FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Maroš Mačak
Oponent práce:	Ing. Jiří Buček, Ph.D.
Název práce:	Inteligentní bezpečnostní systém – sekce zabezpečený vstup
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 12. 6. 2019

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
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.

Komentář:
Student splnil zadání.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*85 (B)*

Popis kritéria:
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.

Komentář:
Práce je logicky členěna a přehledná. Po obsahové stránce bych studentovi vytknul poněkud povrchní popis standardů a zkoumaných čteček v kapitole 2.6. Volba algoritmu HMAC pro odvození diverzifikovaných klíčů pro čipové karty není zcela opodstatněna. Zvolený algoritmus je bezpečný, ale vzhledem k omezené paměti mohl student použít stejný základní algoritmus pro autentizaci i odvozování klíče, tj. buď v obou případě AES, nebo HMAC.

Po formální stránce obsahuje jen drobné chyby, například na začátku kapitoly před první podkapitolou by bylo vhodné napsat aspoň odstavec o tom, co je obsahem dané kapitoly. Ve své práci student nechává tyto části prázdné.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*75 (C)*

Popis kritéria:
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

Komentář:
Přílohou jsou zdrojové kódy pro Arduino a pro Java kartu. Rovněž jsou přiloženy zdrojové kódy knihoven pro Arduino, které student použil ve své práci. Student označil svoje zdrojové kódy názvem bakalářské práce, ale v kódech pro Arduino kromě souboru Main.ino nenapsal svoje jméno. Bylo by vhodnější, kdyby student svým jménem označil každý zdrojový soubor, který vytvořil.

Ve zdrojovém souboru k čipové kartě má student chybu při alokaci dočasného pole při obsluze instrukce INSTR_ENCRYPT. Volání JCSystem.makeTransientByteArray sice vytváří pole v tranzientní paměti, tj. RAM, ale alokace samotná je perzistentní. To znamená, že po nějakém počtu autentizací karta přestane fungovat, protože dojde tranzientní paměť, tato metoda pokaždé vyvolá výjimku, a karta odešle chybový status word.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*85 (B)*

Popis kritéria:
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.

Komentář:

Výsledkem je pěkná demonstrace použití čipových karet při zabezpečení garáže. V aktuální podobě se jedná se spíše o výukovou pomůcku, jelikož pro ostré nasazení by bylo nutno řešit mnoho dalších problémů včetně mechanické odolnosti, zálohování při výpadku napájení apod., a i bezpečnost zařízení by musela projít důkladnější analýzou. Pro další rozvoj systému by možná bylo vhodné přejít na jinou platformu základní desky s větším množstvím dostupné paměti (to ale nebylo úkolem studenta).

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*
5. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

Jak byste vyřešil výše zmíněný problém s nadbytečnou alokací dočasného pole při INSTR_ENCRYPT?

Ve své práci píšete, že při obsazení paměti flash v Arduinu nad určitou mez (ale ne 100%) přestane být program stabilní, a proto jste musel odstranit některé části programu. Takové chování je podivné, spíš to vypadá, jako by došla RAM (přepsání dat zásobníkem). Sledoval jste i obsazení paměti RAM?

Uvažoval jste scénář útoku, kdy pasivní útočník odposlouchává komunikaci s čipovou kartou při inicializaci klíče? Jak byste případnou zranitelnost ošetřil?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*85 (B)*

Popis kritéria:
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.

Text hodnocení:

Studentova práce je zdařilá. Přestože student narazil na mnoho problémů s testovanými čtečkami karet, dokázal se s nimi vypořádat a vytvořit funkční celek. Práci hodnotím jako velmi dobrou.

Podpis oponenta práce: