ThreatModelingASummaryOfAvailableMethods

O artigo oferece uma visão geral das metodologias de modelagem de ameaças disponíveis, destacando a necessidade de adaptar essas abordagens às complexidades crescentes dos sistemas de software e sistemas ciber-físicos.

Principais Pontos:

1. **Importância da Modelagem de Ameaças:**
    - Sistemas de software enfrentam uma variedade de ameaças que evoluem constantemente com as mudanças tecnológicas.
    - As ameaças podem originar-se de dentro ou de fora das organizações, com impactos potencialmente devastadores, como a interrupção completa do sistema ou o vazamento de informações sensíveis, afetando a confiança do consumidor.
2. **Abstrações na Modelagem de Ameaças:**
    - **Ativos:** Recursos que precisam ser protegidos, como processos, usuários, componentes de software ou fontes de dados.
    - **Vetores e Alvos de Ataque:** Pontos de entrada e caminhos que os atacantes podem utilizar para comprometer os ativos.
3. **Metodologias de Modelagem de Ameaças:**
    - **STRIDE:**
        - Foca no design detalhado do sistema utilizando Diagramas de Fluxo de Dados (DFDs) para identificar entidades, eventos e limites do sistema.
        - Fácil de adotar, mas pode ser demorado e gerar um grande número de ameaças à medida que a complexidade do sistema aumenta.
        - Aplicado com sucesso em sistemas exclusivamente cibernéticos e ciber-físicos.
    - **PASTA (Process for Attack Simulation & Threat Analysis):**
        - Integra objetivos de negócios e requisitos técnicos, utilizando ferramentas de design e elicitação em diferentes estágios.
        - Envolve decisores-chave e requer input de operações, governança, arquitetura e desenvolvimento.
        - Considerado um framework centrado em riscos com uma perspectiva centrada no atacante, produzindo enumeração e pontuação de ameaças.
    - **LINDDUN:**
        - Inicia com um DFD para definir fluxos de dados, armazenamentos de dados, processos e entidades externas.
        - Analisa sistematicamente cada elemento do modelo a partir das categorias de ameaças, construindo árvores de ameaças.
        - Método intensivo em mão de obra e tempo, semelhante ao STRIDE na geração rápida de ameaças conforme a complexidade do sistema aumenta.
    - **Attack Trees:**
        - Diagramas que representam ataques em forma de árvore, com o objetivo do ataque na raiz e as maneiras de alcançá-lo nas folhas.

        - Amplamente aplicado em sistemas cibernéticos e ciber-físicos, facilitando a decomposição de ameaças de alto nível em ameaças relacionadas.
4. **Desafios das Metodologias:**
    - **Complexidade e Escalabilidade:**
        - Métodos como STRIDE e LINDDUN enfrentam desafios na gestão da crescente quantidade de ameaças em sistemas complexos.
    - **Integração com Processos de Desenvolvimento:**
        - Necessidade de integrar a modelagem de ameaças com práticas de desenvolvimento ágil e DevSecOps.
    - **Avaliação de Riscos:**
        - Técnicas como DREAD podem adicionar complexidade sem definir claramente suas escalas, tornando a avaliação de riscos menos precisa.
5. **Considerações para Sistemas Ciber-Físicos:**
    - A integração de sistemas de software com infraestruturas físicas, como carros inteligentes, aumenta a vulnerabilidade a ameaças que fabricantes de infraestruturas físicas tradicionais podem não considerar.
    - A modelagem de ameaças com múltiplos stakeholders é crucial para capturar uma ampla gama de tipos de ameaças.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** A análise das diferentes metodologias destaca a necessidade de escolher ou combinar métodos que melhor atendam às demandas de organizações não-hierárquicas, garantindo uma cobertura eficaz das ameaças.
- **Governança e Segurança:** A integração de abordagens centradas em riscos e atacantes, como PASTA, pode informar o desenvolvimento de protocolos que valorizem a governança horizontal e a distribuição de controle.
- **Frameworks de Segurança:** A utilização de DFDs e a categorização de ameaças em métodos como STRIDE e LINDDUN podem ser adaptadas para criar frameworks que suportem a transparência e colaboração em organizações horizontais.