Utilização de Modelos Evolutivos para Classificar Padrões de Ataque em Modelos de Ameaça*

*Relatório técnico de Computação Evolucionista

1st Eduardo Santos de Oliveira Marques
Graduate Program in Computational Modeling
Federal University of Juiz de Fora
Juiz de Fora, Brazil
email address or ORCID

2nd Alex Borges Vieira
Department of Computer Science
Federal University of Juiz de Fora
Juiz de Fora, Brazil
email address or ORCID

3rd Heder Soares Bernardino
Department of Computer Science
Federal University of Juiz de Fora
Juiz de Fora, Brazil
email address or ORCID

***Abstract*—This document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

***Index Terms*—component, formatting, style, styling, insert.**

I. Introdução

A segurança cibernética, também conhecida como cibersegurança, pode ser compreendida como o conjunto de práticas destinadas à proteção de sistemas computacionais, dispositivos móveis, redes e dados contra acessos não autorizados e ataques maliciosos [1]. Com o avanço exponencial da tecnologia e a crescente interconectividade dos sistemas, essa área tornou-se um pilar essencial não apenas para o funcionamento seguro da infraestrutura digital tradicional, mas também para sistemas mais complexos, como os sistemas ciberfísicos [2]. Nesse contexto, torna-se fundamental dispor de instrumentos capazes de organizar e descrever o amplo espectro de ameaças existentes, de modo a apoiar tanto a análise quanto a mitigação de riscos.

Dentre esses instrumentos, catálogos de ataque cibernéticos, como o CAPEC (*Common Attack Pattern Enumeration and Classification*) [3], e modelos de ameaças, como o STRIDE (*Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service* e *Elevation of Privilege*) vêm sendo amplamente utilizados para apoiar a segurança em um nível sistêmico [4]. Tais catálogos e modelos oferecem mecanismos valiosos para descrever, classificar e compreender vulnerabilidades exploráveis por agentes maliciosos.

O CAPEC contribui de forma significativa para a caracterização tática dos ataques, fornecendo uma visão estruturada dos padrões utilizados em atividades hostis. O STRIDE, por sua vez, organiza as ameaças em seis categorias, facilitando contramedidas e ações a serem realizadas. A integração entre abordagens como CAPEC e STRIDE representa, portanto, uma oportunidade de fortalecer a análise de riscos ao combinar a descrição detalhada de ataques com uma estrutura de classificação de ameaças de alto nível. No entanto, a literatura apresenta lacunas quanto à integração desse catálogo com modelos de ameaça voltados à análise sistêmica, como o STRIDE.

Um dos trabalhos mais relevantes nesse sentido é o projeto *CAPEC-STRIDE Mapping*, desenvolvido por Brett Crawley [5], no qual foram construídos mapas mentais relacionando padrões de ataque às categorias do STRIDE. Apesar de sua contribuição, tal associação é realizada principalmente a partir dos relacionamentos entre os padrões de ataque, sem considerar de forma explícita os atributos ou propriedades de segurança que cada ataque pode violar. Além disso, a maior parte dos ataques catalogados no CAPEC é vinculada a apenas uma categoria do STRIDE, o que pode limitar a representatividade e a utilidade prática dessa classificação.

Diante dessas limitações, este trabalho propõe o desenvolvimento de um algoritmo de agrupamento capaz de organizar os registros do CAPEC em seis grupos distintos, estabelecendo sua associação às categorias do STRIDE com base nos atributos e propriedades de segurança violadas. Tal abordagem busca oferecer uma classificação mais robusta e alinhada à natureza heterogênea das ameaças cibernéticas, contribuindo para uma análise mais precisa e para a mitigação de riscos em cenários complexos.

A. Objetivo

O objetivo central deste trabalho é investigar a viabilidade de mapear os registros da base CAPEC para as categorias do modelo STRIDE a partir de seus atributos, buscando identificar se tais informações são suficientes para apoiar uma classificação coerente de ameaças. Diferentemente de abordagens anteriores, que apresentam apenas o resultado final do mapeamento sem detalhar o processo adotado, propõe-se aqui a utilização de técnicas de aprendizado não supervisionado, com foco em algoritmos de clusterização. Especificamente, pretende-se:

1) Avaliar a relevância dos atributos disponíveis no CAPEC para a caracterização das propriedades de segurança violadas;

Identify applicable funding agency here. If none, delete this.

2) Agrupar os registros em seis categorias correspondentes ao STRIDE, utilizando modelos de clusterização;
3) **Comparar o desempenho de algoritmos evolutivos com métodos tradicionais de clusterização, a fim de analisar a qualidade e a consistência dos agrupamentos obtidos.**

Com isso, busca-se oferecer uma abordagem mais transparente e fundamentada para o mapeamento entre CAPEC e STRIDE, explorando o potencial dos algoritmos evolutivos na análise de bases de ataques cibernéticos.

II. Referencial Teórico

A seguir, serão apresentados mais detalhes sobre os padrões de ataque CAPEC e o modelo de ameaças STRIDE.

A. Padrões de Ataque

O *Common Attack Pattern Enumeration and Classification* (CAPEC) [3] é um catálogo online de padrões de ataques, contendo mais de 500 registros. Um padrão de ataque é uma descrição dos atributos e abordagens comuns usados pelos adversários para explorar pontos fracos conhecidos nos sistemas cibernéticos [6]. Esses padrões descrevem os desafios enfrentados por atacantes e os métodos utilizados para superá-los. A estrutura dos padrões CAPEC é inspirada no conceito de padrões de design, amplamente utilizado em engenharia de software, porém, em vez de representar soluções construtivas, os padrões CAPEC descrevem estratégias destrutivas, derivadas da análise sistemática de incidentes reais e práticas observadas em cenários de ataque do mundo real, permitindo capturar estratégias típicas de exploração observadas em cenários concretos.

Adicionar uma Figura

B. Modelo de Ameaças

O STRIDE é uma metodologia desenvolvida pela Microsoft utilizada para identificar e categorizar ameaças cibernéticas em sistemas computacionais [7]. O termo STRIDE é derivado das letras iniciais de diferentes ameaças, sendo classificadas com base nos objetivos e propósitos de ataques. As ameaças são: falsificação (*Spoofing*), adulteração (*Tampering*), repúdio (*Repudiation*), divulgação de informações (*Information disclosure*), negação de serviço (*Denial of Service* - DoS) e elevação de privilégio (*Elevation of privilege*). Essas categorias correspondem diretamente às propriedades de cibersegurança que podem ser comprometidas por ataques, como autenticidade, integridade, confidencialidade, disponibilidade, não repúdio e autorização, conforme ilustrado na Tabela I [8].

III. Trabalhos na Literatura

Não existem muitos trabalhos na literatura referentes a este problema, a maioria dos projetos envolve o reacionamento do CAPEC com outras bases de segurança, tais como o CVE e ATT&CK. Os trabalhos que envolvem o CAPEC com o modelo de amaeça geralmente envolvem a cosntrução de um Farmnework, basendo-se em relacionamentos já desenvolvidos. O maior exenplo encontrado é evneicadio no trabalho desenvoldio por Breet Craley, onde ele gersa oas relacianmentos, esse relaciandmento foi encontrado em diversos trabalhos, tais como: Colcoar os trabhlos que envolvem esses relacionamentos.

A. Ostering

O trabalho de Ostering consiste em classificações baseadas nos relacionamentos, inspirando-se em teoria dos grafos [9]. Como mencionado anteriormente, o principal objetivo deste trabalho é classificar os padrões de ataque de acordo com os atributos referentes as consequências dos ataques.

B. Mecanismos de ataque

IV. Metodologia

Falar da metodologia aplicada

A. Aquisição e tratamento dos dados

Os dados utilizados neste trabalho foram extraídos de fontes oficiais mantidas pela MITRE e por colaboradores da comunidade. O catálogo CAPEC foi obtido em formato XML, enquanto o mapeamento STRIDE-CAPEC foi disponibilizado em JSON. Abaixo são apresentadas as informações referentes aos dados utilizados:

- **CAPEC**
  - **Data de aquisição:** 31/10/2024
  - **Arquivo:** `capec_v3.9.xml`

TABLE I
Categorias de ameaças STRIDE

Letra	Ameaça	Propriedade violada
S	Falsificação de identidade	Autenticação
T	Adulteração de dados	Integridade
R	Repúdio	Não repúdio
I	Divulgação de informações	Confidencialidade
D	Negação de serviço	Disponibilidade
E	Elevação de privilégio	Autorização

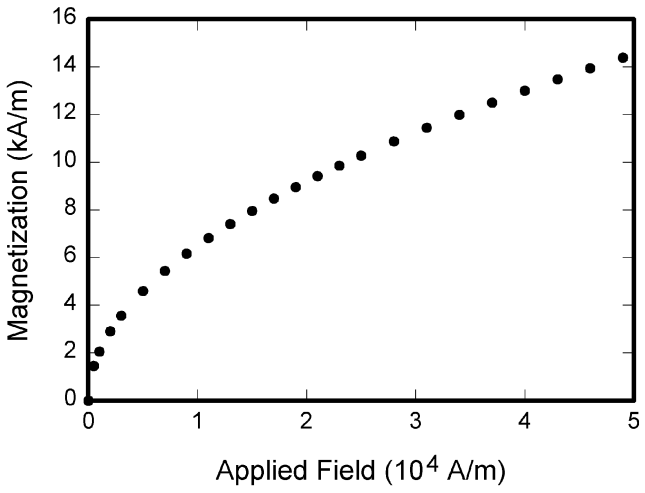

Fig. 1. Example of a figure caption.

  - **Fonte:** https://capec.mitre.org/data/downloads.html
- **STRIDE-CAPEC Mapping**
  - **Data de aquisição:** 30/10/2024
  - **Arquivo:** `capec-stride-mapping.json`
  - **Fonte:** https://ostering.com/blog/2022/03/07/capec-stride-mapping/

O processo para realizar a conversão e a reestruturação do catálogo de ataque para o formato JSON foi conduzido por meio de *scripts* desenvolvidos em Python, que realizaram as seguintes tarefas: (i) extração dos dados brutos, (ii) transformação de estruturas hierárquicas XML em objetos JSON, (iii) padronização de nomenclaturas e atributos, e (iv) organização dos relacionamentos entre entidades de forma compatível com a modelagem proposta. Com relação ao processamento dos dados do mapeamento STRIDE-CAPEC, foram removidas as hierarquias e links presentes no documento, obtendo-se apenas os ataques presentes em cada categoria.

Após a transformação dos arquivos, realizou-se o devido tratamento dos dados, onde foram realizados os seguintes processos: (i) remoção de registros obsoletos (marcados como *DEPRECATED*), (ii) seleção apenas de registros que possuem o mapeamento STRIDE e os atributos utilizados para o código, e (iii) balanceamento dos mapeamentos realizados.

Falar sobre o balanceamento dos dados

Falar que não pretendemos utilizar CAPECs de alto nível, apenas CAPECs que tenham os atributos que serão utilizados

Falar das concentrações presentes em algumas categorias

Como o objetivo deste trabalho é agrupar os CAPECs e comparar seus resultados, optou-se por não gerar dados artificiais, considerando que que tais dados poderiam gerar tendências nos resultados. Como optou-se não usar esse método, as classificações envolvendo repúdio não foram consideradas, visto que possuem poucos registros.

Falar do pré-processamento dos dados

B. Análise dos atributos

Os principais atributos a serem selecioandos para a construção dos clusters são o *Scope* e *Impact*, onde eles são respectivamente falar dos seus significados. As Tabelas II e indicam a quantidade de atributos presentes no catálogo CAPEC.

As cores em azul representam os atributos de *Scope* que mais apareceram por categoria STRIDE, enquanto as cores em verde indicam as representações presentes de acordo com a Tabela I.

Ao comparar os resultados presentes no atributo *Scope* da Tabela IV com as propriedades violadas na Tabela I, observa-se que as classificações realizadas pelo mapeamento STRIDE-CAPEC da Ostering possui algumas discrepâncias, sendo principalmente:

- As classificações estão concentradas em *Confidentiality*;
- Falsificação possui poucos resultados em *Authentication*;

TABLE II
DISTRIBUIÇÃO DE SCOPES NO CATÁLOGO CAPEC

Scope	**N°**	**Tradução**
Access Control	189	Controle de acesso
Accountability	19	Responsabilidade
Authentication	32	Autenticação
Authorization	217	Autorização
Availability	172	Disponibilidade
Confidentiality	466	Confidenciabilidade
Integrity	227	Integridade
Non-Repudiation	16	Não repúdio
Other	5	Outros

TABLE III
DISTRIBUIÇÃO DE SCOPES NO CATÁLOGO CAPEC

Scope	**N°**	**Tradução**
Alter Execution Logic	12	Alterar lógica de execução
Bypass Protection Mechanism	76	Passar pelo mecanismo de proteção
Execute Unauthorized Commands	121	Executar comandos não autorizados
Gain Privileges	135	Ganhar privilégios
Hide Activities	45	Esconder atividades
Modify Data	119	Modificar dados
Other	72	Outros
Read Data	187	Ler dados
Resource Consumption	34	Consumo de recursos
Unreliable Execution	42	Execução não confiável

- Repúdio não possui resultados em *Non-Repudiation*;

Comparando os resultados diretamente com a tabela, têm-se:

- Falsificação → 6° em Autenticação
- Adulteração de dados → 2° em Integridade
- Repúdio → 9° em Não repúdio
- Divulgação de informações → 1° em Confidencialidade
- Negação de serviço → 1° em Disponibilidade
- Elevação de privilégio → 2° em Autorização

Falar dos atributos e da quantidade presente na base

Ao avaliar os resultados presentes na Tabela IV, observa-se que há uma concentração muito grande no atributo *Confidentiality*, o que já entra em contraste com a Tabela I. É importante notar que não é uma regra ter uma categoria associada a cada propriedade de segurança violada, mas faz mais sentido realizar tais associações.

TABLE IV
DISTRIBUIÇÃO DE SCOPES POR CATEGORIA STRIDE

Scope	**S**	**T**	**R**	**I**	**D**	**E**
Access Control	14	45	1	46	3	80
Accountability	4	2	0	1	0	12
Authentication	**9**	2	0	0	0	21
Authorization	18	50	1	45	3	**100**
Availability	15	74	3	3	**28**	49
Confidentiality	**38**	**108**	3	**136**	9	**172**
Integrity	35	**83**	**4**	6	2	97
Non-Repudiation	4	1	**0**	0	0	11
Other	4	0	0	1	0	0

TABLE V
DISTRIBUIÇÃO DE IMPACTS POR CATEGORIA STRIDE

Scope	S	T	R	I	D	E
Alter Execution Logic	2	8	0	0	1	1
Bypass Protection Mechanism	5	12	0	38	1	20
Execute Unauthorized Commands	8	**57**	1	0	2	53
Gain Privileges	16	35	1	7	2	**74**
Hide Activities	2	4	0	38	0	1
Modify Data	12	43	**3**	5	0	56
Other	**19**	1	1	35	11	5
Read Data	14	40	1	**58**	3	71
Resource Consumption	0	14	0	1	**15**	4
Unreliable Execution	2	26	1	1	5	7

C. Construção do Algoritmo

D. Modelos utilizados

Falar sobre os modelos utilizados

V. Resultados e Discussões

Uma das principais diferenças identificadas entre os resultados obtidos no estudo e no mapemaneto da OStering é que o projetop realziado através da curadoria especializada é muito baseado nos relacionamentos presentes ao padrões de ataque, enquanto que no modelo proposto, utilzia-se princiaplemnte as principais conseguqneica envolvuidas no atque, não basenado-nos relacionamentos.

VI. Conclusões

Texto.

VII. Trabalhos futuros

Também falar em trabalhos futuros, dizer que pode usar o CWE e também tentar usar a descrição e o nome do CAPEC pra tentar classificar no STRIDE

Acknowledgment

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression “one of us (R. B. G.) thanks . . .”. Instead, try “R. B. G. thanks. . .”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

References

[1] J. Martínez Torres, C. Iglesias Comesaña, and P. J. García-Nieto, “Review: Machine learning techniques applied to cybersecurity,” *International Journal of Machine Learning and Cybernetics*, vol. 10, no. 10, pp. 2823–2836, 2019.

[2] J. Martinez, N. Quintano, A. Ruiz, I. Santamaria, I. M. de Soria, and J. Arias, “Security debt: Characteristics, product life-cycle integration and items,” in *2021 IEEE/ACM International Conference on Technical Debt (TechDebt)*, pp. 1–5, IEEE, 2021.

[3] MITRE Corporation, “Common Attack Pattern Enumeration and Classification.” https://capec.mitre.org/, 2024. Accessado em: 2024-10-31.

[4] A. Shostack, *Threat Modeling: Designing for Security*. Wiley, 2014.

[5] O. B. Crawley, “Capec-stride mapping,” 2022. Acesso em: 16 de Janeiro de 2025.

[6] F. Mariotti, A. Bondavalli, P. Lollini, L. Montecchi, and S. Nardi, “An extension of the advise meta modeling framework and its application for an early-stage security analysis of a public transport supervision system,” *Journal of Reliable Intelligent Environments*, vol. 9, no. 3, pp. 263–281, 2023.

[7] F. Swiderski and W. Snyder, *Threat modeling*. Microsoft Press, 2004.

[8] N. Shevchenko, T. A. Chick, P. O’Riordan, T. P. Scanlon, and C. Woody, “Threat modeling: a summary of available methods,” *Software Engineering Institute— Carnegie Mellon University*, pp. 1–24, 2018.

[9] J. A. Valadares, S. M. Villela, H. S. Bernardino, G. D. Gonçalves, and A. B. Vieira, “Mapping user behaviors to identify professional accounts in ethereum using semi-supervised learning,” *Expert Systems with Applications*, vol. 229, p. 120438, 2023.