Bezpečnost Bluetooth

1. ÚVOD

Bluetooth se stal velmi populární technologií pro komunikaci a synchronizaci dat mezi mobilními zařízeními na velmi krátkou vzdálenost. Přes některé informace o potenciálních útocích na Bluetooth je třeba předeslat, že v bezdrátové komunikaci patří Bluetooth k nejbezpečnějším. V rámci bezpečnostní politiky je ale potřeba přezkoumat nasazení Bluetooth v podnikové komunikaci, seznámit se s reálným nebezpečím implementace technologie na konkrétních produktech. Bluetooth je nejstarší technologií, která slouží k bezdrátové *ad hoc* komunikaci s malým dosahem (do 10 m) mezi přenosnými zařízeními (od mobilních telefonů, PDA, až k laptopům), stacionární výpočetní technikou (PC, myš, klávesnice, tiskárny, skenery) a v poslední době i spotřební elektronikou (audio zařízení, fotoaparáty). Bluetooth ale není jedinou technologií, která patří mezi malé (osobní) bezdrátové sítě, jako nestarší je ale nejrozšířenější.

V současnosti existuje několik norem pro bezdrátovou komunikaci na krátkou vzdálenost, tzv. WPAN (Wireless Personal Area Network), bluetooth náleží specifikace **802.15.1** z roku 2002 (Bluetooth, pro komunikaci na vzdálenost do 10 m rychlostí do 1 Mbit/s v pásmu 2,4 GHz).

Technologie Bluetooth měla primárně sloužit jako náhrada kabelů na krátkou vzdálenost mezi počítači a periferními zařízeními, pro sdílení a přenos souborů, tisk a elektronickou komunikaci v rámci kanceláře. Kromě komunikačních a výpočetních systémů lze dnes Bluetooth využít i v domácích sítích pro komunikaci se spotřební elektronikou a domácími spotřebiči. V podnikovém prostředí se Bluetooth ujal pro výměnu vizitek či synchronizaci souborů, e-mailů či kalendářů mezi PDA a laptopy.

Bluetooth jako náhrada kabelů měl také poskytovat odpovídající zabezpečení komunikace. Jako každá rádiová komunikace je však náchylnější na odposlech, a tak je zabezpečení komunikace, uživatelů a dat složitější. Malý dosah Bluetooth přispívá k zabezpečení, ale nahodilá topologie sítě příliš bezpečnosti neprospívá.

Rádiový systém Bluetooth původně vyvinula společnost *Ericsson* (název byl zvolen podle přizdívky dánského krále z 10. století Haralda Blĺtanda). Vývojem Bluetooth se zabývá od roku 1998 Bluetooth SIG (Special Interest Group). IEEE přijal Bluetooth 1.1 jako první normu pro WPAN pod označením 802.15.1. Norma nabízí WPAN pracující rychlostí 1 Mbit/s na fyzické vrstvě, přičemž propustnost uživatelských dat se *pohybuje do 720 kbit/s.*

2. ZÁKLADNÍ VLASTNOSTI BLUETOOTH

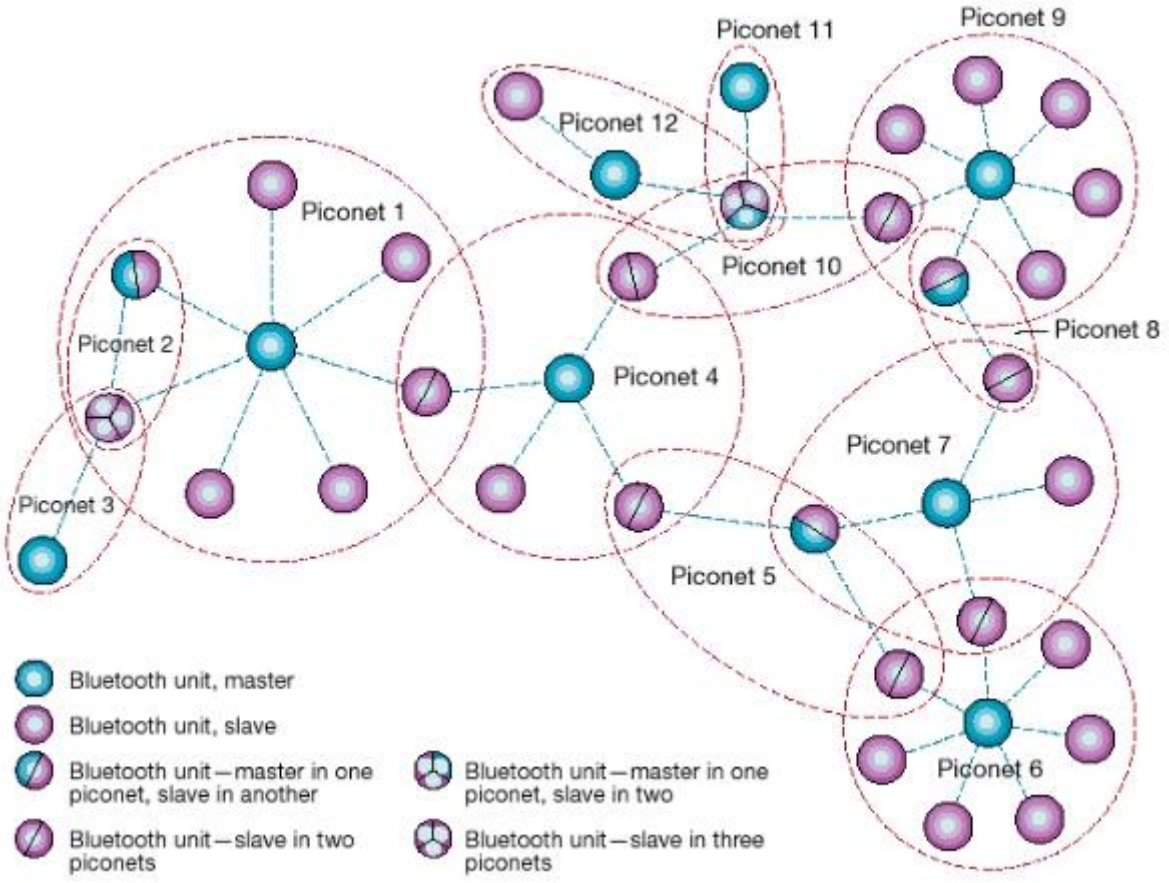
Základní vlastnosti Bluetooth se dají shrnout do tří bodů.

- **Účel:** nahodilá (ad hoc) rádiová komunikace bez závislosti na síťové infrastruktuře (přístupovém bodu) pro výměnu informací mezi dvěma stanicemi (dvoubodová), nebo více stanicemi (mnohobodová topologie).

- **Funkčnost:** v pásmu 2,4 GHz, od 10 cm do 10 m, symetricky rychlostí 433 kbit/s, asymetricky 723/57 kbit/s, maximálně tři simultánní hlasové kanály o 64 kbit/s;
- **Aplikace:** výpočetní a komunikační technika (podnikové sítě), spotřební elektronika (domácí sítě), telematické systémy v automobilech.

Topologie Bluetooth umožňuje nahodilé *(ad hoc)* seskupení komunikujících zařízení (zařízení se může snadno kdykoli připojit nebo odpojit od sítě, v režimu tzv. *spontaneous networking)* a není závislá na síťové infrastruktuře (na rozdíl od většiny dnes používaných bezdrátových lokálních sítí, typicky Wi-Fi). Komunikující zařízení se v síti chovají jako rovnocenná.

Bluetooth podporuje jak dvoubodovou tak mnohabodovou komunikaci. Pokud je více stanic propojeno do sítě s topologií hvězda, tzv. pikosítě *(piconet),* jedna rádiová stanice působí jako hlavní *(master)* a může simultánně obsloužit až 7 podřízených *(slave)* zařízení. Veškerou komunikaci řídí hlavní rádiová stanice a podřízená stanice může komunikovat s ostatními výhradně prostřednictvím hlavní stanice. Pikosítě lze dále sdružovat do tzv. rozprostřených sítí *(scatternets),* viz obrázek 2.1.



Obrázek 2. 1

Bluetooth pracuje v bezlicenčním kmitočtovém pásmu 2,4 GHz, které využívá také celá řada dalších zařízení včetně mikrovlnných trub či bezdrátových lokálních sítí. Rušení s ostatními zařízeními se brání tím, že na fyzické vrstvě používá metodu rozprostřeného spektra **FHSS** *(Frequency-Hopping Spread Spectrum),* kdy na jednom kmitočtu se vysílá vždy jen po dobu 625 ps.

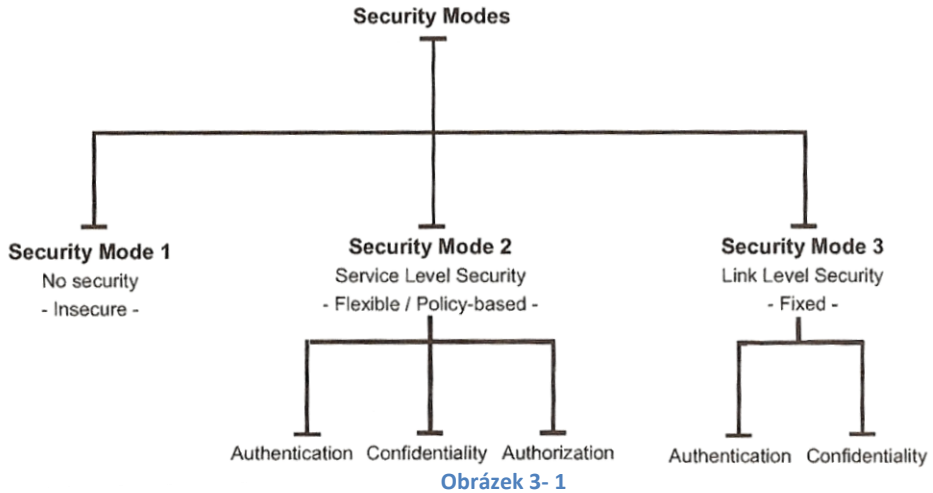
Velmi rychlé přeskoky mezi kmitočty přispívají k implicitní bezpečnosti Bluetooth, protože ztěžují odposlech. Malý dosah sítě do 10 m je s ohledem na bezpečnost také výhodou např. ve srovnání se sítěmi WLAN, které mají dosah stovek metrů.

3. BEZPEČNOSTNÍ SLUŽBY BLUETOOTH

Bluetooth poskytuje tři základní bezpečnostní služby: **autentizaci** (ověření totožnosti komunikujících stran), **důvěrnost** (ochrana před odposloucháváním) a **autorizaci** (povolení přístupu ke službám). Specifikace nabízí tři úrovně bezpečnosti, dvě úrovně důvěry vůči zařízení a tři úrovně bezpečnosti služby.

Zařízení Bluetooth může pracovat v jednom ze tří **bezpečnostních režimů:**

- **bez zabezpečení** - promiskuitní režim umožňující jakémukoli jinému zařízení navázat komunikaci
- **bezpečnost na úrovni služeb** - zajišťuje autorizaci přístupu ke službám na daném zařízení
- **bezpečnost na úrovni spoje** - zařízení iniciuje bezpečnostní postupy (autentizace a šifrování) před vlastním navázáním spojení.



Obrázek 3- 1

Řízení přístupu lze zajistit prostřednictvím volby bezpečnostního režimu pro službu (služby vyžadující autentizaci a autorizaci, služby vyžadující pouze autentizaci, či služby dostupné všem) a úrovně důvěry či zařízení (důvěryhodné a nedůvěryhodné).

4. ZÁKLADNÍ SLOŽKY BEZPEČNOSTNI BLUETOOTH

- Přeskakování mezi kmitočty
- Jedinečná adresa zařízení
- Klíče odvozené z PIN
- Autentizace zařízení sdíleným 128bitovým klíčem
- Důvěrnost dat zajištěná proudovou šifrou konfigurovatelné délky(8-128 bitů)

Zařízení s podporou Bluetooth jsou sice schopna se vzájemně lokalizovat, ale komunikace mezi nimi už vyžaduje zásah uživatele ve fázi inicializace, kdy se dvě komunikující stanice vzájemně párují *(pairing* nebo *bonding process).* Nejprve se vygeneruje inicializační klíč na základě identického PIN na obou zařízeních, unikátní adresy vyzyvatele (BD_ADDR) a čísla náhodně vygenerovaného ověřovatelem a odlišného pro každou transakci.

PIN je dlouhý 8 až 128 bitů (nejčastěji se používá PIN v délce čtyř číslic) a bud' jej může uživatel zadávat ručně, nebo může být uložen v paměti zařízení. Pokud se používá pouze čtyřmístný PIN, měl by uživatel nastavit svoji hodnotu (neponechávat implicitní 0000). Pouze u zařízení s minimální pamětí a minimálním uživatelským rozhraním je PIN pevně zadaný již ve výrobě.

Adresa (v délce 48 bitů jako u síťové karty) je jedinečná pro každé zařízení a je veřejná. Veřejné je také náhodné číslo (v délce 128 bitů), které je ovšem nepředvídatelné pro každou transakci.

Inicializační fáze výměny informací je nejnebezpečnější, protože není nijak chráněna, proto se nedoporučuje realizovat proces párování na veřejných místech, kde hrozí odposlech. S pomocí inicializačního klíče se následně vygeneruje **klíč spoje** *(link key),* který sdílí dvojice stanic a na jehož základě probíhá autentizace a šifrování spoje. Tento klíč je tajný a zařízení jej nikdy nevysílá. Je potřeba zdůraznit, že bezpečnostní mechanismy se vztahují pouze na jednotlivé spoje, jak naznačuje následující obrázek.

1.1. PARAMETRY ZAŘÍZENÍ PRO ZABEZPEČENÍ

- BD_ADDR - adresa zařízení;
- PIN - přidělený vlastníkem zařízení nebo výrobcem
- privátní klíč zařízení *(unit key)* - vygenerován při prvním použití zařízení s použitím generátoru náhodných čísel

5. AUTENTIZACE A ŠIFROVÁNÍ BLUETOOTH

V Bluetooth se autentizuje zařízení, nikoli uživatel. Pro autentizaci se používá klíč spoje. Tím může být buď klíč zařízení, kombinační klíč, či hlavní klíč. Klíč zařízení *(unit key)* se generuje při instalaci zařízení a aplikace při inicializaci rozhodne, čí klíč zařízení se použije jako klíč daného spoje (Typicky klíč zařízení s omezenou pamětí, do níž se další klíč nevejde). Kombinační klíč *(combination key)* se po dohodě generuje ve fázi inicializace kombinací klíčů komunikujícího páru stanic. Je bezpečnější než použití klíče zařízení, který je stejný pro jakoukoli komunikaci daného zařízení.

Klíč spoje může být bud' trvalý (uložený v paměti nezávislé na napájení nebo dočasný. Trvalý klíč lze použít ve stejném tvaru i pro další spojení (typicky klíč zařízení, nicméně uživatel jej může změnit. Dočasný klíč slouží pouze pro danou relaci, např. pro mnohobodovou komunikaci, kde všichni Účastníci musí sdílet jeden hlavní klíč *(master key),* který nahrazuje jednotlivé klíče spoje.

Vlastní proces autentizace, který probíhá na úrovni spoje (prostřednictvím Bluetooth čipu), používá princip výzva-odpověď. Vyzyvatel zašle svoji adresu a od druhé komunikující strany dostane náhodné číslo. Na základě těchto hodnot a sdíleného klíče spoje se pomocí autentizační funkce

spočítá výsledek, který si obě strany porovnají. Specifikace neřídí, kdo ověřuje totožnost koho, takže závisí na aplikaci, zda se použije jednostranná nebo vzájemná autentizace. Cílem je ve dvou krocích ověřit, zda druhá strana zná sdílený klíč. Tento proces někdy může být pro uživatele skrytý, protože zařízení se mohou automaticky autentizovat, jakmile se octnou v dosahu vysílání.

1.2. AUTENTIZAČNÍ KLÍČ

- **inicializační klíč** = BD_ADDR + PIN + náhodné číslo -> **klíč spoje** (sdílený klíč);.
- alternativně se klíčem spoje stane **klíč zařízení**

1.3. ŠIFROVACÍ KLÍČ

Šifrovací klíč se odvozuje od autentizačního klíče, ovšem pro každý paket nově. Délka šifrovacího klíče (mezi 8 až 128 bity) se musí mezi komunikujícími stranami předem dohodnout. Oddělení klíčů pak umožňuje použít slabší zabezpečení kratším klíčem, aniž by se ovlivnila síla autentizace. Vlastní režim šifrování přenášených dat pak závisí mj. na typu klíče spoje.

