AnAttackTreeBasedRisk

No artigo "Attack Tree based Risk Assessment for Location Privacy in Wireless Sensor Networks", C. descreve a construção de uma árvore de ataque utilizando uma estratégia de refinamento descendente e passo a passo. O vazamento de privacidade de localização, denotado por G, é estabelecido como o objetivo principal do atacante. A abordagem da árvore de ataque, proposta por Bruce Schneier, oferece uma maneira formal e metodológica de descrever a segurança de sistemas com base em diferentes ataques. A estrutura da árvore de ataque utiliza um nó raiz que representa o objetivo final, com nós filhos representando diferentes formas de alcançar esse objetivo. Cada nó filho pode ser subdividido em subobjetivos, continuando o processo até que todos os eventos se tornem nós folha. A relação lógica entre os nós é representada por portas OR e AND, onde portas OR indicam métodos alternativos de ataque e portas AND

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.

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.

FoundationsofAttackTrees

No documento intitulado "Foundations of Attack Trees", são abordados os conceitos fundamentais e a estrutura das árvores de ataque, uma ferramenta essencial para a modelagem e análise de ameaças em sistemas de segurança. As principais ideias discutidas incluem:

- **Definição e Estrutura das Árvores de Ataque**:
    - **Árvore de Ataque**: Estrutura hierárquica onde os nós representam ataques. O nó raiz corresponde ao objetivo global do atacante.
    - **Refinamentos**: Os nós filhos refinam o objetivo do nó pai. Esses refinamentos podem ser:
        - **Conjuntivos (AND)**: Indicam que múltiplos sub-objetivos devem ser alcançados para atingir o objetivo principal.
        - **Disjuntivos (OR)**: Representam alternativas, onde atingir qualquer um dos sub-objetivos é suficiente para alcançar o objetivo principal.
    - **Nós Folha**: Representam ataques que não podem ser refinados ulteriormente, constituindo os componentes básicos do ataque.
- **Atributos de Segurança na Análise de Árvores de Ataque**:
    - Após a modelagem dos possíveis ataques em uma árvore de ataque, é possível analisar diversos atributos da segurança do sistema, conforme sugerido por Schneier. Exemplos de atributos incluem:
        - **Possibilidade vs. Impossibilidade**: Avaliação da viabilidade dos ataques.
        - **Custo**: Recursos necessários para executar o ataque.
        - **Necessidade de Ferramentas Especiais**: Determina se o ataque requer ferramentas ou conhecimentos específicos.
    - **Combinação de Valores**: Os nós podem ter valores booleanos e contínuos, permitindo a formulação de declarações complexas sobre os ataques, como "ataque mais barato com maior probabilidade de sucesso".
- **Conceito de "Attack Suite"**:
    - Uma árvore de ataque define um conjunto de ataques possíveis, denominado **attack suite**.
    - Cada ataque dentro do attack suite é composto por múltiplos componentes de ataque, que podem ocorrer mais de uma vez dentro do mesmo ataque.
    - Os componentes de ataque são considerados no nível mais baixo de abstração, sem estrutura interna.
    - A semântica das attack suites pode ser caracterizada através da travessia da árvore ou da reescrita da árvore para uma forma normal, facilitando a manipulação e análise das árvores de ataque.
- **Construção e Manipulação de Árvores de Ataque**:
    - **Construção**: Envolve a identificação do objetivo principal e a decomposição hierárquica em sub-objetivos até atingir os ataques básicos.

- **Reescrita**: Utiliza regras de reescrita para adicionar estrutura a um conjunto de ataques não estruturado ou para reequilibrar a árvore de ataque, tornando-a mais eficiente para análise.

Relevância para a Pesquisa

A compreensão das fundações das árvores de ataque é crucial para a modelagem de ameaças em organizações não-hierárquicas, como proposto na sua tese de mestrado. As árvores de ataque proporcionam uma estrutura formal e metodológica para decompor e analisar de forma sistemática os possíveis vetores de ataque, alinhando-se com o objetivo de criar um protocolo que valorize a horizontalidade organizacional como um ativo estratégico.

Ao utilizar refinamentos conjuntivos e disjuntivos, as árvores de ataque permitem a representação detalhada de ameaças complexas e a identificação de múltiplas vias de ataque, o que é especialmente relevante em estruturas organizacionais distribuídas e descentralizadas. Além disso, a análise de atributos de segurança, como custo e possibilidade, facilita a avaliação de riscos e a priorização de contramedidas, aspectos fundamentais para a governança horizontal e a confiança distribuída.

O conceito de attack suite complementa a necessidade de considerar um conjunto abrangente de ameaças, promovendo uma visão holística da segurança organizacional. A capacidade de reescrever e manipular árvores de ataque também suporta a adaptabilidade e a escalabilidade necessárias para organizações que operam em ambientes dinâmicos e em constante evolução. Dessa forma, as fundações das árvores de ataque contribuem significativamente para o desenvolvimento de um protocolo robusto de modelagem de ameaças, alinhado com os objetivos específicos da pesquisa em estruturas organizacionais não-hierárquicas.

RiskCentricThreatModeling

Resumo da Anotação

No artigo "Risk Centric Threat Modeling Process for Attack Simulation and Threat Analysis", é apresentada uma metodologia centrada em riscos para a modelagem de ameaças, denominada PASTA (Process for Attack Simulation and Threat Analysis). As principais ideias e componentes abordados no texto incluem:

- **Importância de um Processo de Segurança Eficaz**:
    - Um processo de segurança bem-sucedido deve ser repetível, mensurável, produzir resultados e envolver múltiplas partes interessadas além das áreas tradicionais de segurança e conformidade.
    - A metodologia PASTA oferece um método linear que aborda esses requisitos, facilitando a integração de diversos stakeholders no processo de modelagem de ameaças.
- **Desafios Inerentes à Modelagem de Ameaças**:
    - Cultura organizacional, recursos disponíveis, maturidade dos processos e controles, e suporte executivo são desafios significativos.
    - PASTA promove coesão entre grupos de segurança em operações, governança, arquitetura e desenvolvimento, mitigando esses desafios.
- **Benefícios da Metodologia PASTA**:
    - **Cohesão entre Grupos de Segurança**: Facilita a colaboração entre diferentes departamentos, como operações, governança, arquitetura e desenvolvimento.
    - **Economia de Recursos**: Ao incorporar a governança de segurança no início dos esforços de desenvolvimento, reduz lacunas de conformidade, descobertas de auditoria e questões de risco.
    - **Compreensão Aprofundada das Fontes de Ataque**: Evita o uso de scripts de ataque prefabricados, promovendo uma compreensão mais detalhada das vulnerabilidades e como os ataques realmente exploram essas fraquezas.
    - **Treinamento e Conscientização em Segurança**: Integra princípios de segurança no fluxo de trabalho normal do SDLC, melhorando a compreensão dos desenvolvedores e outros profissionais sobre como a inação em medidas corretivas pode introduzir riscos.
    - **Abordagem Colaborativa**: Reduz a mentalidade adversarial entre equipes de segurança e outras áreas, promovendo uma colaboração mais harmoniosa.
- **Componentes do Processo PASTA**:
    - **Stage I: Definição dos Objetivos (DO)**: Derivação de requisitos de segurança e conformidade, determinação dos impactos de negócios e perfil de risco.
    - **Stage II: Definição do Escopo Técnico (DTS)**: Enumeração de detalhes técnicos, incluindo usuários, contas funcionais, componentes de software e infraestrutura de terceiros.
    - **Stage III: Decomposição e Análise da Aplicação (ADA)**: Decomposição da aplicação em elementos funcionais básicos, tipos de usuários, dados acessados e controles de segurança.

    - **Stage IV: Análise de Ameaças (TA)**: Identificação e análise de ameaças específicas contra os componentes e ativos da aplicação.
    - **Stage V: Análise de Fraquezas e Vulnerabilidades (WVA)**: Associação de ameaças com vulnerabilidades previamente identificadas e análise das fraquezas nos controles de segurança.
    - **Stage VI: Modelagem e Simulação de Ataques (AMS)**: Análise de cenários de ataque para determinar a probabilidade e impactos técnicos, utilizando árvores de ataque para identificar os caminhos de ataque mais prováveis.
    - **Stage VII: Análise e Gestão de Riscos (RAM)**: Identificação dos impactos técnicos e de negócios, e determinação das medidas de segurança para mitigar os riscos identificados.
- **Uso de Árvores de Ataque**:
    - As árvores de ataque são utilizadas para aprender sobre os objetivos e métodos dos atacantes, determinando caminhos de menor resistência e custo, aumentando a probabilidade de execução e dano à aplicação.
    - A construção de casos de teste de simulação de ataques permite verificar a eficácia das medidas de segurança preventivas e detectivas implementadas.

