



Posudek vedoucího bakalářské práce

Jméno studenta: Petr MORAVEC
Téma práce: Bezpečné autentifikované bezdrátové připojení
Cíle práce: Popsat slabiny a úskali bezpečného bezdrátového spojení a navrhnout bezpečné autentifikované bezdrátové připojení k síti odolné vůči neoprávněným uživatelům. Realizovat server, který bude řídit autentifikaci uživatelů a logovat přístupy jakož i neoprávněné pokusy o připojení.

Náročnost zadání bakalářské práce na:

- teoretické znalosti: vyšší,
- praktické zkušenosti: vyšší,
- podkladové materiály (vstupní data) a jejich zpracování: střední.

A. Slovní hodnocení:

Naplnění cíle práce:
Práce poskytuje přehled zabezpečení bezdrátových sítí, navrhuje řešení a implementaci, čímž splňuje stanovené cíle. Nicméně bych si představoval, že poskytne větší přehled možných zařízení AP pro vybrané řešení zabezpečení připojení.
Logická stavba a stylistická úroveň práce:
Text je logicky členěn do navazujících kapitol, nicméně na některých místech popis neodpovídá logickým krokům. Např. na str. 29 student nejprve tvrdí, že je nutné nainstalovat databázi MySQL, a teprve v následující sekci zmiňuje, že vlastně databáze MySQL nutná není, ale že ji zvolil sám. V další sekci navíc zmiňuje možnost správy uživatelů zcela bez jakékoli databáze. V práci se vyskytují chyby, zejména ve shodě rodu (např. str. 10: „tyto místa“, str. 11: „volba by mohlo“, str. 20: „mohou být využity hesla“, str. 26: „jsou vhodné všechny uvedené zabezpečení“, „Všechny zabezpečení jsou“, str. 27: „tyto zabezpečení neumožňují“, str. 29: „MySQL databáze není obsažen“) a jiné (např. „obranou je v aktualizace firewall“ na str. 16, kde navíc mělo být místo „firewall“ slovo „firmware“, rozdělení „Route-/rOS“). Kapitola 5 (Nastavení klienta) sice pojednává o nastavení klientské části serveru RADIUS, ale nejedná se o nastavení klientského Wi-Fi zařízení. Titulek je proto mírně zavádějící.
Využití záměrů, námětů a návrhů v praxi:
V praxi dobře využitelné pro organizace, které potřebují dát svým uživatelům možnost bezdrátového připojení (středního až většího rozsahu) k síti, ale připojení cizích uživatelů je nežádoucí.
Případné další hodnocení (připomínky k práci):
Chybí shrnutí (zhodnocení) kapitoly 1.5 (WPA a RADIUS). Na str. 25 se říká, že jedinou možností pro řešení pro síť s kontrolovaným přístupem je server RADIUS bez bližšího zdůvodnění. Nicméně lze si představit zabezpečení i na jiné úrovni než přímo na úrovni Wi-Fi, případně jinou metodu než RADIUS. Na str. 28 se tvrdí, že „Cena serveru se pohybuje od 15 000 Kč.“, což je v kontrastu s tvrzením na str. 27, že – cituji „RADIUS server není hardwarově náročný, proto stačí pro provoz i méně výkonnější server nebo server pro jiné služby.“. Navíc server FreeRADIUS může běžet i přímo na RouterBoardu, pokud se RouterOS nahradí Linuxem (např. distribucí OpenWrt), což je mnohem levnější než celý server. Nadpis 4.3.1 pak hovoří o vytvoření klíče, ale v popisu vzniklého souboru je uvedeno, že se jedná o certifikát. V navazujících sekcích je popis spousty certifikátů a klíčů, o kterých se čtenář nedozví, proč se generují a k čemu vůbec slouží.

B. Kriteriaální hodnocení:

Kritéria hodnocení práce	Úroveň	Připomínky
Úroveň dokumentu		
logická stavba práce	průměrné	
stylistická úroveň	průměrné	
práce s literaturou včetně citací	průměrné	
formální úprava práce (text, grafy, tabulky)	průměrné	
Teoretická část		
rozsah a úroveň zpracování rešerše	průměrné	Přehled zabezpečení Wi-Fi v pořádku, přehled možných AP mohl být širší.
formulace teoretických východisek pro praktickou část	průměrné	
odborné zvládnutí problematiky	průměrné	
Praktická část – produkt (řešení)		
adekvátnost použitých metod, SW, postupů	průměrné	
kvalita návrhu řešení	průměrné	
komplexnost řešení	komplexní	
návrh datových struktur	nelze hodnotit	
uživatelské rozhraní	nelze hodnotit	
odborné zvládnutí problematiky	průměrné	
rozpracovanost	dokončeno	Neměl jsme možnost řešení vyzkoušet.
využitelnost praktické části v praxi	ve větší míře	Vhodné pro nastavení kontrolovaného (autentifikovaného) zabezpečení přístupu k bezdrátovému připojení (např. ve firmách a školách).
Praktická část – popis		
popis řešení v bakalářské práci	průměrné	
ostatní přílohy (tabulky, grafy, výpočty, ...)	nelze hodnotit	
uživatelská příručka	nelze hodnotit	
Uložení dokumentu/ů bakalářské práce na CD	ano	
Uložení výsledku praktické části na CD	ano	
Stupeň splnění cíle práce	splněn	

C. Otázky k obhajobě (max. 2):

1. V první větě sekce 4.3 píšete „Certifikát je zašifrovaná informace, ...“. Co je to přesně certifikát a k čemu slouží?
Podrobněji vysvětlete význam všech klíčů a certifikátů zmiňovaných v sekci 4.3.
2. Zadání bylo vytvořeno také v souladu s požadavky sdružení hkfree.org. Bude vaše řešení sdružením využito?

Doporučení k obhajobě:

ano

Navržený klasifikační stupeň:

velmi dobře minus

Posudek vypracoval(a):

Jméno, tituly: Mgr. Tomáš Hudec

Zaměstnavatel: UPa, FEI, KIT

V Pardubicích dne 27. 8. 2010

Podpis: