Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Petr Svoboda** **Oponent:** **Ing. Josef Kaderka, Ph.D.**

Studijní program:	**Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Akademický rok:	**2010/2011**
Téma diplomové práce:	**Zjištění reálného stavu zabezpečení bezdrátových Wi-Fi přenosů ve vybrané oblasti**

Hodnocení práce:

Na základě podrobného prostudování diplomové práce Bc. Petra Svobody (dále diplomanta) konstatuji: Předloženou diplomovou považuji za úplnou. Je dosti rozsáhlá, obsahuje 105 stran včetně seznamů použité literatury, zkratek apod. Text práce je vhodně rozvržen. V textu práce lze nalézt jen minimum pravopisných chyb, diplomant však poměrně často volí hovorové vyjadřování či technický slang. V celé práci se také velmi důsledně dopouští jedné typografické chyby: mezi hodnotu a jednotku (tj. rozměr) nevkládá mezeru.

Diplomant vhodným způsobem uvádí základní teoretické podklady a to v prvních třech kapitolách; zabývá se všeobecnými otázkami bezdrátových lokálních počítačových sítí, dále pak otázkami bezpečnosti, kde seznamuje se standardními možnostmi zabezpečení a dále pak útokům na bezdrátové sítě.

Poněkud sporný se mi jeví úvod do kapitoly 4., zabývající se „citlivými daty přenášenými přes Internet". V úvodní části diplomant uvádí „... přenos skutečně důležitých dat, jejichž únik by mohl způsobit nezměrné škody." Pokud by taková data měla být skutečně přenášena bezdrátovou sítí, by bylo nutno užít externí bezpečnostní mechanismy (u utajovaných informací musí být certifikované, například IP nebo linkové šifrátory), a naplnit další legislativní požadavky, např. bezpečnostní prověrky fyzických osob či právnických, jestliže by tyto měly být s utajovanými informacemi seznamovány. V ostatních případech, jako je přenos či shromažďování citlivých údajů nebo údajů majících charakter obchodního tajemství, je situace sice volnější, ale i tak je třeba znát a respektovat příslušné zásady. Diplomant toto ve své práci dobře rozebírá.

Jako autorův význačný přínos hodnotím návrh dotazníkového průzkumu, jeho realizaci a vyhodnocení, obdobně pak průzkum skutečného stavu zabezpečení bezdrátových sítí ve vybraných lokalitách. Obě tyto aktivity jsou podrobněji popsány ve druhé polovině práce, označené jako Praktická část. Zde je uvedeno množství vhodně komentovaných grafů, různě interpretujících zjištěné údaje. Poslední část práce pak rozebírá zkušenosti získané se zabezpečením bezdrátových sítí ve firemním sektoru. Tady mám určité pochybnosti o smysluplnosti hodnocení zabezpečení sítí v restauracích a podobných zařízeních, kdy tyto sítě slouží hostům jako doplňková služba. Domnívám se, že na takovýchto místech je zbytečné sítě zabezpečovat. Nicméně získané poznatky hodnotím pozitivně.

K textu závěru práce: tento bych vzhledem k rozsahu práce čekal poněkud delší, diskusi výsledků apod.; nicméně domnívám se, že diplomant odvedl solidní výkon.

Řešený úkol za středně obtížný. Autorův vlastní přínos vidím zejména v provedených výzkumech a monitorování bezdrátových sítí v několika lokalitách a samozřejmě příslušná vyhodnocení.

Diplomant podle mne prokázal pracovitost a solidní tvůrčí schopnosti v oblastí bezdrátových lokálních počítačových sítí a jejich bezpečnosti. Realizace dotazníkové akce a návštěvy firem musely znamenat značnou časovou zátěž. K práci mám některé nikoliv zásadní komentáře a konkrétní připomínky, které uvádím na níže.

Při obhajobě by měl diplomant reagovat na následující dotazy: při monitorování použil síťovou kartu Atheros AR9285, která, jak sám uvádí pracuje pouze v pásmu 2,4 GHz. Má diplomant představu o využívání pásma 5 GHz, resp. pokusil se provést nějaké výzkumy i zde? Diplomant zjistil, že v řadě případů není využíváno adekvátní zabezpečení. Jaká opatření by navrhoval pro zlepšení situace v této oblasti?

Celkové hodnocení práce:
Známku uvede vedoucí dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě".

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení
B – velmi dobře.
V případě hodnocení stupněm „F – nedostatečně" uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 31.5.2011

Podpis oponenta diplomové práce

Některé konkrétní připomínky k diplomové práci Bc. Petra Svobody:

1.1 Není zcela správné hovořit o WiFi jako o bezdrátovém Internetu, zejména s uvedením roku 1990. Přenosová rychlost 1-2 Mb/s pro řadu aplikací samozřejmě bohatě postačuje.

