Posudek oponenta diplomové práce

Práce: Forensic RAM dump image analyser
Autor: Ivor Kollár
Oponent: Martin Děcký

Předložená diplomová práce pana Kollára se zabývá analýzou obrazu fyzické paměti počítače. V úvodu autor stručně uvádí motivaci takové analýzy, následně představuje některé existující nástroje a postupy pro získání a analýzu obrazu fyzické paměti a ve zbytku textu popisuje vlastní nástroj Foriana, který umožňuje získat některé zajímavé informace z obrazu fyzické paměti.

Přes velmi zajímavé téma je práce pro čtenáře jistým zklamáním. Autor v textu nakousne mnoho zajímavých otázek, bohužel se málokteré věnuje detailněji než na úrovni letmého popisu. Například problematika získání obrazu paměti pomocí rozhraní FireWire by si jistě zasloužila podrobnější rozbor, kde by autor podal konkrétní zkušenosti a doporučení pro použití této metody (volba isochronního nebo neisochronního, quad nebo blokového přenosu, optimální velikost přenášeného bloku apod.). Vyžadovat po autorovi vlastní zkušenost s „cold boot" metodou by bylo zřejmě nad rámec požadavků diplomové práce, nicméně fakt, že autora nenapadla možnost čtení alespoň části fyzické paměti metodou „hot boot" (kdy firmware většiny počítačů může velkou část fyzické paměti netknutou), nebo že u metody čtení /dev/mem v Linuxu neuvádí možnost přístupu k libovolné fyzické stránce pomocí operace mmap(), je poněkud zarážející.

Ke kladům práce patří především algoritmus „The Longest-Nearest", který je v nástroji Foriana použit k elegantnímu nalezení některých datových struktur Linuxu, a také heuristika pro nalezení stránkovací tabulky na platformě x86. Bohužel nástroji Foriana chybí v anotaci slibované vlastnosti jako podpora více cílových architektur a operačních systémů (mimo Linux/x86) a hledání kryptografických klíčů. Z dalších zajímavých (ale opomenutých) vlastností, které by nebyly příliš složité na implementaci, lze namátkou uvést heuristiku pro detekci bloků strojového kódu v datových stránkách (indikace útoků metodou buffer/stack overflow), pokus o nalezení zásobníkových rámců (resp. trap rámců) běžících vláken, případně využití debuggovacích informací ve stylu CTF (Compact C Type Format), které mohou být v některých systémech v paměti obsaženy.

Přiložený nástroj Foriana je funkční, ovšem kvalita jeho zdrojového kódu (rozsah přibližně 1300 LOC) je velmi diskutabilní. Kód je sice rozumně komentován, ale je poměrně neupravený a není příliš dobře členěn na logické části, které by usnadnily jeho rozšiřování například pro analýzu obrazů jiných operačních systémů než je Linux. Celkově působí dojmem rozdělané a nedokončené práce.

Po formální, jazykové a typografické stránce lze práci vytknout jen drobné nedostatky (které lze jistě po pozorném pročtení snadno opravit). Například hned v kapitole 1.2 se dozvídáme, k čemu je Foriana navržena, aniž bychom v nějaké úvodní větě zjistili, co to vlastně je (to si čtenář po krátkém zmatení musí odvodit z kontextu).

Závěrem lze říci, že text práce i přiložený software jdou správnou cestou, ale rozsahem a propracovaností odpovídají spíše bakalářské práci. Bylo by vhodné, aby autor obojí výrazně rozšířil. V současné podobě práci nedoporučuji k obhajobě.

V Praze, 31. srpna 2009.