FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš, Ph.D.
Student:	Adam Škoda
Název práce:	Útok Shatter a technologie User Interface Privilege Isolation
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	26. května 2024

Hodnotící kritéria

1. Splnění zadání

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

Student plně vyřešil všechny body zmíněné v zadání, a to výrazně důkladněji, než samo zadání očekávalo.

2. Písemná část práce 99 / 100 (A)

Textová část práce je vynikající. Student napřed popsal základní koncepty práce se zprávami v operačním systému Windows, na to navázal detailním popisem útoku Shatter včetně jeho návazností a následně popsal a analyzoval řešení, která Microsoft v reakci na tento útok implementoval. Tuto část velice oceňuji, protože jde o oblast, která nebyla jinde dostatečně popsána a když už, tak ne ve své komplexnosti. V této práci dostane čtenář kompletní přehled, i včetně návodu, jak svou aplikaci upravit tak, aby mohla dostupných obran využít. Obdobně uživatel dostane doporučení, jak posílit ochranu svého systému i navzdory tomu, že vývojář aplikace třeba obranné kroky nepodstoupil, protože o nich nevěděl.

Po jazykové a technické stránce nemám výhrady. Narazil jsem na zcela minimální počet překlepů, což u práce takového rozsahu považuji za výborné.

Velmi oceňuji slovníček klíčových pojmů před začátkem samotného textu.

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

Nepísemnou část práce tvoří zejména zdrojové kódy a výsledky experimentů studenta a dále různé pomocné programy, které mohou být velmi užitečné i pro uživatele (nastavení

integrity levelu pro soubor nebo spuštění nového procesu se zadaným integrity levelem). Kód programů je velmi pěkně napsaný a dobře doprovází napsaný text.

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

Práce přináší detailní rozbor důležité, ale dosud velmi špatně zdokumentované bezpečnostní funkcionality operačních systémů Windows. Na jednom místě tak vývojář dostane všechny informace, které potřebuje k tomu, aby mohl tyto funkcionality využít a lépe tak zabezpečit svoji aplikaci proti některým běžným typům útoků. I pokročilý uživatel-neprogramátor může mít z práce prospěch díky tomu, že mu tato poskytuje vysvětlení a nástroje pro to, aby mohl sám souborům a procesům nastavit odlišné úrovně integrity a tak navýšit bezpečnost svého systému i v případech, kdy sám vývojář obranné techniky neimplementoval.

5. Aktivita studenta

- [1] **výborná aktivita**
- [2] velmi dobrá aktivita
- [3] průměrná aktivita
- [4] slabší, ale ještě dostatečná aktivita
- [5] nedostatečná aktivita

6. Samostatnost studenta

- [1] **výborná samostatnost**
- [2] velmi dobrá samostatnost
- [3] průměrná samostatnost
- [4] slabší, ale ještě dostatečná samostatnost
- [5] nedostatečná samostatnost

Celkové hodnocení 99 /100 (A)

Techniky Mandatory Integrity Control a User Interface Privilege Isolation mají sloužit jako bezpečnostní prvek pro ochranu GUI aplikací ve Windows v jejich vzájemné interakci, bohužel jsou však velmi špatně dokumentovány a v důsledku jen minimálně využívány vývojáři. Předložená bakalářská práce toto umožňuje změnit, protože na jednom místě předkládá jak důkladný popis toho, k čemu vlastně tyto techniky slouží, tak dokumentaci postupů, jak je využít, a také analýzu toho, pro které situace fungují a pro které ne. Velkým přínosem jsou také vytvořené programy, které lze využít nejen jako demonstraci využití popisovaných technik, ale také z uživatelské strany jako nástroje pro zlepšení bezpečnosti systému navzdory tomu, že vývojář aplikace třeba sám popsané techniky nepoužil. Podle mě jde o vynikající dílo a s radostí hodnotím známkou A (výborně).

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.

Aktivita studenta

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.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

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.