HODNOCENÍ RECENZENTA BAKALÁŘSKÉ PRÁCE

Autor práce:	**Jan Podavka**
Vedoucí práce:	**Ing. Jaromír Veber, Ph.D.**
Recenzent práce:	**Ing. Tomáš Klíma**
Kvalifikace recenzenta:	KSA FIS VŠE, Bezpečnostní analytik ČNB
Název práce:	**Webové aplikace a vliv šifrování na jejich rychlost**
Cíl práce (viz zadání):	Zhodnotit vliv vybraných šifrovacích algoritmů na rychlost webové aplikace a velikost databáze.
Povaha bakalářské práce:	analýza problémové situace

V hodnocení používejte stupně 1-4 (výborně / dobře / podprůměrně / nevyhovuje) – vybraný stupeň zaškrtněte křížkem.

	1	2	3	4		1	2	3	4
Náročnost tématu									
Aplikace teoretických znalostí	☒	☐	☐	☐	Podkladové materiály a literatura	☐	☒	☐	☐
Praktické dovednosti a zkušenosti	☒	☐	☐	☐	Originalita tématu	☐	☒	☐	☐
Věcné aspekty (obsahová stránka)									
Splnění cíle práce	☒	☐	☐	☐	Výběr a vhodnost použitých metod	☐	☒	☐	☐
Závěry práce (jasné a srozumitelné)	☐	☒	☐	☐	Logická stavba práce	☐	☒	☐	☐
Vlastní přínos studenta	☒	☐	☐	☐	Hloubka provedené analýzy	☐	☒	☐	☐
Formální aspekty práce									
Práce s literaturou (citace)	☐	☒	☐	☐	Úprava (text, obrázky, popisky, ...)	☐	☒	☐	☐
Jasnost a srozumitelnost formulací	☐	☒	☐	☐	Jazyková úroveň, pravopis	☐	☐	☒	☐

Navržená známka:	**VELMI DOBŘE**

Navržená známka není žádnou formou průměru z výše uvedených kritérií, jedná se o celkové hodnocení práce.

V Praze dne 6. června 2014

podpis recenzenta BP

Doplňující otázky a připomínky k obhajobě:

Autor se v práci soustředí na problematiku vlivu šifrování na rychlost webových aplikací.

V první části seznamuje čtenáře se základními pojmy a principy kryptografie, dále představuje jednotlivé šifry, z nichž u některých je v praktické části ověřen jejich vliv na rychlost webové aplikace s použitím testovací platformy Raspberry Pi.

Na práci hodnotím kladně vysokou úroveň odbornosti, která je patrná z provedení testů v poslední části, stejně tak výběr testovací platformy Raspberry Pi, která je v současné době pro podobné experimenty značně populární.

Práce neobsahuje terminologický slovník a řešerše je značně minimalistického rozsahu. Teoretické kapitoly jsou značně deskriptivního charakteru a předkládají základy kryptografie, které jsou nutné k pochopení praktické části. Kapitola 5.10 by buď měla obsahovat kompletní výčet známých zranitelností webových apikací (např. dle OWASP top ten), nebo by měla být vynechána.

Jazyková a slohová úroveň je místy na hraně akademického stylu, autor se v některých kapitolách vyjadřuje až příliš heslovitě, také by měl zvážit použití 1.os. j.č.

vzor formuláře: září 2010

Části 8.1 Zhodnocení šifrování dat ve webové aplikaci a 8.2 Přínosy práce by měly být umístěny před závěrem a část 8.1 by zasloužila přepracování a rozšíření.

Na základě výše zmíněného navrhuji hodnotit stupněm VELMI DOBŘE.

Otázky:

Jaké výsledky autor očekává, pokud by se pro představený experiment využil výkonný server (namísto relativně slabého Raspberry Pi), u kterého by průběh experimentu významněji nezatížil žádný systémový zdroj?

V případě potřeby pokračujte na další stránce.

vzor formuláře: září 2010