FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Josef Kokeš, Ph.D.
Student:	Filip Touš
Název práce:	Analýza programového kódu v realném čase
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	8. června 2024

Hodnotící kritéria

1. Splnění zadání

▸ [1] **zadání splněno**
[2] zadání splněno s menšími výhradami
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

Zadání je poměrně komplikované, i řada studentů magisterského oboru by s ním měla potíže.

2. Písemná část práce 95 / 100 (A)

Text práce je výborný. Zarazila mě poněkud neobvyklá struktura na začátku, ale předává potřebnou informaci v potřebné míře. Váhám nad tím, zda bylo nezbytné mít tak rozsáhlou kapitolu 3 s implementačními detaily, ta by se možná více hodila do přílohy a mohla tak uvolnit prostor detailnějšímu teoretickému rozboru, faktem však je, že stávající popis teorie i praxe je dostačující - aspoň pro člověka, který popisované koncepty zná. Velmi vítám kapitolu 5, ve které student ukazuje použití aplikace na několika příkladech, včetně rozboru, které postupy v nich fungovaly a které nikoliv. Příklady jsou vhodně voleny tak, že dávají uživateli dobrý výchozí bod pro použití programu i na jiné aplikace.

Nejsem stoprocentně přesvědčen o tom, že zvolená cesta poolu spustitelných náhrad funkcí je ideální, uvítal bych minimálně diskusi použití jedné společné obsluhy volané instrukcí CALL (z návratové adresy pak zjistíme adresu nalezené funkce; vede to na sice pomalejší ale zato jednodušší kód s jedinou obslužnou funkcí a zbavuje nás to nutnosti používat ne zrovna ideální nastavení PAGE_EXECUTE_READWRITE pro ochranu paměti).

3. Nepísemná část, přílohy 95 / 100 (A)

Nepísemnou část práce tvoří studentem vytvořený program, který dovoluje rychle nalézt funkci v rozsáhlejším programu. Program je vhodně členěn do zdrojových i binárních

souborů, je čistě napsaný a plní svoji funkci. Byl jsem poněkud skeptický k tomu, zda zvolená metoda skutečně může fungovat, výsledky ale ukazují, že může. Jedinou skutečnou výhradu k programu mám k tomu, že aplikace vyžaduje oprávnění SE_DEBUG_NAME, pro které nemá žádný důvod (toto oprávnění je potřeba pouze pro práci s procesy jiných uživatelů).

Součástí přílohy podle mě mohly být demonstrační soubory pro odzkoušení aplikace, zejména soubor se seznamem funkcí. Jistě by šlo vzít nějaký freeware (například Notepad++), udělat na něm obdobné experimenty, jako jsou popisované v kapitole 5, a následně přiložit vše, co je potřeba pro jejich zopakování. Ideálem by pak byl pomocný program pro konverzi .pdb, .map nebo .dbg souborů do formátu, který vytvořená aplikace používá. Nemusí mít nutně každý nástroj IDA (i když vytvořený skript lze použít i ve Free verzi).

Není přiložen zdrojový kód bakalářské práce samotné.

4. Hodnocení výsledků, jejich využitelnost 100 /100 (A)

Výsledkem práce je program, který umožňuje výrazně usnadnit reverzní inženýrství aplikací tím, že dokáže rychle najít klíčovou část programu, ve které se provádí uživatelem požadovaná činnost. Jde o dosti specifické použití, ale pro toto použití jde o výborný nástroj, který analytikovi velmi pomůže.

Celkové hodnocení 98 /100 (A)

Odevzdaná bakalářská práce je na velmi vysoké úrovni, jak po stránce textu, tak po stránce vytvořené aplikace. Jsou v ní části, které by bylo možné zlepšit, ale jde vesměs jen o drobnosti, které nijak výrazně nezmenšují kvalitu celku a jsou více než kompenzovány tím, že jde o zadání, které by klidně mohlo být použito i pro práci diplomovou. Práci doporučuji k obhajobě a hodnotím známkou A.

Otázky k obhajobě

1) Zvažoval jste možnost unifikované obsluhy jedinou funkcí, která je naznačena v hodnocení textové části?

2) Jaký je přínos podmínky if (strstr(prefix, "sub_") != -1) ve skriptu pro IDA Free? Zahazuje všechny pojmenované funkce, což i komentujete na konci sekce 2.4. - ale k čemu je to dobré?

Instrukce

Splnění zadání

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.

Písemná část práce

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. 52/2021, 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.

Nepísemná část, přílohy

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.

Hodnocení výsledků, jejich využitelnost

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.

Celkové hodnocení

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.