)? The results provided via the application of PTMOL and the application of an ad hoc technique are compared to answer the research question. Based on this, the following null hypothesis was formulated:

$$H_0 : \mu \left\{ \text{Rel} = \frac{VP_{ptmol}}{VP_{ptmol} + FN_{ptmol}} \right\} < 0.80$$

The false negatives (FN) represented in the null hypothesis indicate the threats identified by the privacy experts, which possibly would not be considered in the PTMOL threat catalog. It can be observed that the definition of reliability is similar to the concept of recall used in the previous study. Therefore, for consistency, the same limit of 80% was used. With this, the expectation is that PTMOL finds at least 80% of the total number of existing threats in the evaluated scenario.

6.5 Results

An oracle (reference solution) was created by the PTMOL experts in order to provide an estimate of how many privacy threats could be found in the scenario under analysis. The PTMOL experts applied the language to the class diagram and identified a total of 40 threats, as shown in Table 5. Although the oracle is the reference for the study's quantitative analysis, the study participants could make assumptions that differed from the oracle. Thus, the reference solution is used only as a basis for comparison.

Table 5. Reference solution indicating type and number of threats in the study scenario

Privacy Threats	Number of Threats
Profile cloning	5
Threat to reputation	4
Cyberstalking	4
Disclosure of information	9
Surveillance	1
Facial recognition	2
Identity Theft	2
Inference/Tracking	13
Unauthorized Recording	0
Total	40

Based on the oracle produced, the PTMOL experts carefully examined the reports produced by the privacy experts in order to identify the threats pointed out by them and, subsequently, compare them with the threat diagnosis produced by the PTMOL experts. Table 6 presents the set of threats indicated by the study participants in their reports, as well as the source of the threat, i.e., the ID of the participant who indicated it.

Table 6. Threats identified by privacy experts

Privacy Threats	Source
Phishing	P3, P4, P7
Targeted advertising	P1, P7
Doxing	P7
Extortion	P7
Privilege Elevation	P5, P7
Location Disclosure	P4, P5, P7
Personal Data Extraction	P2, P6
Information leakage	P2, P3, P4, P5, P6, P7
Improper Access	P2, P3, P6
Indiscriminate photo download	P5
Sensitive Data Exposure	P1, P4

From a quantitative perspective, the experts that applied PTMOL identified 40 threats, while the study participants found, ad hoc, 11 threats in the provided scenario. In general, it was found that the threats pointed out by the participants were the same or similar to the threats identified by the PTMOL experts, although they were described using different nomenclatures. In order to establish a valid and traceable comparison between the results produced by the study participants and by the PTMOL experts, each threat indicated by the participants was associated with a corresponding PTMOL threat, so that it was possible to check the conceptual relationship between the threats. This analysis can be seen in Table 7.

Table 7. Association of threats pointed out by privacy experts and PTMOL threats

Threats/PTMOL	Threats/Privacy Experts
Reputation Threat	Privilege Elevation, Extortion
Cyberstalking	Extortion
Information Disclosure	Location Disclosure, Exposure, Data Leakage, Doxing
Facial Recognition	Indiscriminate Photo Download
Identity Theft	Phishing, Unauthorized Access to Private Data
Inference/Tracking	Targeted Advertising, Personal Data Extraction

From this comparative analysis, it is possible to observe that all the threats indicated in the reports produced by the privacy experts for the provided scenario are foreseen in the PTMOL threat catalog. The threats of Surveillance and Profile Cloning were not indicated or perceived in the scenario by the study participants. This indicates that there was no incidence of false negatives, in other words, threats that could possibly not be being considered by PTMOL. The identified results indicate that, through the generated oracle, there were a total of 40 threats in the evaluated scenario (true positives - TP) and all potential threats detected by the privacy experts were already predicted by the PTMOL catalog (0 false negatives - FN). This results in a 100% reliability rate for the language threat modeling process. Therefore, there is evidence to refute the null hypothesis, indicating that PTMOL achieved optimal and satisfactory coverage compared to the threat diagnosis produced by the privacy experts.

Although the results of a single experience cannot be generalized to other contexts, it is believed that the results ob-

tained in this study indicate that PTMOL has relevant support for specialists and non-specialists to reach an adequate level in modeling privacy threats. In addition, privacy experts can use PTMOL as a support to avoid gaps in their ad hoc threat identification activities, as it was possible to observe that a structured support for threat modeling guarantees a more complete diagnosis and a more robust analysis of threats.

