Hodnocení vedoucího závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Jan Král
Vedoucí práce: Ing. Josef Kokeš
Název práce: Bezpečnostní incidenty v SSL/TLS implementacích
Obor: Informační technologie

Datum vytvoření: 17. 1. 2018

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	*1=mimořádně náročné zadání,* *2=náročnější zadání,* ***3=průměrně náročné zadání,*** *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Zadání se zabývá analýzou zranitelností vzniklých nesprávnou implementací SSL/TLS protokolů. Zejména v posledních letech se objevila řada takových, téma je proto velmi aktuální a s dostatkem materiálů ke studiu.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. 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 splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Zadání bylo splněno.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	***1=splňuje požadavky,*** *2=splňuje požadavky s menšími výhradami,* *3=splňuje požadavky s většími výhradami,* *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Délka práce splňuje stanovené požadavky, kdyby však byla rozsáhlejší, její hodnotu by to navýšilo.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*85 (B)*

Popis kritéria:
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.

Komentář:
Po faktické stránce nemám práci mnoho co vytknout. Uvítal bych, kdyby popis známých útoků byl v některých případech detailnější, např. u DROWN nebo Triple Handshake citelně chybí důkazy jednotlivých tvrzení, které by pomohly srozumitelnosti. Vyhodnocení výsledků mohlo být detailnější.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*95 (A)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3.

Komentář:
Formální stránka práce je výborná. Našel jsem asi tři chybějící čárky a v poslední příloze nesprávné vzorce pro šifrování a dešifrování RSA (chybí znak ^, takže místo mocnění nacházíme v textu násobení).

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*95 (A)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
K literatuře nemám výhrady.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*70 (C)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Práce replikuje jinými prostředky už dříve známé výsledky, což je přiměřené tomu, že jde o práci bakalářskou. Přínosem autora je implementace obou směrů útoku Heartbleed - tzn. nejen útok klienta na server, ale také útok serveru na klienta. Analýza nasbíraných dat však mohla být podrobnější.

Za výrazný problém považuji odstranění copyrightových komentářů ze souborů client.c a heartbleed.c. Použité licence výslovně vyžadují, aby tyto komentáře zůstaly zachovány, což se nestalo. To je hrubá chyba, ke které nemělo dojít a na kterou bych studenta upozornil, kdybych kód viděl před odevzdáním, nepovažuji ji však za tak závažnou, aby zamezovala obhajobě práce - skutečné zdroje jsou odkazovány jak ze zdrojového kódu, tak z textu práce, tzn. autorství nebylo závažně narušeno.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Odvedená práce slouží jako dobrá názorná demonstrace rizik spojených s implementací kryptografických protokolů. To byl její účel a tento účel podle mě dobře plní.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
9. Aktivita a samostatnost studenta v průběhu řešení	9a: *1=výborná aktivita,* *2=velmi dobrá aktivita,* ***3=průměrná aktivita,*** *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 9b: *1=výborná samostatnost,* ***2=velmi dobrá samostatnost,*** *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatné tvůrčí práce (9b).

Komentář:
Student pracoval převážně samostatně, konzultace se týkaly spíš zaměření a cílů práce než toho, jak jich dosáhnout.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*75 (C)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Odevzdaná práce vykazuje solidní úroveň. Po obsahové i formální stránce je prakticky bez výhrad, zároveň ale skončila příliš brzy, než aby dosáhla výjimečné kvality - s ohledem na čas, který byl k dispozici, jsem doufal, že se dostaneme dále. Hodnotil bych stupněm B - velmi dobře, kdyby nebylo nepříjemnosti s licencí výše. Kvůli té bohužel musím hodnocení snížit. Navrhuji tedy komisi, aby práci ohodnotila stupněm C - dobře.

Podpis vedoucího práce: