Posudek na diplomovou práci

Metody sledování chování procesů na Windows

David Matoušek

Cílem práce bylo prozkoumat možnosti jednotlivých metod dynamické analýzy neznámých programů a navrhnout systém pro sledování procesů pomocí virtualizace. Nedílnou součástí bylo i vypracování pilotní implementace navrženého systému včetně ukázek na modelové situaci.

Kapitola dva stručně popisuje fungování systému a procesů vzhledem ke zvolené tématice dynamické analýzy procesů.

Kapitola tři představuje metody používané ve sledovacích systémech bez použití vizualizace. Zde bych rád ozřejmil, že používání poněkud netradičního českého termínu „hákování" jako náhrada za anglický běžně používaný termín „hooking" bylo zvoleno po několikanásobné konzultaci s vedoucím diplomové práce vzhledem k tomu, že žádný jiný rozumný český termín neexistuje.

V kapitole čtyři se pak autor věnuje metodám používaných ve sledovacích systémech s použitím virtualizace. I v této kapitole, stejně jako v předchozí, autor prokazuje značné znalosti v dané oblasti.

Pátá kapitola se pak věnuje srovnání a popisu výhod a nevýhod několika volně dostupných sledovacích systémů.

Šestá a sedmá kapitola tvoří jádro diplomové práce. V šesté kapitole je popsán výběr virtualizačního software a provedené úpravy na něm tak, aby vyhovoval zvolenému systému sledování procesů. Sedmá kapitola pak popisuje samotný návrh a implementaci systému pro sledování procesů nazývaný PABOV. V textu záměrně nejsou popsány podrobnosti o pokročilých implementačních technikách (např. hákování jádra) vzhledem k tomu, že by se zbytečně zacházelo v samotném textu do konkrétních podrobností okolo jedné technické záležitosti, navíc si lze příslušné techniky dohledat v přiloženém zdrojovém kódu. Zde moje nejvážnější připomínka spíše směřuje k tomu, že vzhledem k návrhu a realizaci je program vázán na jeden konkrétní operační systém včetně jeho update/service packu. V případě použití na jiné verzi OS bude zapotřebí spustit přiložený nástroj a připravit soubor, nicméně nejsem si jistý, že to dokáže i někdo jiný než autor a ani si nejsem jistý, že to bude pracovat na všech OS. Další výtkou budiž práce pouze s 32-bitovými OS, v dnešní době bych očekával i nějaké řešení pro 64-bitové OS. Poslední výtka se pak týká výstupních filtrů, které jsou v současnosti spíše v demonstračním režimu a zdaleka nepředstavují všechny možnosti systému. Tuto řadu mých výtek je však nutné vzít v kontextu toho, že se jedná o pilotní implementaci, nikoliv dokonalé komerční řešení, kde by tyto výtky byly jistě závažné.

Osmá kapitola pak srovnává vybrané sledovací systémy a implementovaný systém na několika známých vzorcích malware. Ukazuje se, že zvolený systém sledování je celkem dost úspěšný v porovnání s ostatními systémy.

Textová část práce prošla řadou úprav a konečná podoba již plně vyhovuje standardům kladeným na diplomové práce na MFF UK.

Práce celkově splnila svůj cíl, ukázala možnosti sledování procesů pomocí virtualizace včetně pilotní implementace sledovacího nástroje.

Doporučuji proto tuto diplomovou práci k obhajobě.

25.1.2010

RNDr. Jakub Yaghob, Ph.D.
KSI, MFF UK