7 Limitations

Every study has limitations and they need to be reported. The main limitation of this study is related to the study participants who, as privacy experts, may have provided biased perceptions in relation to their own beliefs, thus causing distortions in the interpretation of reality and consequent distortions in the results obtained. To reduce this limitation, we sought to select specialists with greater experience.

8 Conclusions and Future Works

Privacy has become a primary concern among social network users. Users can become the victims of privacy threats such as identity theft, cyberstalking or information disclosure due to personal data revealed in their profiles. 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.

As such, this paper aims to support threat modeling in OSNs, with a specific focus on user privacy. To achieve this purpose, we defined 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. This language was developed from evidence gathered in the literature and was empirically evaluated through experimental study.

Initially, an experimental study was performed to evaluate the completeness, correctness, productivity, ease of use, usefulness, and intended future use of PTMOL. As PTMOL can be used during the design phase of the software development lifecycle, the evaluation took into account the perspective of potential system designers. The quantitative analysis of the study indicated good results for the correctness and completeness of the PTMOL threat modeling process. The results for usefulness and ease of use indicators were generally positive. As it is a conceptual modeling intended to be applied at the design level, the results produced by the team of designers need to be detailed enough to guarantee a quality interpretation of the threat scenario under analysis.

Through qualitative analysis, improvements in PTMOL based on empirical evidence were identified, such as the need to include and adapt elements of the language to allow the effective representation of all aspects of threat modeling. All improvements have now been implemented.

Finally, a case study was carried out with the purpose of examining the reliability of the results produced by the mod-

eling process proposed by PTMOL. For this, PTMOL had to compete with privacy experts. In this sense, seven experts were asked to detect privacy threats using their own procedures and these results were compared with those of PTMOL. The results obtained in this study indicated that PTMOL achieved satisfactory coverage compared to the threat diagnosis produced by expert participants, and as such reached 100% reliability. In addition, privacy experts can use PTMOL as a support to avoid gaps in their ad hoc threat identification activities.

The obtained results open up new research perspectives that can be explored in future work. The changes implemented in PTMOL were based on the results of empirical studies, which made it possible to improve the general quality of language. As future perspectives, we highlight the continuity of empirical studies to evaluate the new version of PTMOL with the purpose of increasing the reliability of the results obtained. A new study may be carried out, with experimental conditions similar to the previous ones, in order to evaluate the improved version of PTMOL. These results can then be compared with previous ones to determine whether the changes actually result in improvements to our proposal. Another interesting validation would be to further evaluate PTMOL in a professional environment. Up until the present moment, the study participants were mostly students; however, as the proposed improvements resulted in a more complete version of PTMOL, it would be interesting to examine how professionals in an industrial environment perceive the use of the language. Finally, we intend to add some tool support to the PTMOL methodology to reach an even bigger audience.

9 Acknowledgments

We thank the participants of the study. We also thank the Brazilian Symposium on Human Factors in Computer Systems for the invitation to submit an extended version of the paper "PTMOL: a suitable approach for modeling privacy threats in online social networks" to compose a special issue of the JIS-SBC Journal on Interactive Systems. This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001. This work was partially supported by Amazonas State Research Support Foundation - FAPEAM - through the POSGRAD project.

References

- Abawajy, J. H., Ninggal, M. I. H., and Herawan, T. (2016). Privacy preserving social network data publication. *IEEE communications surveys & tutorials*, 18(3):1974–1997.
- Abid, Y., Imine, A., and Rusinowitch, M. (2018). Online testing of user profile resilience against inference attacks in social networks. In *European Conference on Advances in Databases and Information Systems*, pages 105–117. Springer.
- Aktypi, A., Nurse, J., and Goldsmith, M. (2017). Unwinding ariadne's identity thread: Privacy risks with fitness

