ThreatModellingSurvey

O artigo apresenta uma visão geral das metodologias de modelagem de ameaças, com ênfase nas árvores de ataque como uma abordagem utilizada para modelar ameaças a sistemas de software.

Principais Pontos:

1. **Árvores de Ataque:**
    - **Estrutura:** Utiliza uma estrutura em árvore onde o objetivo do ataque está no nó raiz e as diferentes formas de alcançá-lo estão nos nós folhas. Cada nó pode representar um sub-objetivo, com os filhos indicando as maneiras de atingir esse sub-objetivo.
    - **Nodos OR e AND:** Nodos OR representam alternativas para atingir um objetivo, enquanto nodos AND representam diferentes etapas necessárias para alcançar o mesmo objetivo.
    - **Atribuição de Valores:** Valores são atribuídos manualmente aos nós folhas, dependendo do especialista em segurança e do engenheiro de sistema. Esses valores podem incluir tempo necessário para completar uma etapa, despesas operacionais, expertise requerida, etc.
2. **Ferramentas Automatizadas:**
    - **SecureI Tree:** Ferramenta gráfica desenvolvida pela Amenaz Technologies que suporta a modelagem de árvores de ataque. Baseia-se em um modelo matemático de árvores de ataque e utiliza algoritmos matemáticos para calcular os riscos de segurança.
    - **Aplicações Bem-sucedidas:** SecureI Tree tem sido aplicada com sucesso em diversas áreas, como edifícios, oleodutos e linhas de transmissão elétrica.
3. **Vantagens e Limitações:**
    - **Vantagens:** Estrutura clara e visual que facilita a compreensão das diferentes formas de ataques e suas interdependências. Suporte para a inclusão de diversos atributos que enriquecem a análise de risco.
    - **Limitações:** Processo de atribuição de valores é manual e depende fortemente da expertise dos profissionais envolvidos, o que pode introduzir vieses e inconsistências.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** A utilização de árvores de ataque oferece uma abordagem estruturada que pode ser adaptada para refletir as dinâmicas de organizações horizontais, facilitando a identificação de múltiplas vias de ataque e a distribuição de responsabilidades na análise de segurança.
- **Governança e Segurança:** A estrutura hierárquica inerente às árvores de ataque contrasta com a governança horizontal, destacando a necessidade de metodologias que possam ser adaptadas para ambientes menos centralizados.
- **Frameworks de Segurança:** Ferramentas como SecureI Tree demonstram a viabilidade de automatizar aspectos da modelagem de ameaças, o que pode ser integrado em frameworks de segurança que suportem a colaboração e a flexibilidade necessárias em organizações não-hierárquicas.