FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš
Student:	Jan Kalivoda
Název práce:	Bezpečnostní zranitelnosti v Lightning Network
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	19. 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

2. Písemná část práce 90 /100 (A)

Písemná část práce může v úvodu působit mírně frivolně a ne jako technický text, její zbytek je ale proveden velice pěkně. Student seznámí čtenáře s nutným minimem pro pochopení Bitcoinu i na něm postavené Lightning Network, následně popíše jednotlivé známé útoky včetně doporučení pro uživatele, jak se jim bránit. V předposlední kapitole pak detailně zachycuje průběh útoku, kterým útočník okrade oběť o veškeré prostředky, které jí dříve zaplatil.

Po technické stránce jsem s prací vesměs spokojen. Obsahuje stále menší množství jazykových chyb (typicky v čárkách nebo i-y), ale ne příliš mnoho. Na některých stránkách (nejviditelněji 56) text vytéká ze šablony stránky do okrajů. Zatímco u podsekcí 3.x je existence jedné podpodsekce logická a odůvodněná, u kapitoly 4 tomu tak není - buď mělo být sekcí více, nebo měla být sekce 4.1 součástí popisu kapitoly a podpodsekce se měly stát podsekcemi.

3. Nepísemná část, přílohy 90 /100 (A)

U práce není žádná veřejná příloha, což je ale naprosto v pořádku - cílem práce bylo popsat zranitelnosti v protokolu, ty jsou z principu nezávislé na konkrétní implementaci. Jediná implementačně závislá část je úprava v C-lightning, která odstraní jednu z ochran na straně aplikace a umožní útočníkovi snadno podvádět, což je pochopitelně nežádoucí

publikovat (útočník v ostré síti to sice dokáže snadno udělat i sám, ale není důvod mu v tom pomáhat).

4. Hodnocení výsledků, jejich využitelnost 95 /100 (A)

Odevzdaná bakalářská práce je velmi přínosná už tím, že srozumitelně a na jednom místě shrnuje známé zranitelnosti v Lightning Network. Měla by tak být povinným čtením pro všechny potenciální uživatele, aby věděli, na co si mají dávat pozor, pokud chtějí této sítě využívat. Prezentovaný příklad útoku je jistě dost přesvědčivý pro každého uživatele. Jen je trochu škoda, že jazykem práce je čeština, v angličtině by se její užitečnost ještě výrazně zvýšila.

5. Aktivita studenta

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

6. Samostatnost studenta

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

Celkové hodnocení 92 /100 (A)

Student nastudoval problematiku Lightning Network a bezpečnosti jejího protokolu, uspořádal známé útoky a doporučil uživateli obranu. Zároveň v kapitole 4 přesvědčivě ukázal, že nejde jen o teoretický koncept ale o vážné problémy, kterých si každý uživatel musí být vědom předtím, než síť začne používat. Doporučuji práci k obhajobě a hodnotím známkou A=výborně.

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.