- trackers and online social networks. volume 2017-January, pages 1–11.
- Al-Asmari, H. and Saleh, M. (2019). A conceptual framework for measuring personal privacy risks in facebook on-line social network.
- Ali, S., Islam, N., Rauf, A., Din, I. U., Guizani, M., and Rodrigues, J. J. (2018). Privacy and security issues in online social networks. *Future Internet*, 10(12):114.
- Ali, S., Rauf, A., Islam, N., and Farman, H. (2019). A framework for secure and privacy protected collaborative contents sharing using public osn. *Cluster Computing*, 22:7275–7286.
- Altman, I. (1975). The environment and social behavior: Privacy, personal space, territory, and crowding.
- Basili, V. R. (1996). The role of experimentation in software engineering: past, current, and future. In *Proceedings of IEEE 18th International Conference on Software Engineering*, pages 442–449. IEEE.
- Bioglio, L., Capecchi, S., Peiretti, F., Sayed, D., Torasso, A., and Pensa, R. (2019). A social network simulation game to raise awareness of privacy among school children. *IEEE Transactions on Learning Technologies*, 12(4):456–469.
- Casas, I., Hurtado, J., and Zhu, X. (2015). Social network privacy: Issues and measurement. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9419:488–502.
- Cavoukian, A. et al. (2009). Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada*, 5:12.
- Davies, H. (2015). Ted cruz using firm that harvested data on millions of unwitting facebook users. *the Guardian*, 11:2015.
- De, S. and Imine, A. (2018a). Privacy scoring of social network user profiles through risk analysis. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10694 LNCS:227–243.
- De, S. and Imine, A. (2018b). To reveal or not to reveal: Balancing user-centric social benefit and privacy in online social networks. pages 1157–1164.
- Derlega, V. J. and Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues*, 33(3):102–115.
- Dong, C. and Zhou, B. (2016). Privacy inference analysis on event-based social networks. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10047 LNCS:421–438.
- Fernandez, A., Abrahão, S., Insfran, E., and Matera, M. (2012). Further analysis on the validation of a usability inspection method for model-driven web development. In *Proceedings of the ACM-IEEE international symposium on Empirical software engineering and measurement*, pages 153–156.
- Fogues, R., Such, J., Espinosa, A., and Garcia-Fornes, A. (2015). Open challenges in relationship-based privacy mechanisms for social network services. *International Journal of Human-Computer Interaction*, 31(5):350–370.
- Jaafar, O. and Birregah, B. (2015). Multi-layered graph-based model for social engineering vulnerability assessment. In *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pages 1480–1488. IEEE.
- Joyee De, S. and Imine, A. (2019). On consent in online social networks: Privacy impacts and research directions (short paper). *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11391 LNCS:128–135.
- Kagan, D., Alpert, G. F., and Fire, M. (2020). Zooming into video conferencing privacy and security threats. *arXiv preprint arXiv:2007.01059*.
- Kavianpour, S., Ismail, Z., and Mohtasebi, A. (2011). Effectiveness of using integrated algorithm in preserving privacy of social network sites users. *Communications in Computer and Information Science*, 167 CCIS(PART 2):237–249.
- Khan, R., McLaughlin, K., Laverty, D., and Sezer, S. (2017). Stride-based threat modeling for cyber-physical systems. In *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pages 1–6. IEEE.
- Kim, K. H., Kim, K., and Kim, H. K. (2021). Stride-based threat modeling and dread evaluation for the distributed control system in the oil refinery. *ETRI Journal*.
- Kumar, H., Jain, S., and Srivastava, R. (2017). Risk analysis of online social networks. pages 846–851.
- Laitenberger, O. and Dreyer, H. M. (1998). Evaluating the usefulness and the ease of use of a web-based inspection data collection tool. In *Proceedings Fifth International Software Metrics Symposium. Metrics (Cat. No. 98TB100262)*, pages 122–132. IEEE.
- Laorden, C., Sanz, B., Alvarez, G., and Bringas, P. G. (2010). A threat model approach to threats and vulnerabilities in on-line social networks. In *Computational Intelligence in Security for Information Systems 2010*, pages 135–142. Springer.
- Lazar, J. and Barbosa, S. D. (2017). Introduction to human-computer interaction. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, pages 1202–1204.
- Lowson, B. (2005). How designers think. the design process demystified. *Tehran: University of Shahid-Beheshti*.
- Mahmood, S. (2012). New privacy threats for facebook and twitter users. pages 164–169.
- Marangunić, N. and Granić, A. (2015). Technology acceptance model: a literature review from 1986 to 2013. *Universal access in the information society*, 14:81–95.
- Oukemeni, S., Rifà-Pous, H., and Puig, J. M. M. (2019). Privacy analysis on microblogging online social networks: a survey. *ACM Computing Surveys (CSUR)*, 52(3):1–36.
- Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Suny Press.
- Pfützmann, A. and Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.
- Potteiger, B., Martins, G., and Koutsoukos, X. (2016). Software and attack centric integrated threat modeling for

- quantitative risk assessment. In *Proceedings of the Symposium and Bootcamp on the Science of Security*, pages 99–108.
- Preece, J., Rogers, Y., Sharp, H., Benyon, D., Holland, S., and Carey, T. (1994). *Human-computer interaction*. Addison-Wesley Longman Ltd.
- Rannenbergh, K. (2011). Iso/iec standardization of identity management and privacy technologies. *Datenschutz und Datensicherheit-DuD*, 35(1):27–29.
- Rathore, S., Sharma, P., Loia, V., Jeong, Y.-S., and Park, J. (2017). Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, 421:43–69.
- Sanz, B., Laorden, C., Alvarez, G., and Bringas, P. G. (2010). A threat model approach to attacks and countermeasures in on-line social networks. In *Proceedings of the 11th Reunion Espanola de Criptografia y Seguridad de la Informaci3n (RECSI)*, pages 343–348.
- Scandariato, R., Wuyts, K., and Joosen, W. (2015). A descriptive study of microsoft’s threat modeling technique. *Requirements Engineering*, 20(2):163–180.
- Shi, Z., Graffi, K., Starobinski, D., and Matyunin, N. (2021). Threat modeling tools: A taxonomy. *IEEE Security & Privacy*, (01):2–13.
- Shokri, R., Theodorakopoulos, G., Troncoso, C., Hubaux, J.-P., and Le Boudec, J.-Y. (2012). Protecting location privacy: optimal strategy against localization attacks. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 617–627.
- Shostack, A. (2008). Experiences threat modeling at microsoft. *MODSEC@ MoDELS*, 2008:35.
- Shostack, A. (2014). *Threat modeling: Designing for security*. John Wiley & Sons.
- Shull, F., Carver, J., and Travassos, G. H. (2001). An empirical methodology for introducing software processes. *ACM SIGSOFT Software Engineering Notes*, 26(5):288–296.
- Siddula, M., Li, L., and Li, Y. (2018). An empirical study on the privacy preservation of online social networks. *IEEE Access*, 6:19912–19922.
- Solon, O. (2018). Facebook says cambridge analytica may have gained 37m more users’ data. *The Guardian*, 4.
- Sramka, M. (2012). Privacy scores: Assessing privacy risks beyond social networks. *Infocommunications Journal*, 4(4):36–41.
- Tucker, R., Tucker, C., and Zheng, J. (2015). Privacy pal: Improving permission safety awareness of third party applications in online social networks. pages 1268–1273.
- UcedaVelez, T. and Morana, M. M. (2015). *Risk Centric Threat Modeling: process for attack simulation and threat analysis*. John Wiley & Sons.
- Vu, H., Law, R., and Li, G. (2019). Breach of traveller privacy in location-based social media. *Current Issues in Tourism*, 22(15):1825–1840.
- Wang, Y. and Nepali, R. (2015). Privacy threat modeling framework for online social networks. pages 358–363.
- Watanabe, C., Amagasa, T., and Liu, L. (2011). Privacy risks and countermeasures in publishing and mining social network data. pages 55–66.
- Wen, G., Liu, H., Yan, J., and Wu, Z. (2018). A privacy analysis method to anonymous graph based on bayes rule in social networks. pages 469–472.
- Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., and Wesslén, A. (2012). *Experimentation in software engineering*. Springer Science & Business Media.
- Wuyts, K., Van Landuyt, D., Hovsepian, A., and Joosen, W. (2018). Effective and efficient privacy threat modeling through domain refinements. In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, pages 1175–1178.
- Xiong, W. and Lagerström, R. (2019). Threat modeling—a systematic literature review. *Computers & security*, 84:53–69.
- Xu, H., Teo, H.-H., and Tan, B. (2005). Predicting the adoption of location-based services: the role of trust and perceived privacy risk. *ICIS 2005 proceedings*, page 71.
- Zeng, Y., Sun, Y., Xing, L., and Vokkarane, V. (2015). A study of online social network privacy via the tape framework. *IEEE Journal on Selected Topics in Signal Processing*, 9(7):1270–1284.
- Zheleva, E. and Getoor, L. (2009). To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In *Proceedings of the 18th international conference on World wide web*, pages 531–540.
- Zheleva, E. and Getoor, L. (2011). Privacy in social networks: A survey. In *Social network data analytics*, pages 277–306. Springer.