

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	Detekce škodlivých souborů pomocí metod statické analýzy
Jméno autora:	Štěpán Dvořák
Typ práce:	bakalářská
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra počítačů
Vedoucí práce:	Ing. Jan Stiborek
Pracoviště vedoucího práce:	centrum umělé inteligence FEL

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání	náročnější
<i>Hodnocení náročnosti zadání závěrečné práce.</i>	
Autoři škodlivého software (malware) se neustále snaží vylepšovat svoje přístupy (packing, polymorfni malware, atd.) což dělá danou problematiku velice komplikovanou.	

Splnění zadání	splněno
<i>Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.</i>	
Zadání bylo bezechyby splněno.	

Zvolený postup řešení	vynikající
<i>Posuďte, zda student zvolil správný postup nebo metody řešení.</i>	
Student zvolil vhodný postup řešení daného problému, které důsledně otestoval na reálných datech.	

Odborná úroveň	A - výborně
<i>Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.</i>	
Student provedl rešerši literatury, zhodnotil výhody a nevýhody jednotlivých postupů, které následně zkombinoval a obohatil o vlastní nápady. Navržené řešení experimentálně ověřil na dostatečně velkém a reálném vzorku dat.	

Formální a jazyková úroveň, rozsah práce	A - výborně
<i>Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.</i>	
Kladně hodnotím, že práce je psána anglicky s minimem typografických a gramatických chyb.	

Výběr zdrojů, korektnost citací	A - výborně
<i>Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.</i>	
Všechny zdroje a převzaté myšlenky jsou vhodně citovány v souladu se zvyklostmi a normami.	

Další komentáře a hodnocení	
<i>Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.</i>	
Student navrhl řešení, které má velký potenciál pro praktické využití. Experimenty jsou dostatečně detailní a ukazují signifikantní vylepšení state-of-the-art.	

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

Předložená práce navrhuje netriviální řešení komplexního problému klasifikace binárních souborů (portable executable files), které v současné době představují jeden ze základních způsobů šíření škodlivého software. Student si během práce osvojil základy vědecké práce, což se projevilo na vysoké kvalitě předkládané práce. Navržené řešení je experimentálně ověřeno, jsou detailně popsány jeho silné i slabé stránky a nastíněny možnosti dalšího rozšíření.

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **A - výborně**.

Datum: 6.6.2018

Podpis:

Jan Stiborek