



Posudek oponenta závěrečné práce

Oponent práce: Ing. Ivana Trummová
Student: Matěj Douša
Název práce: Kritéria pro hodnocení bezpečnosti kryptografických knihoven
Obor / specializace: Informační bezpečnost 2021
Vytvořeno dne: 9. 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

Cílem práce bylo na základě nastudování problematiky bezpečnosti softwaru a navržení metodiky, jak pro obecnou knihovnu nalézt a vyhodnotit typické chyby určit hlavní kritéria, která ovlivňují bezpečnost knihovny a jejího použití. Tyto cíle byly autorem splněny a v práci byly popsány.

2. Písemná část práce

85 /100 (B)

Práce se dobře četla - je napsaná jazykem, který je přesný, a je dobře členěná, neobsahuje části, které by podle mě byly zbytečné. Hned ze začátku (sekce 1.1.1, 1.1.2, 1.1.3), a v kapitole 2 je popis zásad, respektive hrozeb relativně stručný, a myslím si, že např. výčet hrozeb by mohl být i košatější.

Pro vysvětlení open-source a closed-source softwaru možná nebyla potřeba celá kapitola, ale popis je dostatečný a zařazení těchto sekcí bylo nezbytné.

Zbytek práce je přehledný, obsahově mi tam nic nechybí a oceňuji, že je popsáno, kde končí rešerše a ve které části začíná praktická aplikace kritérií na knihovny. Na konci nechybí diskuze výsledků (i když bych, při jejich rozsahu, čekala diskuzi také rozsáhlejší), kde autor výsledky zasazuje do kontextu a shrnuje svoje závěry z práce.

3. Nepísemná část, přílohy

0 /100 (F)

Práce přílohy neobsahuje, hodnocení je tedy irelevantní.

4. Hodnocení výsledků, jejich využitelnost

90 /100 (A)

Jak autor sám uvádí, bakalářská práce vznikala v rámci projektu s NÚKIB, její praktické využití tedy vyplývá z poptávky zadavatelů projektu. Student v práci jasně popisuje, jakým způsobem k výsledkům přišel a uvádí, jak mohou být využity. Jediný nedostatek, který autor sám uvádí ve shrnutí, je způsob dohledávání chyb přes CVE - metoda nepřinesla očekávané výsledky a bylo by vhodné rozmyslet, jakým jiným způsobem chyby vyhodnotit.

Celkové hodnocení

90 /100 (A)

Práce na mě působí jako velmi vydařená, s jasně popsáním praktickým využitím a relativně dostatečně popsanou a nastudovanou teoretickou částí.

Otázky k obhajobě

Jak probíhala spolupráce v rámci vašeho projektu a čím se vaše práce odlišuje od vašich dvou kolegů se stejným tématem?

Instrukce

Splnění zadání

Posudte, 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, posudte 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 posudte, 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. Posudte správnost používání formálních zápisů obsažených v práci. Posudte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posudte, 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.