FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jiří Smítka
Student:	Kirill Leonov
Název práce:	Kritéria pro hodnocení bezpečnosti kryptografických knihoven
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	11. 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

Splněno bez výhrad.

2. Písemná část práce 85 /100 (B)

Práce je po formální stránce v pořádku. Autor se v českém jazyce dopouští drobných pravopisných chyb a nesprávných obratů, což prozrazuje, že čeština není jeho rodným jazykem. Věcné chyby se v práci nevyskytují. Domnívám se, že první kapitola by mohla být více zaměřená na témata, která budou relevantní při návrhu metodiky pro hodnocení knihoven.

3. Nepísemná část, přílohy 0 /100 (F)

Práce je svojí povahou pouze písemná - nemá žádnou praktickou část.

4. Hodnocení výsledků, jejich využitelnost 85 /100 (B)

Autor navrhl jednoduchou metodiku pro hodnocení, zda je (a do jaké míry) bezpečné využít testovanou knihovnu ve svém projektu. Navržená metodika je ve své podstatě celkem jednoduchá a snadno použitelná. Trochu se této jednoduchosti obávám, nevím, zda opravdu pokrývá všechna potenciální nebezpečenstva vyplývající z různých způsobů vývoje softwaru.

Celkové hodnocení

85 /100 (B)

Autor splnil zadání. Navržená metodika je v praxi určitě použitelná, minimálně jako prvotní orientační test.

Otázky k obhajobě

Tabulka 3.1: Jako pozitivum je hodnoceno, že libsodium nabízí nerozsáhlé low-level API s potenciálně nebezpečnými primitivy. Proč je to pozitivum a jak moc jsou nebezpečná potenciálně nebezpečná primitiva? Neměla by se v tomto smyslu upravit metodika?

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.