

Posudek diplomové práce

Autor: Bc. Martin Labuť

Název: Estimating the Attacker's Cost for Exploiting Computer Network Vulnerabilities

Posudek vypracoval oponent práce: Ing. Jakub Stejskal

Práce měla za úkol prozkoumat dostupná data týkající se slabín počítačových sítí a navrhnout, implementovat a otestovat systém odhadující na jejich základě cenu útoku. Autor splnil veškeré cíle vytyčené v zadání.

Největší výzvou této práce je zřejmě nedostatečné množství a kvalita dat a autor navrhl řadu kreativních postupů, jak tento problém překonat. V některých pasážích však dostatečně nevysvětluje své volby. Ve třetí kapitole je například navrženo cenu vývoje útoku odhadovat pomocí výše odměny za odhalení příslušné slabiny. Diskuzi přiměřenosti této aproximace a jejich úskalí však mohl být věnován větší prostor.

Rešeršní kapitola čtenáře dostatečně uvádí do problematiky, ale zcela chybí popis předchozího stavu výzkumu dané problematiky a srovnání s výsledky jiných experimentů. V návrhové části autor opomněl uvést zdroje, které použil při návrhu operací evolučního algoritmu a lineárního regresoru.

To vše znesnadňuje určit rozsah provedené původní práce a přispívá tomu, že lze jen těžko posoudit přínos jejích výsledků. Autor sám však v závěru hodnotí odhady jako nepřesné a nepříliš užitečné. Jako vedlejší přínos uvádí schopnost systému agregovat data z různých zdrojů.

Jako metodu pro učení estimátorů bylo zvoleno genetické programování pro jeho snadnou interpretovatelnost. Oceňuji snahu o interpretaci a kritickou analýzu nalezených modelů. Popis experimentů je vhodně doplněn výslednými daty a obrazovou dokumentací.

Samotný zdrojový kód se zdá být relativně dobře strukturovaný, čitelný a vhodný pro další použití, avšak v implementační části textu postrádám jeho podrobnou dokumentaci, stejně jako popis použitých technologií a návod k použití nástroje.

Jazyková úroveň textu, jeho srozumitelnost a čitelnost je dobrá a formální nedostatky (gramatiky, slohu, popisů obrazové přílohy a odkazů na ní) jsou ojedinělé a přiměřené rozsahu textu. Členění obsahu a typografie práce je bez větších vad, chybí však seznamy obrázků, tabulek, použitých symbolů a termínů.

Předloženou diplomovou práci hodnotím známkou D-uspokojivě.

16. 1. 2016