Posudek oponenta bakalářské práce

Student: Dorda Tomáš
Téma: Mobilní aplikace - Deník jako chat (id 22892)
Oponent: Dobeš Petr, Ing., UPGM FIT VUT

1. Náročnost zadání — průměrně obtížné zadání

Téma práce spadá mezi průměrně obtížná zadání.

2. Splnění požadavků zadání — zadání splněno

Zadání bakalářské práce bylo splněno.

3. Rozsah technické zprávy — je v obvyklém rozmezí

Technická zpráva má obvyklý rozsah.

4. Prezentační úroveň předložené práce — 80 b. (B)

Text práce je psaný jasně a srozumitelně. Práce je vhodně strukturovaná a je dobře čitelná. Pouze místy je tok textu při čtení mírně narušený některými drobnostmi, jako například odstavcem, který obsahuje pouze jednu větu.

Z hlediska celkové osnovy práce by bylo vhodnější zařadit kapitolu "Použité technologie" až za kapitolu s návrhem aplikace. Kapitola "Návrh řešení" by tak v textu lépe navazovala na kapitolu s průzkumem existujících aplikací, ze které čerpá a na kterou se velmi často odkazuje.

V kapitole 2, "Průzkum současných řešení", je uvedeno, že "Na Google Play se nachází desítky aplikací pro vedení deníků, ale pro vedení deníku formou chatu zatím existuje pouze aplikace Chat Journal ..." V celé kapitole jsou následně popsány pouze dvě aplikace (Chat Journal a Messenger). Nejsou zde nijak zmíněny vlastnosti ostatních aplikací pro psaní deníků, které nemají charakter chatu. Vzhledem k zaměření práce na vedení deníku na mobilním zařízení by bylo vhodné uvést alespoň jejich stručný souhrnný popis a jejich hlavní vlastnosti. Ve vyhodnocení práce by potom mohlo být zajímavé prozkoumat, jak uživatelé hodnotí vytvořený deník na bázi chatu v porovnání s některou z ostatních existujících deníkových aplikací.

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

Z typografického hlediska má práce poměrně dobrou úpravu. Celkový dojem místy kazí některé drobné typografické nedostatky, například text přeteklý za okraj odstavce na straně 26, nebo několikanásobný výskyt symbolu "??" místo reference na obrázek na straně 5 (pravděpodobně jde o obrázek č. 2.2). Dále by z typografického hlediska bylo o něco vhodnější psát popisy tabulek nad tabulku místo pod.

Po jazykové stránce je práce psaná dobře. Jedinou drobností je občasná nekonzistence při používání pasivu a první osoby, respektive změna z jednoho na druhé v krátkém úseku textu. (Na straně 1 došlo ke změně dokonce v průběhu jediné věty, což působí mírně rušivě: "Je použit relativně nový framework Flutter pro multiplatformní vývoj a použil jsem návrhový vzor Bloc.")

6. Práce s literaturou — 90 b. (A)

Použité zdroje jsou vzhledem k tématu práce v pořádku. Citační zvyklosti i citační etika jsou dodrženy.

7. Realizační výstup — 70 b. (C)

Mobilní aplikace, která v rámci bakalářské práce vznikla, je z hlediska uživatelského rozhraní dobře zpracovaná. Pozitivně hodnotím zejména iterativní přístup k vývoji, postupné experimentování a prozkoumávání možností a neustálé zjišťování zpětné vazby od uživatelů. Díky zakomponovaní poznatků a zpětné vazby od testerů je tak výsledná aplikace uživatelsky přívětivá a má čisté rozhraní.

Z implementačního hlediska jsou použitý framework a knihovny vhodně zvolené.

Samotná funkcionalita je spíše základní. Zde je nutné přihlédnout k tomu, že jedním z cílů práce je, aby výsledná aplikace byla minimalistická. V některých ohledech by nicméně i tak měla být aplikace úplnější. Je škoda, že

například chybí alespoň jednoduchá možnost importu a exportu pro umožnění přenosu dat při výměně mobilního zařízení, nebo není možné vyhledávat ve více denících zároveň, pokud uživatel neví, do kterého z nich hledanou poznámku uložil.

Za účelem zabezpečení jsou v aplikaci implementované dvě možnosti. První z nich je zašifrování uložených záznamů, pro které jsou v práci využity standardní postupy symetrické kryptografie pro šifrování dat. V kódu je ovšem při ukládání hesla nevhodně pracováno s přidáváním tzv. "soli", která by měla být náhodně generovaná, je ale napevno nastavená (a tudíž pro všechny uživatele na všech zařízeních stejná).

Druhou bezpečnostní funkcí aplikace je skrytí deníku ze seznamu. To je zajištěno pomocí tajné sekvence znaků, kterou si uživatel zvolí, a následně k deníku přistupuje přes zadání této sekvence do vyhledávání. Zde ovšem nastávají dva problémy. Významným problémem je to, že tajná sekvence znaků je ukládána přímo v "plaintext" reprezentaci. Potenciální útočník tak při hledání tajnou frázi okamžitě uvidí v datech aplikace. To může mít navíc pro uživatele další následky, vzhledem k tomu, že uživatelé můžou tuto sekvenci znaků chápat jako heslo a mohou mít stejné heslo nastavené i u jiných služeb (například emailu). Druhým problémem je pak samotné zadávání sekvence do otevřeného textového pole pro vyhledávání. Současné klávesnice na mobilních zařízeních mnohdy fungují tak, že se učí často zadávaná slova nebo fráze a následně je uživateli nabízejí v našeptávači. Pokud se tedy cizí uživatel bude snažit odhalit skrytý deník, je dokonce možné, že mu při tomto pokusu klávesnice tajnou frázi sama nabídne.

8. Využitelnost výsledků

Vytvořená aplikace je zveřejněná na Google Play a je tak využitelná na mobilních zařízeních se systémem Android.

9. Otázky k obhajobě

- Jak navrhujete opravit popsané bezpečnostní problémy při skrývání deníku? Jak bude nutné upravit kód a jak uživatelské rozhraní?
- Bude možné navrhované opravy implementovat tak, aby současní uživatelé nepřišli o žádná data?

10. Souhrnné hodnocení

75 b. dobře (C)

Po stránce uživatelského rozhraní je aplikace pěkně zpracovaná. Implementovaná funkcionalita je v souladu s cílem práce spíše základní, mohla by být trochu propracovanější. Z hlediska bezpečnosti má práce několik výše popsaných nedostatků, které by nicméně v rámci případného budoucího vývoje neměl být problém opravit.

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

V Brně dne: 24. června 2020

Dobeš Petr, Ing.
oponent