FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Jan Pešek
Oponent práce:	Ing. Tomáš Zahradnický, Ph.D.
Název práce:	Podpora CryptoAPI Next Generation v OpenSSL
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 14. 6. 2020

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
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.

Komentář:
Student měl za úkol se seznámit s knihovnami OpenSSL a CryptoAPI: Next Generation (CNG) a dále navrhnout a implementovat modul pro knihovnu OpenSSL propojující OpenSSL s CNG. Vytýčené body zadání v práci nacházím, považuji tedy zadání za splněné.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*85 (B)*

Popis kritéria:
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. 26/2017, 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.

Komentář:
Jazyková stránka práce. Nacházím zbytečné anglicismy typu defaultní (str. 1), open source nástrojů, callback tří funkcí, standardní file stream operace, zjednodušené message funkce, připravená enum funkce, friendly name, wide char řetězec, uložen do bufferu.

Typografická stránka práce. Velmi dobrá, nacházím jen drobnosti jako například parchant-vdovu na straně 14.

Logická stránka práce. Nemám připomínky.

Obsahová stránka. Ocenil bych obrázky struktur navíc k jejich popisu. Číst si o polích struktur pouze v textu je trochu nepohodlné. Nacházím drobné nepřesnosti typu: Formát certifikátu je definován standardem X.509, obsahuje informace o vlastníkovi, vystavovateli, platnosti a veřejny? klíč [28] (str. 13) — chybí digitální podpis vystavovatele certifikátu a další pole. win32 namísto Win32. Datový typ SECURITY_STATUS je vnitřně typem HRESULT hr. Pro ověřování zda jde o chybu anebo o úspěch by se mělo používat makro FAILED(hr) anebo SUCCEEDED(hr). Testy jako např. na straně 23 while (status == ERROR_SUCCESS) nebudou fungovat, pokud by funkce vrátila jiný kód úspěchu než ERROR_SUCCESS. Nacházím několik drobných překlepů (keypec místo keyspec).

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*92 (A)*

Popis kritéria:
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

Komentář:
Navržený a vytvořený modul pro OpenSSL je funkční. Zdrojový kód je dobře dokumentovaný.

Nacházím vážnou paměťovou chybu ve ascii2wide. Je alokován blok paměti na zásobníku pomocí funkce alloca a je uložen do ukazatele na konstantní řetězec. C umožňuje automaticky přidat const. Pokud by byl datový typ LPWSTR, nemuselo by o řádek níže být použito přetypování. Problém nastává, že blok alokovaný pomocí alloca je vracen z funkce ven. Tato paměť přestává být platná okamžikem návratu z funkce a jde o tzv. „dangling pointer“.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*90 (A)*

Popis kritéria:
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.

Komentář:
Výsledky práce pouvažuji na jednu stranu za výborné, avšak je trochu škoda, že se student rozhodl práci psát česky. Modul by mohl podle mého názoru získat větší pozornost, kdyby byla práce psána anglicky a byla vystavena na některém z repozitářů jako GitHub a případně nabídnuta autorům OpenSSL.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*
5. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
1. Na straně 45 se píše kód, který načítá modul a veřejný exponent. Mám za to, že obsahuje chybu, protože surová struktura keyBlob se přetypovává pro přičítání posunutí na ukazatel na strukturu BCRYPT_RSAKEY_BLOB namísto na unsigned char*. Přičtení hodnoty offset bude mít za následek přičtení násobně vyšší hodnoty než kdyby byl keyBlob přetypován na char*. Student by měl objasnit, zda jde o chybu anebo ne a proč.

2. Jakým způsobem a proč dojde k pádu aplikace, pokud se projeví paměťová chyba ve funkci ascii2wide v souboru e_cng.c? (Postačí rozkreslit zásobník funkce a funkce nadřazené)

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*95 (A)*

Popis kritéria:
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.

Text hodnocení:
Bakalářskou práci pana Jana Peška doporučuji k obhajobě a hodnotím ji stupněm A (výborně). Práce svým záběrem překračuje požadavky kladené na bakalářskou práci, proto navrhuji zvážení jejího ocenění.

Podpis oponenta práce: