Posudek oponenta bakalářské práce

Student: Brna Filip
Téma: Analýza bezpečnosti a použitelnosti kryptoměnových peněženek (id 25097)
Oponent: Homoliak Ivan, Ing., Ph.D., UITS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Zadanie vychádzalo praktickej potreby porovnať vlastnosti krytpomenových peňaženiek.

2. Splnění požadavků zadání **zadání splněno**

3. Rozsah technické zprávy **je v obvyklém rozmezí**

Práca obsahuje 57 latex-om vysádzaných strán vrátane referencií a príloh a je teda v obvyklom rozmedzí. Počet normostrán ľahko prevyšuje 80.

4. Prezentační úroveň předložené práce **70 b. (C)**

Práca je pre čitateľa pochopiteľná, jednotlivé kapitoly na seba logicky nadväzujú. Rozsahy a prehľadnosť väčšiny kapitol sú prípustné.

Mám niekoľko výhrad, ktoré zhrniem v nasledovnom.
Sekciu 2.1 študent pomenoval *Kryptografia* no zaoberá sa v nej len šifrovaním a dešifrovaním správ. Študent popisuje v sekcii 4.1 útok hrubou silou ale neuvádza akých peňaženiek sa to týka. Študent uvádza, Že útoku evil maid (Sekcia 4.3) je možné predísť pomocou vynucovania silných hesiel a nastavenie časového limitu uzamknutia obrazovky na zariadení. To však nie je pravda, keďže cieľom tohto útoku je získanie hesla alebo PINu. V kapitole 3 študent mieša jablká z hruškami. Konkrétne v sekciách 3.1 až 3.9 popisuje testovacie scenáre a v sekciách 3.10-3.6 útoky na peňaženky.

Z hľadiska použiteľnosti mi chýba v práci užívateľská štúdia, ktorá by kvantitatívne ohodnotila použiteľnosť prevedenia operácií nad jednotlivými peňaženkami. Z tohto hľadiska som očakával, že študent aspoň v niektorých prípadoch ohodnotí intuitívnosť použitia peňaženiek pre niektoré operácie. Študent uvádza, že smart kontrakt je program, ktorý sa spustí v prípade splnenia počiatočných podmienok, pričom už neuvádza, čo myslí počiatočnými podmienkami.

Ďalej hodnotenie použiteľnosti by mohlo byť uskutočnené na dostatočne veľkej vzorke užívateľov aby nadobudlo vypovedajúcu hodnotu. No toto nebolo súčasťou zadania.

5. Formální úprava technické zprávy **80 b. (B)**

Celkovo je práca na nadpriemernej typografickej aj jazykovej úrovni. Práca obsahuje len minimum jazykových chýb.

Odkaz na sekciu 2.2 v úvode neobsahuje slovo sekcia. Študent používa citácie bez akejkoľvek medzery.

6. Práce s literaturou **80 b. (B)**

Práca s literatúrou je na vyhovujúcej úrovni. Zvolené študijné pramene sú relevantné a sú aj odlíšené od vlastných výsledkov. Treba tiež poznamenať, že väščina referencií sú webového charakteru. V tejto oblasti je to však opodstatnené.

7. Realizační výstup **70 b. (C)**

Realizačným riešením sa v tejto práci myslí porovnanie vlastností kryptopeňaženiek a návrh doporučení pre jednotlivé prípady použitia. Tieto hodnotím ako splnené.

8. Využitelnost výsledků

Výsledky sú využiteľné v budúcich užívateľských štúdiach použiteľnosti kryptopeňaženiek. Takéto štúdie by mali byť prevedené na dostatočne veľkej vzorke užívateľov.

9. Otázky k obhajobě

- Aké nevýhody majú smart kontraktové peňaženky?
- Ako sa dá brániť voči fault injection útokom na hardwarové kryptopeňaženky, známym tiež ako glitching?
- Akých kryptopeňaženiek sa týka útok hrubou silou?

10. Souhrnné hodnocení **75 b. dobře (C)**

Práca je štandardne obtiažneho zadania. Zadanie bolo splnené vo všetkých bodoch. Študent volil vhodnú literatúru. Práca poskytuje ucelené výsledky. V práci mi chýba užívateľská štúdia, no toto nebolo špecifikované v zadaní. Celkovo prácu hodnotím stupňom C **(75 bodov)**.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 3. června 2022

Homoliak Ivan, Ing., Ph.D.
oponent