FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Dr.-Ing. Martin Novotný
Student:	Martin Šimůnek
Název práce:	Přenosný přístupový identifikační systém využívající technologii NFC a umožňující komunikaci přes GSM bránu
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	9. června 2021

Hodnotící kritéria

1. Splnění zadání

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

Nejsem si zcela jistý, zda byl splněn 3. bod zadání: "3) Analyzujte a navrhněte bezpečné řešení s ohledem na omezené zdroje platformy Arduino.". Vysvětlení je v následujícím odstavci.

2. Písemná část práce

60 / 100 (D)

-- Autor v úvodu děkuje "svým přátelům a známým, kteří ... mu pomohli s korekturou jeho práce", nicméně obávám se, že jeho přátelé nedočetli dále nežli za první kapitolu. Práce je psaná specifickým druhem češtiny, který se používá například při komunikaci na sociálních sítích. Například, jakkoliv je text (převážně) srozumitelný, některé věty - v češtině, slovesném to jazyce - trpí absencí přísudku. Větu "Čtečka z důvodu, že jazykem pro Arduino je podmnožina jazyka C/C++." (na straně 18) jsem pak nepochopil vůbec.
-- Zaznamenal jsem jeden výskyt termínu autentizace a vícero výskytů termínu autentifikace. Doporučuji sjednotit na autentizace.
-- Kapitola Analýza v podstatě chybí. V analýze je zapotřebí rozebrat a prozkoumat všechny varianty řešení. Na základě této analýzy se následně provádí návrh. Kapitola 3 nazvaná analýza však rovnou uvádí zvolená řešení a je tak de facto součástí následujících kapitol 4 a 5. Příklad: Na straně 23 autor uvádí "Byla prozkoumána i existence ostatních knihoven, které nabízejí i jiné funkce, avšak bylo shledáno, že tyto funkce nejsou nijak zásadní pro funkčnost tohoto projektu." V této větě autor neuvádí: a) jaké knihovny byky prozkoumány, b) jaké jiné funkce tyto knihovny nabízejí a c) proč tyto funkce nejsou zásadní rpo funkčnost projektu. Koneckonců, nikde jsem v textu nenašel požadavek, jaké funkce by vlastně měla knihovna poskytovat ...

-- Text práce více popisuje "co to dělá" a "jaké prostředky jsme použili" nežli "jak to funguje". Z textu je obtížné, či spíše nemožné, například vydedukovat, jak vypadá protokol. Co se například přesně děje, když uživatel přiloží kartu ke čtečce? Jaká konkrétní data se pošlou ze čtečky na server, jaký je jejich formát a které části dat jsou zašifrovány a jak? V práci jsem nenašel žádný diagram, který by to popisoval; obrázky 3.2-3.4 jsou v tomto ohledu nedostatečné.
-- Pokud jsem to správně pochopil, autor navrhl vlastní (proprietární) protokol. Pokud to tak je, zajímalo by mě, proč autor raději nevyšel ze standardu? Vlastní tvorba představuje vysoké riziko bezpečnostních děr, a v tom případě by nebyl naplněn 3. bod zadání: "3) Analyzujte a navrhněte bezpečné řešení s ohledem na omezené zdroje platformy Arduino."

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

Přiložené médium obsahuje vytvořený software, který je, zdá se, dobře komentovaný.

4. Hodnocení výsledků, jejich využitelnost 75 /100 (C)

Měl jsem možnost vidět prototyp, který se zdá být funkčním. Vzhledem k tomu, že klíčové části návrhu (protokol) nejsou důkladně zdokumentovány, nelze ověřit bezpečnost tohoto zařízení. Pokud navíc byl protokol navržen přímo autorem, pak jsou obavy o bezpečnost tohoto zařízení oprávněné. V tomto ohledu práce nesplňuje soudobé standardy vývoje kryptografických zařízení.

Celkové hodnocení 70 /100 (C)

Zařízení je, zdá se, funkční. Hodnocení snižuji vzhledem k písemné části práce, kdy analýza de facto chybí, a některé klíčové části návrhu jsou nedostatečně zdokumentované.

Otázky k obhajobě

1. Co se přesně děje, když uživatel přiloží kartu ke čtečce? Jak vypadá protokol? Jaká konkrétní data se pošlou ze čtečky na server, jaký je jejich formát a které části dat jsou zašifrovány a jak?
2. Pokud jsem to správně pochopil, autor navrhl vlastní (proprietární) protokol. Pokud to tak je, zajímalo by mě, proč autor raději nevyšel ze standardu? Vlastní tvorba představuje vysoké riziko bezpečnostních děr, a v tom případě by nebyl naplněn 3. bod zadání: "3) Analyzujte a navrhněte bezpečné řešení s ohledem na omezené zdroje platformy Arduino."

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. 26/2017, 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.