FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jiří Buček, Ph.D.
Student:	Konstantin Filip Moisidis
Název práce:	Bezpečné cloudové úložiště pro správce hesel KeePass
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	6. června 2022

Hodnotící kritéria

1. Splnění zadání

[1] zadání splněno
▸ **[2] zadání splněno s menšími výhradami**
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

Zadání bylo splněno, ale řešení nebylo dotaženo do prakticky použitelné podoby. Může sloužit alespoň jako proof-of-concept.

2. Písemná část práce 65 / 100 (D)

Práce přináší zajímavý pokus o vylepšení software KeePass o ukládání databáze hesel na cloudovém úložišti se zabezpečením dvoufaktorovou autentizací.
V práci mi chybí důkladnější úvaha nad účelem a způsobem použití navrhovaného modulu. Ukládání databáze hesel do cloudu může být užitečné, ale i výběr technologií je potřeba přizpůsobit potřebám koncového uživatele.
Fáze návrhu v práci chybí, po analýze možností se student věnuje rovnou implementaci. Přehlednosti práce by prospělo také vhodné použití diagramů, ty se vyskytují ale až v kapitole o bezpečnostní analýze (a nejsou dostatečné pro návrh).
Kapitola bezpečnostní analýzy je stručná, ale obsahuje základní rozbor bezpečnostních aspektů vytvořené části aplikace.
Seznam literatury obsahuje chyby ve jménech a některé odkazy na online zdroje nefungují správně.

3. Nepísemná část, přílohy 60 / 100 (D)

Přiložené zdrojové kódy v jazyce C# jsou co do úrovně komentování poněkud nevyrovnané a jednotlivé soubory nemají uvedeno jméno autora. Některé volby parametrů jsou nepraktické, např. v GoogleAuth.cs se nachází napevno nastavené ID klienta a bezpečnostní token pro přístup k GoogleDrive.

4. Hodnocení výsledků, jejich využitelnost 50 /100 (E)

Výsledkem je spíše prvotní nástřel modulu do programu KeePass, v aktuální podobě není prakticky použitelný. Pro praktické použití by bylo potřeba se důkladněji znovu soustředit na jednotlivé části už od fáze návrhu, a také zpracovat rozumnou dokumentaci. Pro použití v programu, jako ke KeePass, je potřeba nejen aby byl program funkční, ale i aby byl důvěryhodný.

Celkové hodnocení 60 /100 (D)

Student se snažil naplnit ze zpětného pohledu možná příliš ambiciózní zadání kombinace cloudového ukládání databáze hesel a dvoufaktorové autentizace, a to včetně bezpečnostní analýzy. Podařilo se mu vytvořit prototyp řešení, který však nedosahuje úrovně potřebné pro praktickou použitelnost. Přes uvedené výhrady student splnil zadání a prokázal schopnost samostatné tvůrčí práce.

Otázky k obhajobě

Co znamená číslo 3 ve funkci Encrypt v TSS.cs: byte[] aesKey = tpm.GetRandom(3);?
Když se na zadání práce díváte znovu s přispěním získaných zkušeností, co považujete na něm za nejobtížnější?

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.