



## Posudek oponenta závěrečné práce

**Student:** Jaroslav Kříž  
**Oponent práce:** Ing. Simona Buchovecká  
**Název práce:** Bezpečnostní analýza Linux Unified Key Setup (LUKS)  
**Obor:** Bezpečnost a informační technologie

**Datum vytvoření:** 22. 5. 2019

<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení – následující škálou 1 až 4:</b>
<b>1. Splnění zadání</b>	<b>1=zadání splněno, 2=zadání splněno s menšími výhradami, 3=zadání splněno s většími výhradami, 4=zadání nesplněno</b>
<b>Popis kritéria:</b> 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.	
<b>Komentář:</b> Zadání bylo splněno, student reflektoval ve své práci všechny dílčí požadavky.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</b>
<b>2. Písemná část práce</b>	<b>95 (A)</b>
<b>Popis kritéria:</b> 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.	
<b>Komentář:</b> Práce je po věcné i formální stránce dobře zpracovaná, logicky členěna a všechny části jsou informačně bohaté. Drobnou výtka mám jen ke kapitole 4.4., kde mohlo být lépe specifikováno, které části kódu byly v rámci práce prostudovány (a tudíž byla prověřena jejich bezpečnost/korektní implementace).	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</b>
<b>3. Nepísemná část, přílohy</b>	<b>80 (B)</b>
<b>Popis kritéria:</b> 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	
<b>Komentář:</b> Nepísemnou část práce tvoří zdrojové kódy reimplementace LUKS a zdrojové kódy slovníkových útoků - kód by pro zlepšení čitelnosti zasloužil komentáře.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</b>
<b>4. Hodnocení výsledků, jejich využitelnost</b>	<b>95 (A)</b>
<b>Popis kritéria:</b> 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.	
<b>Komentář:</b> Výsledkem práce je bezpečnostní analýza LUKS, potvrzení správnosti implementace použitých algoritmů a otestování odolnosti vůči slovníkovým útokům, včetně doporučení k výběru šifry a operačního módu. Práce tak může sloužit jako nezávislé hodnocení při výběru řešení pro šifrování diskových oddílů, tak i pro orientaci uživatele v dané problematice.	

Hodnotící kritérium:

Způsob hodnocení – nehodnotí se

## 5. Otázky k obhajobě

Popis kritéria:

Uvedte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odřádkami).

Otázky:

- Jako jedno z míst s možným bezpečnostním dopadem byla identifikována podpora operačních módů ECB a CBC a podpora šifry CAST5 - jaké šifry a operační módy využívají ostatní porovnávané nástroje (VeraCrypt, Bitlocker)?

Hodnotící kritérium:

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

## 6. Celkové hodnocení

92 (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 doporučuji k obhajobě a hodnotím stupněm A.

Podpis oponenta práce: