AdvancedThreatModeling

O documento apresenta uma visão abrangente sobre a modelagem de ameaças, definindo-a como um processo para identificar, enumerar e priorizar ameaças potenciais a partir da perspectiva de um atacante hipotético. Baseia-se em definições de fontes como a Wikipedia e Shull (2016a), estabelecendo que um método de modelagem de ameaças (TMM) cria uma abstração de um sistema de software para identificar as habilidades e objetivos dos atacantes, gerando e catalogando ameaças que o sistema deve mitigar.

Quem Realiza a Modelagem de Ameaças?

- **Vendedores como Microsoft:** Desenvolveram e utilizam o método STRIDE, disponibilizando-o gratuitamente.
- **Organizações Governamentais como o DoD:** Mandato para o DoD, com diversos métodos baseados em padrões NIST e checklists.
- **Organizações Comerciais:** Incluem setores como automotivo e financeiro, utilizando métodos como STRIDE, OCTAVE e árvores de ataque.
- **BSIMM:** Identifica os modelos de ataque como uma prática de nível 1.

Conceitos Fundamentais:

- **Segurança Não é Binária:** Reconhece que a segurança é uma função de diversos fatores, como o atacante, seus recursos, a probabilidade e as condições.
- **Vulnerabilidade de Segurança:** Definida como uma fraqueza que permite a um atacante contornar controles de segurança, exigindo uma susceptibilidade do sistema, acesso do atacante à falha e capacidade para explorá-la.

Ferramentas e Metodologias de Modelagem de Ameaças:

- **Security Cards:** Ferramenta de brainstorming para explorar amplamente ameaças de segurança e privacidade, promovendo a mentalidade de segurança. Inclui exercícios práticos com cenários específicos, como veículos autônomos não tripulados.
- **Personas e Persona non Grata (PnG):** Utilização de descrições detalhadas de personas para guiar decisões de desenvolvimento e introdução de PnGs para representar usuários ou atacantes indesejados, auxiliando na compreensão e defesa contra usuários maliciosos.

Metodologias de Modelagem de Ameaças:

- **VAST (Visual, Simple, and Agile Threat Modeling):** Destinado a grandes e médias organizações que adotam metodologias ágeis, visando consistência na saída dos modelos de ameaças.
- **Trike Threat Model:** Focado em auditoria de segurança a partir de uma perspectiva de gerenciamento de riscos, com o objetivo de gerar modelos de ameaças de forma confiável e repetível.
- **PASTA (Process for Attack Simulation & Threat Analysis):** Processo de sete etapas que inclui definição de objetivos de negócios e segurança, decomposição de aplicações, análise de ameaças, análise de vulnerabilidades, modelagem e simulação de ataques, e análise e gestão de riscos.

Implementação de Modelos de Ameaças:

- **Trike Implementation:** Envolve a identificação dos objetivos do sistema, análise de atores e ativos, criação de Diagramas de Fluxo de Dados (DFDs), construção de gráficos de ataque, determinação de vulnerabilidades e aplicação de soluções, além de avaliação de riscos e estratégias de mitigação.
- **PASTA Process:** Inclui etapas detalhadas para definir objetivos, decompor aplicações, analisar ameaças e vulnerabilidades, modelar e simular ataques, e realizar análise e gestão de riscos, integrando requisitos de negócios e de segurança.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** O documento oferece uma base sólida sobre as diversas metodologias de modelagem de ameaças, destacando a necessidade de adaptação a diferentes contextos organizacionais, o que é crucial para o desenvolvimento de um protocolo focado em estruturas não-hierárquicas.
- **Análise Crítica:** Ao discutir as limitações de métodos como STRIDE e a importância de considerar especificidades de sistemas diversos, o documento incentiva a busca por abordagens que acomodem a horizontalidade organizacional, alinhando-se com o objetivo de tratar a horizontalidade como um ativo estratégico.
- **Governança e Segurança:** As metodologias apresentadas, como VAST, Trike e PASTA, fornecem insights sobre a integração de diferentes frameworks de segurança e governança, essenciais para desenvolver um protocolo que valorize a governança distribuída e robusta em organizações horizontais.