FoundationsofAttackTrees

No documento intitulado "Foundations of Attack Trees", são abordados os conceitos fundamentais e a estrutura das árvores de ataque, uma ferramenta essencial para a modelagem e análise de ameaças em sistemas de segurança. As principais ideias discutidas incluem:

- **Definição e Estrutura das Árvores de Ataque**:
    - **Árvore de Ataque**: Estrutura hierárquica onde os nós representam ataques. O nó raiz corresponde ao objetivo global do atacante.
    - **Refinamentos**: Os nós filhos refinam o objetivo do nó pai. Esses refinamentos podem ser:
        - **Conjuntivos (AND)**: Indicam que múltiplos sub-objetivos devem ser alcançados para atingir o objetivo principal.
        - **Disjuntivos (OR)**: Representam alternativas, onde atingir qualquer um dos sub-objetivos é suficiente para alcançar o objetivo principal.
    - **Nós Folha**: Representam ataques que não podem ser refinados ulteriormente, constituindo os componentes básicos do ataque.
- **Atributos de Segurança na Análise de Árvores de Ataque**:
    - Após a modelagem dos possíveis ataques em uma árvore de ataque, é possível analisar diversos atributos da segurança do sistema, conforme sugerido por Schneier. Exemplos de atributos incluem:
        - **Possibilidade vs. Impossibilidade**: Avaliação da viabilidade dos ataques.
        - **Custo**: Recursos necessários para executar o ataque.
        - **Necessidade de Ferramentas Especiais**: Determina se o ataque requer ferramentas ou conhecimentos específicos.
    - **Combinação de Valores**: Os nós podem ter valores booleanos e contínuos, permitindo a formulação de declarações complexas sobre os ataques, como "ataque mais barato com maior probabilidade de sucesso".
- **Conceito de "Attack Suite"**:
    - Uma árvore de ataque define um conjunto de ataques possíveis, denominado **attack suite**.
    - Cada ataque dentro do attack suite é composto por múltiplos componentes de ataque, que podem ocorrer mais de uma vez dentro do mesmo ataque.
    - Os componentes de ataque são considerados no nível mais baixo de abstração, sem estrutura interna.
    - A semântica das attack suites pode ser caracterizada através da travessia da árvore ou da reescrita da árvore para uma forma normal, facilitando a manipulação e análise das árvores de ataque.
- **Construção e Manipulação de Árvores de Ataque**:
    - **Construção**: Envolve a identificação do objetivo principal e a decomposição hierárquica em sub-objetivos até atingir os ataques básicos.

- **Reescrita**: Utiliza regras de reescrita para adicionar estrutura a um conjunto de ataques não estruturado ou para reequilibrar a árvore de ataque, tornando-a mais eficiente para análise.

Relevância para a Pesquisa

A compreensão das fundações das árvores de ataque é crucial para a modelagem de ameaças em organizações não-hierárquicas, como proposto na sua tese de mestrado. As árvores de ataque proporcionam uma estrutura formal e metodológica para decompor e analisar de forma sistemática os possíveis vetores de ataque, alinhando-se com o objetivo de criar um protocolo que valorize a horizontalidade organizacional como um ativo estratégico.

Ao utilizar refinamentos conjuntivos e disjuntivos, as árvores de ataque permitem a representação detalhada de ameaças complexas e a identificação de múltiplas vias de ataque, o que é especialmente relevante em estruturas organizacionais distribuídas e descentralizadas. Além disso, a análise de atributos de segurança, como custo e possibilidade, facilita a avaliação de riscos e a priorização de contramedidas, aspectos fundamentais para a governança horizontal e a confiança distribuída.

O conceito de attack suite complementa a necessidade de considerar um conjunto abrangente de ameaças, promovendo uma visão holística da segurança organizacional. A capacidade de reescrever e manipular árvores de ataque também suporta a adaptabilidade e a escalabilidade necessárias para organizações que operam em ambientes dinâmicos e em constante evolução. Dessa forma, as fundações das árvores de ataque contribuem significativamente para o desenvolvimento de um protocolo robusto de modelagem de ameaças, alinhado com os objetivos específicos da pesquisa em estruturas organizacionais não-hierárquicas.