Posudek oponenta diplomové práce

Práce: Forensic RAM dump image analyser
Autor: Ivor Kollár
Oponent: Vlastimil Babka
Rok: 2010

Předložená diplomová práce se zabývá návrhem a implementací nástroje Foriana pro usnadnění forenzní analýzy obrazu fyzické paměti počítače. Tento nástroj by měl podporovat několik architektur a operačních systémů, extrakci hesel a kryptografických klíčů, výpis procesů a modulů či driverů.

Největším přínosem práce je zřejmě návrh a implementace algoritmu "Longest-Nearest", kterým lze nalézt některé datové struktury kernelu jako je seznam procesů či modulů, a jehož funkčnost byla ověřena kromě Linuxu i na systémech Windows a BSD. Uspokojivá je i podpora více architektur (x86, x86_64 a ARM) s heuristikami pro detekci stránkovacích tabulek a možností rozšíření o další architektury.

Slabší částí práce je zejména extrakce kryptografických klíčů a hesel. Autor dochází k závěru, že existující nástroje pro kryptografické klíče jsou dostatečné, použitá implementace je tedy převzatá. Pro extrakci hesel je implementován jen velmi základní skript. Výhodou nástroje Foriana je přitom možnost získat souvislý obraz paměti jednotlivého procesu a tím omezit počet false positives a zabránit fragmentaci hledané informace. Je tedy škoda, že tato možnost nebyla ani lépe uživatelsky integrována, ani experimentálně zhodnocen její přínos.

Práce samotná je psána v anglickém jazyce poněkud kostrbaté, ale dostačující úrovně. Struktura práce je vyhovující, plynulost a logická návaznost textu je však slabší. Často si čtenář některé souvislosti musí domýšlet nebo už sám dobře problematiku znát, neboť jsou nastíněny jen částečně (například v sekcích nazvaných "Problem definition"). Popis struktury implementace je poněkud nekonzistentní (detailní popis abstrakce architektury oproti velmi nejasnému popisu abstrakce operačního systému).

Priložený nástroj Foriana o rozsahu zhruba 4200 SLOC trpí nedostatky jak ve struktuře tak ve kvalitě zdrojového kódu. Snaha abstrahovat implementační detaily architektur a operačních systémů je na půli cesty. Implementace jsou sice v oddělených modulech, velmi matoucí je ale výskyt konstant a funkcí souvisejících s operačním systémem v includech pro architektury. V kódu se často vyskytují velmi dlouhé funkce s až čtyřmi úrovněmi vnoření a nepojmenované číselné konstanty.

Závěrem lze říci, že práce splňuje zadání, ovšem s dílčími nedostatky jak v textu tak zejména v kvalitě implementace. Práci doporučuji k obhajobě.

V Praze, 31. srpna 2010

Vlastimil Babka