Recenzní posudek diplomové práce

Bc. Jan Bouda: Aplikace IQ House – ovládání inteligentního domu pomocí zařízení iPad

Hlavním cílem hodnocené DP bylo navrhnout a implementovat mobilní aplikaci pro řízení inteligentních domů. Celá práce je tedy výrazně prakticky zaměřena.

V úvodu práce autor nejprve popisuje dostupné aplikace pro řízení inteligentních domů včetně jejich porovnání a shrnutí jejich možností použití. Dále autor popisuje stávající webovou aplikaci IQ House a technologii PhoneGap, která je použita pro vytvoření výsledné aplikace.

V realizační části (kapitoly 5 a 6) autor nejprve popisuje návrh mobilní aplikace. V rámci návrhu je popsán výběr programovacího jazyka, výběr knihoven a frameworků a výsledné rozložení mobilní aplikace. Dále jsou zde popsány úpravy nadřazené aplikace pro správnou funkčnost výsledné aplikace. V kapitole 6 jsou již popsány jednotlivé funkce a jejich implementace včetně začlenění frameworku AngularJS do mobilní aplikace.

K práci je přiložené CD, které obsahuje text diplomové práce, distribuci PhoneGap a aplikaci vzniklou v rámci diplomové práce.

Práce je dobře strukturovaná. Autor nejprve popisuje technologie, u kterých také uvádí zdroje. Teprve poté popisuje jejich použití ve výsledné aplikaci. V celé práci jsem objevil minimum pravopisných chyb, což zlepšuje její čitelnost.

Na autorovi oceňuji, že musel nastudovat velké množství knihoven a frameworků, které v následně v práci spojil a použil pro vytvoření finální aplikace. Navíc v rámci práce nevytvářel jen mobilní aplikaci, ale také musel přizpůsobit nadřazenou aplikaci, která je již hotová a autor tudíž musel nastudovat i její funkčnost. Dále také oceňuji, že autor v rámci přílohy sepsal návod na vytvoření vlastního pluginu do PhoneGapu, což může pomoci budoucím vývojářům, kteří budou potřebovat také napsat vlastní plugin v tomto prostředí.

K celé práci bych měl výtku vzhledem k bezpečnosti. Autor uvádí, že pro komunikaci se serverem je možné použít protokol *https*. Nicméně je to pouze možnost, takže předpokládám, že se běžně používá protokol *http*. V tomto případě je tedy možné odposlechnout celou komunikaci pro nastavení jednotlivých komponent v domě (např. posloupnost pro odzabezpečení a pro otevření garáže). Zároveň je možné i odposlechnout vysílání zašifrovaného hesla, pro jehož zašifrování byl použit algoritmus MD5. Tento algoritmus byl ale shledán zranitelným a pro rozluštění původního textu (hesla) je možné použít tzv. rainbow attack. Dokonce existují webové stránky, které se o toto rozluštění pokoušejí on-line. Nicméně autor uvádí, že na bezpečnost aplikace se zaměří v budoucí práci a navíc bezpečnost je v tomto případě spíše záležitost serveru, nikoli mobilní aplikace. Pokud server jiné zabezpečení nepodporuje, těžko se přidává do mobilní aplikace. Implementace serveru nebyla cílem práce.

SOUHLASÍ
S ORIGINÁLEM

V citované literatuře autor hojně využívá on-line zdroje, což se dá vzhledem k povaze výsledné aplikace očekávat. Veškerou citovanou literaturu považuji za relevantní.

K předložené práci mám následující dotazy:

- V práci uvádíte, že používáte MD5 pro šifrování přenášeného hesla. Umožňuje Váš program použít i jiné hashovací algoritmy? Pokud ne, jako dlouho by trvalo přidání jiného hashovacího algoritmu do aplikace?
- V práci uvádíte, že komunikace **může** běžet po šifrovaném protokolu *https*. Uveďte, jak moc je v tomto případě aplikace odolná proti odposlechu (pokud uživatel použije např. veřejný Wi-Fi přístupový bod).

Závěrem konstatuji, že diplomant při zpracování DP prokázal jak odpovídající teoretické znalosti, tak i potřebnou programátorskou zkušenost. Výtka, kterou jsem uvedl výše, je spíše námět na budoucí práci nežli výtka přímo k diplomové práci. Diplomovou práci proto doporučuji k obhajobě a hodnotím stupněm

Výborně

V Plzni dne 26.8.2013

Pavel Bžoch
.....

Ing. Pavel Bžoch

SOUHLASÍ
S ORIGINÁLEM

Západočeská univerzita v Plzni
Fakulta aplikovaných věd
katedra informatiky a výpočetní techniky
②