FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Otto Hollmann
Vedoucí: práce:	Ing. Josef Kokeš
Název práce:	Zjednodušení výběru šifrových sad v protokolech SSL/TLS
Obor:	Počítačová bezpečnost

Datum vytvoření: 19. 1. 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 si zvolil ambiciozní zadání, jehož cílem byla taková úprava knihovny OpenSSL, která by odstranila v ní existující nedostatky v uživatelské volbě šifrových sad. Aby to student mohl splnit, musel dosti detailně nastudovat jak fungování knihovny OpenSSL, tak rozdíly mezi protokoly TLS 1.2 a TLS 1.3, a následně vymyslet a provést úpravy v takové kvalitě, aby neovlivnil negativně stávající bezpečnostní parametry knihovny. To vše činí zadání výrazně náročnějším než jsou obvyklá zadání. Stanovené cíle student splnil.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*90 (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:

Písemná práce je na velmi vysoké úrovni. Popisuje vše, co je potřebné pro porozumění problému i jeho řešení, s téměř ideální úrovní detailů. Velmi vítám výborně provedenou kapitolu 5 (Testování) a přílohu B (ukázku konfigurace a vysvětlení výběru šifrové sady). Mírně slabší je úvod, jehož přechody mezi odstavci působí poněkud neuspořádaným dojmem a podle mě ne zcela přesvědčivě vysvětlují čtenáři podstatu problému. - Po jazykové stránce je práce velmi kvalitní, napočítal jsem do 10 chyb, vesměs v čárkách; nejvíce vadí překlep v českém abstraktu, záměna slova "respectable" a "respective" v anglickém a slovo "optimálnější" na straně 14.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*99 (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:

Vytvořená úprava OpenSSL je skoro perfektní. Kód je kvalitně napsaný i okomentovaný a dodržuje kódovací standardy OpenSSL. Za velký přínos považuji dodržení kompatibility se stávajícím aplikačním rozhraním a s nastavením existujících klientů a serverů a velkou otevřenost vytvořené úpravy do budoucna, na rozdíl od dosavadní implementace v OpenSSL. Uvítal bych nicméně, kdyby byl kód před odpushováním do veřejně přístupného repozitáře rebasován na aktuální stav vývoje OpenSSL, aby byly všechny změnové commity v běžně používaných GUI pro Git vidět pohromadě a ne rozházené přes celou dobu vývoje.

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:

Hlavním výsledkem práce je úprava v OpenSSL, která umožňuje jednoduchým a univerzálním způsobem vybírat šifrové sady v různých verzích protokolu TLS. Jde o poměrně specifický problém, který patrně většina uživatelů ani nezaznamená, ale pro ty uživatele, kteří ho potřebují vyřešit, je vytvořená úprava nesmírně užitečná. Obecným přínosem do budoucna dále je, že stejný kód umožní snadnou adaptaci na případný budoucí vývoj v protokolech TLS, na který dosavadní implementace nebyla připravena a fakticky by vyžadovala vytvoření třetího nekompatibilního konfiguračního rozhraní.

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:

Studentovi nemám co vytknout. Pracoval průběžně, kvalitně a velmi samostatně, všechny problémy dokázal zanalyzovat, navrhnout řešení a to správně naimplementovat.

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:

Práci pana Hollmanna považuji za mimořádně kvalitní. Provedl důkladnou analýzu problému a navrhl pro něj velice elegantní řešení, které následně výborně naimplementoval a otestoval v prakticky používaných aplikacích. Tak nějak si představuji kvalitně provedenou inženýrskou práci. Práci tedy doporučuji k obhajobě a hodnotím známkou A - výborně.

Podpis vedoucího práce: