Posudek diplomové práce

Forensic RAM dump image analyser

Autor: Ivor Kollár
Vedoucí práce: RNDr. Viliam Holub, PhD
Rok: 2010

Diplomová práce se zabývá analyzováním snímku paměti počítače. Výsledná implementace Foriana extrahuje z obrazu paměti v souboru mimo jiné seznam procesů, modulů a oteřených souborů, rekonstrukci lineárního adresového prostoru systému a detekci šifrovacích klíčů.

Práce začíná motivací a pokračuje příliš stručným úvodem do problematiky a popisem současných dostupných nástrojů spolu s jejich hlavním zaměřením. Kapitola 3 rozebírá detekci a obranu detekce šifrovacích klíčů v datech. Je zmiňována myšlenka ukrytí klíčů v cache procesoru, ale více je popisována samotná detekce. Pro vyhledávání se autor rozhodl použít již hotové klihovny a nástroje a tedy nejsou jako takové novým přínosem. Kapitola končí rozebíráním pravděpodobností chyb v RAM při vypnutí obnovování a seznamem vzorů pro vyhledávání bezpečnostních prvků jako např. hesel a klíčů.

Kapitola 4 představuje jádro práce – pravděpodobnostní rozlišování struktur. Mimo jiné popisuje algoritmus The Longest-Nearest, který má ambice prohledávat předem neznámé (určitými pravidly omezené) datové struktury.

Kapitola 5 pak popisuje implementaci nástroje Foriana využívající výše popsané techniky. Jsou popsány jednotlivé kroky programu, počínajíc úvodní identifikací systému, nalezení tabulky virtuálních stránek, interpretací tabulek, přeložení do lineárního prostoru, nalezení procesů a dalších struktur a to pro různé operační systémy. Dále následuje popis uživatelského rozhraní.

Kapitola 8 práci uzavírá shodnocením výstupů programu pro různé ukázkové systémy.

Od poslední neúspěšné obhajoby autor úspěšně implementoval některé námitky oponentů, bohužel ale nikoli všechny. Nutno podotkout, že jsem doporučoval práci v současné podobě ještě neodevzdávat a lépe zpracovat minimálně analytickou srovnávací část. Text práce působí velice stroze, což lze částečně dát za vinu použití anglického jazyka, který je samozřejmně težší používat než jazyk rodný. Struktura práce měla být lépe rozdělena na část analytickou a část faktického vývoje a přínosu. Zdrojové kódy implementace Foriana jsou dobře okomentované a přehledné. Práce vyžadovala dobrou znalost architektur IA32, AMD64 a ARM a vnitřní struktury jádra operačních systémů. Diplomovou práci doporučuji k obhajobě.

1.9.2010
Viliam Holub