Energytheftdetectionissues

No artigo "Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid", é explorada a aplicação da abordagem de árvores de ataque para modelar ameaças relacionadas ao roubo de energia em Infraestruturas de Medição Avançada (AMI) na rede elétrica inteligente. As principais ideias abordadas incluem:

- **Abordagem de Árvore de Ataque**:
    - Proposta por Bruce Schneier, a abordagem de árvore de ataque oferece uma forma formal e metódica de descrever a segurança de sistemas com base em diferentes ataques.
    - A árvore de ataque enumera todas as ações potenciais que um atacante poderia utilizar para acessar o sistema-alvo, com cada ramo representando um conjunto de etapas intermediárias necessárias para alcançar o objetivo final.
    - A estrutura da árvore utiliza portas lógicas OR e AND para representar métodos alternativos de ataque e diferentes etapas para atingir o mesmo objetivo, respectivamente.
- **Tipos de Atacantes Motivados a Cometer Roubo de Energia**:
    - **Clientes**: Em países em desenvolvimento, motivados por infraestrutura deficiente, pobreza e irregularidades nos sistemas de medição e distribuição. Em países desenvolvidos, indivíduos que cultivam maconha ilegalmente roubam eletricidade para mascarar o consumo total e evitar inspeções policiais.
    - **Crime Organizado**: Motivados pela monetização do roubo de energia. Aproveitam as capacidades de computação e rede da AMI para criar ferramentas de software e hardware que comprometem medidores inteligentes, explorando aspectos de design como o uso extensivo da mesma senha em vários medidores para amplificar os lucros ao comprometer um único medidor.
    - **Insiders de Empresas de Utilidade**: Funcionários internos que, apesar de serem implicitamente confiáveis, podem cometer fraudes ou serem maliciosos. É preferível que os sistemas das empresas de utilidade implementem uma gestão adequada de clientes e grupos para garantir propriedades como a separação de funções.
- **Modelo de Ameaça Baseado em Árvore de Ataque para Roubo de Energia em AMI**:
    - **Construção da Árvore de Ataque**:
        - **Passo 0**: Definir o objetivo geral do atacante como "Roubo de Energia" na AMI.
        - **Passo 1**: Decompor o objetivo G em sub-objetivos: Interromper a Medição, Manipular a Demanda Armazenada e Modificar na Rede. O propósito do atacante pode ser alcançado se qualquer um dos três componentes for atingido.
        - **Passo 2**: Continuar a decomposição passo a passo até que a tarefa não possa ser dividida em partes menores, resultando na árvore de ataque completa que representa as ações e sub-ações necessárias para o roubo de energia.

Relevância para a Pesquisa

A utilização da abordagem de árvores de ataque para modelar o roubo de energia em Infraestruturas de Medição Avançada (AMI) demonstra a aplicabilidade dessa metodologia em contextos organizacionais

descentralizados e não-hierárquicos. Ao identificar e decompor sistematicamente os objetivos e sub-objetivos dos atacantes, a pesquisa contribui para a compreensão das vulnerabilidades específicas em estruturas horizontais. Além disso, a categorização dos tipos de atacantes, incluindo clientes, crime organizado e insiders, oferece uma visão abrangente dos diversos vetores de ameaça que devem ser considerados ao desenvolver um protocolo de modelagem de ameaças. Essa abordagem alinhada com a horizontalidade como ativo estratégico facilita a criação de contramedidas eficazes e a avaliação de riscos em ambientes distribuídos, reforçando a governança horizontal e a confiança distribuída como elementos centrais na segurança organizacional.