Relevância para a Pesquisa

A metodologia PASTA apresentada no artigo é altamente relevante para a pesquisa em modelagem de ameaças em organizações não-hierárquicas. Sua abordagem centrada em riscos e estrutura linear facilita a criação de um protocolo de modelagem de ameaças que considera a horizontalidade organizacional como um ativo estratégico. Especificamente:

- **Integração de Stakeholders**: PASTA promove a colaboração entre diversas áreas da organização, alinhando-se com a necessidade de estruturas horizontais que valorizam a participação distribuída e a confiança compartilhada.
- **Avaliação Abrangente de Riscos**: A abordagem detalhada de PASTA para identificar e analisar ameaças e vulnerabilidades permite uma compreensão aprofundada das nuances específicas das organizações descentralizadas, onde os vetores de ataque podem ser mais variados e complexos.
- **Uso de Árvores de Ataque**: A aplicação de árvores de ataque dentro do PASTA facilita a representação estruturada das ameaças, permitindo uma análise sistemática e a identificação de caminhos de ataque que consideram a distribuição de responsabilidades e a ausência de uma hierarquia rígida.
- **Escalabilidade e Adaptabilidade**: A metodologia PASTA, com seus estágios bem definidos, suporta a escalabilidade necessária para organizações distribuídas e a adaptabilidade para incorporar novas ameaças e mudanças organizacionais, essenciais para manter a segurança em ambientes dinâmicos.
- **Treinamento e Conscientização**: Ao integrar princípios de segurança no fluxo de trabalho normal, PASTA contribui para a construção de uma cultura de segurança distribuída, onde todos

os membros da organização estão conscientes e engajados na mitigação de riscos, reforçando a governança horizontal.

Portanto, a aplicação da metodologia PASTA na modelagem de ameaças proporciona uma base robusta para desenvolver um protocolo que valorize a estrutura horizontal das organizações, promovendo uma abordagem colaborativa e abrangente para a segurança cibernética. Isso está diretamente alinhado com os objetivos específicos da pesquisa de criar um protocolo que utilize a horizontalidade como um ativo estratégico, além de apoiar a análise de modelos de governança, confiança distribuída e frameworks de segurança.

PnGRequirementsPhaseThreatModeling

No artigo "Crowd Sourcing the Creation of Personae Non Gratae for Requirements-Phase Threat Modeling", é apresentada uma abordagem inovadora para a modelagem de ameaças durante a fase de requisitos de desenvolvimento de sistemas, utilizando Personae non Gratae (PnGs). As principais ideias abordadas incluem:

- **Definição de Personae non Gratae (PnGs)**:
    - Inspiradas nas personas usadas em design de experiência do usuário (UX), as PnGs representam usuários archetypais que interagem com o sistema de maneiras indesejadas, comprometendo sua segurança.
    - Diferente das personas tradicionais, que enfocam usuários legítimos, as PnGs focam em usuários mal-intencionados, auxiliando na antecipação de abusos e vulnerabilidades.
- **Comparação com Outros Métodos de Modelagem de Ameaças**:
    - Em um estudo recente, as árvores de ataque baseadas em PnGs demonstraram maior consistência em comparação com métodos como STRIDE e Security Cards.
    - No entanto, nenhum método individual identificou todas as ameaças possíveis, o que motivou a exploração do uso de crowd-sourcing para identificar ameaças de forma mais abrangente.
- **Crowd-Sourcing na Identificação de Ameaças**:
    - A abordagem proposta utiliza técnicas de recuperação de informação para analisar e consolidar ameaças identificadas por múltiplos colaboradores.
    - O processo culmina na construção de um modelo de ameaças unificado, auxiliado por analistas humanos, que incorpora uma gama mais ampla de cenários de ataque.
- **Estrutura e Etapas do Artigo**:
    - **Seção II**: Visão geral das técnicas existentes de modelagem de ameaças.
    - **Seção III**: Descrição detalhada das PnGs e sua contribuição para a modelagem de ameaças.
    - **Seções IV e V**: Métodos de coleta e análise de dados do estudo.
    - **Conclusão**: Discussão dos resultados preliminares, ameaças à validade e considerações finais.
- **Vantagens das PnGs**:
    - Promovem uma análise mais focada nas capacidades e motivações dos atacantes.
    - Facilitam a identificação de vulnerabilidades específicas ao considerar diferentes perfis de atacantes.
    - Melhoram a abrangência e a consistência dos modelos de ameaças através da colaboração coletiva.

Relevância para a Pesquisa

A utilização de Personae non Gratae (PnGs) na modelagem de ameaças, conforme descrito no artigo, é altamente relevante para a pesquisa em modelagem de ameaças em organizações não-hierárquicas. As PnGs permitem uma abordagem mais detalhada e diversificada na identificação de vetores de ataque,

refletindo melhor a complexidade e a distribuição de responsabilidades em estruturas horizontais. Além disso, a integração de métodos de crowd-sourcing para a criação de PnGs amplia a abrangência das ameaças identificadas, promovendo uma visão mais completa e colaborativa das possíveis vulnerabilidades.

Especificamente:

- **Alinhamento com Estruturas Horizontais**: A abordagem colaborativa e distribuída do crowd-sourcing ressoa com a natureza não-hierárquica das organizações focadas na pesquisa, permitindo a participação de diversos stakeholders na identificação de ameaças.
- **Melhoria na Consistência dos Modelos de Ameaças**: Ao utilizar PnGs, que demonstraram maior consistência em estudos comparativos, a pesquisa pode desenvolver modelos de ameaças mais robustos e confiáveis, essenciais para a criação de um protocolo de modelagem de ameaças eficaz.
- **Inclusão de Diversas Perspectivas de Atacantes**: As PnGs facilitam a consideração de múltiplos perfis de atacantes, o que é crucial para organizações descentralizadas onde as ameaças podem ser variadas e multifacetadas.
- **Suporte à Governança Horizontal e Confiança Distribuída**: A metodologia proposta reforça a governança horizontal ao promover uma análise de ameaças que considera a colaboração e a confiança distribuída, elementos centrais para a segurança organizacional em estruturas não-hierárquicas.

PersonaeNonGratae

No artigo "How Well Do You Know Your Personae Non Gratae", são exploradas técnicas avançadas para a modelagem de ameaças durante a fase de requisitos de desenvolvimento de sistemas, com ênfase na utilização de Personae Non Gratae (PnGs). As principais ideias abordadas incluem:

- **Limitações das Abordagens Tradicionais**:
    - **Checklists e Regulamentações**: Embora úteis para garantir a consideração de questões de segurança comuns, como controle de acesso e logs de auditoria (exemplo: HIPAA para dados de saúde), essas abordagens são insuficientes para identificar riscos de segurança específicos e únicos de uma aplicação.
- **Técnicas Avançadas para Modelagem de Ameaças**:
    - **Personae Non Gratae (PnGs)**:
        - **Definição**: Inspiradas nas personas utilizadas em design de experiência do usuário (UX), as PnGs representam usuários archetypais que interagem com o sistema de maneiras indesejadas, comprometendo sua segurança.
        - **Objetivo**: Ajudar a antecipar abusos e vulnerabilidades, fornecendo uma abordagem mais sistemática para identificar como usuários mal-intencionados podem explorar o sistema.
        - **Exemplo**: "Hugh", um jovem que pretende atacar o sistema, cujos objetivos podem ser especificados para expor pontos de vulnerabilidade.
    - **Misuse Cases (Casos de Uso de Abuso)**:
        - **Definição**: Extensões dos diagramas de casos de uso tradicionais que incluem atores maliciosos e seus casos de uso indesejados.
        - **Objetivo**: Determinar antecipadamente como o produto de software deve responder a usos não intencionais ou maliciosos, ajudando a identificar e mitigar ameaças específicas.
        - **Exemplo**: Diagramas que mostram interações entre atores legítimos (como um solicitante de seguro) e atores maliciosos (como um cracker que tenta obter informações privadas).
    - **Anotação de Diagramas de Atividades com Preocupações de Segurança**:
        - **Definição**: Adição de elementos relacionados à segurança em diagramas de atividades para documentar necessidades de privacidade, capacidades de auditoria e requisitos de não repúdio.
        - **Objetivo**: Integrar considerações de segurança diretamente no fluxo de trabalho do sistema, facilitando a identificação de pontos críticos onde a segurança pode ser comprometida.
- **Vantagens das PnGs**:
    - **Abordagem Sistemática**: Promove uma análise detalhada das capacidades e motivações dos atacantes, permitindo a identificação de vulnerabilidades específicas.

- **Consistência na Modelagem de Ameaças**: Estudos comparativos indicam que modelos de ameaças baseados em PnGs apresentam maior consistência em comparação com métodos tradicionais como STRIDE e Security Cards.
- **Crowd-Sourcing na Identificação de Ameaças**: A utilização de técnicas de recuperação de informação e colaboração coletiva para consolidar ameaças identificadas, resultando em modelos de ameaças mais abrangentes e robustos.

Relevância para a Pesquisa

A utilização de Personae Non Gratae (PnGs) na modelagem de ameaças, conforme apresentado no artigo, é altamente relevante para a pesquisa em modelagem de ameaças em organizações não-hierárquicas. As PnGs proporcionam uma abordagem estruturada e sistemática para identificar e analisar vetores de ataque específicos, alinhando-se com o objetivo de criar um protocolo que valorize a horizontalidade organizacional como um ativo estratégico.

Especificamente:

- **Alinhamento com Estruturas Horizontais**: A abordagem colaborativa e distribuída do uso de PnGs ressoa com a natureza não-hierárquica das organizações focalizadas na pesquisa, permitindo a participação de diversos stakeholders na identificação de ameaças. Isso fortalece a confiança distribuída e a governança horizontal, pilares centrais da pesquisa.
- **Identificação de Ameaças Únicas**: Ao ir além de checklists e regulamentações, as PnGs facilitam a identificação de ameaças únicas e específicas que podem emergir em ambientes descentralizados, onde responsabilidades e funções são distribuídas entre múltiplos participantes.
- **Melhoria na Consistência e Abrangência dos Modelos de Ameaças**: A aplicação de PnGs, especialmente quando combinada com métodos de crowd-sourcing, resulta em modelos de ameaças mais consistentes e abrangentes. Isso é crucial para organizações não-hierárquicas, onde a diversidade de operações e interações pode introduzir uma variedade maior de vetores de ataque.
- **Integração com Outras Técnicas de Modelagem**: A combinação de PnGs com misuse cases e a anotação de diagramas de atividades com preocupações de segurança proporciona uma visão multifacetada das ameaças, permitindo uma avaliação de riscos mais detalhada e a implementação de contramedidas eficazes.
- **Facilitação de uma Cultura de Segurança Distribuída**: Ao integrar princípios de segurança no fluxo de trabalho normal através das PnGs, a metodologia contribui para a construção de uma cultura de segurança distribuída, onde todos os membros da organização estão conscientes e engajados na mitigação de riscos, reforçando a governança horizontal.

SecurityCardsToolkit

No documento "A Security Threat Brainstorming Toolkit", são apresentados recursos e atividades destinados a facilitar a identificação e análise de ameaças de segurança em sistemas tecnológicos. As principais componentes abordadas incluem:

- **Títulos das Cartas (Card Titles)**:
    - **Motivações do Adversário**:
        - Acesso ou Conveniência
        - Curiosidade ou Tédio
        - Desejo ou Obsessão
        - Diplomacia ou Guerra
        - Maldade ou Vingança
        - Dinheiro
        - Política
        - Proteção
        - Religião
        - Auto-Promoção
        - Visão de Mundo
        - Motivações Incomuns
    - **Recursos do Adversário**:
        - Expertise (Especialização)
        - Um Mundo Futuro
        - Impunidade
        - Capacidades Internas
        - Conhecimento Interno
        - Dinheiro
        - Poder e Influência
        - Tempo
        - Ferramentas
        - Recursos Incomuns
    - **Métodos do Adversário**:
        - Encobrimento de Ataque
        - Ataque Indireto
        - Manipulação ou Coerção
        - Ataque em Múltiplas Fases
        - Ataque Físico
        - Processos
        - Ataque Tecnológico
        - Métodos Incomuns
    - **Impacto Humano**:
        - A Biósfera
        - Bem-Estar Emocional
        - Bem-Estar Financeiro

        - Dados Pessoais
        - Bem-Estar Físico
        - Relacionamentos
        - Bem-Estar Social
        - Impactos Incomuns
- **Exemplo de Atividade**:
    - Trabalhar em grupos de 3-5 pessoas.
    - Considerar um sistema tecnológico exemplo ou um sistema que está sendo projetado.
    - Percorrer o baralho de cartas e familiarizar-se com as dimensões e as cartas. Garantir a leitura de pelo menos uma carta de cada dimensão na íntegra.
    - Dentro de cada dimensão, classificar as cartas em ordem de relevância para o sistema e o nível de risco que elas apresentam.
    - Justificar a classificação das cartas nessa ordem.
    - Identificar cenários de ataque específicos que surgiram. Perfis de atacantes particulares começam a emergir?
- **Recursos Adicionais**:
    - Writeups completos e outras atividades estão disponíveis em securitycards.cs.washington.edu.

Relevância para a Pesquisa

A utilização de um **Security Threat Brainstorming Toolkit**, como apresentado no artigo, é altamente relevante para a modelagem de ameaças em organizações não-hierárquicas, conforme os objetivos da pesquisa. Este toolkit oferece uma abordagem estruturada e colaborativa para identificar e categorizar potenciais ameaças, o que é essencial em ambientes onde a governança e a responsabilidade são distribuídas de forma horizontal. Especificamente:

- **Facilitação da Colaboração Distribuída**: A atividade de brainstorming em grupo promove a participação de múltiplos stakeholders, alinhando-se com a estrutura não-hierárquica das organizações focadas na pesquisa. Isso permite a inclusão de diversas perspectivas na identificação de ameaças, reforçando a confiança distribuída.
- **Identificação Abrangente de Vetores de Ataque**: As categorias de motivações, recursos e métodos dos adversários, bem como os impactos humanos, fornecem um quadro detalhado para a análise de ameaças. Isso é particularmente útil para organizações horizontais, onde as ameaças podem ser variadas e complexas, exigindo uma abordagem multifacetada para a modelagem de riscos.
- **Flexibilidade e Adaptabilidade**: O uso de cartas permite que a equipe de modelagem de ameaças adapte e personalize a identificação de riscos conforme as especificidades do sistema ou projeto em questão. Esta flexibilidade é crucial para organizações descentralizadas que operam em contextos dinâmicos e em constante evolução.
- **Melhoria da Consistência e Profundidade na Análise de Ameaças**: Ao seguir uma metodologia padronizada de classificação e justificativa das ameaças, o toolkit ajuda a assegurar

que todas as áreas relevantes sejam consideradas, aumentando a consistência e a profundidade dos modelos de ameaça desenvolvidos. Isso contribui para a criação de protocolos de segurança mais robustos e abrangentes.

- **Desenvolvimento de Cenários de Ataque Realistas**: A identificação de perfis de atacantes e cenários de ataque emergentes a partir das atividades propostas permite a criação de modelos de ameaça que refletem melhor as possíveis realidades enfrentadas pelas organizações. Isso é alinhado com o objetivo de desenvolver um protocolo que considere a horizontalidade como um ativo estratégico, garantindo que as contramedidas sejam eficazes e contextualizadas.

AttackTreesforProtectingBiometric

Resumo da Anotação

No artigo "Attack Trees for Protecting Biometric Systems against Evolving Presentation Attacks", é discutida a utilização do **Security Cards**, um kit de ferramentas para brainstorming de ameaças de segurança desenvolvido por T. Denning, B. Friedman e T. Kohno. As principais características e componentes abordados no texto incluem:

- **Security Cards**:
    - **Estrutura**: Consiste em 42 cartas divididas em quatro dimensões principais:
        1. **Impacto Humano (Human Impact)**: Examina como violações de segurança podem afetar os indivíduos, como violação de privacidade, evasão de repercussões legais ou risco de perda de vida em atividades terroristas.
        2. **Motivações do Adversário (Adversary's Motivations)**: Descreve os motivos que levam alguém a atacar um sistema, variando de fatores ideológicos, religiosos e políticos a conveniência e auto-promoção.
        3. **Recursos do Adversário (Adversary's Resources)**: Analisa os ativos que podem estar amplamente disponíveis e ser utilizados para lançar um ataque de identidade, incluindo ferramentas de hardware e software, expertise em personificação técnica ou social, e capacidade de influenciar ações de pessoas.
        4. **Métodos do Adversário (Adversary's Methods)**: Explora as abordagens de alto nível que podem ser usadas para realizar um ataque, como manipulação de pessoas, adesão a processos burocráticos ou regras específicas de tratamento de exceções.
- **Objetivo da Metodologia**:
    - **Categorizar e Avaliar Vulnerabilidades**: Fornece uma maneira prática de categorizar e avaliar vulnerabilidades em sistemas de coleta e gestão de identidade.
    - **Estimular Pensamento Criativo e Abrangente**: Promove um pensamento amplo e criativo sobre a segurança de sistemas biométricos, ajudando desenvolvedores e mantenedores a identificar vetores de ataque específicos que podem não ser cobertos por abordagens tradicionais como checklists e regulamentações.
    - **Compreensão de Técnicas de Ataque**: Facilita a compreensão das técnicas e padrões de ataque já utilizados e postula aqueles que podem ser tentados no futuro, ajudando a antecipar ameaças não previstas.
- **Exemplo de Atividade com Security Cards**:
    - **Trabalho em Grupos**: Grupos de 3-5 pessoas consideram um sistema tecnológico exemplo ou em desenvolvimento.
    - **Familiarização com as Cartas**: Leitura de pelo menos uma carta de cada dimensão para entender os diferentes aspectos das ameaças.
    - **Classificação das Cartas**: Dentro de cada dimensão, as cartas são classificadas em ordem de relevância e risco para o sistema analisado.

- **Justificação e Identificação de Cenários**: Justificar a classificação das cartas e identificar cenários de ataque específicos que emergem, bem como perfis de atacantes.

Relevância para a Pesquisa

A utilização do **Security Threat Brainstorming Toolkit**, como apresentado no artigo, é altamente relevante para a pesquisa em modelagem de ameaças em organizações não-hierárquicas, alinhando-se diretamente com os objetivos de desenvolver um protocolo que valorize a horizontalidade organizacional como um ativo estratégico. Especificamente:

- **Abordagem Estruturada e Colaborativa**: O uso das **Security Cards** facilita a colaboração entre diversos stakeholders, promovendo uma participação distribuída que é característica das estruturas horizontais. Isso reforça a confiança distribuída e a governança horizontal, elementos centrais na segurança organizacional em ambientes descentralizados.
- **Identificação Abrangente de Ameaças**: As quatro dimensões das cartas permitem uma análise detalhada e multifacetada das possíveis ameaças, assegurando que aspectos como impacto humano, motivações, recursos e métodos dos adversários sejam considerados de forma holística. Isso é crucial para organizações não-hierárquicas, onde as ameaças podem ser mais diversificadas e complexas.
- **Estimulação de Pensamento Criativo**: Ao incentivar o pensamento criativo e abrangente sobre ameaças, o toolkit ajuda a identificar vetores de ataque que poderiam passar despercebidos em abordagens mais tradicionais. Isso é especialmente importante em estruturas horizontais, onde a distribuição de responsabilidades pode introduzir novas vulnerabilidades.
- **Flexibilidade e Adaptabilidade**: A metodologia das **Security Cards** é flexível e adaptável, permitindo que as organizações ajustem a identificação de ameaças conforme suas necessidades específicas e contextos operacionais. Essa adaptabilidade é essencial para organizações descentralizadas que operam em ambientes dinâmicos e em constante evolução.
- **Melhoria na Consistência e Profundidade dos Modelos de Ameaça**: Ao seguir uma metodologia padronizada para categorizar e avaliar ameaças, as **Security Cards** asseguram uma maior consistência e profundidade na análise de riscos. Isso contribui para a criação de modelos de ameaça mais robustos e confiáveis, fundamentais para a segurança em estruturas organizacionais horizontais.
- **Desenvolvimento de Contramedidas Eficazes**: A identificação sistemática das ameaças facilita a implementação de contramedidas eficazes e contextualizadas, alinhadas com a distribuição de responsabilidades e a ausência de uma hierarquia rígida. Isso garante que as medidas de segurança sejam apropriadas e eficazes para mitigar os riscos identificados.

CyberThreatModeling
No artigo "Cyber Threat Modeling: An Evaluation of Three Methods", são avaliadas três metodologias distintas de modelagem de ameaças cibernéticas: **STRIDE**, **Security Cards** e **Persona Non Grata**. As principais observações e conclusões do estudo incluem:

- **STRIDE**:
    - **Desenvolvimento e Aplicação**: Desenvolvido pela Microsoft, o STRIDE é uma abordagem amplamente adotada que envolve a modelagem de sistemas e subsistemas, analisando como os dados fluem através deles. Utiliza uma abordagem baseada em checklists, categorizando ameaças em seis categorias (confidencialidade, integridade, disponibilidade, etc.).
    - **Vantagens**: Baixo número de falsos positivos e ideal para equipes com pouca expertise em segurança, pois a abordagem de checklist limita a geração de falsos positivos.
    - **Desvantagens**: Aplicar checklists a componentes variados de sistemas pode ser uma tarefa onerosa e pode levar a resultados inconsistentes, dependendo da composição e experiência das equipes.
- **Security Cards**:
    - **Desenvolvimento e Aplicação**: Desenvolvido pela Universidade de Washington, o Security Cards é um toolkit de brainstorming que utiliza 42 cartas divididas em quatro dimensões: Impacto Humano, Motivações do Adversário, Recursos do Adversário e Métodos do Adversário.
    - **Vantagens**: Promove maior criatividade e identificação de ataques incomuns ou sofisticados, resultando em maior eficácia na identificação de tipos variados de ameaças.
    - **Desvantagens**: Gera um alto número de falsos positivos e apresenta grande variabilidade nos resultados entre diferentes equipes, tornando-se ideal para cenários onde se valoriza uma gama mais ampla de resultados em detrimento da consistência.
- **Persona Non Grata**:
    - **Desenvolvimento e Aplicação**: Desenvolvido pela Universidade DePaul, o Persona Non Grata foca em identificar atacantes, suas motivações e capacidades. Envolve a criação de perfis de atacantes para guiar a identificação de vetores de ataque.
    - **Vantagens**: Reduz o número de falsos positivos e promove a consistência na identificação de ameaças, sendo ideal para análises onde se busca identificar ameaças prioritárias com alto grau de confiança.
    - **Desvantagens**: Pode não fornecer uma visão abrangente das ameaças, identificando apenas um subconjunto consistente de tipos de ameaças, o que limita a compreensão completa das possíveis vulnerabilidades.

Relevância para a Pesquisa

A avaliação comparativa das metodologias **STRIDE**, **Security Cards** e **Persona Non Grata** é extremamente relevante para a pesquisa em modelagem de ameaças em organizações não-hierárquicas. As principais considerações incluem:

- **Adaptação às Estruturas Horizontais**: A diversidade de abordagens oferece insights sobre como diferentes métodos podem ser adaptados para ambientes organizacionais distribuídos e colaborativos. Por exemplo, o **Security Cards** promove uma colaboração criativa, alinhando-se bem com estruturas horizontais que valorizam a participação distribuída.
- **Equilíbrio entre Consistência e Abrangência**: A comparação mostra que métodos como **STRIDE** e **Persona Non Grata** oferecem maior consistência e menor incidência de falsos positivos, enquanto **Security Cards** proporciona uma identificação mais abrangente de ameaças. Esse equilíbrio é crucial para desenvolver um protocolo que valorize a horizontalidade, garantindo tanto a confiabilidade quanto a abrangência na identificação de riscos.
- **Facilitação da Colaboração e Inclusão de Diversas Perspectivas**: Métodos que incentivam a colaboração, como o **Security Cards**, podem ser particularmente benéficos para organizações não-hierárquicas, onde a contribuição de múltiplos stakeholders é essencial. Isso reforça a confiança distribuída e a governança horizontal, pilares fundamentais para a segurança organizacional em ambientes descentralizados.
- **Flexibilidade e Adaptabilidade**: A variabilidade observada no **Security Cards** sugere que, embora este método possa ser mais suscetível a inconsistências, ele também oferece uma maior flexibilidade para adaptar a modelagem de ameaças às especificidades de cada organização. Isso é alinhado com a necessidade de protocolos que possam se ajustar dinamicamente às mudanças e à evolução das ameaças em estruturas horizontais.
- **Identificação de Vetores de Ataque Prioritários**: A abordagem do **Persona Non Grata** para focar em ameaças prioritárias com alta confiança pode ser integrada com outras metodologias para garantir que as ameaças mais críticas sejam identificadas de forma consistente, complementando a abrangência oferecida por métodos mais criativos.

