AHybridThreatModelingMethod

O artigo discute a importância de realizar análises de ameaças sistemáticas, rigorosas e personalizadas para identificar e documentar métodos de ataque potenciais, conforme sugerido por Hilburn (2013) e Opdahl (2009). Define-se um método de modelagem de ameaças (TMM) como uma abordagem para criar uma abstração de um sistema de software, visando identificar as capacidades e objetivos dos atacantes e, a partir disso, gerar e catalogar possíveis ameaças que o sistema deve mitigar (Shull, 2016a).

Os Diagramas de Fluxo de Dados (DFDs) são utilizados para representar graficamente como um sistema funciona, incluindo interações entre armazenamentos de dados, processos, fluxos de dados e entidades externas (Shostak, 2014). O método STRIDE é abordado como uma ferramenta que utiliza checklists para associar elementos do DFD a categorias de ameaças, sendo acessível por meio de referências ou ferramentas específicas. Embora o STRIDE seja adequado para equipes com pouca expertise em segurança devido à sua abordagem baseada em checklists, ele exige um esforço significativo para aplicar essas listas e depende fortemente da criação precisa dos DFDs.

Os autores propõem o desenvolvimento de um método híbrido (hTMM) que combina aspectos dos Security Cards e do PnG, visando capturar as melhores características de ambos os modelos, além das lições aprendidas com o STRIDE. Reconhecem que o hTMM pode evoluir após a realização de projetos de modelagem de ameaças de médio a grande porte, além de estudos de caso menores e pesquisas anteriores conduzidas por estudantes.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** O artigo fornece uma base para a criação de métodos híbridos de modelagem de ameaças, relevante para desenvolver um protocolo adaptado a estruturas organizacionais horizontais.
- **Análise Crítica:** Destaca as limitações de métodos existentes como o STRIDE, incentivando a busca por abordagens mais eficientes e adaptáveis.
- **Governança e Segurança:** A integração de diferentes métodos pode contribuir para uma governança mais robusta e distribuída, alinhando-se com os objetivos de tratar a horizontalidade como ativo estratégico.

AbcCrypto

O artigo aborda as limitações dos paradigmas de modelagem de ameaças existentes, que majoritariamente focam em aplicações de software ou sistemas distribuídos com poucos tipos de participantes. Propõe-se o modelo ABC, especificamente adaptado para o domínio das criptomoedas, introduzindo novas categorias de ameaças que consideram as motivações financeiras dos atacantes e os novos tipos de ativos críticos associados a esse ecossistema.

O modelo ABC diferencia-se por não utilizar uma lista pré-definida de ameaças generalizadas. Em vez disso, reconhece que incentivos financeiros e análises econômicas desempenham papéis fundamentais em diversas etapas do processo de design, incluindo a avaliação de riscos e a mitigação de ataques que não podem ser neutralizados criptograficamente. Essa abordagem permite uma priorização das ameaças com base no potencial de dano financeiro, favorecendo aquelas que oferecem maiores recompensas aos atacantes.

Além disso, o artigo enfatiza que diferentes tipos de sistemas possuem requisitos distintos para a modelagem de ameaças, reforçando a necessidade de ferramentas especializadas para sistemas emergentes como as criptomoedas. O processo de modelagem de ameaças no ABC resulta em uma lista documentada de cenários de ameaças impactantes, servindo como um guia para os projetistas na segurança do sistema. A priorização das ameaças baseia-se na análise do impacto financeiro potencial, alinhando-se com mecanismos de detecção e punição que utilizam incentivos racionais e análise de teoria dos jogos para mitigação e gestão de riscos.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** O modelo ABC exemplifica a necessidade de adaptar métodos de modelagem de ameaças para contextos específicos, como o das criptomoedas, o que pode inspirar abordagens semelhantes para organizações não-hierárquicas.
- **Análise Crítica:** O artigo destaca a importância de considerar motivações financeiras e ativos únicos, incentivando uma análise mais aprofundada das particularidades das estruturas organizacionais horizontais na modelagem de ameaças.
- **Governança e Segurança:** A integração de incentivos econômicos e análises de risco no modelo ABC pode contribuir para o desenvolvimento de protocolos que valorizem a horizontalidade como um ativo estratégico, promovendo uma governança mais robusta e distribuída.

AdvancedThreatModeling

O documento apresenta uma visão abrangente sobre a modelagem de ameaças, definindo-a como um processo para identificar, enumerar e priorizar ameaças potenciais a partir da perspectiva de um atacante hipotético. Baseia-se em definições de fontes como a Wikipedia e Shull (2016a), estabelecendo que um método de modelagem de ameaças (TMM) cria uma abstração de um sistema de software para identificar as habilidades e objetivos dos atacantes, gerando e catalogando ameaças que o sistema deve mitigar.

Quem Realiza a Modelagem de Ameaças?

- **Vendedores como Microsoft:** Desenvolveram e utilizam o método STRIDE, disponibilizando-o gratuitamente.
- **Organizações Governamentais como o DoD:** Mandato para o DoD, com diversos métodos baseados em padrões NIST e checklists.
- **Organizações Comerciais:** Incluem setores como automotivo e financeiro, utilizando métodos como STRIDE, OCTAVE e árvores de ataque.
- **BSIMM:** Identifica os modelos de ataque como uma prática de nível 1.

Conceitos Fundamentais:

- **Segurança Não é Binária:** Reconhece que a segurança é uma função de diversos fatores, como o atacante, seus recursos, a probabilidade e as condições.
- **Vulnerabilidade de Segurança:** Definida como uma fraqueza que permite a um atacante contornar controles de segurança, exigindo uma susceptibilidade do sistema, acesso do atacante à falha e capacidade para explorá-la.

Ferramentas e Metodologias de Modelagem de Ameaças:

- **Security Cards:** Ferramenta de brainstorming para explorar amplamente ameaças de segurança e privacidade, promovendo a mentalidade de segurança. Inclui exercícios práticos com cenários específicos, como veículos autônomos não tripulados.
- **Personas e Persona non Grata (PnG):** Utilização de descrições detalhadas de personas para guiar decisões de desenvolvimento e introdução de PnGs para representar usuários ou atacantes indesejados, auxiliando na compreensão e defesa contra usuários maliciosos.

Metodologias de Modelagem de Ameaças:

- **VAST (Visual, Simple, and Agile Threat Modeling):** Destinado a grandes e médias organizações que adotam metodologias ágeis, visando consistência na saída dos modelos de ameaças.
- **Trike Threat Model:** Focado em auditoria de segurança a partir de uma perspectiva de gerenciamento de riscos, com o objetivo de gerar modelos de ameaças de forma confiável e repetível.
- **PASTA (Process for Attack Simulation & Threat Analysis):** Processo de sete etapas que inclui definição de objetivos de negócios e segurança, decomposição de aplicações, análise de ameaças, análise de vulnerabilidades, modelagem e simulação de ataques, e análise e gestão de riscos.

Implementação de Modelos de Ameaças:

- **Trike Implementation:** Envolve a identificação dos objetivos do sistema, análise de atores e ativos, criação de Diagramas de Fluxo de Dados (DFDs), construção de gráficos de ataque, determinação de vulnerabilidades e aplicação de soluções, além de avaliação de riscos e estratégias de mitigação.
- **PASTA Process:** Inclui etapas detalhadas para definir objetivos, decompor aplicações, analisar ameaças e vulnerabilidades, modelar e simular ataques, e realizar análise e gestão de riscos, integrando requisitos de negócios e de segurança.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** O documento oferece uma base sólida sobre as diversas metodologias de modelagem de ameaças, destacando a necessidade de adaptação a diferentes contextos organizacionais, o que é crucial para o desenvolvimento de um protocolo focado em estruturas não-hierárquicas.
- **Análise Crítica:** Ao discutir as limitações de métodos como STRIDE e a importância de considerar especificidades de sistemas diversos, o documento incentiva a busca por abordagens que acomodem a horizontalidade organizacional, alinhando-se com o objetivo de tratar a horizontalidade como um ativo estratégico.
- **Governança e Segurança:** As metodologias apresentadas, como VAST, Trike e PASTA, fornecem insights sobre a integração de diferentes frameworks de segurança e governança, essenciais para desenvolver um protocolo que valorize a governança distribuída e robusta em organizações horizontais.

Colbac

Título: COLBAC Shifting Cybersecurity from Hierarchical to Horizontal Designs

O artigo aborda a discrepância entre as estruturas de governança organizacional horizontal e os sistemas de controle de acesso hierárquicos atualmente utilizados em tecnologias de segurança cibernética. Utilizando pesquisa etnográfica, o estudo examina casos específicos, como o de um sindicato democrático que transicionou para uma estrutura mais horizontal, mas enfrentou desafios devido ao controle centralizado de senhas e acessos digitais por indivíduos ou pequenos grupos hierarquizados.

Principais Pontos Abordados:

1. **Desajuste entre Governança Organizacional e Tecnológica:**
    - **Exemplo Prático:** O sindicato que adotou uma estrutura democrática enfrentou dificuldades quando os detentores de poder anterior se recusaram a compartilhar senhas, resultando em controle indevido das comunicações digitais.
    - **Problema Geral:** A incompatibilidade entre governança horizontal e sistemas de controle de acesso hierárquicos, que perpetuam a centralização de poder.
2. **Limitações dos Sistemas de Controle de Acesso Hierárquicos:**
    - **Controle Discricionário de Acesso:** Permite que o proprietário de um objeto decida quem pode acessar ou modificar, criando uma hierarquia implícita.
    - **Centralização de Poder:** A necessidade de um proprietário para gerenciar permissões leva à concentração de autoridade, contrariando princípios de governança horizontal.
3. **Proposta de COLBAC (Collaborative Blockchain Access Control):**
    - **Autorização Horizontal:** Desenvolvimento de protocolos participativos que permitem autorizações dinâmicas e flexíveis, ajustando-se às necessidades da organização sem comprometer a horizontalidade.
    - **Participação Democrática:** Implementação de mecanismos que permitem a rápida centralização temporária em situações de crise ou que exigem expertise específica, mantendo a capacidade de retornar a uma estrutura horizontal.
4. **Desafios e Considerações:**
    - **Identificação de Stakeholders:** Determinar quem faz parte do coletivo e como diferentes partes interessadas interagem dentro do sistema.
    - **Usabilidade e Experiência do Usuário:** Garantir que os sistemas de segurança horizontal sejam utilizáveis e eficazes, evitando problemas como fadiga de votação.
    - **Interação com Sistemas Centralizados:** Explorar como sistemas baseados em COLBAC podem interagir com solicitações externas, como aquelas de autoridades legais, sem comprometer a segurança horizontal.
5. **Exemplos de Sistemas Horizontais:**
    - **Criptomoedas:** Embora Bitcoin utilize um protocolo de consenso que promove a horizontalidade teórica, na prática, enfrenta centralização devido à concentração de recursos e poder entre mineradores e desenvolvedores.

- **Forks e Hacks:** Incidentes como o hack da DAO e forks do Bitcoin ilustram as limitações dos sistemas atuais em manter uma governança verdadeiramente horizontal.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** O artigo destaca a necessidade de desenvolver modelos de ameaças que considerem estruturas de governança horizontal, alinhando-se com o objetivo de criar um protocolo que valorize a horizontalidade como um ativo estratégico.
- **Governança e Segurança:** A proposta de COLBAC oferece uma abordagem inovadora para alinhar os sistemas de controle de acesso com estruturas organizacionais descentralizadas, contribuindo para uma governança mais robusta e distribuída.
- **Análise Crítica:** Ao identificar as falhas dos sistemas hierárquicos em contextos horizontais, o estudo incentiva a busca por soluções que promovam a participação democrática e limitem a centralização de poder, essencial para organizações não-hierárquicas.
- **Frameworks de Segurança:** A integração de protocolos participativos e dinâmicos, como o COLBAC, pode informar o desenvolvimento de frameworks de segurança que suportem a flexibilidade e adaptabilidade necessárias em estruturas organizacionais horizontais.

CoReTM

O artigo aborda a importância de abordagens colaborativas na modelagem de ameaças, especialmente diante do aumento do número de sistemas de informação, funcionários e ativos críticos que necessitam de proteção. Destaca-se que a inclusão de diversos especialistas, dependendo do tipo de ativo em modelagem, é essencial para uma análise abrangente.

As ferramentas existentes não suportam adequadamente a colaboração em processos modernos, como metodologias ágeis e DevSecOps, pois estão vinculadas a metodologias subjacentes específicas. Em resposta a essa limitação, a implementação prototípica do CoReTM oferece:

1. **Editor Colaborativo Baseado em Anotações:** Facilita a contribuição síncrona e assíncrona de múltiplos colaboradores.
2. **Relatórios Automatizados de Ameaças:** Gera documentação sistemática das ameaças identificadas.
3. **Integração com DevOps:** Suporta a modelagem de ameaças em diversas combinações de estilos de reuniões, adaptando-se a diferentes fluxos de trabalho.

O artigo também revisa metodologias existentes de modelagem de ameaças, como STRIDE, CAPEC, ATT&CK, OWASP e Attack Trees, discutindo suas categorias de ameaças, abordagens e limitações em contextos colaborativos. Destaca-se que metodologias como PASTA e Trike apresentam complexidades adicionais ao buscar uma análise de riscos mais detalhada.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** CoReTM exemplifica uma abordagem que facilita a colaboração na modelagem de ameaças, alinhando-se com a necessidade de participação distribuída em estruturas organizacionais horizontais.
- **Governança e Segurança:** A integração com DevOps e a flexibilidade para diferentes estilos de reuniões refletem a adaptabilidade necessária para governanças horizontais.
- **Frameworks de Segurança:** A análise comparativa com metodologias como STRIDE e PASTA fornece insights sobre a combinação de diferentes frameworks para fortalecer a modelagem de ameaças em organizações não-hierárquicas.

DemystifyingTheThreatModelingProcess

Título: Demystifying the Threat-Modeling Process

O artigo explora a aplicação da modelagem de ameaças no desenvolvimento de produtos, utilizando a abordagem da Microsoft. Destaca-se a importância de tratar a modelagem de ameaças como parte integrante do processo de design e especificação.

Principais Pontos:

1. **Escopo do Processo:**
    - Modelar ameaças para todo o produto pode ser excessivamente complexo, enquanto focar em funcionalidades individuais é simplista.
    - A abordagem recomendada foca em grupos lógicos de funcionalidades, chamados componentes.
2. **Pontos de Entrada:**
    - Representam interfaces com outros softwares, hardwares e usuários.
    - Cada ponto de entrada é atribuído a um nível de confiança que indica a confiabilidade na troca de dados.
    - Sistemas mais complexos podem ter níveis de confiança adicionais.
3. **Ativos Protegidos:**
    - Recursos com os quais o componente interage e que precisam ser protegidos contra roubo, modificação ou interrupção.
    - Exemplos comuns incluem dados sensíveis, processos críticos e comunicações internas.
    - É essencial listar os níveis de confiança necessários para acessar cada ativo.
4. **Diagramas de Fluxo de Dados (DFD):**
    - Representação gráfica do componente, exibindo entradas, saídas e processos internos.
    - Utiliza cores para mapear níveis de confiança: verde (confiado), vermelho (não confiável) e laranja (parcialmente confiável).
    - Formas diferentes no diagrama indicam processos lógicos (círculos), entidades externas (retângulos) e armazenamentos de dados passivos (linhas horizontais duplas).
5. **Entidades Externas:**
    - Incluem pontos de entrada ou dependências sobre os quais não há controle direto, como bibliotecas, programas externos, máquinas remotas, dispositivos e pessoas.
    - Cada entidade externa deve corresponder a um ou mais pontos de entrada ou dependências.
    - Podem enviar ou receber dados conforme os níveis de confiança estabelecidos.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** A segmentação por componentes e a definição de níveis de confiança podem ser adaptadas para estruturas organizacionais horizontais, facilitando a distribuição de responsabilidades e a redução da centralização de poder.

- **Governança e Segurança:** A categorização clara de pontos de entrada e ativos protegidos contribui para a criação de protocolos que respeitem a governança horizontal, promovendo uma distribuição equilibrada de controle e acesso.
- **Frameworks de Segurança:** A utilização de DFDs e a classificação de confiança podem ser incorporadas em frameworks de segurança que suportem a transparência e a colaboração inerentes a organizações não-hierárquicas.

EvaluationofCompetingThreatModeling

Título: Evaluation of Competing Threat Modeling Methodologies

O artigo avalia diferentes métodos de modelagem de ameaças (TMMs), destacando que nenhum método é igualmente eficaz na identificação de todos os tipos de ameaças.

