Posudek oponenta bakalářské práce

Student: Malínek Libor
Téma: Uživatelské rozhraní pro decentralizované národní volby (id 25141)
Oponent: Malinka Kamil, Mgr., Ph.D., UITS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

2. Splnění požadavků zadání **zadání splněno**

Jedná se o implementační BP s jasně ohraničeným rámcem.

3. Rozsah technické zprávy **splňuje pouze minimální požadavky**

Práce je extrémně stručná. Rozsah zprávy je uměle navýšen 9 stranami, kdy každá obsahuje jeden obrovský obrázek rozhraní. Dále pak práce obsahuje množství prázdných částí stran (např. str. 8 a 9) nebo nadměrných obrázků.

4. Prezentační úroveň předložené práce **35 b. (F)**

Logická struktura práce je na velmi nízké úrovni. Navíc obsahově nepokrývá mnoho částí, které byly evidentně implementovány a prezentovány. Text je často zkratkovitý (protokol je tvořen knihovnami?). Některé části nejsou nijak vztaženy k řešenému problému ani dále rozvedeny - např. GAS a cena voleb. Kapitola tři prezentuje technologie o kterých pouze předpokládám, že byly použity. Nijak není popsáno, proč byly zvoleny a jaké byly zvažované alternativy. V práci mi chybí alespoň základní specifikace funkčních a nefunkčních požadavků na navrhované řešení. Popis tvorby výsledků hlasování je nejasný. Obdobně analýza bezpečnostních funkcí je stručná, nepokrývá některé zásadní oblasti (práce s klíči uživatelů) a chybí lepší interpretace zjištění. Popis testování je stručný, chybí demografie testovací kupiny.

5. Formální úprava technické zprávy **35 b. (F)**

Formální úprava práce je na velmi nízké úrovni. Dochází k nelogickému umístění obrázků, práce je nedostatečně formátována (např. velké množství bílých míst, nevhodné rozměry obrázků, divné znaky místo jmen v referencích). Obsahuje velké množství překlepů a chyb (patrně způsobeno špatným překladem).

6. Práce s literaturou **75 b. (C)**

Odkazované zdroje jsou relevantní tématu a vhodně vybrány. Práce obsahuje jeden odkaz na wikipedii (model Actor), což nepovažuji za vhodné.

7. Realizační výstup **75 b. (C)**

Prezentované uživatelské rozhraní je velmi minimalistické a uživatelsky nepřívětivé (absence nápovědy a vysvětlení jednotlivých fází, dlouhé hexadecimální kódy jako identifikátory, nejasná nutnost opravy hlasování apod). Řešení obsahuje několik návrhových chyb - očekává, že si uživatel vytvoří, exportuje a importuje soukromý klíč se kterým ovšem pracuje v otevřené formě. Navíc rozhraní tuto část nedostatečně pokrývá. Naopak pozitivně hodnotím snahu o začlenění do stylu státní správy.
Proces volby byl implementován a je funkční pro nízké počty hlasujících, vyšší nebylo možno otestovat.
V rámci prezentace řešení bylo studentem konstatováno, že nad rámec zadání bylo nutné kompletně reimplementovat existující volební protokol v RUSTu. Dle mého názoru je tato implementace vydařená, výrazným způsobem rozšiřuje původní rámec zadání a je hlavním důvodem, proč pozitivně hodnotím realizační výstup.

8. Využitelnost výsledků

Práce může sloužit jako demonstrační aplikace použitého protokolu elektronických voleb.

9. Otázky k obhajobě

1. Proč jste nástroj rozšiřoval o ověření správnosti hlasování? Aktuální mechanismus voleb to neumožňuje.
2. Jakým způsobem máte ochráněnou aplikaci před úpravou kódu tak, aby bylo ovlivněno hlasování?
3. Proč jste nevyužil volně dostupé výpočetní zdroje pro testování většího rozsahu (např. služby Metacentra)?

10. Souhrnné hodnocení **49 b. nevyhovující (F)**

Implementační část je na solidní úrovni, kterou ovšem snižuje design UX a některé zmíněné problémy (např. stručná bezpečnostní analýza). Na druhou stranu obsahuje implementaci volebního protokolu, což považuji nad rámec zadání. Hlavním důvodem mého hodnocení je tak nedostatečně zpracovaná textová část, která by zasloužila přepracovat a rozšířit o chybějící části. Práci tak v celkovém hodnocení nemohu doporučit k obhajobě a navrhuji hodnocení "F".

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

V Brně dne: 29. května 2022

Malinka Kamil, Mgr., Ph.D.
oponent