Posudek oponenta závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Bc. Tomáš Hradský
Oponent práce: Ing. Josef Kokeš
Název práce: Skrývání virtuálního prostředí před malwarem
Obor: Počítačová bezpečnost

Datum vytvoření: 25. 5. 2017

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	***1=mimořádně náročné zadání,*** *2=náročnější zadání, 3=průměrně náročné zadání, 4=lehčí, ale ještě dostatečně náročné zadání, 5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Práce se zabývá možnostmi, jak pozměnit chování virtualizačního SW tak, aby tento nebyl snadno detekovatelný "zevnitř". To je velmi obtížné, protože je nutné řešit velkou škálu ukazatelů na různých úrovních, od chování virtuálního i fyzického hardwaru přes hypervisor až k virtuálnímu operačnímu systému.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami, 3=zadání splněno s většími výhradami, 4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Zadání bylo splněno.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	***1=splňuje požadavky,*** *2=splňuje požadavky s menšími výhradami, 3=splňuje požadavky s většími výhradami, 4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Rozsah písemné zprávy je nadprůměrný, ale přiměřený popisované problematice.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*95 (A)*

Popis kritéria:
Posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře.

Komentář:
Věcná i logická stránka práce je výborná. Oceňuji zejména kapitolu 3, která se zabývá podporou CPU pro virtualizaci v podobě, která stručná, srozumitelná a přitom přesná. Dále velmi vítám to, že se student zabýval i ne zcela zřejmými otázkami, jako jestli skrývání hypervisoru není vlastně na škodu. Nedostatky se najdou, nejde ale o nic fatálního: Použitý RNG nijak neřeší přístup z více vláken najednou. Chybí náznak, jak zhruba by probíhala identifikace původce instrukce CPUID, aby tato nemohla posloužit k detekci hypervisoru. Není řešeno, ani na úrovni diskuse, detekování hypervisoru podle komplexních projevů namísto jednotlivých znaků, např. podle textů uvnitř oken nebo podle seznamu funkcí importovaných do procesů. Místy čtenář narazí na nesoulad mezi popisem v textu práce a v reálné implementaci (např. modul u RNG, nekonečná smyčka v textové verzi funkce 6.2); reálná implementace je ve všech mnou zkoumaných případech správně.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*80 (B)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.

Komentář:
Ve formální stránce práce bohužel narážíme na nedostatky. V obsahu se objevil i odkaz na "odkaz na tuto práci". Klíčová slova až na konci stránky s abstraktem nepůsobí dobře. Autor konzistentně používá spojovníky místo pomlček. V několika případech jsem narazil na jednopísmennou spojku na konci řádku.

Jazyková stránka je daleko nejslabší částí práce. Jde zejména o chybějící čárky kolem vedlejších vět (velmi častý problém) a mnohdy hovorové či slangové výrazy ("chycení malwaru", "spousty", "pár", "kilometry daleko" atd,), které do odborného textu nepatří. Anglický název práce je špatně ("malware" nemá tvar množného čísla "malwares").

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*90 (A)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Množství i relevance zdrojů je v pořádku, jejich zápis je však netradiční. Až na výjimky není uveden autor, vesměs proto, že není znám; bylo by vhodné hledat zdroje s autory. Seznam literatury by měl být pokud možno řazen jinak než podle umístění v textu.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*95 (A)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Výsledky studentem dosažené jsou velmi dobré, výrazně překonávají moje očekávání, čeho bude možné dosáhnout. Podařilo se zamaskovat značné množství zdrojů, které mohou posloužit k identifikaci virtuálního stroje. Určitým problémem je, že není dobře oddělen kód studenta od kódu Virtual Boxu a od soukromých úprav, které si do Virtual Boxu zavedla firma Avast, takže je poměrně obtížné převzít vytvořený program a aplikovat ho na novější verzi Virtual Boxu. Zároveň je otázka, jestli kvůli tomu nedochází k prozrazení firemního know-how.

V částech programu, které jsem zkoumal, jsem narazil na už výše zmíněný nesoulad mezi textem a kódem. Hodně mi vadí, že si student Počítačové bezpečnosti píše vlastní verze knihovních funkcí (!), zvlášť když jde o inherentně nebezpečné strcpy, strcat apod.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Zkoumaná problematika není zcela nová a neznámá, ale dosažené výsledky jsou velice dobré. Jejich praktické uplatnění se očekává pouze ve velmi specializovaných případech (analýza malware), ale tam jsou extrémně užitečné, protože zabrání malwaru v tom, aby detekoval virtuální prostředí a na základě toho zastavil ty svoje části, které by vedly k jeho automatické detekci.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
1) Je skutečně potřeba, aby se data randomizovala po každém restartu? I změna jména programu po resetu by mohla být detekována! Zvažoval jste možnost, že by identifikační konstanty byly specifické pro konkrétní instalaci hypervisoru (tzn. určovaly by se ne při kompilaci, ale např. v rámci instalace hypervisoru/hosta)?

2) Máte nějaký námět, jak reálně řešit možnost zneužití komunikačního kanálu s hypervisorem?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*95 (A)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Student si pro svoji práci zvolil originální, vysoce specializovanou a značně náročnou oblast. Provedl velice pěknou analýzu možností, které má malware pro detekci hypervisoru, a přinesl náměty, jak tyto možnosti blokovat. Řadu z nich také úspěšně implementoval, a to v neobvykle vysokém rozsahu i kvalitě. Výsledkem je program, který sice není pro každého, ale tomu, kdo jej potřebuje, je velice užitečný. Ze všech těchto důvodů navrhuji hodnotit práci známkou A - výborně.

Podpis oponenta práce: