TECHNICKÁ UNIVERZITA V LIBERCI

Fakulta mechatroniky a mezioborových inženýrských studií

Studijní program: B2612 – Elektrotechnika a informatika

Studijní obor: 2612R011 – Elektronické informační a řídící systémy

Bezpečnost Bluetooth

Bluetooth Security

Bakalářská práce

Autor: **Alena Mlejnková**

Vedoucí práce: Mgr. Jiří Vraný

V Liberci 10. 5. 2006

Prohlášení

Byl(a) jsem seznámen(a) s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 o právu autorském, zejména § 60 (školní dílo).

Beru na vědomí, že TUL má právo na uzavření licenční smlouvy o užití mé BP a prohlašuji, že **s o u h l a s í m** s případným užitím mé bakalářské práce (prodej, zapůjčení apod.).

Jsem si vědom(a) toho, že užít své bakalářské práce či poskytnout licenci k jejímu využití mohu jen se souhlasem TUL, která má právo ode mne požadovat přiměřený příspěvek na úhradu nákladů, vynaložených univerzitou na vytvoření díla (až do jejich skutečné výše).

Bakalářskou práci jsem vypracoval(a) samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

Datum

Podpis

Anotace

Bluetooth je velmi rozšířená bezdrátová technologie pro WPAN. Cíl této práce je seznámení s touto technologií, její bezpečnost a používané metody zabezpečení.

Na začátku práce je podrobný popis principů a vlastností technologie Bluetooth. V další části je uvedena obecná charakteristika bezpečnosti Bluetooth a zabezpečení Bluetooth na spojové vrstvě. Dále jsou zmíněny programy, které pomáhají zabezpečení na aplikační vrstvě a známé útoky na Bluetooth. V závěru je uvedeno doporučení, jak bezpečně spravovat zařízení.

Annotation

Bluetooth is very extended technology for WPAN. Purpose of this work is identification of this technology, its security and used methods safeguard.

On the beginning of the work is a particular description of principles and features of Bluetooth technology. In next part there is general characteristic of Bluetooth security and link level security of Bluetooth. Further there are spoken of programs, which help on the application link and known attacks on Bluetooth. In the end there is a recommendation for safe administration of Bluetooth devices.

OBSAH

Seznam obrázků

Zkratky

ACL	Asynchronous Connectionless
ACO	Authenticated Ciphering Offset
AFH	Adaptive Frequency Hopping
AMA	Active Member Address
BD_ADDR	Bluetooth Device Address
COF	Cipering Offset Number
DAI	Direct Audio Input
DoS	Denial of Service
EDR	Enhanced Data Rate
FHSS	Frequency Hopping Spread Spectrum
GPRS	General Packet Radio Service
HCI	Host Controller Interface
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equipment Identity
IP	Internet Protokol
ISM	Industrial Scientific Medicine
L2CAP	Local Link Communicatin and Adaption Protokol
LLC	Local Link Control
LM	Link Mnger
LMP	Link Manger Protokol
LSFR	Linear Feedback Shift Registers
MAC	Media Access Control
MMS	Multi Media Service
OBEX	Object Exchange Protokol
PIN	Personal Identification Number
PMA	Parked Member Address
PPP	Point-to-Point Protokol
QoS	Quality of Service
UWB	Ultra WideBand
WAP	Wireless Application Protocol
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network

WPAN	Wireless Personal Area Network
RFCOMM	Radio Frequency Communications
SAFER	Secure And Fast Encryption Routine
SAP	Service Access Points
SCO	Synchnous Connection Oriented
SDP	Service Discovery Protokol
SIG	Special Industry Group
SMS	Short Message Service
SRES	Signed Response
TCP	Transmission Control Protokol
TCS Binary	Telephony Control Specification Binary
TDD	Time Division Duplex
TDMA	Time Division Multiple Access

Jednotky

veličina	**značka**	**jednotka**
informace	b	bit
frekvence	f	Herz
délka	m	metr
rychlost	s	sekunda
zisk izotropní antény	dBi	decibel izotropní

Úvod

Žijeme ve světě bezdrátová komunikace, která nás denně obklopuje stále častěji, a proto je třeba se zamyslet nad její bezpečností. Zvláště oblíbená technologie pro bezdrátový přenos na krátké vzdálenosti je Bluetooth. Cílem této práce je seznámení se zařízením, zaměřit se na jeho bezpečnost a prozkoumat dostupné metody zabezpečení.

Na začátku této práce je malé zasvěcení do obecných záležitostí, kde jsou uvedeny jednotlivé normy, historie Bluetooth, její architektura, topologie sítě, specifikace, adresace zařízení a využití tohoto zařízení. Následuje kapitola věnovaná obecněji bezpečnosti Bluetooth, probírá tři možnosti zabezpečení. Největší část práce je věnována zabezpečení na spojové vrstvě, jejíž součástí jsou procesy autentifikace, párování a šifrování za pomoci generování klíčů. Práce se také zmiňuje o zabezpečení na aplikační vrstvě a popisuje několik aplikací zabývající se touto problematikou. Dále pak následuje popis dobře známých i méně známých útoků a virů, které mohou napadnout mobilní telefon, PDA či další mobilní zařízení.

1 Seznámení se zařízením Bluetooth

Bluetooth je jednou z technologií pro bezdrátový přenos dat, díky své jednoduchosti muže být implementován nejen do počítače, telefonů, ale i do aut a dalších zařízeních.

Obrázek 1.1: Bluetooth USB zařízení [A]

1.1 Normalizace bezdrátových sítí

Bluetooth převzalo jako normu IEEE 802.15 pro bezdrátové osobní sítě (Wireless Personal Area Network, WPAN)

IEEE 802.15 lze rozdělit do několika skupin:

- 802.15.1 – **WPAN Bluetooth** – norma pro WPAN na základě specifikace Bluetooth 1.1
- 802.15.2 – **Coexistence** – zabývá se koexistencí všech bezdrátových technologií vytvořených v rámci IEEE 802, nejen WPAN ale i WLAN a WMAN
- 802.15.3 – **WPAN High Rate** – cílem je specifikovat rychlou bezdrátovou osobní síť (11-55 Mbit/s), pracující opět v pásmu 2,4 GHz, se zabudovanou podporou pro kvalitu služeb (QoS) pro náročné domácí multimediální aplikace (video v reálném čase, vysoce kvalitní audio, přenosy velkých datových souborů), je vyvíjena rychlejší verzi 802.15.3a s kapacitou od 110Mbit/s, která bude založena na technologii UWB(Ultra WideBand)
- 802.15.4 – **WPAN Low Rate** – pracuje na specifikaci pro pomalejší osobní rádiové sítě do 250 kbit/s s minimálními energetickými potřebami, průmyslové označení je ZigBee

Specifikace Bluetooth 1.1 je plně slučitelná s normou 802.15.1. IEEE přidala například specifikaci přístupových bodů služby (Service Access Points, SAPs), což zahrnuje rozhraní LLC/MAC s cílem sjednotit protokoly řízení logického spoje, který je součástí druhé- spojové vrstvy v architektuře v lokálních sítích typu 802. [2]

1.2 Historie Bluetooth

Technologie Bluetooth vznikla jako první z bezdrátových osobních sítí. Vývoj začal v roce 1994, když tým výzkumníků v Ericcson Mobile Communications vyžadoval způsob jak připojit klávesnici k počítači bez kabelu. [19]

Hlavní myšlenka tedy byla odstranit kabely a sjednotit rozdíly, jelikož každé zařízení potřebovalo jiný kabel a jiný konektor. Počet kabelů narůstal a to bylo nepohodlné, kabely překážely. Důraz byl kladen na to, aby cena Bluetooth nepřesáhla cenu kabelu. Mělo být laciné, rychlé a s nízkými požadavky na napájení.

Název této technologie byl převzat od dánského krále jménem Harald II - Blatand v angličtině Harold II - Bluetooth, v překladu jeho přezdívka znamená „Modrý zub“. Právě podle jeho záliby v borůvkách a ostružinách. Tento král v 10. století bez použití násilí sjednotil Skandinávii a i tato technologie měla za úkol sjednotit osobní komunikační a výpočetní zařízení.

Skandinávská firma vytvořila logo uchovávající tradici jména společnosti, logo kombinuje runový znak "H" (Harald), který je podobný hvězdičce a písmeno "B" (Bluetooth), když se pozorně podíváte můžete je oba vidět v logu.

Obrázek 1.2.1: Logo Bluetooth [B]

Vývojem Bluetooth se zabývá od roku 1998 Bluetooth SIG (Special Industry Group), kterou jako neziskové průmyslové sdružení založily firmy Ericsson, IBM, Intel, Nokia a Toshiba.

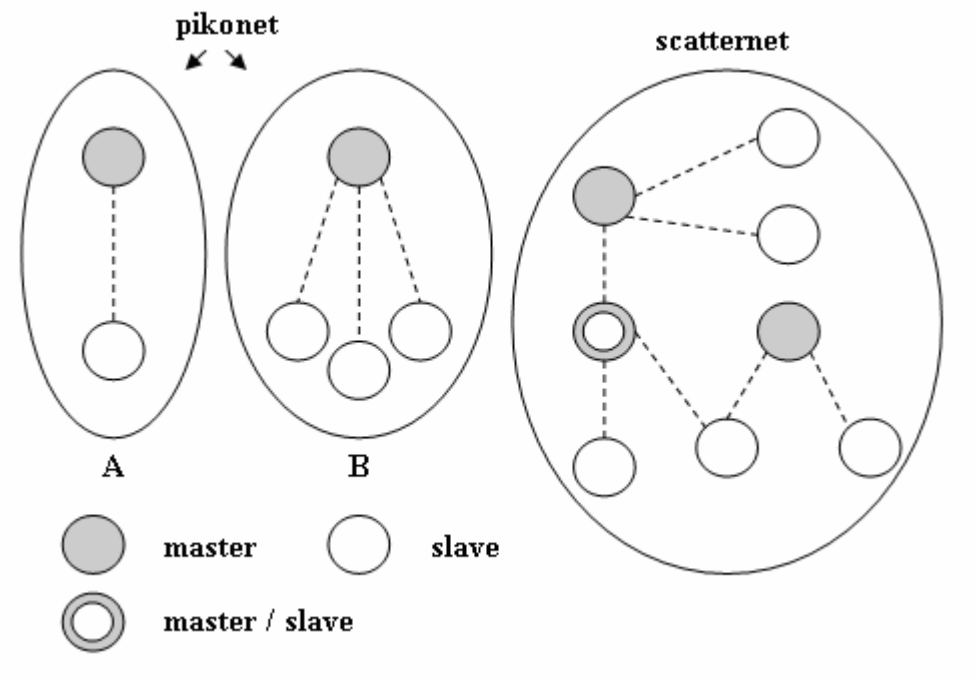
Milníky Bluetooth SIG:

- Bluetooth Special Interest Group (SIG)
- 1999 první verze *Bluetooth* 1.0
- 2000 první *Bluetooth* produkt pro zákazníky vyšel na trh – *Bluetooth* headset a adaptér pro telefon od Ericssonu
- 2001 Bluetooth SIG, Inc. – soukromá obchodní společnost
- 2002 *Bluetooth* bezdrátová technologie –500 kvalifikovaných milníků produktu
- 2003 Bluetooth verze 1.2, prodej přesáhl milion produktů týdně
- 2004 Bluetooth verze 2.0 + Enhanced Data Rate (EDR) – zrychlení přenosu dat
  bylo nainstalováno přes 250 milionů zařízení
  prodej přesáhl 3 miliony týdně
  Bluetooth SIG vítá třítisícího člena
- 2005 Bluetooth SIG oznámil spolupráci s UWB
  prodej stoupl na 5 milionů chipsetů týdně
  Bluetooth SIG vítá 4-tisícího člena [14]

1.3 Topologie Bluetooth

Topologie Bluetooth podporuje dvoubodovou i vícebodovou komunikaci. V případě vícebodové komunikace zařízení tvoří síť ve tvaru hvězdy označovanou jako Pikonet – pikosíť a chovají se rovnocenně. V každé pikosíti je právě jedno zařízení pracující v režimu Master a ostatní pracují v režimu Slave. Zařízení Bluetooth umí pracovat v režimu Mater i Slave, může se mezi nimi přepínat, ale ne pracovat v obou zároveň. Každé zařízení Master může současně obstarat až 7 zařízení Slave.

Několik pikosítí tvoří scatternet (rozprostřené sítě). Zde je samo sebou několik zařízení Master, ale žádný Master nemůže být paralelně Master ve více sítích, ale Slave být může. [1]



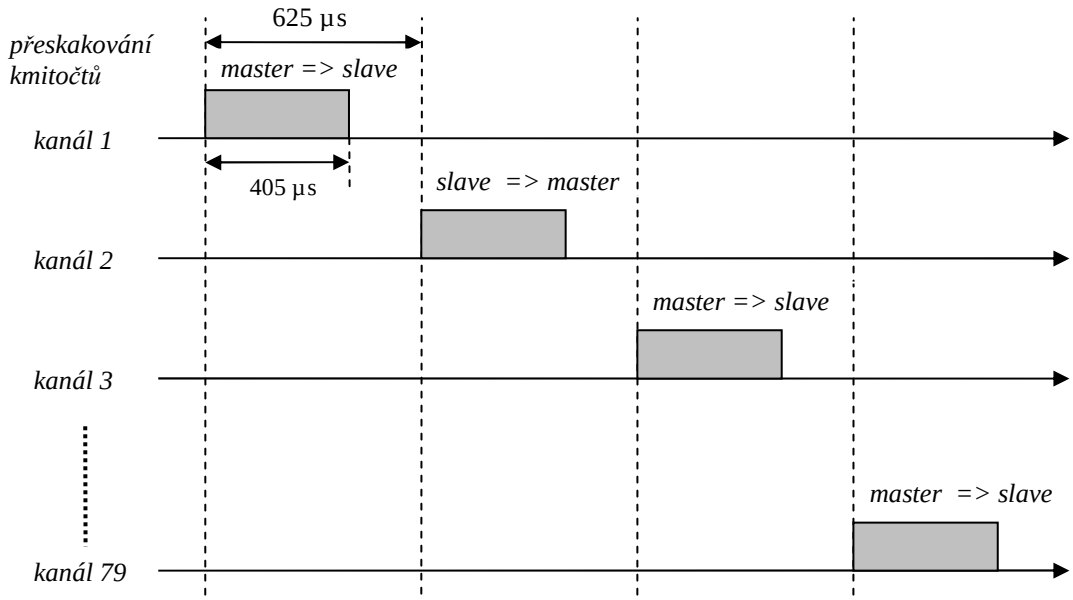
Obrázek 1.3.1: Topologie Bluetooth: A – příklad jednobodového spoje, B – příklad mnohobodového spoje

1.4 Specifikace Bluetooth

Bluetooth verze 1.1

Bluetooth je radiový systém pracující v bezlicenčním pásmu ISM (Industrial Scientific Medicine) 2,4 GHz, na této frekvenci pracuje řada jiných zařízení jako jsou WLAN nebo třeba mikrovlnná trouba, a proto může být dost zarušené. Pro přenos se používá 79 kanálů s šířkou pásma 1 MHz na kanál. Právě kvůli již zmíněnému rušení Bluetooth používá metodu rozprostřeného spektra s přeskakováním kmitočtů FHSS *(Frequency Hopping Spread Spectrum)* to znamená, že každých 625 µs přeskočí na jinou frekvenci, tj. 1600 hopů/s (po každém přenosu - odeslání a příjmu dat). Mezi přijetím a vysláním dalšího paketu musí být ochranná doba nejméně 220 µs, aby se zabránilo případným kolizím. [2] Maximální délka paketu je 2 745 bitů. [19]

Princip posílání, master přenáší pouze v lichých a Slave pouze v sudých časových slotech (viz Obrázek 1.4.1), tento princip se nazývá Time Division Duplex, TDD. [4]



Obrázek 1.4.1: Vysílání Bluetooth

Celá šířka pásma je v rozsahu 2,4 – 2,4835 GHz pro většinu států v Evropě je přenosová frekvence dána vzorcem f = 2405 + k [MHz], kde k = 0,..,78, pro dodržení norem jsou definována ochranná pásma, dolní ochranné pásmo je 2 MHz a horní ochranné pásmo je 3,5 MHz.

Některé státy jako Francie a Španělsko mají šířku pásma omezenou na rozsah 2,4465 – 2,4835 GHz, přenosová frekvence je pak f = 2454 + k [MHz], kde k = 0,..,22, šířka horního i dolního ochranného pásma je 7,5 MHz. Z toho vyplývá, že počet hopů je jen 23. [10]

Dosah zařízení závisí na třídě vysílaného výkonu zařízení (viz tab.1.4.1), většinou je kolem 10 metrů u mobilních telefonů, headsetů nebo pocket PC a 50 či 100 metrů u počítačů, avšak s vyspělým vybavením lze detekovat zařízení Bluetooth i na 1 kilometr. Bluetooth se tedy řadí mezi osobní sítě s malým dosahem WPAN.

Výkonová třída	Maximální výstupní výkon	Očekávaný dosah	Dosah na volném prostranství
1	100 [mW] (20 dBm)	42m	300m
2	2,5 [mW] (4 dBm)	16m	50m
3	1 [mW] (0 dBm)	10m	30m

Tab. 1.4.1: Výkonové třídy a dosah

Bluetooth v nízkovýkonovém režimu má dosah jen 10 m a maximální rychlost přenosu 1 Mbit/s. Když scatternet tvoří 10 pikosítí a pracuje v okruhu o průměru 10 m, znamená to, že agregovaná rychlost všech deseti sítí je 10 Mbit/s a prostorová kapacita je 30 kbit/s na metr čtverečný.

Komunikaci s pikosíti řídí master. Stanice Slave nemůže přímo komunikovat s dalším zařízením Slave, pouze prostřednictvím Mastera. Komunikace je buď asynchronní a nebo synchronní. Master používá TDMA (Time Division Multiple Access) mnohonásobný přístup s časovým dělením, který alokuje časové úseky pro potřebný typ komunikace (synchronní či asynchronní). [4]

Asynchronní komunikace (Asynchronous Connectionless, ACL) je bez spojení. [4] Dosahuje se rychlosti 1 Mbit/s na fyzické vrstvě, přičemž skutečná propustnost dat se pohybuje maximálně kolem 720 kbit/s jedním směrem a 57 kbit/s zpět, což je asymetrické spojení a symetrické spojení 433 kbit/s oběma směry.

Pro přenos hlasu je spojení synchronní (Synchnous Connection Oriented, SCO). [19] Rychlost je 64 kbit/s. Bluetooth nabízí až 3 hlasové kanály pro každý Pikonet. [1]

Bluetooth verze 1.2

Verze 1.2 je plně slučitelná s verzí 1.1. Narozdíl od ní používá adaptivní přeskakování mezi kmitočty (Adaptive Frequency Hopping, AFH), který je využíván kvůli velkému rušení v pásmu 2.4 GHz. AFH využívá volných kmitočtů, které zrovna nejsou využívány jinými zařízeními, tím je zaručeno efektivní využití spektra.

Bluetooth 1.2 je rozšířen o podporu pro kvalitu služby QoS. QoS je velice důležitý pro provoz citlivý na zpoždění, jako je přenos zvuku, hlasu, videa v reálném čase a přenosy velkých datových souborů

Podporuje anonymní režim vysílání – nevysílá se výrobní číslo zařízení. Některá zařízení jsou nakonfigurována, aby po připojení sdílela všechna data, která má, což přináší větší bezpečnostní riziko.

Zapojení a zprovoznění nového zařízení by nemělo trvat uživateli déle než 5 minut.[5]

Došlo k vylepšení zpracování hlasového signálu, tzn. k potlačení šumu a echa.

Bluetooth verze 2.0

Verze 2.0 je zpětně kompatibilní s 1.x. Hlavní novinkou je EDR – zrychlení přenosu dat. Rychlost přenosu 2.1 Mbit/s, což je 3krát rychlejší nežli je u předchozích verzích. [6]

1.5 Adresace zařízení

Každé zařízení disponuje vlastní jedinečnou adresou o délce 48 bitů BD_ADDR (Bluetooth Device Address).

Po navázání spojení v síti obdrží uzel 3b adresu AMA (Active Member Address), čísla od 0 do 6, právě kvůli této indexaci je možné, aby bylo nejvýše 7 zařízení Slave v pinosíti. Uzel Master má vždy adresu AMA = 0.

Pikosíť může dále obsahovat až 256 zařízení Slave v režimu parked. Zařízení je přiřazena 8b adresa PMA (Parked Member Address).

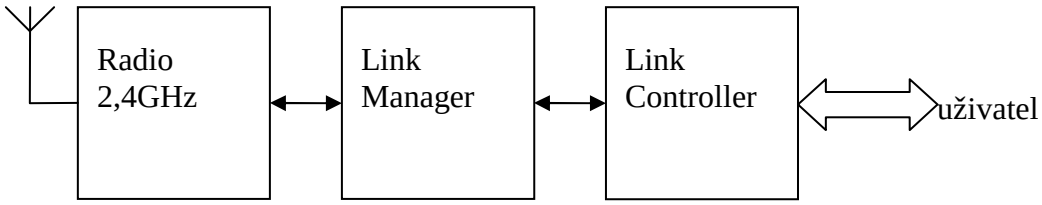
S použitím dalších nových adresací by jich mohlo být i více. [17]

1.6 Technické řešení

Bluetooth systém je složen ze tří částí – komponent

- Bluetooth radio
  je ve funkci vysílač, přijímač
- Bluetooth Link Manager
  připravuje data a zaručuje komunikaci se zařízením s Bluetooth modulem
- Bluetooth Link Controller
  řídí komunikaci, identifikaci, přístup a navázání spojení

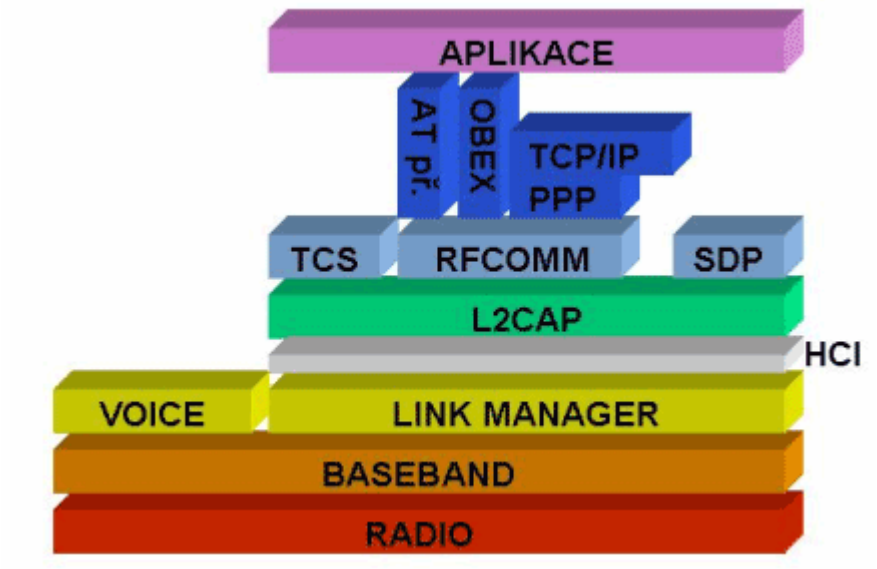
Jelikož byl Bluetooth navrhnut jako alternativa kabelu, neobsahuje žádné analogové vysokofrekvenční součástky, rozměrné a drahé komponenty jako jsou třeba filtry nebo zesilovače. Vše je ovládáno procesorem, který je schopný zpracovat i zarušený signál. [6]



Obrázek 1.6.1: Základní koncepce Bluetooth

1.7 Architektura Bluetooth

Stručný popis protokolů používaných v architektuře Bluetooth.



Obrázek 1.7.1: Vrstvy Bluetooth a jejich pozice[C]

Radio – fyzická vrstva je nejspodnějším protokolem systému Bluetooth. Chová se jako modem ke zpracování rádiových signálů.

Baseband leží nad fyzickou vrstvou. Plní funkci spojové vrstvy, řeší formátování paketů, stará se o vytváření hlaviček, o kontrolní součty, opětovný přenos dat a šifrování a dešifrování. LM je nižší vrstva Baseband, implementuje základní protokoly a procedury. Horní vrstvu Baseband ovládá Link Manager LM a je nastavena použitím LMP.

L2CAP zajišťuje přeformátování velkých kusů dat na menší části přenositelné přes Bluetooth. Poskytuje spojový a bezspojový přenos dat vyšším vrstvám. [19]

HCI je vrstva, která poskytuje jednotné rozhraní a metodu přístupu k hardwaru Bluetooth. [7]

SDP povoluje pro Bluetooth dostat informace o typu zřízení a podporovaných službách, aby bylo možné vytvořit spojení mezi zařízeními. [19]

RFCOMM je emulace RS-232 sériového spojení. Vhodný pro aplikace, které používají k přenosu dat sériový port a protokol. Emulace ovládá signál přes fyzickou vrstvu a poskytuje služby vyšším vrstvám. [7]

TCS Binary definuje řízení, sestavení sériové linky a přenos hlasu i dat mezi Bluetooth zařízeními.[7]

AT Command emuluje služby sériového portu, komunikace s Bluetooth pomocí textových příkazů.

OBEX se stará o data změněná v klient/server modelu a o synchronizaci souborů.

TCP/IP je protokol pro řízení internetové komunikace, spojení mezi počítačem a internetem.

PPP definuje jak je IP přenesený přes sériové Poin-to-Point spojení. [19]

1.8 Stavy uzlů v síti Bluetooth

Pikonet používá pro komunikaci FHSS, tato frekvence je odvozena od adresy master uzlu a posunu (offset). Všechny zařízení slave se musí synchronizovat s frekvencí master. Zařízení nemůže být master ve více pikosítích najednou, jelikož by obě pikosítě měly stejnou posloupnost přeskakovaní.

Životní cyklus uzlu v síti Bluetooth lze rozdělit do několika kategorií:

- Stav standby
- Fáze připojování se dělí na dvě části
    - inquiry a inquiry scan
    - page a page scan
- Fáze připojení čtyři možné stavy
    - park

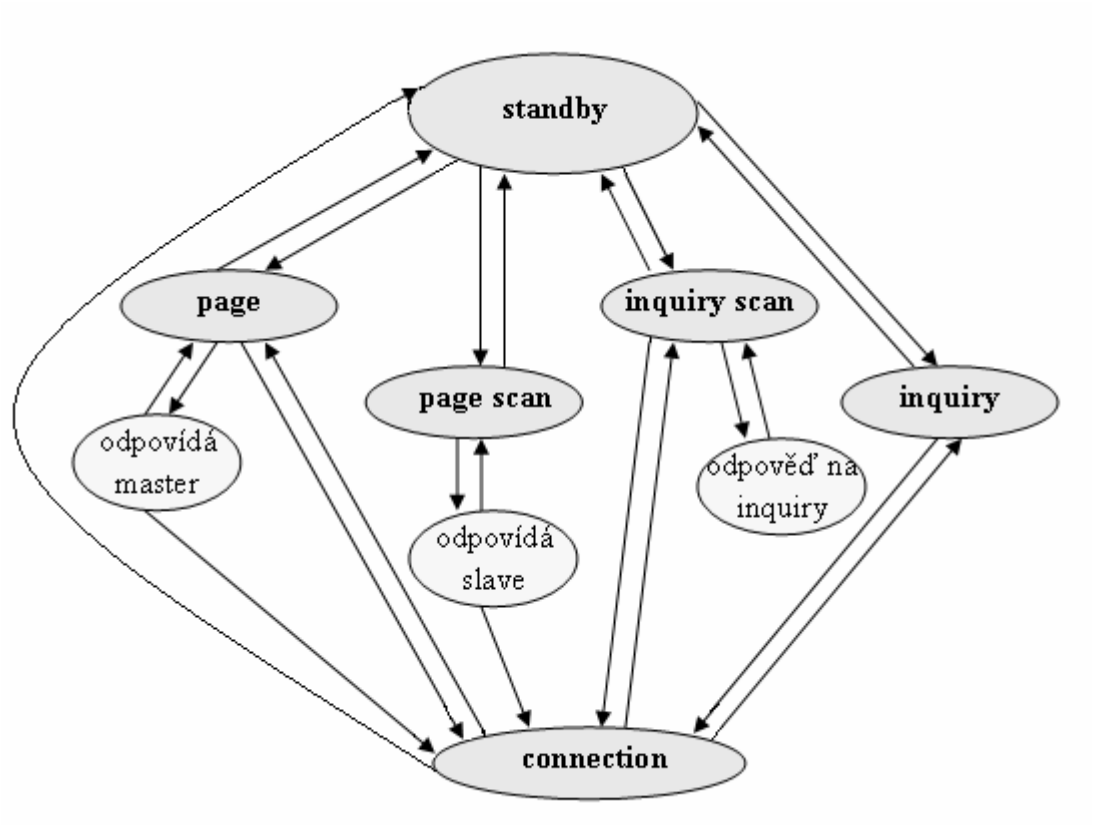
- sniff
- connect
- hold

Po zapnutí se zařízení nachází v režimu standby, není připojeno k žádné pikosíti. Vysílá v pravidelných intervalech inquiry (dotazy) a monitoruje kanál, jestli neuslyší inquiry jiných stanic. Po obdržení inquiry odešle adresu uzlu a stává se stanicí slave a odesilatel dotazu bude master. [2] Tento proces slouží k objevení dvou zařízení. [12]

Page a page scan slouží k vytvoření spojení. Page posílá na kanálech adresu uzlům, které chce připojit. Uzel na ni odpovídá a předává svou adresu a offset. Page vyhodnotí posloupnost a uzel je potom schopen vysílat a přijímat.

Pří navazování spojení Page/Inquiry znamená, že se uzel stane master. Při použití page scan/inquiry scan bude uzel slave.

Pokud chce zařízení v režimu parket komunikovat, je nutné, aby se stalo aktivním zařízením, naopak některé ze 7 aktivních musí přejít do režimu parket. [12]



Obrázek 1.8.1: Stavy uzlů

1.8.1 Aktivní mód

Pokud je slave v aktivním módu, stále poslouchá přenosy od uzlu master. Master pošle pakety aktivnímu slave, ten pokračuje v synchronizaci a informuje, že může poslat paket zpět. Pokud je spojení Point-to-Point, slave poslouchá všechny pakety. Při spojení Point-to-Multipoint stačí, když poslouchá jen hlavičky paketu.

Aktivní stav má nejrychlejší odezvu a potřebuje také nejvíce energie, protože stále přijímá a je připraven odesílat pakety.

1.8.2 Sniff mód

Tento mód umožňuje snížit spotřebu energie tím, že se slave stává aktivní pravidelně. Master pak přenáší pakety jen v určitých intervalech pro jednotlivé slave. Slave poslouchá pakety od master jen na začátku intervalu, když jsou mu odeslány, přijme je, jinak může „spát“ až do dalšího intervalu. Spotřeba energie a schopnost reagovat záleží na délce sniff intervalu. Mód reaguje méně než aktivní mód, a tak si drží sníženou spotřebu energie.

1.8.3 Hold mód

Hold mód zastaví poslouchání paketů pro slave na určitou dobu. Během této doby může slave dělat jiné věci, jako například zakládání spojení s dalším zařízením, či jen spát. Na konci intervalu zase začne naslouchat pakety. Hold mód může být méně reagující než snifff mód, úspora závisí na délce trvání intervalu a na aktivitách slave.

1.8.4 Parked mód

Slave v parket módu udržuje synchronizaci s masterem, ale neprovádí žádné další požadavky jako aktivní mód. Parked dovoluje masterovi organizovat komunikaci s více než jedním slave v pikosíti střídáním aktivního a parked módu. Parked je nejméně reagující, ale má i nejmenší spotřebu energie, pokud zrovna nepřechází z parked do aktivního módu.

1.8.5 Adaptive transmission power (Adaptivní přenosová energie)

Kromě základních módů disponuje Bluetooth i jiným způsobem úspory energie zavoláním Adaptive transmission power. Tento způsob umožňuje, aby slave informoval mastera, že je použitý výkon nevýhodný. Používáním hodnoty indikátoru intenzity přijatého signálu. Pro menší a bezpečnější vzdálenost může slave žádat mastera o použití nižší energie, na velkou vzdálenost či při slabém signálu o větší energii. Master udržuje a upravuje spotřebu energie pro každého slave jednotlivě. [19]

1.9 Aplikace Bluetooth

Jak již bylo řečeno Bluetooth byl vyvinut s cílem odstranit kabely a problémy s konektory, a proto si brzy našel mnoho způsobů využití:

- Headset a Handsfree k mobilním telefonům a do call center pro volné ruce a svobodu od kabelů
- PDA a počítače (Notebooky) - komunikaci, synchronizaci mezi nimi, pro vzdálenou zprávu PC pomocí PDA,
- PC – bezdrátové připojení periferií jako je myš, klávesnice, tiskárna a mnoho dalších
- Mobilní telefony – náhrada kabelu
- Telematické systémy v automobilech – sloužící k vnitro-automobilové komunikaci, na cestách jako prostředky navigace a přístup k informacím případně i internetu. [4]
-

1.9.1 Sluchátko - naslouchákо

Výrobce Eli Bluetooth příslušenství představil sluchátko pro lidi s poškozeným sluchem. Klasické naslouchátko je napojeno přes konektor DAI (Direct Audio Input) na Bluetooth modul. Při použití s telefonem, který podporuje Bluetooth mohou tito lidé bez problémů telefonovat. Zařízeni svými rozměry 27 mm × 16 mm × 11 mm a hmotností 5.2 gramů patří k nejmenším na trhu. [3]

2 Bezpečnost Bluetooth

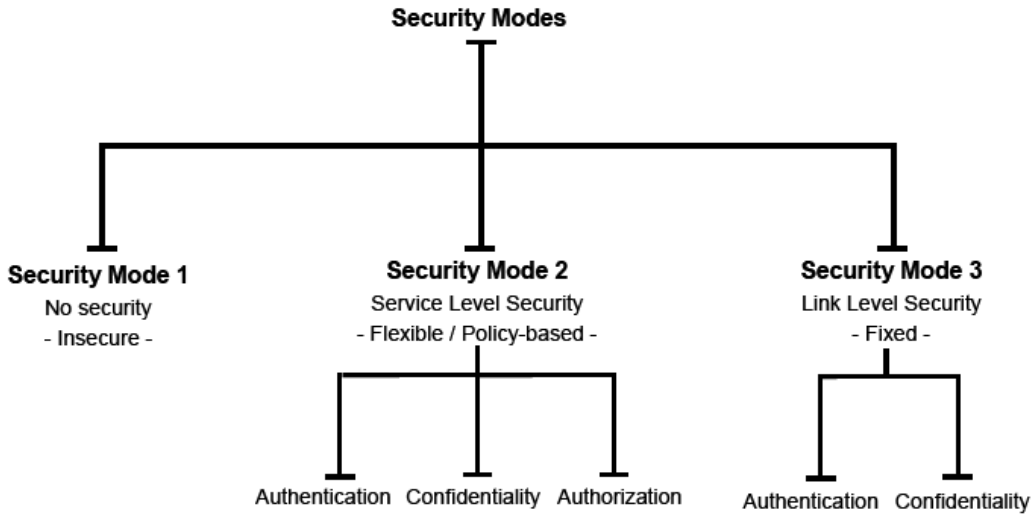
V této kapitole probereme bezpečnost Bluetooth obecně a podíváme se na režimy, které podporuje.

Zařízení má několik způsobů jak zachovat bezpečnost:

- adresa zařízení Bluetooth (DB_ADDR), která má 48 bitů a je unikátní pro každé zařízení
- soukromý autentifikační klíč, který je 128b náhodné číslo používané pro autentifikaci
- soukromý šifrovací klíč dlouhý 8 až 128 bitů, používaný pro šifrování
- náhodné číslo (RAND) generované Bluetooth zařízením

Bezpečnost je rozdělena do tří režimů:

- Žádné zabezpečení (No Security)
- Zabezpečení na úrovni služeb (Service Level Security)
- Zabezpečení na úrovni spoje (Link Level Security)



Obrázek 2.2: Bezpečnostní režimy Bluetooth [19]

Zabezpečení je pro zařízení a služby různé. Pro zařízení to jsou dvě úrovně „důvěryhodné“ a „nedůvěryhodné“ zařízení. Důvěryhodné zařízení má neomezený

přístup ke všem službám. Pro služby to jsou 3 úrovně zabezpečení. Zařízení požadující autorizaci (oprávnění) a autentifikaci (legalizaci), jen autentifikaci, a také zařízení, která jsou přístupná všem zařízením. [17]

2.1 Režim bez zabezpečení

Tento režim dovoluje zařízením připojit se bez bezpečnostních mechanismů. Používá se pro aplikace, kde není vyžadována bezpečnost.

2.2 Zabezpečení na úrovni služeb

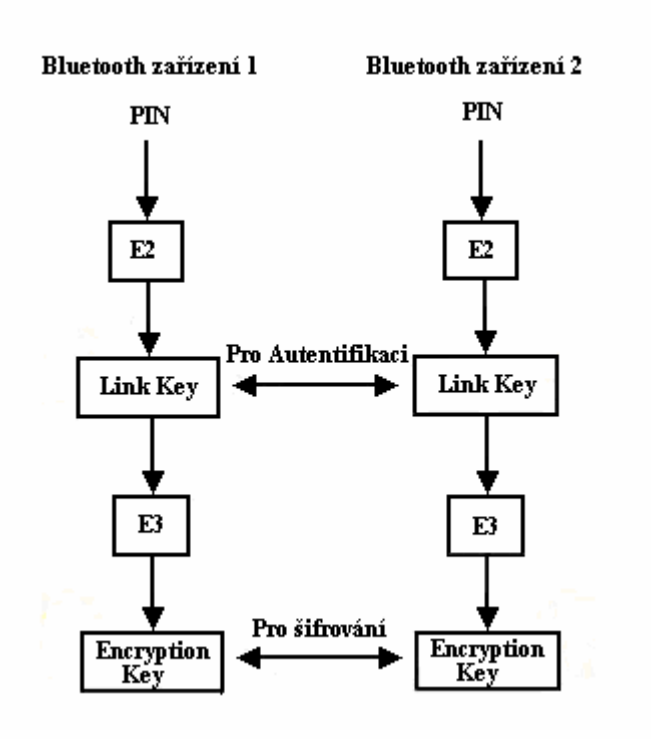
Režimy bezpečnosti jsou zahájeny po založení kanálu na vrstvě protokolu L2CAP. Protokol se nachází na spojové vrstvě a poskytuje spojový a bezspojový přenos dat vyšším vrstvám. Bezpečnostní manažer ovládá přístup k službám a zařízením. Proměnná bezpečnostní politika a úrovně důvěryhodnosti omezují přístup. Může být definováno pro aplikace s různými bezpečnostními požadavky vykonávanými současně. Proto je možné povolit přístup některým zařízením bez poskytnutí přístupu k dalším zařízením. Přichází na řadu autorizace. [19] Autorizace je přidělena po úspěšné autentifikaci, definuje, které operace je možné provádět a jaká data jsou dostupná. [1]

2.3 Zabezpečení na úrovni spoje

Bezpečnost na úrovni spojové vrstvy. Bluetooth začíná zabezpečovat již před založením kanálu. Je to zabudovaný bezpečnostní mechanizmus, nebere v potaz zabezpečení na aplikační vrstvě. Režim podporuje autentifikaci a důvěryhodnost, což je založeno na použití tajného spojovací klíče, který je sdílen párem zařízení. Ke generování tohoto klíče, je použit párovací proces, pokud spolu zařízení komunikují poprvé.[19] Více informací v kapitole 3.

3 Zabezpečení na spojové vrstvě

V systému Bluetooth je k zabezpečení poskytováno mnoho různých typů klíčů. Symetrické šifrovací mechanizmy jsou použity pro autentifikaci, generování klíčů a šifrování na spojové vrstvě.



Obrázek 3.1: Generování a použití klíčů

3.1 Proces párování

Proces párování vyžaduje potvrzení osobního identifikačního klíče, PINu od obou Bluetooth zařízení. [19] Délka PINu použitého u Bluetooth zařízení se může pohybovat mezi jedním až šestnácti oktety (maximálně 128 bitů). Obvyklý čtyřmístný PIN kód je postačující jen pro některé aplikace, avšak aplikace s vyšším požadavkem na zabezpečení potřebují zajisté delší PIN kód. PIN může být pevně dán při výrobě zařízení, obzvláště pokud zařízení disponuje malou pamětí. Často bývá nastaven implicitně na hodnotu 0000 nebo 1234, je doporučeno jej po obdržení zařízení změnit. [17]

3.2 Přidělování klíčů

Veškeré důvěryhodné transakce mezi dvěmi či více stranami jsou řízené spojovacím klíčem. Spojovací klíč je 128b náhodné číslo a používá se při prokazování identity (autentifikaci). Doba životnosti spojovacího klíče závisí na tom, zda je trvalý, může být použit opakovaně, nebo dočasný, jen pro aktuální spojení.

Bluetooth používá několik typů klíčů. Nejdůležitější je spojovací klíč, který může být kombinován z několika klíčů:

- soukromý klíč (unit key)
- hlavní klíč (master key)
- inicializační klíč (init key)
- šifrovací klíč (encryption key)

Použití závisí na typu aplikace.

Soukromý klíč je generován v jednotlivých zařízeních při jeho instalaci. **Kombinovaný klíč** je odvozen od informací dvojice zařízení a generuje se pro každý pár Bluetooth zařízení. **Hlavní klíč** je dočasný klíč, který nahrazuje aktuální spojovací klíč. Toho může být použito, když chce master přenést informace k více než jednomu příjemci. **Inicializační klíč** se používá jako spojovací klíč během inicializačního procesu, kde dosud není žádná jednotka či kombinované klíče, které jsou používané jen během instalace. [17]

Pro generování klíčů a pro autentifikaci se používají algoritmy E0, E1, E3, E21 a E22, které jsou vytvořené na základě symetrického blokového algoritmu SAFER+. E0 je proudová šifra. E1 se používá pro autentifikaci. E3 je algoritmus založený na proudové šifře na bázi LSFR. [1] E21 se používá pro generování kombinovaných a soukromých klíčů, E22 generuje inicializační a hlavní klíče. Důvod k používání algoritmů pro generování klíčů je v první řadě ujistit se, že číslo je „dostatečně“ náhodné.

Inicializační klíč je potřebný, pokud si dvě zařízení spolu přejí komunikovat poprvé. Během inicializačního procesu je PIN kód potvrzen daným zařízením. Inicializační klíč je generován algoritmem E22, který má vstupy v podobě: PIN kódu, BD_ADDR žadatele a 128b náhodného čísla. Výstupní 128b inicializační klíč je používán při

výměně klíče během generování spojovacího klíče. Po výměně je inicializační klíč vyřazen.

Kombinovaný klíč je generován během instalačního procesu, jestliže se ho zařízení rozhodla použít. Je vygenerován oběma zařízeními ve stejnou dobu. Nejprve obě jednotky vygenerují náhodné číslo. Obě zařízení vygenerují klíč Algoritmem E21, který je kombinací náhodného čísla a jejich DB_ADDR. Potom zařízení vymění bezpečně svá náhodná čísla a vytvoří kombinovaný klíč, který budou používat.

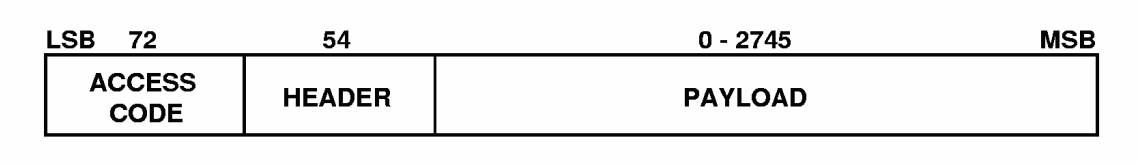
Soukromý klíč je generován algoritmem E21, když se daná operace vykonává Bluetooth zařízením poprvé. Po vytvoření může být uložený v non-volativní paměti (paměť stálá a nezávislá na energii) zařízení a je jen vzácně měněn. Jiné zařízení může použít soukromý klíč tohoto zařízení jako spojovací klíč mezi nimi. Během inicializačního procesu se aplikace rozhoduje, která strana by měla poskytnout soukromý klíč jako spojovací. Jestliže jedno ze zařízení nemá onu paměť (tzn. nepamatuje si žádný další klíč), je použit jeho spojovací klíč.

Hlavní klíč je jediný z popsaných klíčů, který je dočasný. Hlavní klíč je generován masterem pomocí algoritmu E22 se dvěmi 128b náhodnými čísly. Výstup z algoritmu E22 je 128b číslo, stejně jako u generování spojovacího klíče. Náhodné číslo je pak přeneseno k slave zařízení, je vypočítáno oběma zařízeními, masterem i slavem, z algoritmu generující klíč a nynějšího spojovacího klíče. Nový spojovací klíč (hlavní klíč) je po sléze poslán podřízenému zařízení, provedením bitové operace XOR tohoto klíče. Slave může tímto využít hlavní klíč. Tato procedura musí být vykonaná s každým zařízením slave, se kterým chce master použít hlavní klíč.

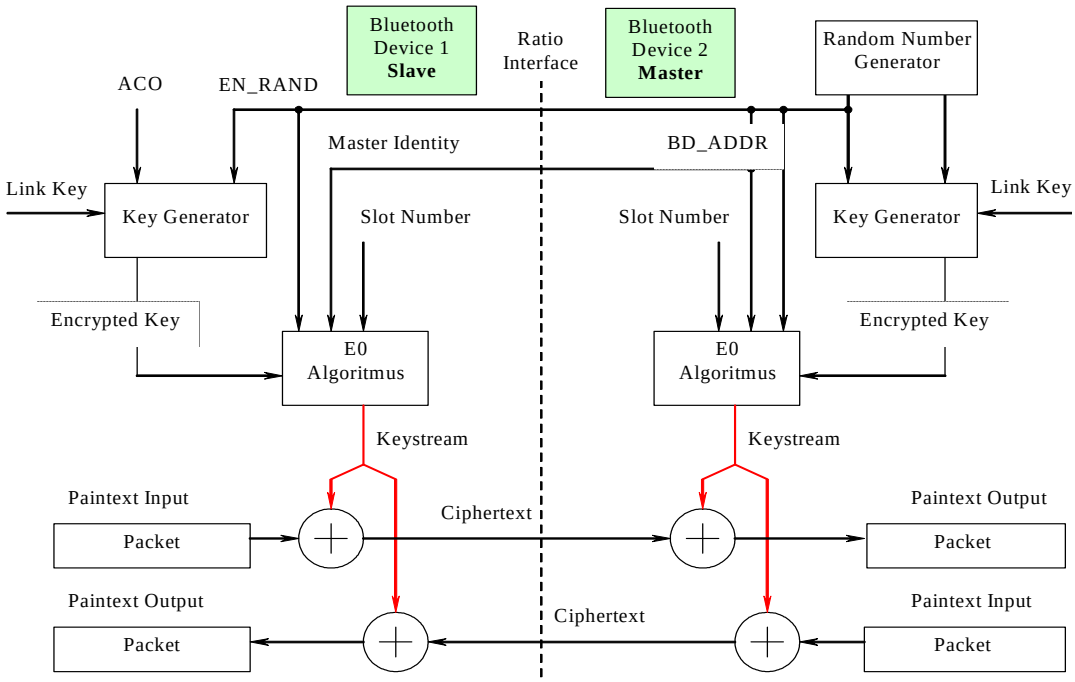
Šifrovací klíč je generován algoritmem E3 z aktuálního spojovacího klíče, 96b šifrovacího čísla COF a 128b náhodného čísla. COF je založeno na ověřovací šifře ACO, která je generována během autentifikačního procesu. Když správce spojení LM aktivuje šifrování, je vygenerován šifrovací klíč. To je automaticky provedeno pokaždé, když Bluetooth potvrdí šifrovací mód. [17]

3.3 Šifrování pro Bluetooth

Systém šifrování pro Bluetooth kóduje tzv. payloads (data, viz. Obrázek 3.3.1) paketů. Kóduje se proudovou šifrou E0, která je re-synchonnizována pro každý payload.



Obrázek 3.3.1: Standardní formát Bluetooth paketu [D]



Obrázek 3.3.2: Bluetooth šifrovací proces

Payload key generátor kombinuje vstupující bity ve vhodném pořadí a posunuje je ke čtyřem lineárním zpětnovazebním posuvným registrům LFSR keystream generátoru. Keystream bity jsou vygenerovány metodou odvozené ze součtu generátoru proudových šifer.

Zařízení používá trvalý spojovací klíč nebo hlavní klíč Pokud je použit soukromý nebo kombinovaný klíč, broadcast přenos není zašifrován. Jednotlivě adresovaná zpráva je buď šifrovaná či nikoli. Jestliže je použitý hlavní klíč, jsou k dispozici tři možné módy.

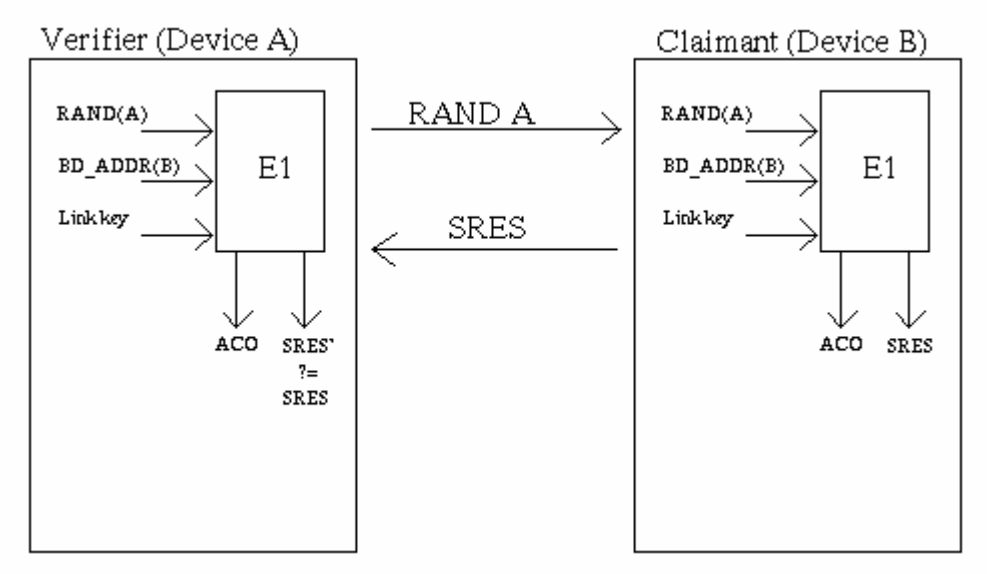
Šifrovací módy:

- mód 1 – nic není šifrováno
- mód 2 – broadcast přenos není šifrovaný, ale jednotlivě adresovaný přenos je šifrován hlavním klíčem
- mód 3 – každý přenos je šifrován

Jelikož je velikost šifrovacího klíče v rozmezí od 8 do 128 bitů, musí se zařízení na použité velikosti dohodnout. Každé zařízení má definovanou maximální možnou délku klíče. Domluva na délce klíče probíhá tak, že hlavní zařízení pošle návrh na délku klíče podřízenému zařízení. Podřízené zařízení klíč buď akceptuje či potvrdí, popř. pošle jiný návrh. Domluva pokračuje do souhlasu na obou stranách a nebo je zrušena použitou aplikací, díky definované minimální přijatelné velikosti klíče. Jestliže nebyl požadavek nikým přijat, aplikace zruší dohadovaní a šifrování nemůže být provedeno. Je to nezbytné k vyhnutí situace, kdy nepovolané zařízení vyvíjí tlak na nedostatečné šifrování za účelem poškození. [17]

3.4 Autentifikace

Bluetooth je založen na principu výzva-odpověď (Challenge-Response), který ověřuje, zda další účastník zná tajný klíč. Protokol používá symetrický klíč. Úspěšná autentifikace je založena na tom, že oba účastníci sdílejí stejný klíč, který je výsledkem ACO a je uložený v obou zařízeních, později je používán pro generování šifrovacího klíče. [17]



Obrázek 3.4.1: Popis autentifikačního procesu [17]

Zařízení A (žadatel) nejprve pošle RAND číslo k zařízení B (ověřovatel) pro autentifikaci, potom oba účastníci použijí autentifikační funkci E1 s náhodným číslem. BD_ADDR zařízení B a aktuální spojovací klíč vyvolají odezvu (SRES). Zařízení A odešle odezvu zařízení B, když se odezvy rovnají, tak jsou zařízení autentifikovaná.

Někdy stačí jen jednostranná autentifikace. Popřípadě může být autentifikace vzájemná, kde obě strany jsou autentifikovány postupně.

Jestliže autentifikace selže, musí počkat určitý čas, než uskuteční další pokus. Časový interval se dvojnásobí po každém následujícím selhání pokusu z té samé adresy dokud nedosáhne maximální doby čekání. Čekací doba klesá exponenciálně k minimu, když nedojde k žádnému selhání pokusu o autentifikaci během časového intervalu. [17]

Další možností je použití třetí důvěryhodné strany, která může ověřovat identitu mezi uživateli [1].

3.5 Zabezpečení Ad hoc

Pro Bluetooth je typické vytváření Ad Hoc sítí. Jsou to sítě, které nemají předem danou strukturu, ta vzniká až za chodu. Vznik sítě by měl být s ohledem na připojování nových uzlů a na odpojování některého uzlu na různých místech, jelikož změny mohou mít vliv na částečnou či úplnou přeměnu struktury sítě.

V ad hoc sítích vytvořených například v konferenčních sálech, je několik možností jak zabezpečit přenos. Především je možné použít kombinované klíče k šifrování přenosu. To znamená, že master zařízení vytváří kombinovaný klíč s každým dalším slave zařízením v síti. Potom je tato informace od slave postupně přeposílána masterem ke všem ostatním slave zařízením.

Další způsob zabezpečení je použití dočasného hlavního klíče. Pak mohou všechny zařízení v síti používat stejný klíč při šifrování přenosu a není třeba oddělené předávání přenosu [17].

4 Zabezpečení na aplikační úrovni

K zabezpečení na aplikační úrovni se používají programy. V následujících kapitolách jsou dva z nich představeny.

