Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTA BAKALÁŘSKÉ PRÁCE

Jméno studenta: David Glevický

Název práce: Zabezpečení bezdrátových sítí proti pokročilýmútokům

Autor posudku: Josef Horálek

Cíl práce: Cílem práce je podrobně představit standardizované prostředí bezdrátových sítí v protokolu IEEE 802.11 a představit možnosti zabezpečení takových sítí a jejich komunikace.

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)			
	A	**C**	**E**	**F**
Práce svým zaměřením odpovídá studovanému oboru	☒	☐	☐	☐
Vymezení cíle a jeho naplnění	☒	☐	☐	☐
Zpracování teoretických aspektů tématu	☐	☒	☐	☐
Zpracování praktických aspektů tématu	☒	☐	☐	☐
Adekvátnost použitých metod, způsob jejich použití	☒	☐	☐	☐
Hloubka a správnost provedené analýzy	☒	☒	☐	☐
Práce s literaturou	☒	☐	☐	☐
Logická stavba a členění práce	☒	☒	☐	☐
Jazyková a terminologická úroveň	☒	☐	☐	☐
Formální úprava a náležitosti práce	☒	☐	☐	☐
Vlastní přínos studenta	☒	☒	☐	☐
Využitelnost výsledků práce v teorii (v praxi)	☒	☐	☐	☐

Dílčí připomínky a náměty:

Autor v kapitole 3.4 uvádí dlouhé seznamy Wi-Fi kanálu v pásmu 2,4 GHz a v pásmu 4,9 až 5 GHz, jejichž informační hodnota vzhledem k tématu práce není nikterak přínosná.
Cíle práce bylo představit algoritmy pro zabezpečení, ale ty v práci uvedeny nejsou. Jejich dostupnost je dostatečná, jako příklad lze uvést článek Guillaume Lehembre, haking 1/2006 dostupný na (http://www.hsc.fr/ressources/articles/haking_wifi/haking_wifi_CZ.pdf), a přispěli by ke kvalitě práce.

Celkové posouzení práce a zdůvodnění výsledné známky:

Předložená práce je zpracována na odpovídající odborné úrovni a to jak v oblasti teoretické, tak hlavně v oblasti praktické. V teoretické části by autor mohl podrobněji zmínit algoritmy a schémata využívání šifrovacích protokolů WEP, WPA a WPA2.
V praktické části se autor podrobně věnuje útoku s podvrženým AP, který patří mezi často využívané v rámci veřejných WiFi sítí a je tedy aktuální. Autor představuje základní principy jak se tomuto útoku bránit, ale z textu je zřejmé, že při využívání veřejných WiFi je potřeba si zachovat „selský rozum".

Jelikož pokud si síť nezabezpečí síťový administrátor sám, nemůže ji již z principu důvěřovat a proto se na veřejných WiFi musíme chovat zodpovědně.
Autor splnil všechny vytyčené cíle a práce splňuje požadavky kladené na bakalářskou práci.

Otázky k obhajobě:

Představte a vysvětlete algoritmus (schéma) mixování klíčů TKIP a šifrování.
Představte postup a logiku fáze autentizace s využitím 802.1X založené na protokolu EAP a autentizační metodě: EAP/TLS s certifikáty klienta a serveru (vyžadující infrastrukturu veřejného klíče), EAP/TTLS nebo PEAP pro hybridní autentizaci (s certifikáty vyžadovanými pouze pro servery).

Práci doporučuji k obhajobě.

Navržená výsledná známka: B - výborně-velmi dobře

V Hradci Králové**, dne 10. května 2016**

podpis