

Zadání diplomové práce



163352

Ústav: Ústav informačních systémů (UIFS)
Student: **Polišenský Jan, Bc.**
Program: Informační technologie a umělá inteligence
Specializace: Kybernetická bezpečnost
Název: **Porovnání klasifikačních metod pro účely detekce maligních domén**
Kategorie: Bezpečnost
Akademický rok: 2024/25

Zadání:

1. Seznamte se s metodami strojového učení se zaměřením na oblast klasifikace.
2. Nastudujte možnosti detekce maligních doménových jmen pomocí metod strojového učení.
3. Z dostatečně velkého seznamu maligních a benigních domén vytvořte anotovanou datovou sadu obsahující data z dostupných zdrojů (informace z DNS, RDAP, TLS certifikátů apod.).
4. Na základě nastudovaných informací a získaných dat vytvořte sadu klasifikátorů s využitím různých klasifikačních metod (rozhodovací stromy, neuronové sítě, SVM aj.), případně jejich kombinací.
5. Experimentálně ověřte a porovnejte použitelnost vytvořených klasifikátorů pomocí standardních metrik.
6. Zhodnoťte dosažené výsledky a navrhněte možná rozšíření.

Literatura:

- Han, Jiawei, Jian Pei, and Hanghang Tong. *Data Mining: Concepts and Techniques*. Morgan Kaufmann, 2022.
- Hajaj, Chen, Nitay Hason, and Amit Dvir. 2022. "Less Is More: Robust and Novel Features for Malicious Domain Detection" *Electronics* 11, č. 6: 969.
- Torroledo, Ivan, Luis David Camacho, and Alejandro Correa Bahnsen. "Hunting malicious TLS certificates with deep neural networks." In *Proceedings of the 11th ACM workshop on Artificial Intelligence and Security*, s. 64-73. 2018.
- Shi, Yong, Gong Chen, and Juntao Li. "Malicious domain name detection based on extreme machine learning." *Neural Processing Letters* 48.3, s. 1347-1357. 2018.

Při obhajobě semestrální části projektu je požadováno:
Body 1 až 3.

Podrobné závazné pokyny pro vypracování práce viz <https://www.fit.vut.cz/study/theses/>

Vedoucí práce: **Hranický Radek, Ing., Ph.D.**
Vedoucí ústavu: Kolář Dušan, doc. Dr. Ing.
Datum zadání: 1.11.2024
Termín pro odevzdání: 21.5.2025
Datum schválení: 22.10.2024