STRIDEthreatmodelingforcyberphysical

No artigo "STRIDE-based Threat Modeling for Cyber-Physical Systems", é apresentada a aplicação da metodologia **STRIDE** na modelagem de ameaças para **Sistemas Ciber-Físicos (CPS)**. As principais ideias e componentes abordados no texto incluem:

- **Definição de Sistemas Ciber-Físicos (CPS)**:
    - **CPS** utilizam Tecnologias de Informação e Comunicação (ICT) para controlar e monitorar processos físicos.
    - Exemplos de infraestruturas críticas incluem **redes elétricas inteligentes (smart grids)**.
- **Metodologias de Modelagem de Segurança e Segurança de Sistemas**:
    - Diversas metodologias existem na literatura, como **STPA-sec** (foco na segurança do sistema), **HAZOP** (foco em perigos e operabilidade do sistema), **SAHARA** (foco em perigos, riscos e segurança), **PASTA** (Process for Attack Simulation and Threat Analysis), **OCTAVE** (foco em ameaças e ativos operacionalmente críticos) e **STRIDE** (foco na identificação de ameaças potenciais em cada subcomponente do sistema).
    - **STRIDE** é escolhido por ser uma abordagem mais leve em comparação com outras metodologias mais complexas e com maior foco em segurança do sistema e riscos.
- **Motivações para o Uso de STRIDE**:
    - **Abordagem Sistemática**: Analisa ameaças cibernéticas contra cada componente do sistema com base no conhecimento técnico.
    - **Abrangência**: Analisa propriedades de segurança como autenticação, autorização, confidencialidade, integridade, não repúdio e disponibilidade em cada componente do sistema.
    - **Compreensão do Impacto**: Proporciona uma compreensão clara do impacto de uma vulnerabilidade em um componente sobre todo o sistema, ajudando a garantir a segurança do sistema no nível dos componentes.
- **Lacuna na Literatura**:
    - Ainda falta um exemplo de framework que mostre a aplicação da abordagem **STRIDE** a um **CPS**.
    - Objetivo do artigo: Fornecer um walkthrough demonstrando que a abordagem leve **STRIDE** pode ser aplicada a um **CPS** para produzir uma categorização eficaz das ameaças específicas do sistema.
- **Aplicação Prática**:
    - **Modelagem de Ameaças com STRIDE** pode ser realizada de duas maneiras:
        1. **STRIDE-por-Elemento**: Analisa o comportamento e as operações de cada componente do sistema. Embora seja mais complexo, pode não identificar ameaças que não são evidentes a partir do Diagrama de Fluxo de Dados (DFD).
        2. **STRIDE-por-Interação**: Enumera ameaças contra interações do sistema considerando tuplas (origem, destino, interação). É mais fácil de realizar e suas estratégias de proteção normalmente são suficientes para proteger o sistema, já

que ataques cibernéticos geralmente envolvem interações maliciosas entre componentes do sistema.

- **Estudo de Caso**:
    - Aplicação da modelagem de ameaças baseada em STRIDE a um **laboratório de teste baseado em sincróforos** com o objetivo de estabelecer medidas de segurança apropriadas para proteger o ambiente.
    - A maioria das aplicações de sincróforos.

Relevância para a Pesquisa

A aplicação da metodologia **STRIDE** na modelagem de ameaças para **Sistemas Ciber-Físicos (CPS)**, conforme descrito no artigo, é altamente relevante para a pesquisa em modelagem de ameaças em **organizações não-hierárquicas**. As principais considerações incluem:

- **Adaptação de Metodologias Leves**: A escolha de **STRIDE** devido à sua abordagem sistemática e leve indica a viabilidade de aplicar metodologias menos complexas em ambientes organizacionais horizontais, onde a agilidade e a eficiência são cruciais.
- **Compreensão Abrangente das Ameaças**: A capacidade de **STRIDE** em analisar propriedades de segurança específicas de cada componente permite uma identificação detalhada das vulnerabilidades, essencial para estruturas organizacionais distribuídas onde a segurança deve ser garantida em múltiplos níveis e componentes.
- **Modelagem por Interação**: A abordagem **STRIDE-por-Interação** oferece uma maneira eficaz de identificar ameaças que surgem das interações entre componentes, o que é particularmente relevante em organizações não-hierárquicas onde as interdependências entre diferentes partes do sistema podem introduzir vulnerabilidades complexas.
- **Aplicação Prática e Exemplificação**: A demonstração prática de **STRIDE** em um laboratório de teste baseado em sincróforos fornece um exemplo concreto de como a metodologia pode ser implementada em sistemas ciber-físicos, oferecendo insights valiosos para a criação de protocolos de modelagem de ameaças adaptados a ambientes descentralizados e multifacetados.
- **Facilidade de Implementação**: A abordagem mais simples de **STRIDE-por-Interação** sugere que metodologias de modelagem de ameaças podem ser implementadas de forma eficiente em organizações horizontais, promovendo uma cultura de segurança sem sobrecarregar as equipes com processos excessivamente complexos.
- **Integração com Outras Metodologias**: A aplicação de **STRIDE** pode ser complementada com outras técnicas de modelagem de ameaças, como **Security Cards** e **Persona Non Grata**, para criar uma abordagem mais robusta e multifacetada que atenda às necessidades específicas das organizações não-hierárquicas.