

Posudek oponenta bakalářské práce

Student: Rek Petr
Téma: Detekce podobnosti zdrojových souborů v jazyce C (id 17996)
Oponent: Kučera Jiří, Ing., UIFS FIT VUT

- 1. Náročnost zadání** **obtížnější zadání**
Zadání hodnotím jako obtížnější jelikož vyžaduje studium problematiky zpětného překladu, která se na bakalářském studijním programu nevyučuje.
- 2. Splnění požadavků zadání** **zadání splněno s podstatným rozšířením**
Zadání bylo beze zbytku splněno a práce obsahuje rozšíření týkající se především realizačního výstupu.
- 3. Rozsah technické zprávy** **přesahuje obvyklé rozmezí**
Text práce sice přesahuje obvyklé rozmezí stanovené pro bakalářskou práci, nicméně je nutné podotknout, že všechny části bakalářské práce jsou pro pochopení a zorientování se v dané problematice nezbytné.
- 4. Prezentací úroveň předložené práce** **95 b. (A)**
Práce je členěna do celkem 10 vzájemně na sebe navazujících kapitol, ve kterých je podrobně rozebírána problematika zpětného inženýrství a porovnávání dekompileovaných souborů, analýza stávajícího a návrh, implementace a testování nového nástroje k tomuto účelu určenému. Text práce je psán velice čtivým a kvalitním slohem a srozumitelně vysvětluje čtenáři vše potřebné.
- 5. Formální úprava technické zprávy** **94 b. (A)**
Práce je napsána kvalitní češtinou. Z typografického hlediska je práce velice úhledná.
- 6. Práce s literaturou** **90 b. (A)**
V rámci práce bylo prostudováno více než 30 studijních pramenů, většinou odborných publikací z oblasti dekompileace a referenčních příruček k použitým softwarovým nástrojům a knihovnám. Všechny převzaté prvky jsou řádně označeny s uvedením odkazu na jejich zdroj. Bibliografické citace jsou úplné a v souladu s citačními zvyklostmi.
- 7. Realizační výstup** **98 b. (A)**
Předloženým softwarovým výstupem je konzolová aplikace porovnávající podobnost dvou souborů napsaných v jazyce C. Aplikace je plně funkční, škálovatelná, rozšiřitelná a v současnosti je nasazena v ostrém provozu ve společnosti *AVG Technologies s.r.o.*, kde nahradila původní nástroj. Součástí aplikace je také úplná uživatelská a programová dokumentace. Zdrojové kódy aplikace jsou napsány s vysokou pečlivostí a svědčí o pokročilých programátorských dovednostech autora. Oproti původní verzi je tato aplikace značně rychlejší, byla řádně otestována mnoha sadami testů, jak jednotkových, tak i regresních a jako bonus dokáže i detekovat podobnost dvou malware souborů, z nichž jeden je produktem metamorfózy toho druhého.
- 8. Využitelnost výsledků**
Vytvořený nástroj je oproti původnímu nástroji pro porovnávání zdrojových souborů značně vylepšen a v současnosti je nasazen v ostrém provozu ve společnosti *AVG Technologies s.r.o.*, kde se používá při testování a vývoji zpětného překladače *Retargetable Decompiler*.
- 9. Otázky k obhajobě**
-
- 10. Souhrnné hodnocení** **96 b. výborně (A)**
Vzhledem k obtížnosti zadání dané především nutností se zorientovat v problematice přesahující rámec bakalářského studia a vzhledem k preciznosti s jakou byla tato práce provedena, navrhuji hodnocení **A (výborně)**.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 1. června 2016

.....
podpis

