

### 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.