Příloha k protokolu o SZZ č.

Student/diplomant:

Vysoká škola: **Univerzita Tomáše Bati ve Zlíně**

Bc. Jiří Straka

Fakulta: **Fakulta aplikované informatiky**

Ústav:

Aprobace

Datum odevzdání posudku: **18. 6. 2007**

Recenzent *)

Diplomové práce

~~Vedoucí *)~~ **Ing. Jaroslav Janoš**

POSUDEK DIPLOMOVÉ PRÁCE

Ochrana dat proti zneužití při přenosu a záznamu mobilními prostředky

Předložená diplomová práce se zabývá aktuální problematikou bezpečnosti přenosu dat v mobilních sítích. Diplomant se zaměřil na oblast zabezpečení bezdrátového přenosu v síti WLAN (přenosová technologie Wi-Fi), dalšími technologiemi bezdrátového přenosu dat (Bluetooth, IR, GPRS, atd.) se v práci nezabývá. Motivací práce bylo navrhnout možné řešení bezpečného bezdrátového přenosu dat na konkrétním příkladu.

Teoretická část práce je zaměřena především na popis způsobů zabezpečení přenosů dat v prostředí WLAN (Wi-Fi sítí). Autor zde uvádí i příklady bezpečnostních konfliktů (útoků) v sítích WLAN a možnosti jejich odhalení, popř. řešení. V této části práce bych uvítal syntézu zjištěných poznatků například ve formě srovnání vlastností protokolů WEP, WPA a WPA2 (protokol WPA2 není v práci zmíněn vůbec) především z hlediska bezpečnosti (odolnost vůči útokům a odtud plynoucí oblast použití). Z formálního hlediska lze této části práci vytknout chybějící přehled citovaných IEEE norem (např. v příloze). Na některých místech jsou označení norem použita chybně - například na straně 8 je uvedena norma pro sítě Wi-Fi jako IEEE 802.11b (správně však měla být uvedena obecná norma IEEE 802.11) nebo na straně 17 se píše, že WPA spadá do normy IEEE 802.11i - do této normy však spadá protokol WPA2. Na straně 18, v kapitole 1.3 je chybně uvedena délka klíče u protokolu WPA – místo 40bitů má být 128bitů.

Praktická část práce představuje návrh zabezpečení přenosu dat v prostředí skladu náhradních dílů. Diplomant uvádí, že architektura systému pro sběr a přenos dat byla zvolena s ohledem na zachování co nejvyšší míry bezpečnosti při nízkých pořizovacích nákladech na použitý hardware. V úvodu praktické části práce však chybí ucelený přehled požadavků, které by měl navrhovaný systém splňovat. Proto nelze jednoznačně posoudit, zda zvolené řešení je nebo není optimální. Z popisu například není jasné, proč má být přístupový bod Wi-Fi sítě (AP) umístěn tak, aby bezdrátový signál mohl být přijímám i před halou. Myslím, že vhodnější by naopak bylo využití

sektorové antény, která by omezila únik rádiového signálu mimo vymezený prostor haly. V kapitole 3.1.2 se diplomant zabývá popisem zvoleného hardware - podle mého názoru zbytečně obšírně. Například rozsáhlý popis vlastností zvolené tiskárny je irelevantní vzhledem k tématu práce (navíc je popis tiskárny uveden i v příloze). Naopak zde chybí například informace o tom, jakým způsobem bude zabezpečeno PC, k němuž má být tiskárna připojena. V kapitole 3.3 je popisováno nastavení přístupového bodu sítě Wi-Fi (AP). V popisu nastavení AP i mobilní čtečky čárového kódu je sice uvedeno, že bude použit protokol WPA, ale konkrétní popis nastavení vlastností WPA chybí. Z popisu nastavení AP dále není jasné, proč byla zvolena statická IP adresa 192.168.1.245, když při nastavení routeru se pro tentýž AP používá adresa 10.16.66.2. Diplomová práce neřeší zabezpečení při zpracování čárových kódů – není jasné, zda čtečky budou komunikovat přímo s databázovým serverem nebo s nějakou aplikací, která komunikaci s databázovým serverem zabezpečí sama. Práce se nezabývá krizovými scénáři, které v praxi mohou nastat – například jak postupovat v případě, že někdo zcizí mobilní čtečku, z níž lze snadno získat konfiguraci sítě a podobně. Co se týká formálních chyb v této části práce, uvedl bych např. chybné měřítko situačního plánu objektu na straně 28 a 37 (uvedeno M 1:2).

Práce je po obsahové i formální stránce na dobré úrovni. Diplomant prokázal inženýrský přístup jak při analýze informací, týkajících se tématu práce, tak i při návrhu modelového příkladu. Rozsah diplomové práce odpovídá požadovanému zadání až na nedostatky, které jsou zmíněny výše. Po formální stránce lze práci vytknout drobné gramatické chyby a překlepy. Seznam použitých symbolů a zkratek, uvedený v příloze, není úplný (chybí např. zkratky AP, WCDMA, RFID, ERP, RSA, atd.). Chybí také přehled norem IEEE (viz výše) a seznam grafů.

Během obhajoby práce by diplomant mohl zodpovědět následující dotazy:

1. Jaké další zásady bezpečnosti by bylo vhodné aplikovat na uvedeném modelovém příkladu (z hlediska omezení přenosu bezdrátového signálu, omezení výpadků hardware, na aplikační vrstvě modelu ISO/OSI, apod.)?
2. V kapitole 4 (Možnosti rozšiřování) je uvedeno, že by bylo možné přidávat další informace ke snímaným a posílaným datům pomocí aplikací, vytvořených ve vývojovém prostředí Microsoft Visual Studio, které je volitelnou součástí čteček. Uveďte konkrétní příklad nějaké aplikace, která by mohla rozšířit funkcionalitu mobilní čtečky ve vztahu k přenášeným datům.

Návrh na klasifikaci diplomové práce: **B velmi dobře**

podpis recenzenta diplomové práce

Ve Zlíně dne **18. 6. 2007**

Stupeň klasifikace	A výborně E dostatečně	B velmi dobře F nedostatečně	C dobře	D uspokojivě