FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš, Ph.D.
Student:	Kirill Leonov
Název práce:	Kritéria pro hodnocení bezpečnosti kryptografických knihoven
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	2. 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

2. Písemná část práce 75 / 100 (C)

Text práce zahajuje student stručným úvodem do problematiky bezpečnosti softwaru, z nějž následně přechází do stručného návrhu, jak hodnotit bezpečnost kryptografických knihoven snáze než plnokrevnou bezpečnostní analýzou, a následně uplatňuje tyto poznatky v nejrozsáhlejší kapitole při analýze knihoven libsodium, Botan a OpenSSL. Tato kapitola je také hlavním přínosem práce.

Z pohledu faktické správnosti nemám výhrady, tam je práce v pořádku. Váhám poněkud nad úvodními kapitolami, které se zdají dosti stručné, první kapitola navíc možná ani není zcela nezbytná pro srozumitelnost zbytku textu; zde by se určité rozšíření textu uplatnilo. I hlavní kapitola by snesla o něco vyšší úroveň podrobnosti, v některých částech se zastavuje o něco dříve, než by bylo ideální (např. v kapitole 3.3.2.7 se bod 4 zdá být poněkud unáhlený). Formální stránka je z větší části v pořádku, z jazykové stránky je znát, že čeština není studentovým rodným jazykem, ale i tak text vykazuje méně chyb, než je obvyklé.

3. Nepísemná část, přílohy 0 / 100 (F)

Nelze hodnotit, práce žádné relevantní přílohy neobsahuje (a nepotřebuje).

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Cílem práce bylo nalézt kritéria pro rychlé a jednoduché rozhodnutí o tom, zda vývojář může do svého projektu použít zvolenou kryptografickou knihovnu a nebo raději hledat jinde. Student se zaměřil na problematiku organizačních aspektů vývoje knihovny, dále na prověření její dokumentace a API, a následně na analýzu chyb v aplikacích, které už knihovnu používají. Všechna tato kritéria se jeví jako použitelná a jejich uplatnění na existujících knihovnách dává výsledky, které vypadají důvěryhodně. Je tedy pravděpodobné, že by se daly uplatnit i na dalších podobných případech.

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 85 /100 (B)

V rámci své bakalářské práce student analyzoval aspekty, pomocí kterých může vývojář rychle vyhodnotit bezpečnost kryptografické knihovny. Svá zjištění následně prakticky ověřil ohodnocením tří známých, spíše nízkoúrovňových kryptografických knihoven (libsodium, Botan, OpenSSL). Jeho výsledky se zdají být důvěryhodné a uplatnitelné i na další knihovny. Určitý nedostatek spatřuji v stručnějším textu, než by bylo ideální, a poněkud chudší úvodní části textu. Přesto však práci doporučuji k obhajobě za hodnotím známkou B - velmi dobře.

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.