FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Vojtěch Miškovský, Ph.D.
Student:	Bc. Matúš Olekšák
Název práce:	Bezpečnostní analýza řídící jednotky pro automobily
Obor / specializace:	Návrh a programování vestavných systémů
Vytvořeno dne:	5. května 2022

Hodnotící kritéria

1. Splnění zadání

- ▸ [1] **zadání splněno**
  [2] zadání splněno s menšími výhradami
  [3] zadání splněno s většími výhradami
  [4] zadání nesplněno

Student zanalyzoval řídící jednotku a navrhl několik způsobů pro získání podpisového klíče. Navržené metody velmi detailně prozkoumal a zdokumentoval. Ačkoli se nepodařilo klíč získat, odvedená práce je zcela v souladu se zadáním, které považuji za bez výhrad splněné.

2. Písemná část práce 95 /100 (A)

Kvalita písemné zprávy je na velmi dobré úrovni. Celý text je informačně velice bohatý a jednotlivé části na sebe logicky navazují. Po formální a typografické stránce nemám výhrady. Jazyková úroveň je nadprůměrná a oceňuji, že vzhledem k publikačnímu potenciálu práce zvolil student anglický jazyk. Práce se zdroji je příkladná.

3. Nepísemná část, přílohy 100 /100 (A)

Nepísemná část se omezuje pouze na pomocné skripty a aplikace, které student využil při experimentech. Nemám k nim výhrady.

4. Hodnocení výsledků, jejich využitelnost 100 /100 (A)

Výsledkem práce je analýza zvolené řídící jednotky, velmi detailní popis jejího fungování, navržené útoky pro získání podpisového klíče a obsáhlá dokumentace k jejich provedení. Vzhledem ke kvalitě dokumentace může být případné další navázání na dosažené výsledky zcela bezproblémové. Dalším dosaženým výsledkem je úspěšný útok korelační odběrovou analýzou na kryptografický algoritmus SipHash, který byl již publikován na

mezinárodní konferenci DDECS a stal se prvním publikovaným útokem pomocí analýzy postranních kanálů na tento algoritmus.

5. Aktivita studenta

▸ [1] **výborná aktivita**
[2] velmi dobrá aktivita
[3] průměrná aktivita
[4] slabší, ale ještě dostatečná aktivita
[5] nedostatečná aktivita

Student práci brzy započal, dobře si ji v čase rozložil, průběžně na ní pracoval a velmi aktivně podstatné kroky konzultoval.

6. Samostatnost studenta

▸ [1] **výborná samostatnost**
[2] velmi dobrá samostatnost
[3] průměrná samostatnost
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Většina konzultací byla spíše informováním vedoucího o postupu prací.

Celkové hodnocení 99 /100 (A)

Student zanalyzoval zvolenou řídící jednotku a následně navrhl a vyzkoušel různé druhy útoků. Ačkoli žádný nebyl úspěšný, student u zvolených útoků vyčerpal dostupné možnosti a všechny postupy byly velmi podrobně a kvalitně zdokumentovány. Jím navržený útok na algoritmus SipHash byl navíc prvním svého druhu a prošel recenzním řízením mezinárodní konference, kde byl publikován. Vzhledem k množství odvedené práce, její kvalitě a publikačnímu výstupu nelze než ohodnotit práci klasifikačním stupněm A a zároveň komisi doporučit její navržení na cenu děkana.

Instrukce

Splnění zadání

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.

Písemná část práce

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. 52/2021, 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.

Nepísemná část, přílohy

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.

Hodnocení výsledků, jejich využitelnost

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.

Aktivita studenta

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.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

Celkové hodnocení

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.