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.