PersonaeNonGratae

No artigo "How Well Do You Know Your Personae Non Gratae", são exploradas técnicas avançadas para a modelagem de ameaças durante a fase de requisitos de desenvolvimento de sistemas, com ênfase na utilização de Personae Non Gratae (PnGs). As principais ideias abordadas incluem:

- **Limitações das Abordagens Tradicionais**:
    - **Checklists e Regulamentações**: Embora úteis para garantir a consideração de questões de segurança comuns, como controle de acesso e logs de auditoria (exemplo: HIPAA para dados de saúde), essas abordagens são insuficientes para identificar riscos de segurança específicos e únicos de uma aplicação.
- **Técnicas Avançadas para Modelagem de Ameaças**:
    - **Personae Non Gratae (PnGs)**:
        - **Definição**: Inspiradas nas personas utilizadas em design de experiência do usuário (UX), as PnGs representam usuários archetypais que interagem com o sistema de maneiras indesejadas, comprometendo sua segurança.
        - **Objetivo**: Ajudar a antecipar abusos e vulnerabilidades, fornecendo uma abordagem mais sistemática para identificar como usuários mal-intencionados podem explorar o sistema.
        - **Exemplo**: "Hugh", um jovem que pretende atacar o sistema, cujos objetivos podem ser especificados para expor pontos de vulnerabilidade.
    - **Misuse Cases (Casos de Uso de Abuso)**:
        - **Definição**: Extensões dos diagramas de casos de uso tradicionais que incluem atores maliciosos e seus casos de uso indesejados.
        - **Objetivo**: Determinar antecipadamente como o produto de software deve responder a usos não intencionais ou maliciosos, ajudando a identificar e mitigar ameaças específicas.
        - **Exemplo**: Diagramas que mostram interações entre atores legítimos (como um solicitante de seguro) e atores maliciosos (como um cracker que tenta obter informações privadas).
    - **Anotação de Diagramas de Atividades com Preocupações de Segurança**:
        - **Definição**: Adição de elementos relacionados à segurança em diagramas de atividades para documentar necessidades de privacidade, capacidades de auditoria e requisitos de não repúdio.
        - **Objetivo**: Integrar considerações de segurança diretamente no fluxo de trabalho do sistema, facilitando a identificação de pontos críticos onde a segurança pode ser comprometida.
- **Vantagens das PnGs**:
    - **Abordagem Sistemática**: Promove uma análise detalhada das capacidades e motivações dos atacantes, permitindo a identificação de vulnerabilidades específicas.

- **Consistência na Modelagem de Ameaças**: Estudos comparativos indicam que modelos de ameaças baseados em PnGs apresentam maior consistência em comparação com métodos tradicionais como STRIDE e Security Cards.
- **Crowd-Sourcing na Identificação de Ameaças**: A utilização de técnicas de recuperação de informação e colaboração coletiva para consolidar ameaças identificadas, resultando em modelos de ameaças mais abrangentes e robustos.

Relevância para a Pesquisa

A utilização de Personae Non Gratae (PnGs) na modelagem de ameaças, conforme apresentado no artigo, é altamente relevante para a pesquisa em modelagem de ameaças em organizações não-hierárquicas. As PnGs proporcionam uma abordagem estruturada e sistemática para identificar e analisar vetores de ataque específicos, alinhando-se com o objetivo de criar um protocolo que valorize a horizontalidade organizacional como um ativo estratégico.

Especificamente:

- **Alinhamento com Estruturas Horizontais**: A abordagem colaborativa e distribuída do uso de PnGs ressoa com a natureza não-hierárquica das organizações focalizadas na pesquisa, permitindo a participação de diversos stakeholders na identificação de ameaças. Isso fortalece a confiança distribuída e a governança horizontal, pilares centrais da pesquisa.
- **Identificação de Ameaças Únicas**: Ao ir além de checklists e regulamentações, as PnGs facilitam a identificação de ameaças únicas e específicas que podem emergir em ambientes descentralizados, onde responsabilidades e funções são distribuídas entre múltiplos participantes.
- **Melhoria na Consistência e Abrangência dos Modelos de Ameaças**: A aplicação de PnGs, especialmente quando combinada com métodos de crowd-sourcing, resulta em modelos de ameaças mais consistentes e abrangentes. Isso é crucial para organizações não-hierárquicas, onde a diversidade de operações e interações pode introduzir uma variedade maior de vetores de ataque.
- **Integração com Outras Técnicas de Modelagem**: A combinação de PnGs com misuse cases e a anotação de diagramas de atividades com preocupações de segurança proporciona uma visão multifacetada das ameaças, permitindo uma avaliação de riscos mais detalhada e a implementação de contramedidas eficazes.
- **Facilitação de uma Cultura de Segurança Distribuída**: Ao integrar princípios de segurança no fluxo de trabalho normal através das PnGs, a metodologia contribui para a construção de uma cultura de segurança distribuída, onde todos os membros da organização estão conscientes e engajados na mitigação de riscos, reforçando a governança horizontal.