Principais Pontos:

1. **Adequação Variada dos TMMs:**
    - Os métodos de modelagem de ameaças não são igualmente adequados para identificar todos os tipos de ameaças.
2. **Trade-offs Entre Métodos:**
    - Os TMMs apresentam compromissos significativos entre a quantidade de ameaças reportadas, a possibilidade de falsos positivos e a frequência de relatórios.
    - Nenhum TMM otimiza todas as dimensões de importância simultaneamente, exigindo escolhas baseadas nas prioridades específicas da organização.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** A identificação dos trade-offs entre diferentes TMMs é essencial para selecionar ou combinar métodos que melhor atendam às necessidades de organizações não-hierárquicas, garantindo uma cobertura eficaz das ameaças relevantes.
- **Análise Crítica:** A constatação de que nenhum TMM atende a todas as dimensões de importância incentiva a busca por abordagens híbridas ou adaptativas, alinhando-se com o objetivo de desenvolver um protocolo de modelagem de ameaças que valorize a horizontalidade organizacional.

ExperiencesThreatModelingAtMicrosoft

O artigo detalha a aplicação prática da modelagem de ameaças na Microsoft, destacando a integração dessa metodologia no processo de desenvolvimento de software para melhorar a segurança dos produtos.

Principais Pontos:

1. **Definições e Abordagens de Modelagem de Ameaças:**
    - **Modelagem de Ameaças:** Processo de identificar, enumerar e priorizar ameaças potenciais a partir da perspectiva de um atacante.
    - **Abstrações Principais:**
        - **Ativos:** Recursos como processos, usuários, componentes de software ou fontes de dados que precisam ser protegidos.
        - **Vetores e Alvos de Ataque:** Pontos de entrada e caminhos que os atacantes podem utilizar para comprometer os ativos.
2. **Tipos de Modelagem de Ameaças:**
    - **Centrada em Ativos:** Envolve avaliação de riscos, aproximação ou classificação dos ativos a serem protegidos.
    - **Centrada em Atacantes:** Inclui a classificação de riscos e a estimativa de recursos, capacidades ou motivações dos atacantes.
    - **Centrada em Software:** Foca na análise detalhada dos componentes de software e suas interações.
3. **Colaboração na Modelagem de Ameaças:**
    - Importância de abordagens colaborativas para envolver diversos especialistas e perspectivas.
    - **CoReTM:** Prototipagem de uma ferramenta que inclui um editor colaborativo baseado em anotações, relatórios automatizados de ameaças e integração com DevOps para suportar diferentes estilos de reuniões e fluxos de trabalho.
4. **Metodologias Utilizadas:**
    - **STRIDE:** Classificação de ameaças em categorias como Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service e Elevation of Privilege.
    - **DREAD:** Técnica de avaliação de riscos que atribui pontuações para Destruction Potential, Reproducibility, Exploitability, Affected Users e Discoverability, embora apresente limitações na definição de escalas.
    - **PASTA e Trike:** Metodologias mais complexas que oferecem uma análise de riscos detalhada, porém com maior complexidade na implementação.
5. **Processo de Modelagem de Ameaças na Microsoft:**
    - **Passos Principais:**
        - **Diagramação:** Utilização de Diagramas de Fluxo de Dados (DFDs) com a adição de "trust boundaries" para identificar processos, armazenamentos de dados, fluxos de dados e entidades externas.

- **Enumeração de Ameaças:** Identificação das ameaças associadas a cada elemento do DFD.
- **Mitigação:** Desenvolvimento de estratégias para mitigar as ameaças identificadas, priorizando redesign, mitigadores padrão como ACLs, mitigadores únicos com cautela ou aceitação de risco conforme as políticas.
- **Verificação:** Validação dos modelos de ameaças através de heurísticas como análise de gráficos dos DFDs, revisão completa do modelo e verificação das mitigações aplicadas.

6. **Heurísticas para Validação de Modelos de Ameaças:**
    - **Análise de Gráficos:** Verificação se os diagramas refletem o código final.
    - **Enumeração Completa:** Garantir que todas as ameaças STRIDE por elemento foram identificadas.
    - **Revisão e Mitigação:** Revisão geral do modelo e confirmação de que cada ameaça foi mitigada adequadamente.
7. **Desafios e Considerações:**
    - **Fatores Humanos:** Inclusão de aspectos relacionados a pessoas dentro do modelo de ameaças, como phishing decorrente de falhas na autenticação.
    - **Usabilidade e Experiência do Usuário:** Necessidade de que as ferramentas e processos de modelagem de ameaças sejam acessíveis e compreensíveis para engenheiros com diferentes níveis de expertise em segurança.
    - **Integração com Desenvolvimento:** Importância da simplicidade e integração das ferramentas de modelagem de ameaças no processo de desenvolvimento para efetivamente identificar e abordar problemas de design.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** A abordagem da Microsoft demonstra a importância de segmentar a modelagem de ameaças por componentes e definir níveis de confiança, o que pode ser adaptado para estruturas organizacionais horizontais, promovendo a distribuição de responsabilidades.
- **Governança e Segurança:** A integração de ferramentas colaborativas como CoReTM e a categorização clara de ameaças e ativos auxiliam na criação de protocolos que respeitam a governança horizontal, facilitando uma distribuição equilibrada de controle e acesso.
- **Frameworks de Segurança:** A utilização de DFDs com "trust boundaries" e a classificação de confiança podem ser incorporadas em frameworks de segurança que suportem transparência e colaboração em organizações não-hierárquicas.

ParticipatoryThreatModelling

O artigo discute a necessidade de incorporar experiências sociais situadas na modelagem de ameaças, em contraste com abordagens tradicionais que dependem das experiências e suposições de especialistas em segurança.

Principais Pontos:

1. **Limitações das Abordagens Impessoais:**
    - Métodos convencionais de modelagem de ameaças frequentemente baseiam-se nas experiências e suposições dos especialistas, negligenciando perspectivas de usuários cotidianos.
    - Exemplos incluem modelos de ameaças para casas inteligentes que não consideram ameaças de parceiros atuais ou antigos.
2. **Crítica ao "God Trick":**
    - Métodos tradicionais aplicam a perspectiva do "deus que vê do nada", ignorando contextos sociais e experiências individuais.
    - Teorias feministas de ponto de vista defendem o uso de experiências socialmente situadas como uma lente alternativa para o conhecimento em ciência social.
3. **Modelagem de Ameaças Participativa:**
    - Reconfiguração das práticas de modelagem de ameaças para focar nas experiências dos cidadãos com ameaças online.
    - Envolvimento de todas as pessoas afetadas no processo de pesquisa, alinhado com formas de ação feministas interseccionais.
4. **Redefinição do Papel Humano na Cibersegurança:**
    - Mudança de "humano como problema" para "humano como solução" nas estratégias de defesa cibernética.
    - Adoção de abordagens "usáveis", "centradas no usuário" e "centradas no humano".
5. **Fatores de Vulnerabilidade Relacionados ao Gênero:**
    - Questões de vulnerabilidade específicas para mulheres, como desconforto ao receber suporte técnico de homens e preocupações sobre privacidade e segurança.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** A incorporação de perspectivas participativas pode enriquecer a modelagem de ameaças em organizações horizontais, garantindo que as experiências e necessidades dos membros sejam consideradas.
- **Governança e Segurança:** Abordagens centradas no usuário promovem uma governança mais inclusiva e distribuída, alinhando-se com a valorização da horizontalidade organizacional.
- **Frameworks de Segurança:** A integração de métodos participativos e centrados no humano pode informar o desenvolvimento de frameworks que respeitem as dinâmicas sociais e promovam a colaboração em ambientes não-hierárquicos.

ThreatModelingASummaryOfAvailableMethods

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

Principais Pontos:

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

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

Relevância para a Pesquisa:

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

ThreatModelingASystematicLiteratureReview

O artigo examina as diversas definições de modelagem de ameaças encontradas na literatura, destacando a multiplicidade e, por vezes, a incompatibilidade dessas definições. Esse estudo visa responder à questão de pesquisa “o que é modelagem de ameaças” e fornecer insights sobre a adoção dessa prática.

