PnGRequirementsPhaseThreatModeling

No artigo "Crowd Sourcing the Creation of Personae Non Gratae for Requirements-Phase Threat Modeling", é apresentada uma abordagem inovadora para a modelagem de ameaças durante a fase de requisitos de desenvolvimento de sistemas, utilizando Personae non Gratae (PnGs). As principais ideias abordadas incluem:

- **Definição de Personae non Gratae (PnGs)**:
    - Inspiradas nas personas usadas em design de experiência do usuário (UX), as PnGs representam usuários archetypais que interagem com o sistema de maneiras indesejadas, comprometendo sua segurança.
    - Diferente das personas tradicionais, que enfocam usuários legítimos, as PnGs focam em usuários mal-intencionados, auxiliando na antecipação de abusos e vulnerabilidades.
- **Comparação com Outros Métodos de Modelagem de Ameaças**:
    - Em um estudo recente, as árvores de ataque baseadas em PnGs demonstraram maior consistência em comparação com métodos como STRIDE e Security Cards.
    - No entanto, nenhum método individual identificou todas as ameaças possíveis, o que motivou a exploração do uso de crowd-sourcing para identificar ameaças de forma mais abrangente.
- **Crowd-Sourcing na Identificação de Ameaças**:
    - A abordagem proposta utiliza técnicas de recuperação de informação para analisar e consolidar ameaças identificadas por múltiplos colaboradores.
    - O processo culmina na construção de um modelo de ameaças unificado, auxiliado por analistas humanos, que incorpora uma gama mais ampla de cenários de ataque.
- **Estrutura e Etapas do Artigo**:
    - **Seção II**: Visão geral das técnicas existentes de modelagem de ameaças.
    - **Seção III**: Descrição detalhada das PnGs e sua contribuição para a modelagem de ameaças.
    - **Seções IV e V**: Métodos de coleta e análise de dados do estudo.
    - **Conclusão**: Discussão dos resultados preliminares, ameaças à validade e considerações finais.
- **Vantagens das PnGs**:
    - Promovem uma análise mais focada nas capacidades e motivações dos atacantes.
    - Facilitam a identificação de vulnerabilidades específicas ao considerar diferentes perfis de atacantes.
    - Melhoram a abrangência e a consistência dos modelos de ameaças através da colaboração coletiva.

Relevância para a Pesquisa

A utilização de Personae non Gratae (PnGs) na modelagem de ameaças, conforme descrito no artigo, é altamente relevante para a pesquisa em modelagem de ameaças em organizações não-hierárquicas. As PnGs permitem uma abordagem mais detalhada e diversificada na identificação de vetores de ataque,

refletindo melhor a complexidade e a distribuição de responsabilidades em estruturas horizontais. Além disso, a integração de métodos de crowd-sourcing para a criação de PnGs amplia a abrangência das ameaças identificadas, promovendo uma visão mais completa e colaborativa das possíveis vulnerabilidades.

Especificamente:

- **Alinhamento com Estruturas Horizontais**: A abordagem colaborativa e distribuída do crowd-sourcing ressoa com a natureza não-hierárquica das organizações focadas na pesquisa, permitindo a participação de diversos stakeholders na identificação de ameaças.
- **Melhoria na Consistência dos Modelos de Ameaças**: Ao utilizar PnGs, que demonstraram maior consistência em estudos comparativos, a pesquisa pode desenvolver modelos de ameaças mais robustos e confiáveis, essenciais para a criação de um protocolo de modelagem de ameaças eficaz.
- **Inclusão de Diversas Perspectivas de Atacantes**: As PnGs facilitam a consideração de múltiplos perfis de atacantes, o que é crucial para organizações descentralizadas onde as ameaças podem ser variadas e multifacetadas.
- **Suporte à Governança Horizontal e Confiança Distribuída**: A metodologia proposta reforça a governança horizontal ao promover uma análise de ameaças que considera a colaboração e a confiança distribuída, elementos centrais para a segurança organizacional em estruturas não-hierárquicas.