šifrovací klíč = klíč spoje + náhodné číslo + BD_ADDR + hlavní takt *(master clock)*

Autentizaci a generování klíčil se používají algoritmy E_0, E_I, E_3, E_{21} a E_{22} vytvořené na bázi symetrického blokového algoritmu **SAFER+** *(Secure And Fast Encryption Routine)* a pro šifrování symetrický tokový algoritmus na bázi posuvného registru s lineární zpětnou vazbou.

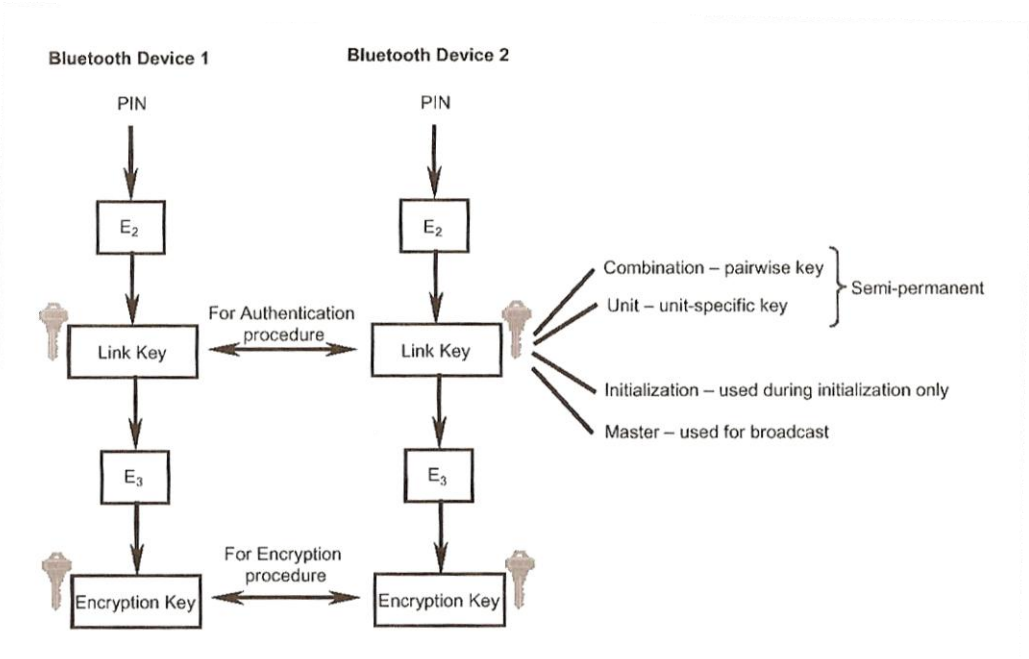
1.4. ROZDÍLY V ZABEZPEČENÍ WLAN A BLUETOOTH

Při autentizaci se v Bluetooth nikdy nepřenáší sítí pár výzva-zašifrovaná odpověď. Navíc algoritmus E_1 nelze invertovat podobně jako XOR použité u WLAN. Pro autentizaci a šifrování se používají u Bluetooth různé klíče.

6. BEZPEČNOSTNÍ POSTUP

Bezpečnostní postup u Bluetooth je následující:

1. vygenerování klíčů dvou zařízení (pomocí algoritmu E_{21});
2. vygenerování inicializačního klíče (E_{22}), autentizace (E_1I) a výměna klíčů spoje podle E_{21}
3. autentizace (E_I), generování šifrovacího klíče (E_3) a šifrování komunikace (Eo).



Starší verze specifikace, Bluetooth 1.0, ponechávala řadu podrobností týkajících se bezpečnosti na výrobcích. Proto zařízení od různých výrobců mohla generovat různé klíče a nemusela pak být schopna navázat spojení. Problémem se stávala situace, kdy se každé zařízení domnívalo, že je hlavní stanicí. Specifikace Bluetooth 1.1 (která se promítla do normy IEEE 802.15.1) vyřešila tento problém vzájemné spolupráce zařízení tak, že hlavní stanice vyžaduje od podřízené stanice potvrzení, že je v podřízené roli.