4.1 AirMagnet BlueSweep

AirMagnet BlueSweep je freewarová (bezplatná) utilita pro analyzování a identifikování blízkého Bluetooth zařízení, ale je poskytována bez technické podpory.

- identifikuje každé místní zařízení
- vidí vzájemná spojení mezi těmito zařízeními
- identifikuje všechny služby přístupné pro každé zařízení
- jednoduchý způsob jak získat přehled o vašem Bluetooth okolí a identifikovat případné bezpečnostní problémy, které by jinak zůstaly bez povšimnutí

Požadavky pro použití:

- MS Windows XP + Service Pack 2
- ovladače pro Bluetooth adaptér
- lépe použít ovladače, kterými disponuje MS Windows XP, nežli dodané od výrobce [16]
-

4.2 Xafe 1.5

Xafe je aplikace, která chrání důležité údaje v PDA. Údaje jako uživatelské jmého, heslo, PINy, výrobní číslo a vše, co by mělo zůstat utajeno. Je použito 128 bitové šifrování. Výrobce tvrdí, že je pravděpodobnější, že se bude hádat heslo metodou pokus omyl, nežli se bude prolamovat samotné šifrování.

Podpora pro všechny PDA [13]

5 Útoky na Bluetooth a jeho možné zneužití

Bluetooth obsahuje mnoho bezpečnostních chyb a děr, které jsou hackerům dobře známé a využívají jich. Skupina Flexilis nedávno představila zařízení BlueSniper rifle, které detekuje zařízení i na 1 km.

Mobilní zařízení, zvláště mobilní telefony s Bluetooth nabývají na oblibě, ale lidé si jejich zranitelnost ne vždy plně uvědomují. Mnoho uživatelů v takovém zařízení schraňují citlivá data a jejich odcizení či zničení znamená citovou, ale v některých případech finanční ztrátu. [9]

BlueSniper Fifle (puška na Bluetooth).

Johm Hering přispěl k útokům svou BlueSniper Fifle. Píše se, že součástky se dají pořídit za několik stovek dolarů a celou pušku lze složit za jediné odpoledne. Nejdražší součástkou alias srdcem pušky je – 400MHz Gumstix 400f-bt, cena se pohybuje kolem dvě stě dolarů. Konstrukcí se stala americká samonabíjecí malorážka Ruger 10/22, na tělo konstrukce jsou přidány ostatní potřebné komponenty. Použití malorážky místo výchozí konstrukce není podmínkou, ne každý si potrpí na tak militantní vzhled. V původní verzi BlueSniper Rifle byla použita anténa 12.9dBi Yagi, ale nyní je vystřídána 14.9 Yagi.

Takto upravená puška, která se připojí k notebooku, má dosah více než jeden kilometr. Puška otevřela možnosti pro detekování zařízení Bluetooth na poměrně velkou vzdálenost a s tím je spojeno riziko zneužití k útoku. Použitím výkonnější antény by nejspíše vzrostla i uvedená vzdálenost. [11]

5.1 Bluejacking

Blujacking se stal populárním mechanismem pro výměnu anonymních zpráv na veřejných místech. Tato technika zneužívá párovacího protokolu, systém, kterým se Bluetooth autentifikují navzájem, zpráva projde během počáteční handshake (podání ruky) fáze. To je možné, protože jméno iniciovaného Bluetooth je zobrazováno na cílovém zařízení jako součást handshake výměny a protokol dovoluje přenést velké pole až 248 znaků. Bluejacking je docela neškodný, ale je zde potenciální bezpečnostní

problém. Protokol pro výměnu informací bývá zneužit. Schopnost spojení s dalším zařízením a výměna, aktualizace či synchronizace dat je důvodem existence Bluetooth. Zneužitá první část procesu párování dovolí Blujackerovi se úspěšně spárovat se zařízením.Všechna data (kalendář, SMS, telefonní seznam) v cílovém zřízení se jim stanou přístupná.

5.2 BlueSnarfing

Dá se říci, že Bluesnarfing je horší verze Bluejackingu. Byl objeven v roce 2003 Adamem Laurem.

Nebezpečí hrozí některým modelům mobilních telefonů od firem Nokie a Sony Ericsson, některé telefony jsou ohroženy i v skrytém režimu. Útok probíhá bez vědomí majitele a nelze nijak odhalit. Bluesniper může bez pozorování kopírovat telefonní seznam, záznamy v kalendáři, měnit nastavení a dokonce číst IMEI mobilního telefonu. Na váš účet si Bluesniper z vašeho telefonu zavolá, pošle textovou (SMS) či multimediální (MMS) zprávu, využije i služeb jako WAP a okrade vás o data potřebná k přístupu k bankovnímu účtu.

Vzhledem k nebezpečí, kterým Bluesnarfing hrozí, nebyly uvedeny podrobnosti, jakým způsobem dochází k útoku. Ale zřejmě problém spočívá v implementaci protokolu pro objektovou výměnu OBEX. Byl přehlédnut fakt, že protokol umožňuje nejen odesílání zpráv, ale také přístup k vyšším funkcím mobilního zařízení. [8]

5.3 Backdoor útok (zadní vrátka)

Backdoor útok využívá zranitelnosti procesu párování. Pokud zrovna majitel nesleduje své zařízení ve správný čas, je spojení se zařízením navázáno, aniž by se dalo všimnout něčeho neobvyklého. Útočník může volně používat prostředky, které mu zařízení dovoluje. Lze získat nejen data z telefonu, ale i dalších zařízení jako je modem, Internet, WAP a GPRS. Backdoor útok používá brány bez vědomí a souhlasu majitele.

5.4 Denial-of-Service útok (popření služeb)

Často používaná a známá zkratka je DoS útok. DoS útok umožňuje útočníkovi znemožnit efektivně ovládat zařízení. Systém narušený DoS útokem je plně zaneprázdněný obsluhou falešných žádostí o připojení nebo falešným přenosem paketů.

5.5 BlueBug útok

BlueBug vytváří sériový profil připojení, tím dává úplný přístup k nastavení AT command, které může být zneužito.

Se speciálním software lze na dálku vypnout telefon, zavolat si a odposlouchávat hovory.

5.6 Disclosure of Keys (odhalení klíče)

Bluetooth modul připojený k počítači, je možné vyměnit za falešný, jehož jediným účelem je, sát od hostitelského zařízení spojovací klíče.

USB moduly či PCMCIA karty lze odstranit z majitelova počítače a následně vložit do odpovídajícího slotu v cizím počítači. Zde dojde k odposlouchání jednoho nebo více klíčů. Jakmile je jednou přečten seznam klíčů, je zařízení vráceno zpět.

Škodlivý software

Trojský kůň přestrojený za něco docela nevinně vypadajícího, umí odeslat databázi klíčů na určené místo, kam má přístup útočník. Pokud je škodlivý kód distribuovaný virem či červem, může se šířit k nespočetně mnoha zařízením.

5.7 Brute-Force útok

Tento útok se dokáže připojit k zařízení dokonce, i když je ve skrytém režimu (no discoverable). Pokud je jednou BD_ADDR útokem zjištěna, další útoky mohou být vykonány bez varování vlastníka, který si myslí, že je neobjevitelný.

5.8 Bluetooth Wardriving (Tracking)

Tento útok mapuje umístění zapnutého Bluetooth zařízení. Od každého zařízení odešle jeho unikátní BD_ADDR, to pak umožňuje sledovat jeho pohybu. K ochraně zařízení proti lokálnímu sledování je potřeba použít anonymní mód..

5.9 Replay útok

Hacker může zaznamenávat Bluetooth přenosy ve všech 79 frekvencích. Z toho vypočítá sekvenci přeskakovaní frekvence, aby mohl zopakovat veškeré přenosy. Bluetooth zařízení není schopno rozpoznat, zda je zpráva nová či stará.

5.10 Viry

Bylo jen otázkou času, kdy se autoři virů zaměří na přenos mezi mobilními zařízeními. Jedná se o viry, které jsou určeny jen pro OS Symbian.

Prvním virem byl Cabir. Z novějších virů lze nezmínit Commwarrior, Mabir.A. a Doomboot.A. [11]

Cabir

Cabir se šíří přes Bluetooth jako soubor caribe.sis, který obsahuje červa. Uživatel musí souhlasit s instalací, aby byl telefon infikován. Potom Cabir hledá pomocí Bluetooth, koho by nakazil. Červ pošle svou kopii prvnímu zařízení, které najde a potom se zamkne v telefonu. Další infikování je možné po restartování telefonu, to znovu aktivuje červa a může nakazit opět jedno zařízení. [22]

CommWarrior

CommWarrior.A je červ, který je schopen šířit se jak přes Bluetooth tak i pomocí MMS zpráv. CommWarrior se šíří jako soubor s příponou SIS a jménem souboru je náhodné, aby uživatel nemohl být varován před určitými názvy. Tento soubor obsahuje červa jako spustitelný soubor commwarrior.exe a bootovací soubor cmmrec.mdl. Po infikování telefonu se automaticky nainstaluje, pak začne hledat přes Bluetooth další zařízení a rozesílat svou kopii, nebo se šířit zprávami MMS [20].

Hlavním rozdílem mezi **CommWarrior.A** a CommWarrior.B je, že CommWarrior B nekontroluje systémové hodiny, jinak má podobný princip. [18]

Mabir.A

Mabir je červ, který se šíří přes Bluetooth, MMS a SMS pod jménem caribe.sis, jako Cabir. Caribe.sis obsahuje soubory caribe.app, caribe.rsc a flo.mdl. Po infikování se nainstaluje spouštěcím souborem caribe.app a hledá další zařízení s Bluetooth, kterým následně posílá svou repliku [21]. Po odeslání souboru se na cíleném telefonu objeví výzva „Install Caribe?“ a je jen na majiteli, zda-li tuto otázku potvrdí. [11]

Doomboot.A

Doomboot je záludný tojský kůň, který s sebou nese červa CommWarrior.B. Doomoot se tváří jako pirácká verze hry Domm 2. Pokud se dostane do telefonu, tak rozesílaním červa do hodiny vybije baterii a způsobí selhání dalšího nabootování telefonu. [23]

5.11 Jak telefony napomáhají vykrádat automobily

Mobilní telefony nebo PDA mohou a pomáhají zlodějům odhalit notebooky v zaparkovaných automobilech. Zloději si osvojili výhodu této technologie, a proto by si lidé měli toto riziko uvědomit. Měli by po odchodu od zaparkovaného automobilu deaktivovat svá zařízení s Bluetooth, jinak ulehčují práci vykradačům automobilů.

Na druhou stranu tato technologie pomáhá při hledání či sledování ukradeného automobilů, které obsahovaly již zmíněný notebook či jiná zařízení s aktivním bluetooth. [15]

Závěr

Se získaným informacemi částečně sepsanými výše lze vyvodit jednoduchý závěr, že je Bluetooth relativně bezpečná technologie.

Bezpečnosti nahrávají skutečnosti, že jde o zařízení na krátkou vzdálenost a z toho vyplívá, že není tak snadno odposlouchatelná. Dále tu je metoda FHSS, zvláště pak ASH, které jsou další výhodou Bluetooth. Přeskakovat mezi vysílacími frekvencemi pomáhá překonat zaručené prostředí a touto nepředvídatelnou sekvencí přeskoků zabraňuje odposlechu nebo ztrátě dat.

Nebezpečnou stránkou Bluetooth je možnost prolomení šifry, obcházení párování, ať už virem nebo jedním z útoků. Nedostatečná je autetnifikace, autetnifikuje se jen zařízení, nikoliv uživatel. Nebezpečí taktéž skýtá sdílení hlavního klíče. Bluetooth nezabezpečuje konečnou fázi přenosu.

Jak zabezpečení pomoci? Změnit implicitní PIN a nastavit ho na co nejdelší, používat kombinaci velkých i malých znaků a číslic. Pro přenos informací, zejména klíčů a hesel, je nutné používat šifrování. Hesla nejlépe nepřenášet vůbec. Neukládat citlivá data do sdílených adresářů. Autentifikovat zařízení vzájemně, použije se kombinovaný klíč, nikoliv klíč zařízení. Nepotvrzovat výzvy k instalaci neznámých souborů a nevyžádaných souborů. Velmi vhodné je doplnit zařízení o zabezpečení na aplikační vrstvě.

Navázáním na vývoj Bluetooth je technologie UWB. Má podobný dosah jako Bluetooth, ale chlubí se větší přenosovou rychlostí. Nástupcem pro Bluetooth by se mohla stát novější technologie ZegBee má přenosovou rychlost srovnatelnou se sériovou linkou. Uplatnění Zegbee by mělo být hlavně v automatizaci.

V budoucnosti by Bluetooth mohlo například automatizovat budovy. Představou je, že máte doma jeden počítač s monitorem a k němu připojené domácí spotřebiče a můžete je ovládat z jednoho místa. Tímto lze ušetřit i za displeje. Dalším možným významem je využití telematických zařízení v automobilovém průmyslu, a to nejen u navigačních a asistenčních systémů, ale také při přístupu k informačním zdrojům, včetně internetu.

Hlavní radou na závěr je, vypněte své Bluetooth, pokud ho nepoužíváte. Při použití nastavte skrytý režim, zúžíte počet možností jak napadnout a zneužít vaše zařízení.

Seznam použité literatury

Knihy:

[1] PUŽMANOVÁ Rita. *Bezpečnost bezdrátové komunikace*. CP Books, a.s. 2005, ISBN 80-251-0791-4, (kap. 7)

[2] PUŽMANOVÁ Rita. *Širokopásmový Internet aneb Přístupové a domácí sítě.* Computer Press 2004, ISBN 80-251-0139-8, (kap. 15)

Internet :

[3] MobileMag.com. *Bluetooth pomůže uživatelům s poškozením sluchu.* [online]. [cit. 28.3.2006]. URL: <mobil.idnes.cz/telefony.asp?r=telefony&c=A051116_110353_telefony_DNO>

[4] PUŽMANOVÁ Rita. *Osobní sítě - Bluetooth a IEEE 802.15.* [online]. [cit. 29.3.2005].
URL: <http://www.lupa.cz/clanky/osobni-site-bluetooth-a-ieee-802-15/>

[5] PUŽMANOVÁ Rita. Modrý *zub aneb Bluetooth, sítě osobní - část 3.* [online]. [cit. 10.4.2006]. URL: <http://www.telnet.cz/content.php?con_id=195>

[6] SVOBODOVÁ Nicola. *Coje to Bluetooth.* [online]. [cit. 1.5.2005].
URL: <http://nikca.blog.cz/>

[7] BRADÁČ Zdeněk, FIEDLER Petr. *Bezdrátové komunikace v automatizační praxi II: standard Bluetooth.* [online]. [cit. 10.4.2006]
URL: </www.automa.cz/automa/2003/au070338.htm>

[8] MAREČEK Ivo. *Dejte si pozor na bluesnarfing!.* [online]. [cit. 30.3.2006].
URL: <www.mobilmania.cz/Profi/AR.asp?ARI=107925>

[9] NOVÁK David. *Raději se neotáčejte, možná na vás míří BlueSniper.* [online]. [cit. 30.3.2006].
URL: <mobil.idnes.cz/tiskni.asp?c=A040806_5265930_mob_tech&r=mob_tech>

[10] MIKÉSKA Zdeněk. *Specifikace rádiové části systému Bluetooth.* [online]. [cit. 30.3.2006]. URL: <www.hw.cz/externi/1167/>

[11] BITTO Ondřej. *Trhání zoubků Bluetooth.* [online]. [cit. 5.4.2006].
URL: <www.lupa.cz/clanky/trhani-zoubku-bluetooth/>

[12] MALÝ Ivo. *Bluetooth – algoritmy pro vytváření ad hoc sítí*. [online]. [cit. 10.4.2006]. URL: <atm.felk.cvut.cz/mps/referaty/2004/maly/bluetooth.html>

[13] *Xafe 1.50.* [online]. [cit. 5.4.2006]. URL: <www.slunecnice.cz/product/Xafe/?SID=056DAAABE4E71129BB1F7998C8B6A9A9>

Anglické texty:

[14] *Bluetooth* History. [online]. [cit. 30.3.2006]. URL: <www.bluetooth.com/Bluetooth/SIG/Who/History/>

[15] Cambridge Newspapers. *Phone pirates in seek and steal mission.* [online]. [cit. 30.3.2006]. URL: <www.cambridge-news.co.uk/news/region_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf>

[16] *AirMagnet BlueSweep.* [online]. [cit. 5.4.2006]. URL: <www.gsec.co.uk/products/index/Wireless_Security/AirMagnet/AirMagnet_BlueSweep/>

[17] VAINIO Juha T. *Bluetooth Security*. [online]. [cit. 5.4.2006]. URL: <www.niksula.hut.fi/~jiitv/bluesec.html>

[18] NIEMELA Jarno. *Commwarrior.B.* [online]. [cit. 7.5.2006]. URL: <www.f-secure.com/v-descs/commwarrior_b.shtml>

[19] JANSSENS Sil. *Attacking Bluetooth devices.* [online]. [cit. 7.5.2006]. URL: <student.vub.ac.be/~sijansse/2e%20lic/BT/Thesis/Thesis.pdf>

[20] HYPPONEN Mikko, NIEMELA Jarno. *Commwarrior.A.* [online]. [cit. 7.5.2006]. URL: <www.f-secure.com/v-descs/commwarrior.shtml>

[21] NIEMELA Jarno. *Mabir.A.* [online]. [cit. 7.5.2006]. URL: <www.f-secure.com/v-descs/mabir.shtml>

[22] NIEMELA Jarno, RAUTIAINEN Sami. C*abir.* [online]. [cit. 7.5.2006]. URL: <www.f-secure.com/v-descs/cabir.shtml>

[23] NIEMELA Jarno. *Doomboot.A.* [online]. [cit. 7.5.2006]. URL: <www.f-secure.com/v-descs/doomboot_a.shtml>

Obrázky:

[A] www.b-speech.cz/data_speed/popis.htm

[B] www.ccc.de/congress/2004/fahrplan/event/66.en.html

[C] www.rdc.cz/index.php?jazyk=0&sid=1&main=sekce&stav=clanek&cid=260&PHPSESSID=811563127c83411ec689a88381f838eb

[D] www.cs.hut.fi/~ctl/btpacket.pdf

[E] www.automa.cz/automa/2003/au070338.htm