Posudek vedoucího diplomové práce

„OPTIMALIZACE DATOVÉ KOMUNIKACE V ODBAVOVACÍCH SYSTÉMECH V DOPRAVĚ“

studentky Bc. Moniky Andršové

Pro svou práci si studentka vybrala téma zabývající se technologií bezkontaktních čipových karet MIFARE v oblasti odbavovacích systémů v dopravě, konkrétně porovnáním dvou vývojových řad karet: MIFARE Classic a MIFARE DESFire. Hlavním cílem práce bylo na základě znalostí základních principů a mechanismů získaných v teoretické části provést optimalizaci datové komunikace probíhající mezi kartou a čtečkou. Optimalizace byla provedena návrhem vhodné struktury uložených dat v paměti a specifikací bezpečnostních mechanismů zaručujících požadovanou úroveň zabezpečení.

Studentka pracovala svědomitě, samostatně, před samotným zahájením práce se pečlivě seznámila jak s poměrně rozsáhlou problematikou technologií bezkontaktních čipových karet, tak s přehledem aplikací v odbavovacích systémech, které se na dané karty umisťují.

Po celou dobu studia se účastnila pravidelných konzultací své práce, své nápady a výsledky diskutovala nejen s vedoucí diplomové práce, ale i s širším kolektivem akademických pracovníků Ústavu aplikované informatiky a s odborníky z Výpočetního a informačního centra ČVUT.

Krom teoretické práce studentka věnovala velké množství času návrhu 6 aplikací pro bezkontaktní čipovou kartu. Velkou pozornost věnovala přípravným pracím včetně namodelování každého procesu v aplikaci QPR. Dále navrhla vlastní strukturu a zabezpečení jednotlivých aplikací pro dvě technologicky odlišné platformy karet MIFARE.

Po formální stránce práce splňuje všechny náležitosti očekávané od diplomové práce. Rozsah vlastního textu je 113 stran, dále práce obsahuje seznam použité literatury a internetových zdrojů, seznam obrázků, seznam tabulek a seznam příloh a poté následují 4 vlastní přílohy: Proces výběru karty MIFARE, Struktura paměti MIFARE Classic, Bloková schémata karet MIFARE a Procesní model využití multiaplikační karty.

Celá práce je rozdělena do 2 hlavních částí a 5 kapitol.

První teoretická část je rozdělena na dvě kapitoly.

První kapitola se věnuje teorii odbavovacích systémů v dopravě.

Druhá kapitola je seznámením s teoretickými základy bezkontaktních čipových karet, technologií karet MIFARE, včetně používaných standardů, popisu adresáře aplikací MAD a způsobů zabezpečení dat. Pozornost je též zaměřena na rychlost zpracování operací. V závěru této kapitoly jsou porovnány dvě nejrozšířenější řady karet MIFARE, vůbec první řada versus řada o 12 let mladší, podporující již technologii „smart“ karet.

V teoretické části je hlavním přínosem podrobná rešeršní činnost seznamujících čtenáře se základními principy datové komunikace probíhající mezi bezkontaktními čipovými kartami MIFARE a odbavovacím terminálem. Dále je zde popsána struktura paměti karty a pravidla ukládání dat v ní. Je vysvětlen princip vyhledávání a zabezpečení dat uložených na kartě, přenášených během komunikace i právě zapisovaných do paměti. Na závěr je zmíněn vliv tohoto zabezpečení na rychlost provádění transakcí, která je důležitým parametrem většiny komerčních aplikací.

V druhé praktické části se studentka zabývá návrhem struktury šesti aplikací podporujících procesy odbavení cestujících a jejich zabezpečením na MIFAREClassic a MIFARE DESFire. Je zde ukázáno, která řada karet MIFARE je vhodnější pro použití v oblasti moderních procesů odbavení cestujících.

Tato část má 3 kapitoly (kapitola 3 až kapitola 5).

V třetí kapitole studentka popisuje použité role subjektů vůči kartě.

Čtvrtá kapitola je stěžejní částí celé práce a zabývá se konkrétními návrhy jednotlivých aplikací na kartě.

Praktická část práce se zabývá optimalizací komunikace karta–terminál za účelem zvýšení efektivity procesů odbavovacích systémů v dopravě. Optimalizace je prováděna na základě vhodného uspořádání datové struktury nahraných aplikací a nastavení odpovídající úrovně zabezpečení dle citlivosti uložených dat vzhledem k nejlepšímu poměru zabezpečení/rychlost.

Ve výsledku je navrženo šest samostatných aplikací, konkrétně se jedná o aplikace Personalizace karty, Elektronická peněženka, Jízdní doklad, Sleva, Věrnostní program a Bike sharing. Při návrhu jsou specifikovány jejich jednotlivé funkce, které mnohokrát nemají význam pouze pro aplikaci samotnou, ale podporují také procesy ostatních aplikací uložených na kartě. Je navržena taková struktura dat a jejich způsob zabezpečení, aby výsledné aplikace měly co možná nejširší záběr využití při schopnosti poskytovat kvalitní služby, které jsou schopny splnit různé kombinace přání uživatele karty.

Následuje poslední kapitola se závěrečným zhodnocením.

Celý text je doplněn mnoha obrázky a tabulkami dokreslujícími dosažené výsledky.

Mohu konstatovat, že studentka splnila zadání diplomové práce, práce je kvalitně zpracována jak po jazykové, tak po věcné stránce.

Velmi kladně hodnotím, že studentka pracovala po celou dobu studia svědomitě, práci průběžně konzultovala.

Konstatuji, že jde o kvalitní práci, na kterou mohou dále navázat další studenti v projektu „ Identifikace a její aplikace v oblasti dopravy“. Struktury jednotlivých aplikací tak, jak jsou navržené v této práci, mohou být inspirací pro další výzkum na toto téma a při návrhu vlastních aplikací v prostředí technologií bezkontaktních čipových karet.

Práci doporučuji k obhajobě a hodnotím ji známkou A – „výborně“.

Ing. Jana Kaliková, Ph.D

Ústav aplikované informatiky v dopravě

V Praze dne 07.01. 2016