ExperiencesThreatModelingAtMicrosoft

O artigo detalha a aplicação prática da modelagem de ameaças na Microsoft, destacando a integração dessa metodologia no processo de desenvolvimento de software para melhorar a segurança dos produtos.

Principais Pontos:

1. **Definições e Abordagens de Modelagem de Ameaças:**
    - **Modelagem de Ameaças:** Processo de identificar, enumerar e priorizar ameaças potenciais a partir da perspectiva de um atacante.
    - **Abstrações Principais:**
        - **Ativos:** Recursos como processos, usuários, componentes de software ou fontes de dados que precisam ser protegidos.
        - **Vetores e Alvos de Ataque:** Pontos de entrada e caminhos que os atacantes podem utilizar para comprometer os ativos.
2. **Tipos de Modelagem de Ameaças:**
    - **Centrada em Ativos:** Envolve avaliação de riscos, aproximação ou classificação dos ativos a serem protegidos.
    - **Centrada em Atacantes:** Inclui a classificação de riscos e a estimativa de recursos, capacidades ou motivações dos atacantes.
    - **Centrada em Software:** Foca na análise detalhada dos componentes de software e suas interações.
3. **Colaboração na Modelagem de Ameaças:**
    - Importância de abordagens colaborativas para envolver diversos especialistas e perspectivas.
    - **CoReTM:** Prototipagem de uma ferramenta que inclui um editor colaborativo baseado em anotações, relatórios automatizados de ameaças e integração com DevOps para suportar diferentes estilos de reuniões e fluxos de trabalho.
4. **Metodologias Utilizadas:**
    - **STRIDE:** Classificação de ameaças em categorias como Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service e Elevation of Privilege.
    - **DREAD:** Técnica de avaliação de riscos que atribui pontuações para Destruction Potential, Reproducibility, Exploitability, Affected Users e Discoverability, embora apresente limitações na definição de escalas.
    - **PASTA e Trike:** Metodologias mais complexas que oferecem uma análise de riscos detalhada, porém com maior complexidade na implementação.
5. **Processo de Modelagem de Ameaças na Microsoft:**
    - **Passos Principais:**
        - **Diagramação:** Utilização de Diagramas de Fluxo de Dados (DFDs) com a adição de "trust boundaries" para identificar processos, armazenamentos de dados, fluxos de dados e entidades externas.

- **Enumeração de Ameaças:** Identificação das ameaças associadas a cada elemento do DFD.
- **Mitigação:** Desenvolvimento de estratégias para mitigar as ameaças identificadas, priorizando redesign, mitigadores padrão como ACLs, mitigadores únicos com cautela ou aceitação de risco conforme as políticas.
- **Verificação:** Validação dos modelos de ameaças através de heurísticas como análise de gráficos dos DFDs, revisão completa do modelo e verificação das mitigações aplicadas.

6. **Heurísticas para Validação de Modelos de Ameaças:**
    - **Análise de Gráficos:** Verificação se os diagramas refletem o código final.
    - **Enumeração Completa:** Garantir que todas as ameaças STRIDE por elemento foram identificadas.
    - **Revisão e Mitigação:** Revisão geral do modelo e confirmação de que cada ameaça foi mitigada adequadamente.
7. **Desafios e Considerações:**
    - **Fatores Humanos:** Inclusão de aspectos relacionados a pessoas dentro do modelo de ameaças, como phishing decorrente de falhas na autenticação.
    - **Usabilidade e Experiência do Usuário:** Necessidade de que as ferramentas e processos de modelagem de ameaças sejam acessíveis e compreensíveis para engenheiros com diferentes níveis de expertise em segurança.
    - **Integração com Desenvolvimento:** Importância da simplicidade e integração das ferramentas de modelagem de ameaças no processo de desenvolvimento para efetivamente identificar e abordar problemas de design.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** A abordagem da Microsoft demonstra a importância de segmentar a modelagem de ameaças por componentes e definir níveis de confiança, o que pode ser adaptado para estruturas organizacionais horizontais, promovendo a distribuição de responsabilidades.
- **Governança e Segurança:** A integração de ferramentas colaborativas como CoReTM e a categorização clara de ameaças e ativos auxiliam na criação de protocolos que respeitam a governança horizontal, facilitando uma distribuição equilibrada de controle e acesso.
- **Frameworks de Segurança:** A utilização de DFDs com "trust boundaries" e a classificação de confiança podem ser incorporadas em frameworks de segurança que suportem transparência e colaboração em organizações não-hierárquicas.