

Posudek bakalářské práce

Matematicko-fyzikální fakulta Univerzity Karlovy v Praze

Autor práce Jan Bodnár
Název práce Application of artificial neural networks for malware detection in HTTPS traffic
Rok odevzdání 2017
Studijní program Informatika **Studijní obor** Obecná informatika

Autor posudku RNDr. Jakub Lokoč, Ph.D. **Role** Vedoucí
Pracoviště KSI MFF UK

Prosím vyplňte hodnocení křížkem u každého kritéria. Hodnocení *OK* označuje práci, která kritérium vhodným způsobem splňuje. Hodnocení *lepší* a *horší* označují splnění nad a pod rámec obvyklý pro bakalářskou práci, hodnocení *nevyhovuje* označuje práci, která by neměla být obhájena. Hodnocení v případě potřeby doplňte komentářem. Komentář prosím doplňte všude, kde je hodnocení jiné než *OK*.

K celé práci	lepší	OK	horší	nevyhovuje
Obtížnost zadání	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Splnění zadání	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rozsah práce ... <i>textová i implementační část, zohlednění náročnosti</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Komentář Autor práce se zaměřil na klasifikaci a podobnostní hledání malware na základě komunikačních charakteristik ve formě agregovaných dostupných atributů HTTPS zpráv. Práce porovnává různé architektury umělých neuronových sítí pomocí FP-50 a PR křivek. Pro potřeby podobnostního hledání autor navrhl síť kombinující autoenkodér a principy siamských sítí. Navržená síť se učí vytvářet novou reprezentaci, která mapuje objekty stejné třídy blíže k sobě. Pomocí t-SNE projekcí pak analyzuje chování reprezentací získaných z navržených sítí. Jelikož měl autor k dispozici pouze dvouhodnotovou anotaci vzorků (malware ano/ne), nebylo možné vyvodit specifické závěry ohledně získaných shluků dat.				

Textová část práce	lepší	OK	horší	nevyhovuje
Formální úprava ... <i>jazyková úroveň, typografická úroveň, citace</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Struktura textu ... <i>kontext, cíle, analýza, návrh, vyhodnocení, úroveň detailu</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Analýza	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vývojová dokumentace	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Uživatelská dokumentace	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Komentář Text práce je dobře logicky strukturován a čitelný. Práce je psána v anglickém jazyce na dobré úrovni. Celá práce je experimentálního charakteru, jejím hlavním těžištěm bylo vyhodnocování velkého množství měření, návrh a konfigurace využívaných modelů.				

Implementační část práce	lepší	OK	horší	nevyhovuje
Kvalita návrhu ... <i>architektura, struktury a algoritmy, použité technologie</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kvalita zpracování ... <i>jmenné konvence, formátování, komentáře, testování</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Stabilita implementace	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Komentář				

Celkové hodnocení Výborně
Práci navrhuji na zvláštní ocenění Ne

Datum 14.8.2017

Podpis