FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Filip Kodýtek, Ph.D.
Student:	Matěj Týfa
Název práce:	Použití fyzicky neklonovatlené funkce k zabezpečení TLS na platformě ESP32
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	5. června 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 bylo splněno v plném rozsahu.

2. Písemná část práce 80 /100 (B)

Práce je dobře členěna, neobsahuje zbytečné části, kladně hodnotím také volbu anglického jazyka pro napsání práce. Student správně citoval zdroje, které jsou k tématu relevantní. Písemna část přesto obsahuje určité nedostatky:
- Od pozdějších kapitol je v textu řada překlepů a gramatických chyb - působí dojmem rychlého sepsání bez kontroly.
- V sekci 4.4.3 není pořádně řečeno, co se myslí "dostatečnou neklonovatelností" - předpokládám, že to v tomto kontextu znamená, že odpověď PUFu má dostatečnou entropii. Pak se délka odpovědi PUFu musí odvíjet od požadované entropie klíče.
- Sekce 9.1 zmiňuje, že generování odpovědi PUFu je v řádech milisekund - není jasné, jestli se tím myslí deep sleep metoda, nebo reset jen samotné vybrané SRAM. Dále je řečeno, že post-processing na konvert klíče pro wolfSSL trvá dlouho - není takto hned zřejmé, co je to za proces, stál by za zmínku i konkrétní čas

3. Nepísemná část, přílohy 95 /100 (A)

Student využil knihovny implementace TLS vhodné pro ESP32, pomocí které vytvořil funkční prototyp a otestoval tak funkcionalitu použití PUF pro generování soukromého klíče pro vybrané zařízení. Zdrojové kódy jsou dobře strukturované a přehledné, místy by zasloužily lepší komentář.

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Výstupem práce je funkční prototyp využívající TLS v kombinaci s PUF. Z této implementace lze dále vycházet, např. lze použít jako dobrý základ pro složitější implementace.

Celkové hodnocení 89 /100 (B)

Práci celkově hodnotím velmi kladně, vytknul bych ji ale určité nedostatky v její písemné části. Proto se nakonec kloním spíše ke známce B.

Otázky k obhajobě

Jako budoucí vylepšení zmiňujete možnost využití jiného typu PUF. Jaký jiný PUF byste na ESP32 použil?
Co konkrétně se myslí post-processingem klíče pro wolfSSL v sekci 9.1? Jak dlouho trvá?

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.