POSUDEK DIPLOMOVÉ PRÁCE

Autor: Bc. Martin Labuť
Název: Odhad cen útočníka za zneužití zranitelností v počítačových sítích
Posudek vypracoval vedoucí: Ing. Karel Durkota

Cílem této diplomové práce bylo prozkoumat, zda je možné odhadovat ceny útoků z veřejně dostupných dat a případně navrhnout jeden nebo více způsobů pomocí technik strojového učení. Student velmi dobře prozkoumal na internetu různé databáze zranitelností a využil všech dostupných informací o zranitelnostech. Student zvolil pro interpretovatelnost svého výsledku učení pomocí genetického programování, což velice oceňuji. Obecně během naší spolupráce přicházel se zajímavými a kreativními způsoby, jak řešit různé nesnáze. Pokud vím, odhadováním cen útoku zranitelností z National Vulnerability Database se nezabývá žádná předchozí literatura. Přínosem práce je první automatizovaný odhad těchto cen.

Experimentální část práce se hodně věnuje výběru správných parametrů genetického programování (funkce křížení, funkce mutace atd.). Bohužel se zdaleka tolik nevěnuje samotnému učení (např. průběh učení Exploit Execution Estimatoru (6.3.4) vůbec není graficky znázorněn) a analýze výsledků, která je velmi povrchní. V jednom experimentu genetické programování vrátilo intuitivně "nesmyslný" výstup (na konci odstavce 6.3.4), ale student již nezkoumá, proč tento výsledek obdržel. Podporují data tento výsledek (čili je smysluplný z pohledu dat), anebo ne? Dále bych velice ocenil, kdyby se student pokusil sestavit vlastní intuitivní vzorec a srovnal jeho kvalitu proti vzorcům z genetického programování, ale rozumím, že to není jednoduchý úkol.

Celá diplomová práce je vypracována v angličtině, což velice oceňuji. Úroveň jazyka a gramatiky je výborná. Co se týče konvencí a ucelenosti, je to horší. Tabulky nejsou umístěné tam, kde se o nich diskutuje (na str. 22 se odkazuje na tabulku, která se nachází na str. 25) a zkratky nejsou sjednocené (Sec. nebo Sect., Fig. nebo fig.). Odstavec 6.2.1.1 se opakuje v 6.2.1.8 a některé termíny a zkratky nejsou jasně definované, (např. jaký je rozdíl mezi PCA3-5 anebo co je A2 v odstavci 6.3.1). Grafy jsou v bitmapách, popisky jsou malé a nečitelné a občas úplně chybí legenda.

Předloženou diplomovou práci hodnotím známkou D - uspokojivě.

Datum: 18. 1. 2016