1.2.1 Text je dosti obtížně srozumitelný. To, co diplomant označuje jako Access Point, je ve skutečnosti kombinované zařízení, skládající se z přístupového bodu a směrovače (provádějícího překlad adres a portů). Typický Access Point je most, pracuje tedy pouze na 2. vrstvě (vyjma řízení), například Cisco 1200, HP A-WA2220 apod.

1.2.2 Přímá viditelnost dvou míst není zárukou kvalitního spojení. Je třeba také zvážit Fresnelovu zónu apod. (viz např. přednášky ing. Miroslava Matýska, Ph.D., Počítačové sítě 1).

1.3 Věta „Na Wi-Fi může být nahlíženo také jako na elektromagnetické záření" zní velmi neodborně. Rovněž pojem „síla záření" spíše implikuje projev okultních sil; diplomant

měl možná na mysli intenzitu elektromagnetického pole.

1.3.1 Kanálů je v pásmu 2,4 GHz definováno celkem 14, ovšem ne všude ve světě lze použít všechny (např. v Evropě 13, v USA a Kanadě 11, v Izrael jen 7).

1.3.2 Písmeno v označení standardu neoznačuje druh modulace, ale konkrétní standard. Např. 802.11b a 802.11g (802.11h) používají stejnou modulaci OFDM.

1.3.2 Zkratka RTS zpravidla neznamená Ready To Send, ale Request To Send (s čímž koresponduje signál Clear To Send, tedy připraven k vysílání).

1.3.4 Režim ad hoc umožňuje vytvářet bezdrátové sítě typu peer to peer, tedy bez centrální autority (přístupového bodu), což nijak nesouvisí s možností či nemožností komunikovat s Internetem; hovořit o zásadní nevýhodě není korektní (tou je spíše problém potenciální rádiové neviditelnosti některého počítače jinými počítači). Totiž pokud by byl některý z počítačů z ad hoc sítě připojen do Internetu například pomocí Ethernetu, mohl by fungovat jako standardní směrovač a pomocí něj by se uživatelé této ad hoc sítě do Internetu dostali.

1.4 Dnes běžná zařízení 802.1n dosahují podstatně vyšší rychlosti. Pojem „přímá viditelnost" je třeba chápat ve smyslu rádiová viditelnost. Podobně „neomezený pohyb" podléhá řadě omezení.

1.5.1 Není jasné, jak si diplomant představuje zákonnou úpravu, která by měla omezit vzájemné rušení a současně umožnit volné používání vybraných části kmitočtového spektra. Všeobecné oprávnění č. VO-R/12/09.2010-12 ČTÚ (které nahrazuje autorem uváděné VO-R/10/03.2007-4) povoluje maximální efektivní vyzářený výkon 100 mW (v pásmu 2,4 GHz), tj. se započtením směrového účinku antény. Používání vyšších výkonů je nelegální a ČTÚ je postihuje. Diplomant se tímto zabývá v dalším textu.

2.2 Nevysílají se betony, ale spíše beacony (beacon = neobsluhovaný maják), tj. rámce, nesoucí informace o daném přístupovém bodu.

2.7 DHCP by mohl usnadnit práci jen velmi prostým útočníkům. Protokol IPv6 bez DHCP (nebo alternativního mechanismu) nelze rozumně provozovat vůbec.

2.8 Autentizace je proces ověření proklamované identity subjektu.

2.8.2 „EAP RESPONSE-ID je pak serverem převeden ..." tímto serverem je přístupový bod (v terminologii 802.1x se užívá obecného pojmu autentizátor). Úvahy o blokování portů by se uplatnily spíše u Ethernetu a přepínačů. Algoritmus MD5 má sice slabiny, ale pro občanské (či domácí) použití vyhovuje. Protokol LEAP byl průkopníkem a čekal jej příslušný osud.

2.8.4 Jiné zabezpečení nežli WPA2 by dnes nemělo být vůbec používáno.

3.1 Denial of Services obecně nemusí využívat zahlcení oběti silným provozem, viz útok Slowloris.

3.5 Nikoliv deautentifikace, ale deautentizace.

5 Citlivé informace a utajované informace je třeba odlišovat.

7.4 Aktivita firmy Google (pořizování videozáznamů) vyvolala v Evropě včetně ČR řadu negativních reakcí a byla pozastavena (u nás na více než rok).

8.5 Počet respondentů (241) je pro daný účel rozhodně postačující. Jisté úskalí představuje okolnost, že jejich výběr nebyl, jak diplomant píše, nezávislý (známí apod.).

10.2.2 Na rozdíl od diplomanta považuji zabezpečení komunikace v restauracích za zbytečnost, která hosty obtěžuje a nikdo rozumný odtud nebude posílat důležité údaje.

10.4.1 I když není zřejmé s pracovníkem kterého štábu AČR (Generálního?) bylo hovořeno, jsou diplomantem uváděné údaje v zásadě přesné.