Linguagem para a Modelagem de Ameaças de Privacidade

Andrey Rodrigues[1], **Maria Lúcia Villela**[2], **Eduardo Feitosa** [3]

[1]Instituto de Ciências Exatas e Tecnologia
Universidade Federal do Amazonas (UFAM) – Itacoatiara – AM – Brasil

[2]Departamento de Informática
Universidade Federal de Viçosa (UFV) – Viçosa – MG – Brasil

[3]Instituto de Computação
Universidade Federal do Amazonas (UFAM) – Manaus – AM – Brasil

andrey.rodrigues@ufam.edu.br, maria.villela@ufv.br,

efeitosa@icomp.ufam.edu.br

Resumo. *Este trabalho apresenta a PTMOL (Privacy Threat Modeling Language), uma linguagem de apoio à modelagem de ameaças de privacidade orientada à Redes Sociais Online (RSOs). A linguagem proposta visa apoiar a busca antecipada por ameaças às quais um usuário poderá estar exposto e quais controles de privacidade uma RSO precisa definir para reduzir os efeitos e consequências dessas ameaças. A linguagem foi avaliada por meio da condução de um conjunto de estudos empíricos que permitiram realizar seus procedimentos de validade e confiabilidade. Os resultados dos estudos indicam que o emprego da linguagem é potencialmente útil para a identificação de ameaças reais de privacidade devido ao caráter exploratório e reflexivo da mesma.*

1. Introdução

As Redes Sociais Online (RSOs) tornaram-se um dos principais fenômenos tecnológicos da Web, ganhando uma popularidade eminente entre seus usuários. Atualmente, essas plataformas fornecem diversas funcionalidades e serviços que atraem cada vez mais usuários. Por exemplo, permitem analisar dados e correlacionar as preferências dos usuários para fornecer serviços avançados e personalizados. Com isso, podem recomendar amigos ou interesses em comum com base nas informações extraídas dos perfis e atividades dos usuários, como preferências, navegação diária, entre outros [Oukemeni et al. 2019].

Com a popularidade mundial dos serviços de RSOs, as pessoas passaram a dedicar tempo e esforço para manter e manipular sua identidade online nesses sistemas. À medida que os usuários confiam cada vez mais nessas aplicações para suas atividades de comunicação, o processamento de dados pessoais por meio dessas redes tem exposto os usuários a diversos tipos de ameaças de privacidade [Rathore et al. 2017, Siddula et al. 2018, Ali et al. 2018]. Uma ameaça de privacidade é um evento indesejável potencial ou real que pode causar divulgação, exposição e uso indevido de dados privados do usuário [Joyee De and Imine 2019, Laorden et al. 2010]. Sua consequência é a violação de privacidade, onde dados pessoais são divulgados a indivíduos ou entidades não autorizados, para fins maliciosos [Abawajy et al. 2016].

Uma estratégia para tratar as questões mencionadas é antecipar a preocupação com a privacidade para as etapas que antecedem o desenvolvimento de aplicações sociais. Na área de Interação Humano-Computador (IHC), diferentes técnicas apoiam o design de sistemas, tais como a criação de personas, modelagem de tarefas, modelagem de interação e construção de *mockups* [Barbosa and Silva 2010]. Entretanto, essas propostas generalistas não possuem características específicas para tratar ameaças de privacidade em nível de design. Técnicas tradicionais de segurança previamente estabelecidas podem oferecer suporte à antecipação da preocupação com ameaças nos estágios iniciais do desenvolvimento de sistemas. Uma técnica amplamente usada nesse contexto é a modelagem de ameaças.

Diante disso, este trabalho apresenta a PTMOL *(Privacy Threat Modeling Language)*, uma linguagem para a modelagem de ameaças em RSOs, com foco na privacidade do usuário [Rodrigues et al. 2023b]. Esta linguagem foi desenvolvida a partir de evidências coletadas na literatura e foi avaliada empiricamente por meio um conjunto de estudos empíricos. A PTMOL permite a busca antecipada por ameaças às quais um usuário poderá está exposto e quais controles de privacidade uma RSO precisa definir para reduzir os efeitos e consequências dessas ameaças. A linguagem pode ser incorporada ao desenvolvimento de RSOs durante a fase de design e pode auxiliar designers e engenheiros de software a introduzir modelagem de ameaças em seus projetos, sem exigir um alto nível de especialidade na área de privacidade.

2. Privacy Threat MOdeling Language - PTMOL

A PTMOL é uma linguagem de apoio a modelagem de ameaças de privacidade em nível de design. Trata-se de uma linguagem porque pode ser utilizada para expressar o conhecimento em uma estrutura que é definida por um conjunto consistente de regras. Com isso, permite que designers de RSOs identifiquem possíveis ameaças de privacidade, suas consequências e como elas podem ser mitigadas. Para realizar esse suporte, a PTMOL possui recursos para o design de ameaças e permite gerar um modelo de ameaças como parte do design. Por ser uma linguagem, a PTMOL é formada pelos seguintes componentes: (a) um vocabulário; (b) a sintaxe; e (c) a semântica. O vocabulário é a coleção de todas as palavras à disposição do designer que podem ser usadas no processo de modelagem. A sintaxe é o conjunto consistente de regras da linguagem, indicando como elas podem ser empregadas durante o processo de modelagem. Por fim, a semântica refere-se ao significado associado aos elementos da linguagem. Quanto ao seu vocabulário, a PTMOL possui os seguintes termos:

- **Ativo**. Atributo relacionado ao alvo (usuário) que possui um valor pessoal.
- **Ameaça**. Uma situação indesejada que pode colocar em risco os ativos do usuário.
- **Fontes de vazamento**. Fontes que operam dentro ou fora do sistema para violar a privacidade do usuário.
- **Usos maliciosos**. Descreve os usos maliciosos previstos que podem afetar a privacidade do usuário.
- **Alerta de prevenção**. Alerta do sistema para informar os usuários sobre qualquer ação que pode causar violações graves para a sua privacidade.
- **Contramedida**. Ações do sistema para mitigar ameaças de privacidade executadas pelas fontes de vazamento.

- **Zona de compartilhamento**. Representa um espaço do sistema onde os ativos do usuário podem ser compartilhados ou coletados.
- **Zona de risco**. Representa um espaço do sistema no qual pode ocorrer ameaças de privacidade.
- **Zona de vazamento**. Representa a porta de acesso indevido aos dados privados do usuário.

Com base no vocabulário da PTMOL, criou-se um conjunto de elementos e regras que determinam a sintaxe da linguagem. Esses elementos e seus relacionamentos são ilustrados na Figura 1, agrupados segundo a sua zona: zona de compartilhamento, zona de risco e zona de vazamento. Tais elementos podem ser utilizados ao final do processo para gerar o modelo de ameaças resultante da modelagem.

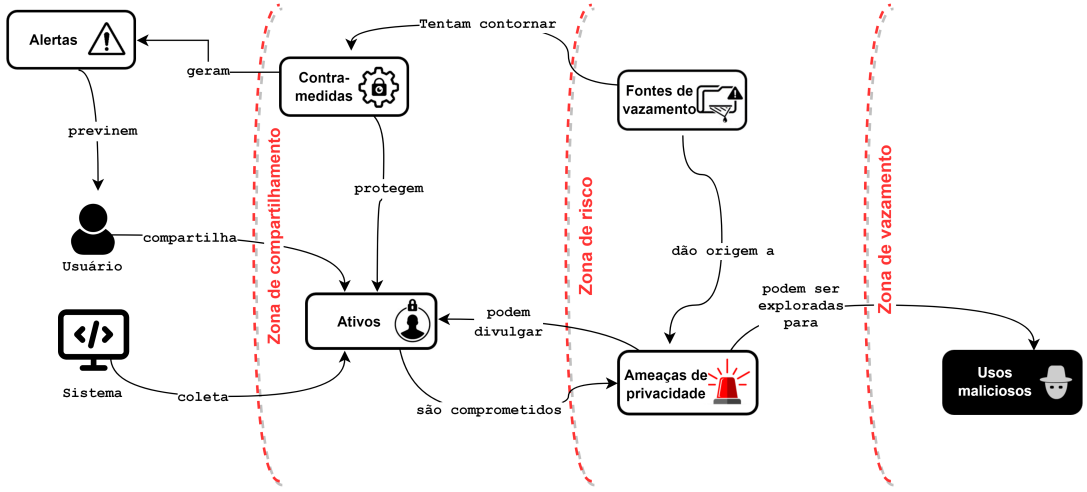

Figura 1. Visão geral sobre as relações entre os elementos da PTMOL

Para apoiar o processo de modelagem de ameaças, a PTMOL dispõe de um conjunto de recursos. O primeiro recurso estabelecido é o catálogo de ameaças, o qual descreve as ameaças mais críticas para a privacidade do usuário. Esse catálogo de ameaças é um recurso de grande valor, pois ajuda o designer a refletir sobre quais cenários de ameaça um usuário está potencialmente exposto. Um segundo recurso previsto é a taxonomia de contramedidas, que pode ser utilizada para prevenir ou mitigar os efeitos das ameaças. Após entender um possível cenário de ameaças ao qual o usuário poderá está exposto, a PTMOL possibilita que o designer defina trechos da sua modelagem de ameaças a partir de padrões, ou *templates,* integrados à linguagem, de modo que sua compreensão sobre o problema e possíveis soluções se amplie.

