FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Filip Kodýtek, Ph.D.
Student:	Bc. Marek Kňazovický
Název práce:	Aktualizace IoT zařízení pomocí PUF
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	7. února 2023

Hodnotící kritéria

1. Splnění zadání

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

Zadání bylo splněno. Problematikou PUF na platformě ESP32 se zde již jiné závěrečné práce zabývaly - jednak z pohledu hodnocení kvality SRAM PUF, ale také z pohledu implementace knihovny, která PUF využívá (např. na generování klíče pro asymetrickou šifru). Není jasné, proč nebylo na výsledky těchto prací navázáno, zadání se mohlo primárně zabývat problematikou OTA update bez zatěžování se implementací vlastního SRAM PUFu.

2. Písemná část práce

80 / 100 (B)

Práce by mohla být přehledněji rozčleněna. Jsou zde dlouhé textové pasáže, kde by bylo vhodné buď doplnit nebo je i nahradit obrázkem/diagramem pro rychlejší pochopení. Např. popis procesu zpracování paměti SRAM pro využití v PUF je v textu velmi nepřehledné. Na pár místech jsou i drobné faktické nejasnosti - např. enrolment fáze u PUF autor zmiňuje zapamatování všech CRP (u Strong PUF přece prakticky nemožné), u vlastností PUF nestačí unikátnost, ale je nutná nepředvídatelnost (unikátnost sama o sobě toto nepostihuje), popis fuzzy extractoru vs error-correcting code je víceméně stejný, není zde jasný rozdíl. Celá práce je psaná v angličtině, což z hlediska použitelnosti výsledné implementace hodnotím kladně, je zde ale opakovaně problém s větnou skladbou, která neodpovídá angličtině, ale češtině (resp. slovenštině). Používané zkratky je vhodné při prvním použití vysvětlit.

3. Nepísemná část, přílohy 90 /100 (A)

Výsledkem je SW (knihovna) implementující PUF a demonstrace ukazující využití této knihovny pro OTA update na platformě ESP32.

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

Hlavním výstupem práce je především demonstrace využití PUF pro OTA update na IoT zařízení.

Celkové hodnocení 80 /100 (B)

Hodnocení této práce snížila její písemná část kvůli struktuře, časté nepřehlednosti způsobené přílišným lpěním na textovém popisu, namísto vytvoření obrázku diagramu, který by danou věc okamžitě vysvětlil. Také není jasný důvod proč se značná část práce zabývala implementací PUF na ESP32, přestože taková implementace již existuje. Přesto práci celkově hodnotím známkou B a doporučuji k obhajobě.

Otázky k obhajobě

Proč nebyly využity existující implementace SRAM PUF na ESP32?
Jaký podíl práce byl věnován studiu a implementaci SRAM PUF vzhledem k samotnému OTA update?
Jaký byl použit samoopravný kód na výstup PUFu?

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.