UncoverSecurityDesignFlawsSTRIDE

No documento "Uncover Security Design Flaws Using The STRIDE Approach" da Microsoft Docs, são abordadas diretrizes e melhores práticas para a aplicação eficaz da metodologia **STRIDE** na modelagem de ameaças de segurança em sistemas complexos. As principais ideias e componentes discutidos incluem:

- **Importância da Precisão nos Diagramas de Fluxo de Dados (DFD)**:
    - **Interações entre Componentes**: Mesmo que os componentes individuais sejam imunes a determinadas ameaças (como spoofing), suas interações podem introduzir vulnerabilidades não previstas. Portanto, garantir a precisão dos DFDs é crucial para identificar corretamente as ameaças.
    - **Tempo Investido na Elaboração dos DFDs**: É fundamental dedicar tempo suficiente para assegurar que todas as partes do sistema estejam representadas de forma adequada no DFD. Isso inclui verificar se todos os fluxos de dados têm origem e destino corretos, evitando fontes ou destinos de dados "mágicos" que não são representados por processos ou atores.
- **Regras Gerais para Construção de DFDs Sensatos**:
    - **Evitar Fontes ou Destinos de Dados Mágicos**: Dados não são criados do nada. Cada fluxo de dados deve ter um processo que lê ou escreve os dados, evitando representações que mostrem dados indo diretamente da cabeça de um usuário para o disco, por exemplo.
    - **Representação Adequada de Processos de Leitura e Escrita**: Garantir que cada armazenamento de dados tenha processos associados que leem ou escrevem esses dados, mantendo a integridade dos fluxos de dados.
    - **Colapsar Elementos Similares Dentro de uma Fronteira de Confiança**: Se elementos são implementados na mesma tecnologia e estão dentro da mesma fronteira de confiança, eles podem ser colapsados em um único elemento para fins de modelagem.
    - **Cuidado ao Modelar Detalhes em Ambos os Lados de uma Fronteira de Confiança**: Utilizar DFDs de contexto e diagramas de detalhamento para evitar a tentação de modelar clientes e servidores simultaneamente em um único modelo, garantindo uma representação clara das interações e das fronteiras de confiança.
- **Desafios e Considerações Adicionais**:
    - **Complexidade de Sistemas Grandes**: Modelar módulos menores de um sistema grande pode ser mais eficiente, mas é essencial considerar como esses módulos interagem para evitar vulnerabilidades emergentes da composição.
    - **Importância das Fronteiras de Confiança**: Identificar pontos onde os dados mudam de um nível de privilégio para outro ajuda a pinpointar áreas críticas onde os dados devem ser analisados para garantir a correção e evitar vazamentos de informações sensíveis.

Relevância para a Pesquisa

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

- **Precisão e Detalhamento nos DFDs**:
    - **Adaptabilidade em Estruturas Horizontais**: Em organizações não-hierárquicas, onde a colaboração e a interação entre diversos componentes são frequentes, a precisão na elaboração dos DFDs é ainda mais crucial para identificar vulnerabilidades que podem surgir das interações dinâmicas entre componentes distribuídos.
    - **Facilidade de Identificação de Ameaças**: DFDs bem elaborados permitem uma identificação mais clara e abrangente das ameaças, alinhando-se com a necessidade de uma modelagem de ameaças robusta e adaptável em ambientes descentralizados.
- **Gestão de Fronteiras de Confiança**:
    - **Segurança Distribuída**: Em organizações horizontais, onde as fronteiras de confiança podem ser menos definidas e mais permeáveis, a capacidade de identificar e gerenciar essas fronteiras é essencial para garantir a segurança integral do sistema.
    - **Mitigação de Riscos em Pontos Críticos**: Focar em fronteiras de confiança ajuda a priorizar áreas onde os dados são mais suscetíveis a ataques, permitindo a implementação de contramedidas eficazes.
- **Eficiência na Modelagem de Ameaças**:
    - **Estratégias de Colaboração**: As regras e diretrizes apresentadas promovem uma abordagem colaborativa na modelagem de ameaças, essencial para organizações não-hierárquicas onde múltiplos stakeholders precisam contribuir para a segurança do sistema.
    - **Redução de Falsos Positivos e Ameaças Omitidas**: Ao seguir as melhores práticas para a criação de DFDs, é possível reduzir a incidência de falsos positivos e garantir uma cobertura mais completa das ameaças, aumentando a confiabilidade do modelo de ameaças.
- **Integração com Outras Metodologias de Modelagem**:
    - **Complementaridade com Security Cards e Persona Non Grata**: A aplicação das diretrizes STRIDE pode ser complementada com abordagens mais criativas e centradas no adversário, como **Security Cards** e **Persona Non Grata**, proporcionando uma visão mais holística e multifacetada das ameaças.
    - **Desenvolvimento de Protocolos Personalizados**: A combinação de metodologias estruturadas e criativas permite a criação de protocolos de modelagem de ameaças que são tanto consistentes quanto abrangentes, atendendo às necessidades específicas de organizações não-hierárquicas.
- **Foco na Proatividade e Prevenção**:

- **Identificação Antecipada de Vulnerabilidades**: A modelagem de ameaças realizada cedo no ciclo de desenvolvimento permite a detecção e mitigação de vulnerabilidades antes que elas se tornem dispendiosas ou difíceis de resolver, promovendo uma cultura de segurança proativa.
- **Revalidação Contínua do Design e Arquitetura**: Revisitar e revalidar constantemente o design do sistema sob a perspectiva de segurança assegura que as contramedidas implementadas permanecem eficazes contra ameaças emergentes.