

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.