Posudek oponenta závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Bc. Jan Vojíř
Oponent práce: Ing. Tomáš Čejka
Název práce: Přístupový systém s využitím RFID karet
Obor: Návrh a programování vestavných systémů

Datum vytvoření: 4. 6. 2017

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	*1=mimořádně náročné zadání,* *2=náročnější zadání,* ***3=průměrně náročné zadání,*** *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Práce se zabývá návrhem a realizací přístupového systému postaveném na technologii RFID. V současné době již existuje spoustu hotových komerčních řešení, avšak tato práce si klade za cíl sestrojit levnější variantu s použitím vybraných dostupných součástek.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. 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 splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Na základě předloženého textu práce a demonstračního videa, vytvořeného studentem, se zdá být prototyp funkční. Během čtení práce a analýzy zdrojových kódů jsem však bohužel ve studentovo řešení nezískal důvěru. Od inženýrské závěrečné práce s názvem "Přístupový systém..." očekávám mnohem větší důraz na bezpečnost, zatímco předložený text ukazuje na základní neznalosti studenta v této oblasti.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	*1=splňuje požadavky,* ***2=splňuje požadavky s menšími výhradami,*** *3=splňuje požadavky s většími výhradami,* *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Rozsah práce sice splňuje požadavky, ale počet stran je zvýšen sekcemi, které naprosto nesouvisí se zadáním práce. Student se například několikrát zmiňuje o použití klávesnice pro zadání hesla (PINu), přičemž v zadání je jasně uvedeno použití RFID karet.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*49 (F)*

Popis kritéria:
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.

Komentář:
Jako minoritní nedostatek práce vnímám politické a ekonomické úvahy, které jsou podle mého názoru naprosto irelevantní nebo dokonce nežádoucí pro text diplomové práce technického oboru. Při čtení jsem však narazil na tvrzení, které naprosto odporuje základním znalostem a tzv. best practices, které by inženýr informatiky měl znát.

Tvrzení, že šifrování a použití certifikátů není potřeba, ukazuje na zcela zásadní bezpečnostní slabinu celého systému. Navíc vedle autentizačních údajů posílaných nezabezpečeným komunikačním kanálem byl v práci použit mechanismus autentizace HTTP AUTH BASIC. To znamená, že uživatelské heslo správce, který je schopen upravovat seznam povolených RFID čipů, je možné jednoduše zjistit pouhým zachycením komunikace a triviálním dekódováním base64 řetězce.

Uložení čitelné podoby hesla ve zdrojových kódech programu považuji také za závažnou chybu. Dnes se běžně používá ukládání hesel v podobě otisků vzniklých hašováním hesla a soli. Dále mám pochybnosti i o předložených zdrojových kódech, kde jsem nenašel ošetření vstupních parametrů, což vede k domněnce, že systém by mohl být zranitelný na SQL injection.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*70 (C)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.

Komentář:
Práce obsahuje překlepy, přesahy a typografické chyby. Jako zásadnější problém vidím jazykovou stránku práce, kde student používá často příliš subjektivní hovorové prostředky namísto striktně objektivního technického hodnocení založeného na výsledcích měření nebo citovaných faktech. (příklady: Úvod: "vítězí cenově na plné čáře a pokud jde o funkčnost a praktičnost implementace a používání, také nemá konkurenci"; Kapitola 1: "který nabral směr raketovou rychlostí" a další.)

Zdrojové kódy nejsou dostatečně (téměř vůbec) dokumentovány, obsahují zakomentované bloky kódu, které ve finální verzi (tzn. odevzdané) již podle mého názoru nemají být.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*60 (D)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Práce obsahuje relativně hodně citovaných zdrojů (celkem 81), ale o jejich nutnosti a vhodnosti mám místy pochybnosti. Myslím, že citace čerpané z encyklopedie Wikipedia jsou snadno nahraditelné jinými, možná důvěrychodnějšími zdroji. Citace jsou občas nevhodně použité, takže v textu není na první pohled jasné, k čemu se citace vztahuje. Výběr některých citací je značně nevhodný např. [44] Ethernet, kde by čtenář čekal spíše odkaz na oficiální dokumenty specifikace. Citace [11] na první pohled neodpovídá citačním zvyklostem a normám.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*50 (E)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Práce neobsahuje žádné výsledky, které by se daly publikovat. Pro realizaci přístupového systému student použil existující technologie a součástky a výsledek není nikterak výrazně inovativní oproti existujícím řešením.

Kapitola 4, která by měla obsahovat popis otestování práce, je stručná a nenabyl jsem dojmu, že 3 stránky textu obsahují popis dostatečného otestování zabezpečovacího systému. Navíc zmíněné 3 stránky obsahují i sekci s výpočtem ceny řešení, kde student zanedbává jakoukoliv cenu práce. Z ekonomického hlediska tento přístup u kalkulace není vhodný.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Předložená práce se zdá být na první pohled funkční.
Po detailnějším prozkoumání mám obavy, že přestože se studentovo řešení tváří jako levnější, po stránce bezpečnosti nevypadá důvěryhodně.
Vzhledem k tomu, že se "levná, ale nezabezpečená řešení" celosvětově ukazují být velkým problémem (velké DDoS útoky z IoT zařízení připojených do internetu), domnívám se, že u diplomové práce je nutné přikládat bezpečnostním aspektům velkou důležitost.
Bezpečnost by měla být v této práci mnohem více akcentována už jen z toho důvodu, že přístupový systém je jedním z bezpečnostních prvků všude tam, kde se takový systém nasazuje.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	
Popis kritéria: Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).	
Otázky: Prosím o stručné odpovědi na následující otázky: 1) V práci tvrdíte, že použití certifikátů je drahé. Co je to letsencrypt.org a co je potřeba k získání certifikátu podepsaného důvěryhodnou CA? 2) Co znamená, když je certifikát self-signed? Jaké bezpečnostní riziko takový certifikát představuje? 3) Jakým způsobem je možné vytvořit vlastní certifikační autoritu? Dalo by se to využít pro proprietární přístupový systém?	

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*49 (F)*
Popis kritéria: Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.	
Text hodnocení: Předložená práce obsahuje řadu nedostatků, které je nutné opravit. V současné podobě podle mého názoru nesplňuje požadavky na kvalitní diplomovou práci, kterou je možné obhájit.	

Podpis oponenta práce: