FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Luigino Camastra
Vedoucí: práce:	Ing. Josef Kokeš
Název práce:	Reverzní analýza UEFI modulů PEI a DXE
Obor:	Počítačová bezpečnost

Datum vytvoření: 27. 5. 2020

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. 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 dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Komentář:

Poměrně náročné zadání, spočívající v analýze startovacího kódu počítače pomocí reverzního inženýrství, student splnil v požadovaném rozsahu a hloubce detailů.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*65 (D)*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále 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. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Komentář:

Písemná část je tím nejslabším článkem celé práce. Rozsahem i obsahem je v pořádku, vykazuje však značné jazykové chyby - v práci stále zůstává mnoho překlepů, velkým nešvarem je nesprávný slovosled překladů původních anglických termínů ("počítačovej firmware architektúry", "zariadenia boot pre-OS" a řada dalších) a časté opakování slov. Zejména v kapitole 5 se pak některé stránky doslova topí ve zkratkách. V důsledku toho je text poměrně obtížně čitelný. Mrzí mě kapitola 7, ve které měl student vyhodnotit výsledky své analýzy; kapitola je bohužel velice krátká a ačkoliv student odvedl velké množství práce na provedené analýze, nedokázal tuto práci "prodat".

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*85 (B)*

Popis kritéria:
Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce
– opakovatelnost experimentů

Komentář:

Student prozkoumal značnou část UEFI firmwaru prostřednictvím reverzní analýzy. Komentovaný (částečně) disassembler PEI a DXE modulů je přiložen k práci. To je nepochybně vhodné řešení, protože jde o čistý text přístupný každému čtenáři. Uvítal bych však, kdyby byly přiloženy i zdrojové IDB soubory pro IDA Pro, které by umožnily pohodlnější prostudování výsledků práce uživatelům, kteří licenci k IDA Pro mají. Moje chyba, že jsem si toho nevšiml před odevzdáním. Přiložená disassembly je také poměrně obtížně čitelná sama o sobě, potřebuje textový doprovod. Komentáře mohly být podrobnější.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*85 (B)*

Popis kritéria:
Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Komentář:

Podle mého názoru práce poskytuje poměrně značný přínos pro ty, kdo se zajímají o průběh startu systému. Popisuje klíčové části bootovacího procesu před tím, než je řízení předáno operačnímu systému, a umožňuje tak čtenáři porozumět tomu, jak start počítače funguje. To je důležité např. pro vývojáře anti-malwarových nástrojů, kteří musí počítat s nástupem EFI-bootovacího malwaru a už s předstihem řešit, jak ho detekovat a zabránit mu v činnosti.

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: *1=výborná aktivita,* ***2=velmi dobrá aktivita,*** *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 5b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Student byl nadprůměrně aktivní, i když v době po začátku koronavirové krize v četnosti konzultací poněkud polevil. Pracoval však samostatně a kdykoliv jsem na něj měl nějaké požadavky, byl schopen je rychle a kvalitně řešit.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*85 (B)*

Popis kritéria:
Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

Text hodnocení:

Předložená diplomová práce řeší značně náročnou problematiku reverzní analýzy startovacího kódu počítače v UEFI firmwaru. Student prozkoumal dva klíčové moduly celého procesu, PEI a DXE, popsal jejich činnost a srovnal ji s oficiální dokumentací. Získal také značné porozumění bootovacímu procesu a věřím, že tyto zkušenosti dokáže uplatnit v praxi. Jazykově problematická textová stránka práce a nadmíru stručná prezentace výsledků mi však brání hodnotit práci jako výbornou, přestože z hlediska množství a kvality odvedené analytické práce jí není mnoho co vytknout - studentovi se však tuto práci nepodařilo plně "prodat".

Podpis vedoucího práce: