FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš, Ph.D.
Student:	Milan Špinka
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 99 / 100 (A)

Písemnou část práce považuji za (téměř) perfektní. Začíná velmi pěkně napsaným úvodem, který i zcela neznalého čtenáře srozumitelně seznámí s řešeným problémem, a na to navazuje neméně dobře sepsanou a vyargumentovanou analýzou toho, co to vlastně bezpečnost software je, jaké specifické problémy vykazuje bezpečné použití kryptografie, návrhem metrik pro snadné a rychlé vyhodnocení bezpečnosti kryptografické knihovny, uplatněním těchto metrik na sadu knihoven pro různé jazyky (OpenSSL, libgcrypt, rustls, ring, cryptography.io, PyCryptodome) a závěrečným vyhodnocením a porovnáním knihoven. Vše je neustále velmi přehledné a srozumitelné, přitom však detailní a velmi důkladně podložené.

"Téměř" v prvním odstavci uvádím proto, že se student místy nedokázal vyhnout nevhodným výrazům jako "moct". Jedná se nicméně o jednotky případů a žádných jiných chyb jsem si nevšiml.

3. Nepísemná část, přílohy 80 / 100 (B)

Práce je analytického charakteru a žádné nepísemné přílohy vlastně nepotřebuje. Přesto čtenář několik velmi užitečných nepísemných výstupů dostane:

1) Aplikaci commitfetch pro analýzu a vizualizaci přispěvovatelů do kódu knihovny. Tato aplikace v této bakalářské práci nebyla využita, vznikla však jako součást projektu, jejž BP řeší, a je v něm také využita. I další řešitelé projektu pak aplikaci ve svých BP používají.

2) Ukázkové kódy pro řešení problému "autentizované zašifrování souboru pomocí hesla" ve všech analyzovaných knihovnách. Tyto mohou posloužit uživateli bakalářské práce pro představu, jak složité (nebo jak jednoduché) může použití knihovny očekávat. Nekladou si ambici být dokonalým řešením problému, ale pokud mohu soudit, zdají se být velmi dobře napsané a mohou tak v jistém smyslu posloužit i jako náhrada oficiální dokumentace (což je např. u OpenSSL nanejvýš vhodné).

3) Výstupy ChatGPT na požadavek, aby umělá inteligence vygenerovala kód pro autentizované zašifrování souboru heslem. Čtenář by je rozhodně neměl používat pro své implementace, protože mnohdy vykazují zásadní chyby - což bylo právě cílem ověřit, jestli se děje. K dokonalosti zde chybí komentář k jednotlivým vygenerovaným kódům, zda jsou správně nebo v čem spočívají jejich zranitelnosti. Toto je shrnuto v textu práce, detailní rozpis by však byl užitečným rozšířením.

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

Výsledky práce jsou podle mě nanejvýš užitečné pro každého vývojáře, který chce ve své aplikaci využít kryptografii a rozvažuje, kterou knihovnu pro tento účel použít. Pokud náhodou zvažuje zrovna knihovny, které byly analyzovány, dostává do rukou rovnou velmi solidní podklad pro rozhodnutí; pokud uvažuje jiné knihovny (např. pracuje v jiném programovacím jazyku), dostává velmi dobře vyargumentovaný seznam vodítek, na která by se měl podívat, rovnou i s ukázkami, jak je vyhodnocovat.

5. Aktivita studenta

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

Student byl po celou dobu vůdčím duchem řešení projektu, přicházel s novými nápady a tyto také aplikoval.

6. Samostatnost studenta

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

Celkové hodnocení 98 /100 (A)

Předloženou práci vnímám jako takřka dokonalou. Student provedl velmi důkladnou a detailní rešerši, kterou ve velmi přehledné podobě zpracoval pro čtenáře, navrhl mu postupy, jak hodnotit bezpečnost kryptografických knihoven, a tyto postupy následně ověřil na 6 různých knihovnách. Velmi vysoko hodnotím originální nápady na řešení, jako je manuální implementace jednoduchého "vysokoúrovňového" problému za účelem

analýzy, jak moc složité to v jednotlivých knihovnách bude, nebo využití ChatGPT pro totéž. Toto je jednoznačně práce, která stojí za zvážení na udělení ceny děkana. Doporučuji k obhajobě a 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.