7. BEZPEČNOSTNÍ SLABINY BLUETOOTH

- **krátké PIN** povoleno - čtyřmístné PIN dává šanci je snadno uhodnout, delší a složitější PIN jsou pro útočníky podstatně větším oříškem
- chybí metoda **distribuce PIN** - ve větší síti je ruční zadávání problematické a přenášet je bezdrátově je z bezpečnostních důvodů nevhodné
- **délka šifrovacího klíče** - musí se na počátku dohodnout a často se volí minimální délka
- **klíč zařízení** *(unit key)* **veřejně dostupný** - lépe jej použít pro generování náhodného klíče, nebo použít sadu klíčů místo jediného klíče zařízení
- **hlavní klíč** - sdílený
- **autentizace** - slabá, na základě výzvy-odpovědi, autentizuje se pouze zařízení, nikoli uživatel
- **proudová šifra E0** - slabá
- **zabezpečení omezeno** pouze na spoj Bluetooth - chybí zabezpečení koncové komunikace

8. ÚTOKY NA BLUETOOTH

Podle nedávného zjištění hrozí zařízením s aktivní podporou Bluetooth hned dva útoky. Útok formou **zadních vrátek** používá standardní párování komunikačních zařízení, kdy zařízení, které původně bylo důvěryhodné a bylo mezitím vyjmuto ze seznamu partnerů, může stále navázat anonymní komunikaci. Tak lze získat neautorizovaný přístup do zařízení bez zobrazení identifikace komunikující strany. A to nejen přístup k uloženým datům, ale také k placeným službám jako přístup k Internetu, WAP či GPRS. Permanentní odstranění seznamu spárovaných zařízení na ochranu před útokem zadními vrátky je sice možné, ale pouze přestavením ve výrobě, čímž se ztratí také veškerá osobní data.

Mobilním telefonům hrozí druhý útok označovaný jako ***bluesnarf.*** Jím lze modifikovat a kopírovat adresář nebo kalendář na mobilu, či získat identifikátor telefonu, a v důsledku dokonce ukrást identitu uživatele, klonovat telefon nebo získat přístup k bankovním účtům majitele telefonu. Jinými slovy nese hrozbu od nepříjemností s odhalením totožnosti a citlivých osobních či podnikových informací až po skutečně finanční újmu.

Bluesnarf obchází proces při párování před vlastní komunikací, takže útočník se může bez varování připojit k cizímu zařízení a získat přístup k určité části uložených dat. Většinou se tak děje v případě, kdy je zařízení viditelné pro ostatní, ale již existují prostředky pro realizaci útoku na zařízeních, která jsou ve skrytém režimu (*non-discoverable*). Pokud napadený uživatel svůj mobil právě nesleduje, o samotném útoku se vůbec nedozví.

Pro uživatele znamená potenciální hrozba *Bluesnarf* v první řadě nutnost přezkoumat, zda mají deaktivovaný Bletooth, pokud ho nepotřebují. Většina zařízení se totiž do rukou uživatelů dostává s aktivovanou podporou Bluetooth již od výrobce.

Podle ***Bluetooth SIG*** (BSIG) je nebezpečí hrozící prostřednictvím *Bluesnarf* na mobilních telefonech relativně velmi malé. Doporučení je jednoznačné: přepnout zařízení do režimu *non-discoverable*, čímž se skryje zařízení tak, aby na veřejných místech na ně nemohl být spáchán útok *snarf*, a to v dosahu až 30m ve volném prostranství. Při tom není pro právoplatného uživatele mobilního telefonu používán aplikací Bluetooth nijak omezeno.

9. DOPORUČENÍ PRO ZABEZPEČENÍ BLUETOOTH

- používat heslo pro přístup k zařízení Bluetooth (pro případ krádeže)
- změnit implicitní PIN a nastavit jej co nejdelší
- předávat PIN mimo komunikaci po síti
- používat vzájemnou autentizaci zařízení na základě kombinačního klíče, nikoli klíče zařízení
- zapnout režim šifrování a dohodnout minimální délku šifrovacího klíče
- neuchovávat citlivá data ve sdílených adresářích
- nespouštět proces párování na veřejnosti, kde lze signál snadno odposlouchávat
- spravovat "viditelnost" vlastního zařízení vůči okolí
- implementovat navíc bezpečnost na aplikační vrstvě