KeepingAheadofOurAdversaries

No artigo "Keeping Ahead of Our Adversaries", são discutidas abordagens para a modelagem de ameaças de segurança em sistemas tecnológicos, com ênfase na utilização do **Security Cards**, um toolkit de brainstorming desenvolvido por Tamara Denning, Batya Friedman e Tadayoshi Kohno. As principais ideias e componentes abordados no texto incluem:

- **Objetivos da Modelagem de Ameaças**:
    - **Identificar Capacidades e Objetivos dos Atacantes**: Compreender as habilidades e metas dos adversários para catalogar ameaças potenciais que o sistema deve mitigar.
    - **Atividade de Requisitos**: A modelagem de ameaças é considerada uma atividade de requisitos, onde a compreensão das necessidades de segurança é essencial para o desenvolvimento de requisitos completos e consistentes.
- **Security Cards: Um Toolkit de Brainstorming para Ameaças de Segurança**:
    - **Estrutura do Toolkit**:
        - **Total de Cartas**: 42 cartas divididas em quatro dimensões principais:
            1. **Impacto Humano (Human Impact)**: Explora como violações de segurança podem afetar os indivíduos e a sociedade, incluindo privacidade pessoal, bem-estar emocional e físico, bem-estar financeiro, relacionamentos e impactos incomuns.
            2. **Motivações do Adversário (Adversary's Motivations)**: Descreve os motivos que levam alguém a atacar um sistema, como malícia, vingança, promoção pessoal, diplomacia ou guerra, entre outros.
            3. **Recursos do Adversário (Adversary's Resources)**: Analisa os ativos que um adversário pode utilizar para lançar um ataque, incluindo ferramentas de hardware e software, expertise técnica, impunidade, conhecimento interno, dinheiro, poder e influência, tempo e recursos incomuns.
            4. **Métodos do Adversário (Adversary's Methods)**: Explora as abordagens de alto nível que um adversário pode utilizar para realizar um ataque, como manipulação de pessoas, ataques indiretos, coerção, ataques multifase, ataques físicos e tecnológicos, entre outros.
    - **Objetivos da Metodologia**:
        - **Categorizar e Avaliar Vulnerabilidades**: Fornece uma maneira prática de categorizar e avaliar as vulnerabilidades de sistemas de coleta e gestão de identidade.
        - **Estimular Pensamento Criativo e Abrangente**: Promove a identificação de ataques incomuns ou sofisticados, ajudando desenvolvedores e mantenedores a antecipar ameaças não previstas por abordagens tradicionais.
        - **Compreensão de Técnicas de Ataque**: Facilita a compreensão das técnicas e padrões de ataque já utilizados e postula aqueles que podem ser tentados no futuro, permitindo a antecipação de ameaças emergentes.

- **Exemplo de Aplicação das Security Cards**:
    - **Contexto**: Aplicação das Security Cards a um Sistema de ICD (Implantable Cardioverter Defibrillator).
    - **Dimensões e Exemplos de Cartas**:
        - **Impacto Humano**:
            1. **Bem-Estar Físico**: Avaliar como um ICD comprometido pode impactar a saúde física dos usuários.
            2. **Bem-Estar Emocional**: Considerar como os pacientes podem se sentir ameaçados à sua saúde.
            3. **Bem-Estar Financeiro e Relacionamentos**: Analisar como um ataque pode descreditar a empresa responsável pelo ICD ou comprometer dados pessoais.
            4. **Dados Pessoais**: Explorar como informações identificadoras armazenadas no dispositivo podem ser usadas por atacantes.
        - **Motivações do Adversário**:
            1. **Malícia ou Vingança**: Atacantes podem visar usuários de ICD por emoções extremas.
            2. **Promoção Pessoal**: Atacantes podem querer demonstrar habilidades técnicas.
            3. **Diplomacia ou Guerra**: Atacantes podem visar inimigos políticos que possuem ICDs.
        - **Recursos do Adversário**:
            1. **Expertise Técnica**: Avaliar as habilidades técnicas dos hackers.
            2. **Impunidade**: Considerar a dificuldade de responsabilizar ou processar o atacante.
            3. **Conhecimento Interno**: Explorar como ex-funcionários com conhecimento detalhado da arquitetura podem comprometer o sistema.
        - **Métodos do Adversário**:
            1. **Ataque Tecnológico**: Utilizar métodos tecnológicos para comprometer o ICD.
            2. **Ataque Multifase**: Alterar o software em escritórios médicos responsáveis pelo envio de comandos ao ICD.
            3. **Ataque Indireto e Encobrimento**: Manipular processos burocráticos ou esconder a origem do ataque.
- **Transição de Ameaças para Requisitos**:
    - **Exemplo de Ameaça**: "Como um especialista em TI com intenção de prejudicar fisicamente um paciente com ICD, lançarei um ataque no dispositivo que alterará os efeitos pretendidos no coração do paciente."
    - **Aplicação**: Utilizar a catalogação de ameaças para melhorar o software em desenvolvimento, transformando ameaças identificadas em requisitos de segurança específicos para mitigar os riscos.

Relevância para a Pesquisa

A utilização do **Security Threat Brainstorming Toolkit**, conforme apresentado no artigo, é altamente relevante para a pesquisa em modelagem de ameaças em organizações não-hierárquicas. Este toolkit oferece uma abordagem estruturada e colaborativa para identificar e categorizar potenciais ameaças, o que é essencial em ambientes onde a governança e a responsabilidade são distribuídas de forma horizontal. Especificamente:

- **Abordagem Estruturada e Colaborativa**: O uso das **Security Cards** facilita a colaboração entre diversos stakeholders, promovendo uma participação distribuída que é característica das estruturas horizontais. Isso reforça a confiança distribuída e a governança horizontal, elementos centrais na segurança organizacional em ambientes descentralizados.
- **Identificação Abrangente de Vetores de Ataque**: As quatro dimensões das cartas permitem uma análise detalhada e multifacetada das possíveis ameaças, assegurando que aspectos como impacto humano, motivações, recursos e métodos dos adversários sejam considerados de forma holística. Isso é crucial para organizações não-hierárquicas, onde as ameaças podem ser mais diversificadas e complexas, exigindo uma abordagem multifacetada para a modelagem de riscos.
- **Estimulação de Pensamento Criativo**: Ao incentivar o pensamento criativo e abrangente sobre ameaças, o toolkit ajuda a identificar vetores de ataque que poderiam passar despercebidos em abordagens mais tradicionais. Isso é especialmente importante em estruturas horizontais, onde a distribuição de responsabilidades pode introduzir novas vulnerabilidades.
- **Flexibilidade e Adaptabilidade**: A metodologia das **Security Cards** é flexível e adaptável, permitindo que as organizações ajustem a identificação de ameaças conforme suas necessidades específicas e contextos operacionais. Essa adaptabilidade é essencial para organizações descentralizadas que operam em ambientes dinâmicos e em constante evolução.
- **Melhoria na Consistência e Profundidade dos Modelos de Ameaça**: Ao seguir uma metodologia padronizada para categorizar e avaliar ameaças, as **Security Cards** asseguram uma maior consistência e profundidade na análise de riscos. Isso contribui para a criação de modelos de ameaça mais robustos e confiáveis, fundamentais para a segurança em estruturas organizacionais horizontais.
- **Desenvolvimento de Contramedidas Eficazes**: A identificação sistemática das ameaças facilita a implementação de contramedidas eficazes e contextualizadas, alinhadas com a distribuição de responsabilidades e a ausência de uma hierarquia rígida. Isso garante que as medidas de segurança sejam apropriadas e eficazes para mitigar os riscos identificados.

MicrosoftThreatModelingTechnique

No artigo "A Descriptive Study of Microsoft's Threat Modeling Technique", é realizada uma análise detalhada da metodologia **STRIDE**, desenvolvida pela Microsoft, como uma técnica baseada em modelos para a modelagem de ameaças cibernéticas. As principais componentes e descobertas do estudo incluem:

- **Metodologia STRIDE**:
    - **Desenvolvimento e Propósito**: STRIDE é uma técnica de modelagem de ameaças desenvolvida pela Microsoft que guia o analista de segurança através de várias atividades para identificar e catalogar ameaças que um sistema deve mitigar.
    - **Etapas da Metodologia**:
        1. **Modelagem do Sistema com Diagramas de Fluxo de Dados (DFD)**: Definir o escopo da análise e produzir um modelo do sistema em revisão usando DFDs, que detalham como a informação flui através de sistemas e subsistemas.
        2. **Mapeamento dos Elementos do DFD para Categorias de Ameaças**: As ameaças são organizadas em seis categorias: Spoofing (S), Tampering (T), Repudiation (R), Information Disclosure (I), Denial of Service (D) e Elevation of Privilege (E). Cada tipo de elemento no DFD é suscetível a uma ou mais dessas categorias.
        3. **Elicitação das Ameaças**: Utilização de checklists específicos para cada categoria de ameaça, facilitando a identificação de ameaças concretas que devem ser consideradas no contexto do sistema analisado.
        4. **Documentação das Ameaças**: Embora STRIDE não exija um formato específico, frequentemente são utilizados casos de uso de abuso (misuse cases) para documentar as ameaças, incluindo informações de segurança como pontos de captura para prevenção ou detecção das ameaças.
- **Resultados do Estudo**:
    - **Percepção da Técnica**: A técnica STRIDE não é percebida como difícil de aplicar.
    - **Produtividade**: A produtividade média foi de 1,8 ameaças por hora, indicando um custo de tempo relativamente alto.
    - **Falsos Positivos**: A média de ameaças incorretas foi baixa, correspondendo a 19–24% do total de ameaças produzidas.
    - **Ameaças Omitidas**: A média de ameaças omitidas foi muito alta, correspondendo a 64–69% do total de ameaças identificadas.
    - **Consistência dos Resultados**: As ameaças identificadas estavam mais relacionadas à composição específica das equipes e sua experiência, resultando em resultados inconsistentes.
    - **Comparação com Outras Técnicas**: Métodos como casos de uso de abuso e árvores de ataque mostraram-se mais eficazes na interpretação e análise dos resultados.

Relevância para a Pesquisa

A avaliação da metodologia **STRIDE** apresentada no artigo é altamente relevante para a pesquisa em modelagem de ameaças em organizações não-hierárquicas, alinhando-se com os objetivos de desenvolver um protocolo que valorize a horizontalidade organizacional como um ativo estratégico. As principais considerações incluem:

- **Eficiência e Produtividade**: A baixa produtividade observada com STRIDE (1,8 ameaças por hora) sugere que, embora a técnica seja acessível para equipes com pouca expertise em segurança, o alto custo de tempo pode ser um impedimento para organizações que operam de forma descentralizada e buscam eficiência na identificação de ameaças.
- **Consistência e Cobertura das Ameaças**: A alta taxa de ameaças omitidas (64–69%) indica uma limitação significativa na capacidade de STRIDE de fornecer uma visão abrangente das ameaças, o que é crucial para estruturas organizacionais horizontais onde a diversidade de operações pode introduzir uma variedade maior de vetores de ataque.
- **Comparação com Outras Metodologias**: A constatação de que métodos alternativos, como casos de uso de abuso e árvores de ataque, oferecem melhores resultados em termos de interpretação e análise, sugere que integrar ou adaptar essas técnicas pode ser benéfico para a criação de um protocolo de modelagem de ameaças mais robusto e confiável.
- **Adaptação às Estruturas Horizontais**: Dado que STRIDE depende fortemente de checklists e categorização padronizada, pode não se adaptar bem a ambientes onde a colaboração e a participação distribuída são essenciais. Métodos que promovem maior criatividade e inclusão de diversas perspectivas, como **Security Cards** e **Persona Non Grata**, podem ser mais adequados para organizações não-hierárquicas.
- **Desenvolvimento de Protocolos Personalizados**: A análise das limitações de STRIDE reforça a necessidade de desenvolver protocolos de modelagem de ameaças que combinem a estrutura e a consistência de STRIDE com a criatividade e a abrangência de outras metodologias. Isso permitirá uma identificação mais completa e eficiente das ameaças, alinhada com a governança horizontal e a confiança distribuída.

ThreatModelingdesigningForSecurity

No livro "Threat Modeling: Designing for Security" de Adam Shostack (2014), são abordados os conceitos fundamentais e as aplicações práticas das árvores de ataque no contexto da modelagem de ameaças de segurança. As principais ideias discutidas no trecho fornecido incluem:

- **Definição de Árvores de Ataque**:
    - Inspiradas na introdução de Bruce Schneier, as árvores de ataque são uma ferramenta formal e metódica para descrever a segurança de sistemas com base em diversos ataques.
    - Estrutura da árvore: o nó raiz representa o objetivo final do ataque, enquanto os nós folha representam diferentes maneiras de alcançar esse objetivo.
- **Aplicações das Árvores de Ataque**:
    - **Encontrar Ameaças**: Utilizar árvores de ataque para identificar possíveis ameaças a um sistema.
    - **Organizar Ameaças**: Estruturar ameaças já identificadas através de outras metodologias ou ferramentas.
    - **Combinação das Duas Abordagens**: Utilizar árvores de ataque tanto para descobrir novas ameaças quanto para organizar aquelas já encontradas.
- **Métodos de Utilização das Árvores de Ataque**:
    - **Uso de Árvores de Ataque Existentes**: Adotar árvores de ataque previamente criadas por outros para auxiliar na identificação de ameaças.
    - **Criação de Árvores de Ataque para Projetos Específicos**: Desenvolver árvores de ataque personalizadas para refletir as ameaças específicas de um projeto em andamento.
    - **Criação de Árvores para Uso Geral**: Elaborar árvores de ataque que possam ser reutilizadas por outras equipes ou projetos, embora isso seja desafiador mesmo para especialistas em segurança.
- **Desafios na Criação de Árvores de Ataque**:
    - A criação de novas árvores de ataque para uso geral é complexa e requer um alto nível de expertise em segurança, tornando-a uma tarefa desafiadora mesmo para profissionais experientes.

Relevância para a Pesquisa

A compreensão e aplicação das **árvores de ataque**, conforme descrito por Adam Shostack, são altamente relevantes para a pesquisa em modelagem de ameaças em organizações não-hierárquicas. As árvores de ataque oferecem uma estrutura formal e sistemática para identificar, categorizar e organizar ameaças potenciais, o que é essencial para ambientes organizacionais horizontais onde a governança e a responsabilidade são distribuídas entre múltiplos stakeholders. Especificamente:

- **Estruturação de Ameaças**: As árvores de ataque permitem decompor ameaças complexas em componentes mais manejáveis, facilitando a identificação de vetores de ataque específicos e a compreensão das interdependências entre diferentes ameaças. Isso alinha-se com o objetivo de

desenvolver um protocolo que valorize a horizontalidade organizacional como um ativo estratégico, garantindo que todas as possíveis ameaças sejam consideradas de forma abrangente.

- **Flexibilidade e Adaptação**: A capacidade de utilizar árvores de ataque existentes ou criar novas árvores específicas para projetos permite uma adaptação flexível às necessidades de organizações não-hierárquicas. Essa flexibilidade é crucial para ambientes descentralizados que exigem respostas dinâmicas e adaptáveis às ameaças emergentes.
- **Colaboração e Compartilhamento de Conhecimento**: A utilização de árvores de ataque pode facilitar a colaboração entre diferentes equipes dentro de uma organização não-hierárquica, promovendo o compartilhamento de conhecimento sobre ameaças e estratégias de mitigação. Isso reforça a confiança distribuída e a governança horizontal, pilares fundamentais para a segurança organizacional em estruturas descentralizadas.
- **Identificação Proativa de Ameaças**: Ao incentivar a criação e utilização de árvores de ataque, a metodologia promove uma abordagem proativa na identificação de ameaças, permitindo que as organizações antecipem e mitiguem riscos antes que eles se materializem. Isso é alinhado com a necessidade de organizações não-hierárquicas de serem ágeis e resilientes diante de um cenário de ameaças cibernéticas em constante evolução.
- **Integração com Outras Metodologias de Modelagem**: As árvores de ataque podem complementar outras técnicas de modelagem de ameaças, como **Security Cards** e **Persona Non Grata**, proporcionando uma visão multifacetada e robusta das ameaças. Essa integração é essencial para desenvolver um protocolo de modelagem de ameaças que seja abrangente e adaptável às particularidades das estruturas organizacionais horizontais.

DREADful

No artigo "DREADful _ Microsoft Learn", são discutidas as metodologias de modelagem de ameaças **STRIDE** e **DREAD**, ambas desenvolvidas e implementadas pela Microsoft. As principais observações e críticas apresentadas incluem:

- **Críticas às Metodologias STRIDE e DREAD**:
  - **Falta de Rigor Acadêmico**: Ambas as metodologias foram alvo de críticas por não terem sido desenvolvidas com rigor acadêmico, o que compromete sua robustez do ponto de vista científico.
  - **Intercorrelações em STRIDE**: A metodologia STRIDE apresenta várias intercorrelações entre suas categorias de ameaças. Por exemplo, a elevação de privilégio (Elevation of Privilege - E) pode implicar spoofing e perda de não-repúdio, além de potencialmente indicar tampering, information disclosure e denial of service. Essa sobreposição resulta em uma classificação menos rigorosa e mais complexa.
  - **Utilidade Prática vs. Rigidez Científica**: Apesar das limitações acadêmicas, STRIDE e DREAD são considerados úteis na prática, especialmente para focar debates e discussões sobre problemas específicos de segurança. Essas metodologias são valorizadas no ambiente corporativo por sua capacidade de organizar e categorizar ameaças de maneira acessível, mesmo que não atendam a padrões acadêmicos rigorosos.
- **Desenvolvimento e Aplicação de DREAD**:
  - **Origem do DREAD**: DREAD surgiu a partir de iniciativas de segurança no Visual Studio e foi uma das primeiras metodologias de segurança antes da implementação da segurança no Windows Server 2003.
  - **Avaliação do DREAD**: Embora o modelo DREAD seja considerado razoável, o principal desafio identificado é a implementação de um escore geral para as ameaças. A dificuldade em atribuir pontuações consistentes compromete a eficácia do modelo.
- **Conclusões Gerais**:
  - **Utilidade Prática**: Mesmo sem rigor acadêmico, as metodologias STRIDE e DREAD são úteis para profissionais de segurança na identificação e categorização de ameaças.
  - **Limitações**: A principal limitação observada é a alta intercorrelação entre categorias em STRIDE e a dificuldade de escore no DREAD, o que pode levar a inconsistências e subestimação de ameaças importantes.

Relevância para a Pesquisa

A avaliação crítica das metodologias **STRIDE** e **DREAD** apresentada no artigo é altamente relevante para a pesquisa em modelagem de ameaças em **organizações não-hierárquicas**, alinhando-se com o objetivo de desenvolver um protocolo que valorize a **horizontalidade organizacional** como um ativo estratégico. As principais considerações incluem:

- **Limitações das Metodologias Existentes**: A falta de rigor acadêmico e as intercorrelações nas categorias de STRIDE indicam que essas metodologias podem não capturar todas as nuances e complexidades presentes em estruturas organizacionais horizontais. Em ambientes

descentralizados, onde as responsabilidades e funções são distribuídas, uma categorização rígida e inter-relacionada de ameaças pode levar a lacunas na identificação de riscos específicos.

- **Necessidade de Metodologias Adaptáveis e Consistentes**: A dificuldade em implementar um escore geral no DREAD ressalta a necessidade de metodologias que ofereçam consistência e precisão na avaliação de ameaças. Para organizações não-hierárquicas, onde a colaboração e a distribuição de responsabilidades são essenciais, uma abordagem que permita uma avaliação mais granular e adaptável das ameaças é crucial.
- **Integração com Abordagens Complementares**: Dado que STRIDE e DREAD têm suas limitações, a pesquisa pode se beneficiar da integração dessas metodologias com outras abordagens mais criativas e colaborativas, como **Security Cards** e **Persona Non Grata**. Essas metodologias podem complementar STRIDE e DREAD, oferecendo uma visão mais abrangente e adaptável das ameaças, alinhada com a governança horizontal e a confiança distribuída.
- **Desenvolvimento de um Protocolo Personalizado**: Considerando as críticas às metodologias existentes, há uma oportunidade significativa para desenvolver um protocolo de modelagem de ameaças que combine a estrutura organizada de STRIDE com a criatividade e adaptabilidade de outras abordagens. Esse protocolo personalizado deve atender às necessidades específicas de organizações não-hierárquicas, garantindo uma identificação e mitigação de ameaças mais eficazes e contextualmente relevantes.
- **Foco na Consistência e Completude**: A alta taxa de ameaças omitidas em STRIDE destaca a importância de garantir que o protocolo de modelagem de ameaças desenvolvido para organizações horizontais seja capaz de identificar uma ampla gama de ameaças de maneira consistente. Isso é essencial para evitar vulnerabilidades que podem ser exploradas em ambientes onde a supervisão centralizada é mínima.

SecurityDevelopmentLifecycle

No eBook "The Security Development Lifecycle" da Microsoft, é discutida a importância e os detalhes do processo de **modelagem de ameaças** como uma atividade crucial no ciclo de vida de desenvolvimento de software. As principais ideias abordadas no trecho fornecido incluem:

- **Importância da Modelagem de Ameaças**:
    - **Prioridade na Segurança**: Se fosse possível escolher apenas uma ação para melhorar a segurança do software – modelagem de ameaças, revisões de código de segurança ou testes de segurança – a modelagem de ameaças seria a escolhida, devido à sua capacidade de identificar problemas de segurança no início do ciclo de desenvolvimento.
    - **Economia de Custos**: Resolver questões de segurança precocemente resulta em significativas economias de custos, pois as correções são mais baratas e menos disruptivas quando feitas nas fases iniciais do desenvolvimento.
- **Benefícios da Modelagem de Ameaças**:
    - **Contribuição para o Gerenciamento de Riscos**: As ameaças identificadas são riscos tanto para os usuários quanto para o ambiente que implementa o software.
    - **Detecção Precoce de Ameaças**: Identificar ameaças antes que o sistema seja codificado permite a resolução de problemas de design de segurança de forma proativa.
    - **Revalidação da Arquitetura e Design**: Revisar o design com foco em segurança e privacidade reforça a robustez do sistema.
    - **Perspectiva Diferente**: Força a equipe de desenvolvimento a considerar o design sob a ótica da segurança e privacidade, focando nos componentes com alta probabilidade de ataque.
    - **Seleção de Contramedidas Adequadas**: Auxilia na escolha das contramedidas apropriadas para o aplicativo e seu ambiente.
    - **Redução da Superfície de Ataque**: Contribui para a redução das áreas vulneráveis do software.
    - **Guia para Revisões de Código e Testes de Penetração**: Orienta processos de revisão de código e testes de penetração, aumentando a eficácia das análises de segurança.
- **Produção e Utilização dos Modelos de Ameaças**:
    - **Documentação**: O principal resultado do processo de modelagem de ameaças é um documento que descreve informações de fundo sobre a aplicação, define o modelo de alto nível (geralmente usando Diagramas de Fluxo de Dados - DFDs), lista os ativos que precisam ser protegidos e as ameaças ao sistema.
    - **Modelagem Modular**: Para sistemas grandes, é mais eficiente modelar módulos menores, mas isso pode levar a lacunas de segurança na composição final do sistema.
    - **Definição de Fronteiras de Confiança**: Identificar fronteiras de confiança ajuda a determinar onde os dados mudam de um nível de privilégio para outro, permitindo a análise de segurança nesses pontos críticos.
- **Processo de Modelagem de Ameaças com STRIDE**:
    - **Etapas da Metodologia STRIDE**:

1. **Definir Cenários de Uso**: Identificar como os usuários interagem com o sistema.
2. **Coletar Dependências Externas**: Listar todos os componentes externos que o sistema utiliza.
3. **Definir Assunções de Segurança**: Estabelecer suposições sobre a segurança do sistema.
4. **Criar Notas de Segurança Externas**: Documentar considerações de segurança externas ao sistema.
5. **Criar DFDs**: Desenvolver Diagramas de Fluxo de Dados para modelar o sistema.
6. **Determinar Tipos de Ameaças**: Categorizar as ameaças conforme o modelo STRIDE.
7. **Identificar Ameaças ao Sistema**: Listar ameaças específicas com base nos DFDs.
8. **Determinar Risco**: Avaliar o nível de risco associado a cada ameaça.
9. **Planejar Mitigações**: Desenvolver estratégias para mitigar os riscos identificados.

- **Descobertas do Estudo**:
    - **Percepção da Técnica STRIDE**: A técnica STRIDE não é considerada difícil de aplicar.
    - **Produtividade**: A produtividade média foi de 1,8 ameaças por hora, indicando um custo de tempo relativamente alto.
    - **Falsos Positivos**: A média de ameaças incorretas foi baixa, correspondendo a 19–24% do total de ameaças produzidas.
    - **Ameaças Omitidas**: A média de ameaças omitidas foi muito alta, correspondendo a 64–69% do total de ameaças identificadas.
    - **Consistência dos Resultados**: As ameaças identificadas estavam mais relacionadas à composição específica das equipes e sua experiência, resultando em resultados inconsistentes.
    - **Comparação com Outras Técnicas**: Métodos como casos de uso de abuso e árvores de ataque mostraram-se mais eficazes na interpretação e análise dos resultados.

Relevância para a Pesquisa

A análise da metodologia **STRIDE** apresentada no eBook da Microsoft é altamente relevante para a pesquisa em modelagem de ameaças em **organizações não-hierárquicas**. As principais considerações incluem:

- **Eficiência e Custo de Tempo**: A produtividade relativamente baixa observada com STRIDE (1,8 ameaças por hora) sugere que, embora a técnica seja acessível para equipes com pouca expertise em segurança, o alto custo de tempo pode ser um impedimento para organizações que operam de forma descentralizada e buscam eficiência na identificação de ameaças.
- **Cobertura de Ameaças**: A alta taxa de ameaças omitidas (64–69%) indica que STRIDE pode não ser suficientemente abrangente para capturar todas as ameaças relevantes em ambientes

organizacionais horizontais, onde a diversidade de operações pode introduzir uma variedade maior de vetores de ataque.

- **Consistência dos Resultados**: A inconsistência dos resultados de STRIDE, devido à variação na composição e experiência das equipes, destaca a necessidade de metodologias que ofereçam uma identificação mais padronizada e abrangente das ameaças, especialmente em estruturas organizacionais distribuídas.
- **Comparação com Outras Metodologias**: A constatação de que métodos alternativos, como casos de uso de abuso e árvores de ataque, oferecem melhores resultados em termos de interpretação e análise, sugere que a integração dessas técnicas pode ser benéfica para a criação de um protocolo de modelagem de ameaças mais robusto e confiável.
- **Adaptação às Estruturas Horizontais**: Considerando que STRIDE depende fortemente de checklists e categorização padronizada, pode não se adaptar bem a ambientes onde a colaboração e a participação distribuída são essenciais. Métodos que promovem maior criatividade e inclusão de diversas perspectivas, como **Security Cards** e **Persona Non Grata**, podem ser mais adequados para organizações não-hierárquicas.
- **Desenvolvimento de Protocolos Personalizados**: A análise das limitações de STRIDE reforça a necessidade de desenvolver protocolos de modelagem de ameaças que combinem a estrutura e a consistência de STRIDE com a criatividade e a abrangência de outras metodologias. Isso permitirá uma identificação mais completa e eficiente das ameaças, alinhada com a governança horizontal e a confiança distribuída.
- **Foco na Consistência e Completude**: A alta taxa de ameaças omitidas em STRIDE destaca a importância de garantir que o protocolo de modelagem de ameaças desenvolvido para organizações horizontais seja capaz de identificar uma ampla gama de ameaças de maneira consistente, evitando vulnerabilidades que podem ser exploradas em ambientes onde a supervisão centralizada é mínima.

SoftwareandattackcentricThreatModeling

No artigo "Software and Attack Centric Integrated Threat Modeling for Quantitative Risk Assessment", são avaliadas diversas metodologias de modelagem de ameaças, destacando suas características, vantagens e limitações. As principais metodologias discutidas incluem:

- **Modelagem de Ameaças Centrada em Ativos (Asset Centric Threat Modeling)**:
    - **Descrição**: Envolve uma estratégia de defesa (blue team) focada na proteção da infraestrutura interna de um sistema. É popular em aplicações de tecnologia da informação e negócios, onde ativos como dados de saúde, fundos monetários ou informações pessoalmente identificáveis precisam ser protegidos contra intrusos externos, de forma semelhante a um cofre bancário no domínio físico.
    - **Vantagem**: Foco nas medidas de segurança mais práticas e comprovadas, conforme identificado pelo SANS Institute em 2013, que priorizam as 20 medidas de segurança mais impactantes para a segurança de rede.
    - **Desvantagem**: Limita-se ao domínio cibernético, concentrando-se principalmente na segurança geral de redes, o que pode não abordar ameaças específicas ou emergentes fora desse escopo.
- **DREAD**:
    - **Descrição**: Metodologia de modelagem de ameaças que utiliza um acrônimo para Damage Potential (Potencial de Dano), Reproducibility (Reprodutibilidade), Exploitability (Explorabilidade), Affected Users (Usuários Afetados) e Discoverability (Descobribilidade). Ao invés de usar variáveis booleanas, DREAD adota uma abordagem numérica, atribuindo valores de 0, 5 e 10 para as primeiras quatro categorias e de 0, 5, 9 e 10 para a última, permitindo o cálculo de uma média que representa o risco total do sistema.
    - **Vantagem**: Proporciona uma avaliação quantitativa dos riscos, facilitando a priorização das ameaças com base em pontuações agregadas.
    - **Desvantagem**: A implementação das pontuações pode ser subjetiva e inconsistente, afetando a confiabilidade das avaliações de risco.
- **TRIKE**:
    - **Descrição**: Framework de modelagem de ameaças de código aberto que se assemelha às metodologias da Microsoft, como STRIDE e DREAD, mas com foco em uma abordagem baseada em risco. TRIKE enfatiza o impacto sobre os stakeholders do sistema, ao invés de apenas categorizar ataques, ameaças e vulnerabilidades.
    - **Vantagem**: Oferece uma perspectiva orientada a riscos, considerando o impacto direto nas partes interessadas, o que pode resultar em uma análise de ameaças mais alinhada com os objetivos de negócios.
    - **Desvantagem**: A abordagem baseada em risco pode ser mais complexa e exigir um entendimento mais profundo dos impactos, tornando a implementação mais trabalhosa.
- **PASTA (Process for Attack Simulation and Threat Analysis)**:

- **Descrição**: Desenvolvido por Uceda Velez et al., PASTA é um framework de modelagem de ameaças que consiste em 7 camadas, oferecendo capacidades de modelagem mais detalhadas do que as ferramentas tradicionais. PASTA foca em simular ataques e analisar ameaças viáveis para um alvo de aplicação específico.
- **Vantagem**: Proporciona uma modelagem de ameaças mais abrangente e detalhada, permitindo uma análise aprofundada das ameaças e suas potenciais consequências.
- **Desvantagem**: O processo extensivo com várias camadas de modelagem pode ser demorado e complexo, exigindo mais recursos e expertise para sua implementação eficaz.

Relevância para a Pesquisa

A avaliação das metodologias **Asset Centric Threat Modeling**, **DREAD**, **TRIKE** e **PASTA** é altamente relevante para a pesquisa em modelagem de ameaças em **organizações não-hierárquicas**, alinhando-se diretamente com o objetivo de desenvolver um protocolo que valorize a **horizontalidade organizacional** como um ativo estratégico. As principais considerações incluem:

- **Adaptação às Estruturas Horizontais**:
    - **PASTA** e **TRIKE**, com suas abordagens detalhadas e baseadas em risco, oferecem uma modelagem de ameaças mais alinhada com a necessidade de compreensão profunda das interações e impactos nas organizações descentralizadas.
    - **DREAD**, embora forneça uma avaliação quantitativa, pode necessitar de adaptações para garantir consistência e reduzir a subjetividade nas pontuações, garantindo que a avaliação de riscos seja confiável e aplicável em estruturas horizontais.
- **Equilíbrio entre Consistência e Abrangência**:
    - **Asset Centric Threat Modeling** foca nas medidas de segurança mais práticas e comprovadas, o que pode ser útil para estabelecer uma base consistente de segurança em organizações distribuídas.
    - **PASTA**, com sua modelagem detalhada, complementa a necessidade de identificar ameaças complexas e multifacetadas que são comuns em ambientes organizacionais não-hierárquicos.
- **Flexibilidade e Adaptabilidade**:
    - A natureza extensiva de **PASTA** permite uma adaptação flexível às necessidades específicas de organizações horizontais, onde a colaboração e a distribuição de responsabilidades são essenciais.
    - **TRIKE**, com seu enfoque em impacto sobre stakeholders, facilita uma abordagem mais personalizada e contextualizada na identificação e mitigação de ameaças, refletindo melhor a dinâmica das organizações não-hierárquicas.
- **Consistência e Redução de Falsos Positivos**:
    - **DREAD** pode enfrentar desafios na consistência das avaliações devido à subjetividade das pontuações, o que pode ser mitigado através de treinamentos e padronizações específicas para ambientes horizontais.

    - **Asset Centric Threat Modeling** e **PASTA** oferecem abordagens que, embora mais complexas, podem proporcionar uma maior consistência e cobertura abrangente das ameaças, minimizando a ocorrência de falsos positivos e assegurando uma identificação mais completa dos riscos.
- **Integração com Outras Metodologias**:
    - A combinação de **PASTA** com outras abordagens mais criativas e colaborativas, como **Security Cards** e **Persona Non Grata**, pode resultar em um protocolo de modelagem de ameaças mais robusto e adaptável, atendendo às especificidades das organizações não-hierárquicas.
    - **TRIKE** e **DREAD** podem ser integrados para fornecer uma avaliação quantitativa complementar à modelagem detalhada de ameaças, oferecendo uma visão mais holística e multifacetada dos riscos.

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.

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.