

OPONENTSKÝ POSUDEK BAKALÁŘSKÉ PRÁCE

Student: Rohla Jaroslav

Oponent: Ulrich Adam, Ing.

Studijní program: Bezpečnostní technologie, systémy a management

Specializace: -

Akademický rok: 2024/2025

Téma bakalářské práce: Detekce škodlivého softwaru pomocí strojového učení

Hodnocení práce:

	A	B	C	D	E	F
	Hodnocení: A – nejlepší; F – nevyhovující					
1. Aktuálnost řešeného tématu	☒	☐	☐	☐	☐	☐
2. Obtížnost zadaného úkolu	☒	☐	☐	☐	☐	☐
3. Splnění všech bodů zadání	☒	☐	☐	☐	☐	☐
4. Vhodnost zvolené metody řešení	☒	☐	☐	☐	☐	☐
5. Logické členění práce	☒	☐	☐	☐	☐	☐
6. Úroveň jazykového zpracování	☐	☒	☐	☐	☐	☐
7. Formální úroveň práce	☐	☒	☐	☐	☐	☐
8. Práce s literaturou a její citace	☒	☐	☐	☐	☐	☐
9. Úroveň zpracování teoretické části	☐	☒	☐	☐	☐	☐
10. Kvalita zpracování praktické části	☐	☒	☐	☐	☐	☐
11. Dosažené výsledky práce	☒	☐	☐	☐	☐	☐
12. Přínos práce a její využití	☒	☐	☐	☐	☐	☐

Celkové hodnocení práce:

Výsledná známka není průměrem výše uvedených hodnocení. Znamku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:

A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.

Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou bakalářskou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Otázky k obhajobě:

Jaká oprávnění byla podle modelu nejvíce riziková – a překvapilo vás to?

Další připomínky, vyjádření, náměty k obhajobě práce (možno pokračovat i na další stránce):

Práce se zabývá detekcí malwaru v Android aplikacích pomocí algoritmů Decision Tree a Random Forest, přičemž využívá dataset .apk souborů. Metodicky je práce velmi zajímavá – oceňuji využití knihovny Androguard pro analýzu oprávnění, stejně jako srovnání různých poměrů tříd (1:2, 1:1, 2:1), což dobře ilustruje chování modelu při různém zastoupení benigních a škodlivých aplikací. Zajímavým prvkem je také analýza feature importance, která pomáhá porozumět tomu, jaké znaky jsou pro model klíčové.

Příprava dat je podrobně zpracována, například s rozlišením mezi běžnými a potenciálně nebezpečnými oprávněními, což dává práci praktický rozměr. Zároveň bych ale doporučil mírné zestručnění textu – některé

pasáže působí zbytečně rozvláčně a čtenář se v nich může snadno ztratit. Výsledky by také mohly být místy více vizuálně zvýrazněny (např. pomocí shrnujících tabulek nebo grafů). Kód vzhledem k studijnímu zaměření nekomentuji. Celkově je práce nadstandardní a čtenáři je přínosem. Hodnotím známkou A.

Datum

4.6.2025

Podpis oponenta bakalářské práce