KATEDRA POČÍTAČOVÉ GRAFIKY A INTERAKCE
FAKULTA ELEKTROTECHNICKÁ
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Hodnocení vedoucího diplomové práce

Student: **Jiří Bauer**
Název: **Detekce anomalit na základě doménových reputací podle klasifikace stažených souborů**
Vedoucí: **Jan Kubr, Ing.**

1 Náročnost a další komentář k zadání

Hodnocení: 2 – náročnější

Zadání hodnotím jako náročnější. Jedná se o práci, která zahrnuje analýzu reputačních systémů a návrh a implementaci takového systému. Použití reputací je v dané oblasti novým přístupem.

2 Splnění zadání

Hodnocení: 1 – splněno

Zadání bylo zcela splněno.

3 Rozsah písemné zprávy

Hodnocení: 1 – splňuje požadavky

Písemná zpráva splňuje požadavky kladené na diplomovou práci. Všechny části písemné zprávy jsou informačně bohaté a pro práci nezbytné.

4 Věcná a logická úroveň práce

Hodnocení: 90 bodů A

Práce je přehledná a dobře čitelná. Logická struktura závěrečné práce je v pořádku a kapitoly na sebe vhodně navazují.

5 Formální úroveň práce

Hodnocení: 89 bodů B

V práci je občas objevují překlepy či špatně formulované věty. Autor někdy používá zbytečně složitá souvětí.

V práci chybí seznam zkratek.

6 Práce se zdroji

Hodnocení: 90 bodů A

Seznam zdrojů je přiměřený a správně citovaný.

7 Hodnocení výsledků, publikační výstupy a ocenění

Hodnocení: 95 bodů A

Analýza, implementace, provedení testů a jejich zhodnocení jsou správné. Práce zcela poskytla hlavní výsledky. Jedná se o jednu z nejlepších prací a doporučuji komisi navrhnout ji na cenu děkana.

8 Komentář o využitelnosti výsledků

Práce poskytla všechny požadované výsledky a může být začleněna do systémů společnosti Avast.

Systém je v současnosti nasazen v reálném provozu.

9 Aktivita a samostatnost studenta v průběhu řešení

1 – výborná aktivita
1 – výborná samostatnost

Student řešil problémy samostatně, práci pravidelně konzultoval a na konzultace byl výborně připraven.

10 Celkové hodnocení

Práce splňuje zadání. Všechny části práce jsou na výborné úrovni. Práce přináší požadované výsledky a implementovaná aplikace je nasazená v reálném provozu.

Práci hodnotím **98 body (A – výborně)**.

11 Otázky k obhajobě

- Jaká by měla být dostatečná úspěšnost reputační služby (text a poznámka na str. 5)?
- Co limituje rychlost zpracování dat? Procesor, paměť, vstupně/výstupní operace?
- Co bude potřeba v aplikaci upravit pro použití celých URL?

V Portu 11. června 2018

Ing. Jan Kubr

Posudek oponenta diplomové práce

Jméno: Bc. Jiří Bauer

Název práce: Detekce anomálií pomocí doménových reputací na základě klasifikace stažených souborů

Jméno oponenta: Ing. Jan Zíka

Diplomová práce se zabývá vývojem systému Marlowe, který je využíván v Avast Software, s. r. o., pro detekci anomalit. Za anomalitu v našem kontextu považujeme dva základní případy:

1. z domény s dobrou reputací byl uživatelem stažen soubor, který byl Avastem označen jako škodlivý;
2. z domény uživatelé stahují větší množství škodlivých souborů, přestože doména jako taková zablokovaná není.

První případ poukazuje na možnost nesprávné detekce souboru (tzv. false positive), druhý naopak na chybějící detekci na URL (tzv. false negative). Oběma těmto scénářům je potřeba ze zřejmých důvodů předcházet.

Vytvořený systém využívá jednak anonymizovaná data od uživatelů a jednak data z ostatních vnitřních systémů, hledá v nich anomality a snaží se je vyřešit, případně nevyřešené incidenty zobrazuje v dashboardu, který byl pro tento účel vytvořen.

Student prokázal schopnost samostatně dokončit projekt většího rozsahu, od návrhu použití jednotlivých technologií, přes implementaci jeho součástí, až po testování a monitorování jeho chodu. Systém funguje v ostrém provozu 5 měsíců bez chyb nebo nutnosti údržby. Zdrojový kód je logicky členěn a je psaný čistým stylem.

Vzhledem k rozmanitosti použitých technologií a rozsahu projektu práci hodnotím jako nadprůměrně náročnou; vzhledem k pečlivému a preciznímu přístupu studenta během jednotlivých fází projektu navrhuji klasifikaci A (výborně).

Ing. Jan Zíka

Praha 25. 5. 2018