FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Josef Kokeš
Student:	Matěj Borský
Název práce:	Simulátor FIDO2 autentizace
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	22. května 2022

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

80 / 100 (B)

Písemná část práce napřed seznámí čtenáře se standardem FIDO2 a následně s návrhem a implementací simulátoru této technologie. Po obsahové stránce se zdá být v pořádku, očekává však od čtenáře poměrně detailní znalosti, kterými tento nemusí disponovat - speciálně sekce 4.3.2 se odkazuje na detaily, které dosud nebyly ani zmíněny, natož vysvětleny, navíc jsou často natolik abstraktně formulovány, že je čtenář nedokáže ani odhadnout. Domnívám se, že by bylo nanejvýš užitečné mezi sekce 4.1 a 4.2 doplnit vysvětlující sekci, která pomůže čtenáři překonat propast mezi "manažerským" popisem na začátku kapitoly 4 a popisem pro programátora-specialistu v sekcích 4.2 a 4.3.

Kapitola 6 (ale také sekce 5.1) je doslova zahlcena programovými výpisy. Nejsem přesvědčen o tom, že jsou pro text skutečně nezbytné, zvlášť v takovém množství - mnohem víc bych uvítal nějakou více symbolickou podobu, tedy diagramy a obrázky (ovšem v čitelné velikosti!), které mi dovolí lépe pochopit vztahy mezi jednotlivými klíčovými částmi aplikace. V tomto smyslu mi daleko užitečnější připadají vypsané hlavní komunikační datové objekty jako ve výpisu 12, 13, 16.

Kapitola 6.2 měla být detailnější - jaké všechny testy byly provedeny a s jakým výsledkem.

Práce vykazuje značné množství chyb zejména v čárkách a také mnoho překlepů, prospěla by jí lepší kontrola před odevzdáním. Sekce 4.1.1 následuje bezprostředně za hlavičkou sekce 4.1, kapitola 6 má podsekci 6.0.1. Z 42 citovaných zdrojů jich pouze 5 má

uvedeného autora, přitom zdroje 1, 2, 6 známého autora mají (potom jsem přestal hledat).

3. Nepísemná část, přílohy 90 /100 (A)

Vyhotovená aplikace plní to, co slibuje zadání - jde o simulátor FIDO2 zařízení, které průběžně zobrazuje jednotlivé kroky autentizace v podobě, aby se zájemce mohl podívat, jaká data vlastně mezi jeho zařízením a cílovým webem cestují.

Základní kontrola částí aplikace, které považuji za nejvíce rizikové, ukazuje dobré i špatné stránky. Aes.cpp správně používá vysokoúrovňové EVP funkce, správně pracuje s buffery a správně testuje návratové hodnoty, naopak nešťastně opakuje identifikátor šifrovací funkce (měl být použit pouze jednou v privátní metodě) nebo určuje velikosti klíče v generateKeyAndIv pomocí literálů namísto a) maximální specifikované velikosti nebo b) hodnot odvozených od použité šifry. ES256.cpp velmi pěkně kontroluje návratové hodnoty, až na metodu getPrivateKey nebo getJsonKeysMap, které tak nečiní a navíc dost riskantně vytváří řetězec z ASCIIZ ukazatele místo aby využily vrácenou délku dat. Pomocný buffer s klíčem by bylo vhodné vymazat bezpečným způsobem a ne nechávat klíč v paměti volně ležet.

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

Práce nemá přímé praktické využití pro běžného uživatele, jde ale o velice efektivní pomůcku pro pochopení principů FIDO2 a pro kontrolu toho, že skutečně komunikace funguje tak, jak říká specifikace. Dovedu si představit i její úpravu do podoby praktického simulátoru, který by šel použít v okamžiku, kdy uživatel usoudí, že nehodlá respektovat požadavky cílového webu na zabezpečení pomocí specifického hardwaru. Přínosem je také mírně srozumitelnější reformulace specifikace společně s implementací, kterou lze použít jako referenční.

Celkové hodnocení 89 /100 (B)

Předložená práce bezpochyby splňuje požadavky na bakalářské práce kladené. Student nastudoval ne úplně triviální specifikaci FIDO2 a pochopil ji do té míry, aby mohl sestavit funkční simulátor pro tento protokol. Je škoda, že své pochopení nerozepsal šířeji a s příklady, výsledkem mohla být i velmi dobrá alternativní dokumentace protokolu; to nyní není docela splněno. Také závěrečná korektura textu mohla být provedena lépe. Přesto práci hodnotím jako velmi dobrou (na hraně výborné) a doporučuji k obhajobě.

Otázky k obhajobě

Bez otázek.

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.