

Posudek oponenta bakalářské práce

Student: Mlejnek Matěj
Téma: Fotografie s časovým razítkem (id 22050)
Oponent: Herout Adam, prof. Ing., Ph.D., UPGM FIT VUT

- 1. Náročnost zadání** **průměrně obtížné zadání**
Zadání je poměrně komplexní - vytvořit mobilní aplikaci zajišťující bezpečnost, řešitel kromě toho vytvářel i server.
Vytvořená aplikace a celé řešení je hodně základní a k průkaznému a bezpečnému řešení zůstala většina práce ještě nenaplněná.
- 2. Splnění požadavků zadání** **zadání splněno**
Zadání bylo formálně naplněno, ale návrh řešení není postavený na hlubších úvahách: ani o uživateli, ani o bezpečnosti. Vytvořené řešení tedy působí dojmem poměrně naivního náčrtu řešení.
- 3. Rozsah technické zprávy** **je v obvyklém rozmezí**
- 4. Prezentační úroveň předložené práce** **65 b. (D)**
V textu chybí důležité informace, které jsou zásadní pro návrh celého systému a mobilní aplikace.
Zejména: kdo je uživatelem aplikace, jaké jsou případy užití, co má aplikace uživateli přinést? Šifrovací klíče jsou uloženy "kdesi" v souborovém systému mobilního zařízení - není diskutována bezpečnost a hlavně jak "pojišťovací agent" bude s těmito klíči bezpečně pracovat pro ověření, atp.
Dále také: jakou úlohu systém vlastně řeší? Jak zvýší bezpečnost fotodokumentace? Kdo a jak a kdy bude ověřovat časové razítko fotografie?
- 5. Formální úprava technické zprávy** **60 b. (D)**
Po formální stránce je práce poměrně nekvalitní. Mnohé obrázky se schématy jsou vloženy rastrově a proto jsou nekvalitní. Práce obsahuje velké množství jazykových chyb i překlepů, které znepříjemňují čtení. Také formátování textu má daleko k dokonalosti. Mnoho kapitol není číslovaných, takže se na ně nedá odkazovat.
- 6. Práce s literaturou** **70 b. (C)**
Práce cituje opravdu impozantní množství zdrojů.
Mohlo by být užitečnější, kdyby se řešitel zaměřil na menší množství zdrojů a extrahoval z nich opravdu podstatné informace: Jak navrhnout UI aplikace, aby co nejlépe sloužila uživateli? Jak navrhnout systém podepisování tak, aby byl **bezpečný** a **užitečný**?
- 7. Realizační výstup** **50 b. (E)**
Uživatelské rozhraní mobilní aplikace a zejména webové aplikace má velice daleko ke kvalitnímu řešení (příloha B).
Je-li cílem vytvořit nástroj, který umožní prokázat čas pořízení fotografie, je na pováženou, že systém podepisování provádí pouze jednou za 24 hodin - to je pro mnoho aplikací naprosto nepřijatelná granularita. Zdrojové soubory jsou ZCELA bez komentářů.
Ve zdrojovém kódu internetového serveru je přímo napsán příkaz pro připojení k MySQL přes uživatele root s prázdným heslem - to není dobré znamení v bakalářské práci, která cituje 60 zdrojů z oblasti kryptografie a bezpečnosti.
Zdrojové kódy vůbec neošetřují výjimečné stavy a chyby - program je spíše takový první proof-of-concept než hotové, odladěné řešení.
Řešitel neodevzdal žádnou přeloženou verzi, ani server není k dispozici online. Ve zdrojových kódech jsou zároveň vymazány konkrétní URL, kde řešitel svoje řešení vyvíjel, takže odevzdané řešení není možné zprovoznit a vyzkoušet. Zároveň není odevzdané žádné video nebo jiný způsob demonstrace, který by ukázal, jak řešení funguje.
- 8. Využitelnost výsledků**
Ne.
- 9. Otázky k obhajobě**
 - Kdo jsou uživatelé systému a jaké jsou jejich (důležité!) případy použití? (stručně prosím, využijte vhodných ilustrací)
 - Jak bezpečné je navržené a vytvořené řešení? Kde jsou slabiny bezpečnosti?
- 10. Souhrnné hodnocení** **50 b. dostatečně (E)**

Vytvořená mobilní aplikace a celý systém mají velice daleko k použitelnosti. Z textu vlastně vůbec není patrné, kdo by měl být uživatelem a jakým způsobem by měl vytvořené řešení používat.

Téma práce - pořizovat fotografie, u kterých je opravdu prokazatelný čas pořízení - bylo vyřešeno přamalo a text se analýzou tohoto problému přamalo zabývá.

Odevzdané řešení nejde bez dalšího zprovoznit a řešitel neodevzdal binární verze, ani žádné provozovatelné demo, ani třeba videozáznam použití svého řešení.

Formální kvalita textu je slabá.

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

V Brně dne: 27. května 2019

.....

podpis