FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Marina Shchavleva
Student:	Bc. Josef Hušek
Název práce:	Bezpečnostní analýza OnlyKey
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	25. srpna 2022

Hodnotící kritéria

1. Splnění zadání

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

Zadání autor splnil a dosáhl významných výsledků, ačkoliv bod zadání "správa kryptografických klíčů" by zasloužil větší zdůraznění.

2. Písemná část práce

60 / 100 (D)

Práce je napsána velmi neformálním stylem, autor často používá výrazy "in my opinion", "I think" a vyjadřuje svůj názor přilíš emotivním jazykem ("blatantly not true", str. 50, "cleverly notice", str. 43), který se nehodí do odborného textu. Text obsahuje nezanedbatelné množství gramatických a typografických chyb. Reference v textu nejsou korektně označeny, například "described in this section - 2.4", str 50 a "[...] can also appear (2.2)", str 15 -- v posledním případě se dá odvodit že se jedná o obrázek pouze z kontextu. Části kódu by měly mít format "Listing", nikoliv "Figure"; způsob formátování kódu použitý v textu je velmi špatně čitelný. Poměrně často se čtenář setká s použitím pojmů a akronymů dříve, než jsou vysvětlené (podsekce 2.1.1, STD a PD profily). URL by zasloužily speciální format pro odkazy. Před citací je třeba mít mezeru ("Statement[1]" vs. "Statement [1]").

Práce obsahuje rozsáhlý popis hardware a software OnlyKey, který by rozhodně mohl být kratší, bez újmy na věcném obsahu a splnění cílů práce. V textu je mnoho přímých citací; v některých případech by autor mohl zkráceně uvést jejích obsah, obzvlášť když hned potom ten obsah vysvětluje. Práce není moc dobře logicky členěná, zasloužila by lehčí změnu struktury, aby bylo zřejmé, jak autor postupoval ve splnění cílů práce.

3. Nepísemná část, přílohy 80 /100 (B)

Nepísemná část práce obsahuje upravené knihovny a firmware pro zjednodušení analýzy, nástroje třetích stran pro vývoj a ovládání OnlyKey, a pomocné skripty v pythonu. Výstupem autora jsou tedy úpravy zdrojových kódů a pomocné skripty. Pomocné nástroje jsou napsány v celku dobře, kód je rozumně členěn.

4. Hodnocení výsledků, jejich využitelnost 85 /100 (B)

Autor našel poměrně velké množství nekonzistencí mezi dokumentaci a skutečným produktem, a také nedokumentované chování, které považuji za nepřípustné v kontextu bezpečnosti. Rozhodně si myslím, že práce je přínosem pro následující vývoj OnlyKey a je motivací pro vylepšení.

Celkové hodnocení 70 /100 (C)

Autor dosáhl zajímavých výsledků, které se skrývají v textu, který se těžko čte kvůli velkému množství chyb, a těžko se posuzuje kvůli nepřímočaré struktuře. Nicméně práci doporučuji k obhajobě s hodnocením C, jelikož autor provedl velké množství analytické práce a dorazil tím k významným výsledkům.

Otázky k obhajobě

V závěru, kde mluvíte o problematice zastínění jednoho ze standardních profilů self-destruct PINem, jste zmínil, že to může být použito ke zvýšení bezpečnosti systému. Jsou v tom jiné problémy, kromě popsaného snížení kvality "user experience"?

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.