FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Miroslav Pospíšek, CSc.
Student:	Kryštof Nevšímal
Název práce:	Možnosti aplikace důkazu s nulovými znalostmi v praxi
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	7. června 2024

Hodnotící kritéria

1. Splnění zadání

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

Splněny byly všechny body zadání. Nad rámec zadání byla vytvořena druhá ukázková aplikace. Jedna ukázková aplikace přímo souvisí s protokolem STARK popsaným v teoretické části, druhá je jednoduchým příkladem autentizace pomocí jména a hesla, přičemž heslo na serveru není uloženo, ani mu není zasíláno.

2. Písemná část práce 100 /100 (A)

Všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Jednotlivé části jsou obsahově vzájemně provázány.
Bakalářská práce se zabývá kryptografickou metodou důkazu s nulovými vlastnostmi (ZKP).
V části popisující tuto metodu (kapitoly 1 a 2) oceňuji zdůraznění základních principů, jednoduché ilustrativní příklady a přehled používaných matematických metod.
Prezentovaný přehled o současném stavu (především odst. 1.4 a 1.5) vychází z historického vývoje, je dostatečně informativní a přitom stručný, vede čtenáře k protokolům STARK a SNARK,
které jsou pak dále podrobněji analyzovány v kap. 2. Protokol STARK je pak použit i v ukázkové aplikaci. Je zde také zmíněna odolnost protokolů vůči tzv. kvantové hrozbě.
Možností praktické aplikace ZKP je celá řada, a ty možnosti, které jsou v práci zmíněny, jsou s ohledem na jejich aktuálnost velmi vhodně zvoleny.
Velmi kladně hodnotím to, že v práci jsou uvedeny dokonce dvě praktické aplikace. První aplikací (napsanou v bezpečnostními analytiky oceňovaném jazyce Rust)
je implementace protokolu STARK v oblasti autentizace. Druhá aplikace ukazuje implementaci protokolu Secure Remote Password, který má oproti běžně používaným

autentizačním metodám používajícím heslo další výhody.
Autor práce nejenže ukázkové aplikace sestavil, ale zhodnotil jejich vlastnosti a ukazuje na nich přednosti a nedostatky ZKP.
Informační zdroje jsou řádně citovány a odlišeny od vlastních výsledků.

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

Příloha obsahuje zdrojovou formu bakalářské práce ve formátu Latex, dále ukázkové aplikace, zdrojový kód, přeložené moduly a návod na použití.
Oceňuji implementaci v jazyce Rust.

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

Přehled možností využití protokolu ZKP ukazuje na jejich vhodnost pro nasazení v několika citlivých a aktuálních oblastech: 1. snížení šance podvodů a manipulace s výsledky voleb při současném zajištění jejich anonymity, 2. odolné metody autentizace mimo jiné snižují šíření škodlivého kódu, 3. možnosti analýzy finančních transakcí bez nutnosti poskytovat citlivá data 4. možnost ověřovat tvrzení při komunikaci mezi stranami, které si vzájemně nechtějí poskytovat informace.
Tím, že upozorňuje na existenci této kryptografické metody, diskutuje její přednosti a nedostatky a ukazuje, že v relativně velmi krátké době je možno sestavit funkční aplikace, může tato práce sloužit jako inspirace a impuls pro využití protokolu ZKP v praxi a řešení řady stávajících technických a i společenských problémů.

5. Aktivita studenta

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

Student byl aktivní, dodržoval dohodnuté termíny. Svá řešení průběžně konzultoval a na konzultace byl připraven.

6. Samostatnost studenta

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

Celkové hodnocení 100 /100 (A)

Stránky ZP, které nejvíce ovlivnily hodnocení: Dodržení zadání, časové rozvržení prací, samostatnost, volba poměru detailnosti a stručnosti při teoretickém popisu algoritmů, snaha o porozumění problematice, schopnost nalézt potřebné informace a zorientovat se v nich.

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.