FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Josef Kokeš
Student:	Patrik Suchopa
Název práce:	Monitorování nechtěného sledování uživatelů mobilními telefony na platformě Android
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	25. května 2022

Hodnotící kritéria

1. Splnění zadání

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

Jak chápu zadání, tak bylo v zásadě splněno, ale není jasné, jestli v takové míře, aby to bylo užitečné. Student provedl velké množství měření, které nějak interpretoval, zároveň ale nijak zvlášť neřešil teoretické základy, na kterých ta měření a jejich vyhodnocení stojí - prostě zachytil využití CPU a paměti a cílové domény komunikací a popsal změny v různých scénářích. Jestli ta měření byla relevantní, jestli pozorované změny něco říkají a jestli to nešlo udělat lépe, tím se příliš nezabývá. Na druhou stranu nemohu vyloučit, že přesně tohle měl student udělat.

Co jednoznačně není splněno je požadavek na prozkoumání vytipovaných potenciálně škodlivých aplikací. Student to vysvětluje už tak značným rozsahem měření, což má pravdu, očekával bych ale, že provede aspoň to vytipování aplikací, které by se mohly zkoumat v navazující práci.

2. Písemná část práce

35 / 100 (F)

Při pohledu do obsahu se může písemná část práce zdát velmi rozsáhlá, ve skutečnosti to tak ale není. Drtivou většinu textu tvoří tabulky a grafy jednotlivých měření, samotný text je spíše v menšině. To je obzvlášť bolestivé v úvodních částech, které jsou všechny extrémně povrchní a podle mě zcela nedostačující pro jejich hlavní účel - připravit stabilní podklad, na kterém se může postavit jádro práce. Skutečně relevantní mi přijdou sekce 5.2 a 6.2-6.4, t.j. asi tři stránky. Očekával bych detailní rozbor toho, co chce student měřit a proč to chce měřit (co si od příslušného měření slibuje ve vztahu k zodpovězení klíčové otázky zadání, tedy jestli je možné, že mobilní telefon může být zneužit pro

sledování uživatele bez jeho vědomí); to ale v práci nenacházím. Student prostě očekává, že nárůst veličiny X v procesu Y znamená, že proces Y vykonává činnost relevantní pro zodpovězení otázky výše, aniž by ale řekl, proč to očekává.

Za velmi podezřelou považuji použitou metodiku. Rovnou přiznávám, že ji jenom odhaduji, protože nikde není systematicky popsána, ale podle zadání i argumentace zřejmě byla myšlena tak, že se systém uvede do určitého definovaného stavu (které potenciálně prozrazující technologie jsou vypnuty a které zapnuty, která aplikace je spuštěna a která ne, apod.), proběhne dlouhodobější měření různých veličin, následně se jedna z charakteristik stavu změní, opět proběhne měření a výsledky měření se porovnají. Což by bylo naprosto v pořádku, kdyby to bylo provedeno precizně. To se ale z textu nedá poznat - pokud to chápu dobře, v telefonu byly zapnuty resp. vypnuty příslušné sledované parametry, ale neproběhl vůbec žádný pokus o dosažení stejného celkového počátečního stavu, co se týká všech ostatních veličin. Pak proběhlo měření, v každém scénáři jinak (na pohled náhodně) dlouhé, které student vykreslil do grafu a metodou "kouknu a vidím" interpretoval, co se dělo. Interpretace samotná vesměs není zdůvodněná, případné zvláštnosti (např. pravidelnosti ve vykresleném grafu) nejsou zkoumány a závěry se nesou v duchu "spotřeba zdroje X byla vyšší/nižší než v předchozím scénáři". Zarážející je naprostá nepřítomnost jakéhokoliv statistického aparátu, i kdyby mělo jít o pouhé použití průměru.

Po jazykové stránce jsem si všiml většího množství chyb v čárkách, jinak ničeho, co by vybočovalo z běžného standardu.

3. Nepísemná část, přílohy 50 /100 (E)

Nepísemná část je nesmírně rozsáhlá, tvoří ji především provedená měření (skoro 700 tisíc souborů!) a následně skripty pro zpracování těchto dat. Nemám důvod nevěřit, že zpracování probíhá podle specifikací, na druhou stranu vzhledem k výhradám v předchozí části není jasné, jestli to zpracování je účelné.

4. Hodnocení výsledků, jejich využitelnost 50 /100 (E)

Obdobně jako u nepísemné části je pro mě obtížné zhodnotit, jestli má vytvořená práce praktický přínos. Mohla by mít, dokonce nelze vyloučit, že má, ale kvůli nedostatečné textové části nemáme žádný objektivní důvod se přiklonit na tu či onu stranu. Mohu souhlasit s tvrzením ze závěru, že odpověď na centrální otázku zadání (může být uživatel Androidu sledován bez svého vědomí?) je ANO, ovšem se zdůvodněním na takové úrovni, že jsme tutéž odpověď mohli dát i bez jakéhokoliv zkoumání.

Celkové hodnocení 50 /100 (E)

Na studentově práci lze jednoznačně ocenit množství provedených měření. Bohužel kvůli chybějícímu teoretickému základu nelze rozhodnout, co vlastně ta měření znamenají a jestli je studentova interpretace správná či nikoliv. V tomto podle mě práce zcela selhává. Lze uznat, že student investoval do získání i zpracování dat mnoho práce, vytvořil si nástroje pro analýzu, připravil si prostředí, které mu vůbec dovolilo ta data získat. Nemohu se zbavit dojmu, že velká část té práce byla zbytečná, protože řešila věci, které nejsou k zadání relevantní, ale provedena byla a ukázala, že si student osvojil něco z

toho, co od bakaláře IT očekáváme. Z tohoto důvodu mi nepřijde správné jeho práci úplně odmítnout, hodnotím ji tedy známkou E - dostatečně.

Otázky k obhajobě

1) Proč jste nepoužil standardní nástroje pro statistickou analýzu naměřených dat?

2) Můžete vysvětlit, jak probíhalo dosažení stejného výchozího stavu (až na konfigurační parametry, které jste cíleně měnil) pro jednotlivé scénáře?

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.

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.