Principais Pontos:

1. **Diversidade de Definições:**
    - As definições de modelagem de ameaças são numerosas e utilizadas de maneiras diferentes, possivelmente incompatíveis, conforme identificado na revisão da literatura.
    - **Definição Ampla de Uzunov e Fernandez (2014):** “Modelagem de ameaças é um processo que pode ser usado para analisar ataques ou ameaças potenciais, e pode também ser suportado por bibliotecas de ameaças ou taxonomias de ataques”. Esta definição é considerada amplamente aplicável e abrange a análise de ameaças suportada por recursos estruturados.
2. **Objetivo da Modelagem de Ameaças:**
    - A modelagem de ameaças visa entender quais ameaças e ataques os métodos de modelagem pretendem proteger. Isso é essencial para adaptar as metodologias às necessidades específicas das organizações, especialmente aquelas com estruturas não-hierárquicas.
    - A classificação das ameaças e ataques é realizada separadamente para diferentes categorias (C1 e C2), com os resultados apresentados em tabelas específicas (Tabela 8 e Tabela 9).
3. **Classificação de Ameaças e Ataques:**
    - **C1 e C2:** As ameaças e ataques são categorizados de forma distinta para cada classe, permitindo uma análise mais detalhada e direcionada.
    - **Tabela 8 e Tabela 9:** Apresentam os resultados da classificação, facilitando a compreensão das diferentes tipologias de ameaças abordadas pelos métodos de modelagem de ameaças.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** A identificação da diversidade nas definições de modelagem de ameaças reforça a necessidade de um protocolo adaptável, capaz de integrar diferentes perspectivas e abordagens para atender às particularidades das organizações não-hierárquicas.
- **Análise Crítica:** A constatação de que não existe uma definição unificada de modelagem de ameaças incentiva a investigação de métodos que sejam flexíveis e possam ser customizados conforme os requisitos específicos da governança horizontal.
- **Frameworks de Segurança:** A classificação detalhada de ameaças e ataques, conforme apresentada nas tabelas, pode informar o desenvolvimento de frameworks que considerem a complexidade e a diversidade das ameaças enfrentadas por estruturas organizacionais distribuídas.

ThreatModellingSurvey

O artigo apresenta uma visão geral das metodologias de modelagem de ameaças, com ênfase nas árvores de ataque como uma abordagem utilizada para modelar ameaças a sistemas de software.

Principais Pontos:

1. **Árvores de Ataque:**
    - **Estrutura:** Utiliza uma estrutura em árvore onde o objetivo do ataque está no nó raiz e as diferentes formas de alcançá-lo estão nos nós folhas. Cada nó pode representar um sub-objetivo, com os filhos indicando as maneiras de atingir esse sub-objetivo.
    - **Nodos OR e AND:** Nodos OR representam alternativas para atingir um objetivo, enquanto nodos AND representam diferentes etapas necessárias para alcançar o mesmo objetivo.
    - **Atribuição de Valores:** Valores são atribuídos manualmente aos nós folhas, dependendo do especialista em segurança e do engenheiro de sistema. Esses valores podem incluir tempo necessário para completar uma etapa, despesas operacionais, expertise requerida, etc.
2. **Ferramentas Automatizadas:**
    - **SecureI Tree:** Ferramenta gráfica desenvolvida pela Amenaz Technologies que suporta a modelagem de árvores de ataque. Baseia-se em um modelo matemático de árvores de ataque e utiliza algoritmos matemáticos para calcular os riscos de segurança.
    - **Aplicações Bem-sucedidas:** SecureI Tree tem sido aplicada com sucesso em diversas áreas, como edifícios, oleodutos e linhas de transmissão elétrica.
3. **Vantagens e Limitações:**
    - **Vantagens:** Estrutura clara e visual que facilita a compreensão das diferentes formas de ataques e suas interdependências. Suporte para a inclusão de diversos atributos que enriquecem a análise de risco.
    - **Limitações:** Processo de atribuição de valores é manual e depende fortemente da expertise dos profissionais envolvidos, o que pode introduzir vieses e inconsistências.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** A utilização de árvores de ataque oferece uma abordagem estruturada que pode ser adaptada para refletir as dinâmicas de organizações horizontais, facilitando a identificação de múltiplas vias de ataque e a distribuição de responsabilidades na análise de segurança.
- **Governança e Segurança:** A estrutura hierárquica inerente às árvores de ataque contrasta com a governança horizontal, destacando a necessidade de metodologias que possam ser adaptadas para ambientes menos centralizados.
- **Frameworks de Segurança:** Ferramentas como SecureI Tree demonstram a viabilidade de automatizar aspectos da modelagem de ameaças, o que pode ser integrado em frameworks de segurança que suportem a colaboração e a flexibilidade necessárias em organizações não-hierárquicas.

ThreatModelingAsABasisForSecurityRequirements

O artigo explora a utilização da modelagem de ameaças como fundamento para a especificação de requisitos de segurança, destacando sua integração no processo de engenharia de segurança de sistemas complexos.

Principais Pontos:

1. **Importância da Modelagem de Ameaças na Engenharia de Segurança:**
    - A modelagem de ameaças é essencial para identificar riscos de segurança, definir requisitos e desenvolver estratégias de recuperação.
    - O processo de engenharia de segurança deve ser iterativo, com feedback contínuo entre as etapas para corrigir falhas iniciais sem que seus efeitos se propaguem.
2. **Integração da Modelagem de Ameaças no Ciclo de Vida do Desenvolvimento:**
    - Incorporar a modelagem de ameaças desde as fases iniciais do design e especificação arquitetural reduz custos e tempo na resolução de problemas de segurança futuros.
    - Mesmo quando a segurança é adicionada posteriormente, a modelagem de ameaças pode ser aplicada de maneira semelhante para identificar e mitigar riscos existentes.
3. **Processo de Modelagem de Ameaças:**
    - **Caracterização do Sistema:** Compreensão completa do sistema, incluindo todos os componentes e suas interações.
    - **Identificação de Ativos e Pontos de Acesso:** Determinação dos recursos que precisam ser protegidos e dos pontos onde o sistema pode ser vulnerável a ataques.
    - **Identificação de Ameaças:** Definição das intenções e capacidades dos adversários, bem como das possíveis formas de comprometer o sistema.
4. **Uso de Diagramas de Fluxo de Dados (DFD):**
    - DFDs são utilizados para dissecar aplicações e sistemas em componentes, facilitando a identificação de ameaças ao seguir o fluxo de dados e comandos processados pelo sistema.
    - A precisão dos DFDs é crucial para a eficácia da modelagem de ameaças, permitindo uma análise detalhada das interações internas e externas.
5. **Avaliação e Priorização de Ameaças:**
    - As ameaças identificadas são analisadas com base em sua criticidade e probabilidade de ocorrência.
    - Decisões são tomadas para mitigar ameaças ou aceitar os riscos associados, equilibrando a segurança com a usabilidade do sistema.
6. **Desafios na Modelagem de Ameaças:**
    - **Complexidade dos Sistemas:** Sistemas altamente complexos dificultam a modelagem completa devido à dificuldade de identificar todos os componentes e caminhos de fluxo de dados.
    - **Dependência da Expertise:** A eficácia da modelagem de ameaças depende fortemente da habilidade e experiência dos engenheiros de segurança.

- **Balanceamento entre Segurança e Usabilidade:** Mitigar todas as ameaças pode comprometer a usabilidade, exigindo um equilíbrio cuidadoso.

7. **Estudos de Caso:**
    - **Software-Defined Radio (SDR):** Análise de ameaças em sistemas de rádio definidos por software, destacando a importância de entender as interações entre componentes de software e infraestrutura física.
    - **VisFlowConnect:** Ferramenta de monitoramento de tráfego de rede que utiliza modelagem de ameaças para identificar e mitigar riscos de segurança.
    - **NVisionCC:** Ferramenta de monitoramento de segurança em clusters, demonstrando a aplicação da modelagem de ameaças em ambientes distribuídos e escaláveis.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** O artigo enfatiza a necessidade de uma abordagem sistemática e integrada na modelagem de ameaças, o que é fundamental para desenvolver um protocolo adaptado a organizações não-hierárquicas.
- **Governança e Segurança:** A integração da modelagem de ameaças no ciclo de vida do desenvolvimento promove uma governança mais robusta e distribuída, alinhando-se com a valorização da horizontalidade organizacional.
- **Frameworks de Segurança:** A utilização de DFDs e a priorização de ameaças com base em criticidade e probabilidade podem ser incorporadas em frameworks que suportem a transparência e colaboração em estruturas organizacionais horizontais.