

Oponentský posudek diplomové práce

Název práce: Vulnerability Reports Analysis and Management

Diplomant: Dušan Domány

Hodnocení práce

Práce se věnuje využití metod dolování z textu (text mining) na dokumenty popisující objevené chyby v softwaru (vulnerability reports). Úvodní kapitoly přináší úvod do problematiky - popisují důležitost zpracování hlášení o chybách při zajišťování informační bezpečnosti a také popisují některé z metod dolování z textu.

Následuje asi nejzajímavější kapitola představující teoretickou část práce, která uvádí dosažené výsledky při aplikaci popsaných metod. Možnosti předkládaných metod vypadají zajímavě a aplikovatelně. Zde obsažená analýza však trpí jistým nedostatkem experimentů. Při klasifikaci se trénovací sada i testovací sada bere z jednoho zdroje dat. Předpokládá se, že výsledky budou stejně použitelné i pro jiné zdroje dat, ovšem toto se netestuje. U možností extrakce informací z textu větší experiment v podstatě chybí. Důvod nedostatku experimentů ovšem vidím (shodně s předkladatelem) v nedostatku ručně anotovaných dat, nad kterými by bylo možné experimenty provést.

Praktická část práce se zabývá popisem a výběrem zdrojů dat a nástroje pro jejich stahování (Advisory Updaters) a převádění na společný formát. Poté je popsán samotný nástroj využívající výsledky teoretické části práce (Vulnerability Management Tool). Je zvláštní, že první nástroj je naprogramován pomocí C# .NET, zatímco druhý v Javě, což jistě znesnadní případnou pozdější integraci obou nástrojů do jednoho nástroje. Aplikace se zdá být funkční, trpí však drobnými dětskými neduhy, například:

- ovládací prvky nemění korektně svou velikost podle velikosti okna,
- aplikace nemá titulek.

Celkově hodnotím práci jako zdařilou.

Závěr

V práci jsem nenašel vážnější nedostatky a považuji ji za zdařilou a užitečnou.

V Praze dne 25. srpna 2011

Mgr. Jakub Galgonek

