



Hodnocení vedoucího závěrečné práce

Student: Lukáš Kozák
Vedoucí práce: Ing. Jiří Buček, Ph.D.
Název práce: Security analysis of hardware crypto wallets
Obor: Bezpečnost a informační technologie

Datum vytvoření: 17. 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 dostatečné 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: Zadání bylo splněno v plném rozsahu.	
Hodnotící kritérium:	Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):
2. Písemná část práce	95 (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: Práce je nadprůměrně rozsáhlá a obsahuje všechny důležité části. Členění práce je logické a jednotlivé kapitoly jsou přiměřeně bohaté. Po věcné ani formální stránce nemám větší výhrady. Z textu práce je vidět i studentův zájem o problematiku a systematický přístup k práci.	
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: Přílohou práce jsou soubory firmware použité pro experimenty s HW krypto-peněženkou Trezor, a také data z osciloskopu naměřená pro demonstraci útoku postranním kanálem a pomocné skripty. Vzhledem k tomu, že nejde o implementační práci, jsou přílohy přiměřené a nemám k nim závažnější výhrady.	
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:

Studentova práce slouží jednak jako úvod do problematiky kryptoměn, a také jako užitečný přehled současné oblasti HW krypto-peněženek a modelu hrozeb, kterým je jejich užití vystaveno. Student přináší podrobnější vhled do bezpečnostních aspektů jednotlivých typů, které jsou na trhu. Zvláštní pozornost byla věnována typu SatoshiLabs Trezor One, pro který byly demonstrovány některé známé zranitelnosti a vysvětlen způsob jejich ošetření.

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 posudte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (5a). Posudte schopnost studenta samostatně tvůrčí práce (5b).

Komentář:

Studentova aktivita i samostatnost je bez výhrad.

Hodnotící kritérium:

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

6. Celkové hodnocení

98 (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:

Student prokázal schopnost samostatné tvůrčí práce. Svého úkolu se zhostil se zaujetím pro věc a s pečlivostí a vytvořil zdařilé dílo. Výsledky studentovy práce lze doporučit jako užitečný studijní materiál pro zájemce o bezpečnost hardwarových krypto-peněženek. Celkově hodnotím práci jako výbornou.

Podpis vedoucího práce: