

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: BC. DOROTÍK LADISLAV

Oponent: Ing. Ladislav Vyskočil

Studijní program: **Inženýrská informatika**
Studijní obor/Specializace: **Kybernetická bezpečnost**
Akademický rok: **2021/2022**

Téma diplomové práce: **Analýza datových sad umožňujících detekci mobilního malwaru**

Hodnocení práce:

Cílem diplomové práce bylo popsat analýzu datových sad umožňujících detekci mobilního malwaru, k jehož dosažení bylo třeba naplnit několik bodů, jejichž přesná specifikace byla součástí zásad uvedených v zadání práce. Diplomová práce je na velmi vysoké odborné úrovni a její zpracování a náročnost je nadstandardní. Všechny body zadání diplomové práce byly splněny v plném rozsahu. Diplomant popisované problematice velmi dobře rozumí a je zřejmé, že v dané oblasti má rozsáhlé zkušenosti.

Diplomová práce je přehledně strukturována a jednotlivé části na sebe logicky navazují. Text práce je zpracován velmi odborně a srozumitelně. Po jazykové stránce nebyly nalezeny žádné pravopisné, nebo stylistické chyby. Po formální stránce je práce vhodným způsobem řazena do logických celků a doplněna upřesňujícími komentáři i odkazy na odpovídající literární či elektronické zdroje. V diplomové práci autor uvádí přiměřené množství obrázků, tabulek a příloh k objasnění popisované problematiky.

V teoretické části byl přehledně popsán aktuální stav řešené problematiky a výzkum zaměřený na Android OS zahrnující popis architektury Android OS, popis modelu oprávnění, podrobný popis komponentů aplikace a popis balíčků aplikací AAB a APK. V závěru teoretické části jsou popsány datové sady mobilního malwaru pro Android OS. Tato část popisuje a hodnotí veřejně dostupné, akademické a profesionální datové sady, zabývá se také tvorbou datových sad, sběrem malwaru a analýzami APK.

V praktické části byl popsán návrh systému v infrastruktuře PT LAB, vybrané datové sady pro sběr dat, dále nástroje pro zpracování dat a jejich integrace, zahrnující databázi, automatizované spouštění, použití unikátního nástroje APK - A Perfect Knife, na jehož vývoji se diplomant aktivně podílel, integraci VirusTotal a extrakci významných charakteristik mobilního malwaru. Závěrem praktické části bylo provedeno vyhodnocení jednotlivých zpracovaných datových sad a popis finální datové sady.

Přínos diplomové práce vidím v komplexnosti a zefektivnění práce při detekci mobilního malwaru a v možnostech využití pro další výzkumy v této oblasti.

Diplomová práce se jeví jako zdařilá a splňující svůj cíl, a proto ji doporučuji předložit k obhajobě.

Otázka k obhajobě: Jak bude pokračovat Váš další výzkum v této problematice?

Celkové hodnocení práce:

Známku 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 diplomovou 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.

Datum 1. 6. 2022

Podpis oponenta diplomové práce