O processo de aplicação da PTMOL permite dividir um processo complexo em tarefas menores, facilitando a identificação de todo o cenário de ameaças. Assim, para iniciar a modelagem de ameaças via *template*, o designer terá que seguir um conjunto atividades para identificar: (i) o que é necessário proteger do usuário (ativos), (ii) quais eventos indesejáveis (ameaças) podem ocorrer e colocar em risco os ativos do usuário; e (iii) quais estratégias adotar (contramedidas) para prevenir ou mitigar os efeitos das ameaças aos dados do usuário.

3. Validação Empírica

Durante o desenvolvimento da PTMOL, testamos a linguagem por meio de um conjunto de estudos empíricos. Inicialmente, dois estudos experimentais foram executados para avaliar a completude, a corretude, a produtividade, a facilidade de uso, utilidade, satisfação percebida e intenção de uso futuro da PTMOL. Os resultados desses estudos estão disponíveis em [Rodrigues et al. 2022, Rodrigues et al. 2023b].

A análise quantitativa dos estudos indicou bons resultados para a corretude e completude do processo de modelagem de ameaças da PTMOL. Os resultados para os indicadores de utilidade e facilidade de uso foram, no geral, positivos. Por se tratar de uma modelagem conceitual destinada para ser aplicada em nível de design, os resultados produzidos pela equipe de design precisam ser detalhados o suficiente para garantir uma interpretação de qualidade do cenário de ameaça sob análise. Além disso, os resultados do segundo estudo também apontaram indícios de que a PTMOL é aplicável até mesmo por profissionais não especialistas em privacidade, pois todos os participantes conseguiram mapear cenários de ameaças mesmo não tendo conhecimento técnico.

Uma vez que os resultados obtidos com os estudos anteriores indicaram a validade e viabilidade da PTMOL, realizou-se um terceiro estudo com o objetivo de compreender o modo com que possíveis designers de sistemas aplicariam o processo de modelagem de ameaças da PTMOL. Os resultados do estudo foram positivos, uma vez que forneceram *insights* relevantes para melhorar a qualidade da PTMOL.

Por fim, um último estudo foi realizado com propósito de examinar a confiabilidade dos resultados produzidos pelo processo de modelagem proposto pela PTMOL. Para isso, a PTMOL teve que competir com especialistas em privacidade. Nesse sentido, sete especialistas foram solicitados a detectar ameaças de privacidade usando seus próprios procedimentos e esses resultados foram comparados com os da PTMOL, tais resultados estão disponíveis em [Rodrigues et al. 2023a]. Os resultados obtidos nesse estudo indicaram que a PTMOL alcançou uma cobertura satisfatória comparativamente ao diagnóstico de ameaças produzido pelos participantes especialistas, atingindo 100% de confiabilidade. Além disso, especialistas em privacidade podem utilizar a PTMOL como um suporte para evitar lacunas em suas atividades *ad hoc* de identificação de ameaças.

4. Conclusão

Este trabalho apresentou a PTMOL *(Privacy Threat Modeling Language*), uma linguagem de apoio à modelagem de ameaças de privacidade orientada à RSOs. A linguagem proposta visa apoiar a busca antecipada por ameaças às quais um usuário poderá está exposto e quais controles de privacidade uma RSO precisa definir para reduzir os efeitos e consequências dessas ameaças. A linguagem foi avaliada por meio da condução de um conjunto de estudos empíricos que permitiram realizar seus procedimentos de validade e confiabilidade. Os resultados dos estudos indicam que o emprego da linguagem é potencialmente útil para a identificação de ameaças reais de privacidade devido ao caráter exploratório e reflexivo da mesma. Portanto, a PTMOL pode ser incorporada ao desenvolvimento de RSOs durante o nível de design e pode auxiliar projetistas e engenheiros de software a introduzir modelagem de ameaças em seus projetos, sem exigir um alto nível de especialidade na área de privacidade.

Referências

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.

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.

Barbosa, S. and Silva, B. (2010). *Interação humano-computador*. Elsevier Brasil.

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. cited By 0.

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.

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.

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. cited By 35.

Rodrigues, A., Villela, M. L., and Feitosa, E. (2022). Ptmol: a suitable approach for modeling privacy threats in online social networks. In *Proceedings of the 21st Brazilian Symposium on Human Factors in Computing Systems*, pages 1–12.

Rodrigues, A., Villela, M. L., and Feitosa, E. (2023a). Exploring how experienced and unexperienced professionals use a privacy threat modeling methodology. *Journal on Interactive Systems*, 14(1):274–291.

Rodrigues, A., Villela, M. L. B., and Feitosa, E. L. (2023b). Privacy threat modeling language. *IEEE Access*, 11:24448–24471.

Siddula, M., Li, L., and Li, Y. (2018). An empirical study on the privacy preservation of online social networks. *IEEE Access*, 6:19912–19922.