FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš, Ph.D.
Student:	Matěj Douša
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 85 /100 (B)

V písemné části student stručně popisuje východiska, ze kterých práce vychází, a potom rychle přechází k analýze toho, jaká kritéria by se dala použít pro odhad bezpečnosti kryptografické knihovny; tato kritéria následně uplatňuje na knihovny OpenSSL, mbedTLS, GnuTLS a WolfSSL. Tyto části jsou velmi dobře zpracovány, volba kritérií je podložená dřívějšími výzkumy a na zvolených knihovnách ukazuje výrazné rozdíly, tedy má potenciál mezi knihovnami dobře rozlišovat. Úvodní část je poněkud slabší v důsledku toho, že stěžejní část práce vznikla jako řešení rozsáhlejšího projektu a student pracoval spíše na těch analytičtějších částech; obsahuje informace, které by obsahovat měla, pro čtenáře budou ale méně srozumitelné, protože jsou až příliš stručné.

Po jazykové ani formální stránce nemám s prací problém, dobře se čte a nezaregistroval jsem žádné výraznější chyby.

3. Nepísemná část, přílohy 0 /100 (F)

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

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

Práce byla analytická, cílem bylo nalézt kritéria, která by umožnila vývojáři rychle a jednoduše odhadnout bezpečnost knihovny a rozhodnout se, zda knihovnu chce použít a

nebo zda raději použije nějakou jinou. Toto se podařilo, a to z několika pohledů - ze samotného procesu vývoje knihovny, zda je důvěryhodný a dává přijatelné záruky i do budoucnosti, z implementačních aspektů použití knihovny (kvalita API, srozumitelnost dokumentace) a také z toho, jaké chyby se vyskytovaly v aplikacích, které už knihovnu použily. Poslední bod se bohužel ukázal jako méně vhodný, než jsme doufali, zjištění i analýza potřebných zdrojů byla příliš náročná ve srovnání s dosaženým přínosem, ale jak organizační aspekty vývoje tak hodnocení použitelnosti vykazují dobré výsledky a domnívám se, že mohou být dobře použity i dalšími vývojáři, až se budou rozhodovat o tom, kterou kryptografickou knihovnu pro svoji aplikaci zvolí.

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 89 /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 čtyř známých, spíše nízkoúrovňových kryptografických knihoven (OpenSSL, mbedTLS, GnuTLS a WolfSSL). Jeho výsledky se zdají být důvěryhodné a uplatnitelné i na další knihovny. Jedinou skutečnou výhradu mám k poměrně stručné úvodní rešeršní části. 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.