FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Jan Pešek
Vedoucí: práce:	Ing. Josef Kokeš
Název práce:	Podpora CryptoAPI Next Generation v OpenSSL
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 7. 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 provedl požadovanou rešerši rozhraní CryptoAPI a CryptoNG a nastudoval tolik z kódu knihovny OpenSSL, aby mohl následně implementovat modul, který deleguje kryptografickou práci OpenSSL na rozhraní CryptoNG. Vypracoval také testovací nástroje, kterými je možné funkčnost modulu ověřit. Tím je zadání splněno.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*93 (A)*

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:

Textová část práce je výrazně nadstandardně zpracovaná. Student postupuje systematicky od seznámení s knihovnou OpenSSL a těmi jejími částmi, které jsou pro vytvoření nového crypto enginu klíčové, přes popis relevantních částí Windows (CryptoAPI, CryptoNG, úložiště certifikátů), k detailnímu popisu existujícího CAPI enginu a k návrhu a vysvětlení úprav, které jsou zapotřebí k vytvoření enginu nového. V kapitole o testování pak popisuje, jak takový engine v aplikaci použít. Text je detailní, hutný, ale přesto dobře srozumitelný. Také po jazykové stránce je v pořádku, zachytil jsem jen několik málo chyb, typicky vynechaných písmenek.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*95 (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:

Student naimplementoval kryptografický engine propojující OpenSSL a CryptoNG. Doprovází ho dvojice testovacích aplikací, která demonstruje použití enginu jak ze strany klienta, tak ze strany serveru. Kód všech těchto součástí je čistý a přehledně napsaný a dělá to, co má. Pokud bych si měl na něco stěžovat, pak na to, že engine je v tuto chvíli ryze dynamický, nebylo vůbec řešeno jeho případné zabudování přímo do projektu OpenSSL, což by byl logický následující krok - ovšem daleko nad rámec zadání.

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

4. Hodnocení výsledků, jejich využitelnost	*95 (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:

Vytvořený kryptografický engine je funkční a řeší sice z určitého pohledu okrajovou, ale přesto důležitou oblast - napojení OpenSSL na aktuální kryptografické rozhraní Microsoftu. To dosud plnil modul CAPI, který už je delší dobou součástí OpenSSL, ten ale vykazuje nedostatky, které ho činí čím dál hůře uplatnitelným - mimo jiné i v tom, že využívá zastaralé a dále nepodporované rozhraní. Reimplementace za pomoci nového rozhraní opět umožňuje uživatelům kombinovat výhody OpenSSL s výhodami Microsoftího rozhraní, např. uložení privátních klíčů na čipovou kartu, a to při kompatibilitě s moderními verzemi protokolu TLS (na rozdíl od enginu CAPI). Uvítal bych nicméně, kdyby se student pokusil prosadit tento engine do oficiálních zdrojových kódů OpenSSL.

Vedlejším přínosem je, že práce může posloužit jako velmi dobrý zdroj informací o problematice vytváření alternativních kryptografických enginů pro OpenSSL. To je s ohledem na známou ne-kvalitu dokumentace OpenSSL také velmi důležité. Škoda jen, že je práce napsána v češtině, tím se dosah tohoto přínosu velmi snižuje.

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: *1=výborná aktivita,* *2=velmi dobrá aktivita,* *3=průměrná aktivita,* ***4=slabší, ale ještě dostatečná aktivita,*** *5=nedostatečná aktivita* 5b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
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 (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Student pracoval z převážné většiny samostatně, konzultací bylo poměrně málo - i při zohlednění koronavirových omezení. Výsledek jeho úsilí však ukazuje, že to ničemu neublížilo.

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:

Vytvořená bakalářská práce je vysoce nadprůměrná ve všech hodnocených ohledech a velmi kvalitně řeší velmi praktický problém. I přes existenci vzoru v podobě enginu CAPI musel student vyřešit celou řadu problémů, které jsou mnohdy velmi špatně (pokud vůbec) zdokumentovány, nesporně tak šlo i o dost náročnou věc. Ze všech těchto důvodů hodnotím práci známkou A-výborně a doporučuji komisi zvážit, zda ji nenavrhnout na ocenění.

Podpis vedoucího práce: