AttackTrees

No documento intitulado "attacktrees", são explorados os conceitos e funcionalidades das árvores de ataque no contexto da segurança de sistemas. As principais ideias abordadas incluem:

- **Definição e Propósitos das Árvores de Ataque**:
    - Representam a segurança de sistemas e subsistemas de forma estruturada.
    - Funcionam como um banco de dados automático que descreve a segurança de um sistema.
    - Capturam e reutilizam conhecimentos especializados.
    - Auxiliam na tomada de decisões para melhorar a segurança ou avaliar o impacto de novos ataques.
- **Funcionamento das Árvores de Ataque**:
    - Representam ataques e contramedidas em uma estrutura de árvore.
    - O nó raiz representa o objetivo do ataque, podendo haver múltiplos nós raiz para diferentes objetivos.
    - Nós folha correspondem a ataques específicos.
- **Valores Booleanos nos Nós**:
    - Atribuição de valores booleanos aos nós folha, como possível vs. impossível.
    - Outros valores booleanos podem incluir "fácil vs. difícil", "barato vs. caro", "legal vs. ilegal", entre outros.
    - Combinação de valores booleanos e contínuos para formular declarações sobre os ataques, como o ataque mais barato com maior probabilidade de sucesso.
- **Construção da Árvore de Ataque**:
    - Passo 0: Identificar os objetivos, cada um constituindo uma árvore de ataque separada.
    - Passo 1: Identificar ataques contra os objetivos e repetir conforme necessário.
    - Passo 2: Integrar árvores de ataque existentes como componentes reutilizáveis para construir árvores específicas.
- **Aplicações das Árvores de Ataque**:
    - Avaliar a vulnerabilidade de um sistema contra ataques específicos ou gerais.
    - Listar suposições de segurança de um sistema.
    - Comparar e classificar diferentes cenários de ataque ou defesa com base nos valores dos nós raiz.
    - Comparar efeitos de diversas contramedidas e a segurança de diferentes produtos.
    - Demonstrar as suposições de segurança e as consequências de sua violação.
    - Otimizar o uso do orçamento de segurança.
- **Escalabilidade das Árvores de Ataque**:
    - Árvores de ataque podem ser parte de árvores maiores, facilitando a análise de sistemas complexos.
    - Mudanças em níveis inferiores propagam-se automaticamente para níveis superiores.
    - Subárvores são componentes reutilizáveis em diferentes contextos onde são aplicáveis.

- **Conclusões**:
    - As árvores de ataque oferecem uma metodologia rigorosa para pensar sobre segurança, proporcionando uma abordagem abrangente e estruturada.
    - Funcionam como uma "cercadura ampla" de segurança, ao contrário de medidas pontuais e isoladas.

Relevância para a Pesquisa

A compreensão aprofundada das árvores de ataque é fundamental para a modelagem de ameaças em organizações não-hierárquicas, pois permite a representação estruturada e detalhada de possíveis vetores de ataque e contramedidas. A metodologia apresentada facilita a identificação de vulnerabilidades específicas e a avaliação de riscos em ambientes descentralizados, alinhando-se diretamente com os objetivos de criar um protocolo que valorize a horizontalidade como ativo estratégico. Além disso, a escalabilidade e a reutilização de componentes das árvores de ataque são particularmente relevantes para organizações que operam de maneira distribuída, permitindo uma análise adaptativa e contínua das ameaças emergentes.