BLUETOOTH

Free your life

A cura di

Di Martino Fabio

Indice generale

Profili di scambio oggetti
- FTP (File Transfer Protocol Profile)
- SP (Synchronization Profile)
- OPP (Object Push Profile)

8 - Sicurezza

Chiavi e sicurezza

Attacchi alla sicurezza
- all' autenticazione
- alla cifratura
- alla comunicazione
- al canale

Vulnerabilità in Bluetooth
- Convalida
- Esposizione
- Casualità
- Deallocazione

Possibili soluzioni

9 - Applicazioni Pratiche
- Bluetooth a casa
- Bluetooth al lavoro
- Bluetooth al negozio
- Bluetooth in automobile
- Bluetooth in valigetta
- Bluetooth e auricolari
- Bluetooth e gioielli digitali

10 - Curiosità
- Toothing
- Bluejacking
- Bluesnarfing

BLUETOOTH

Il nome di questa tecnologia deriva da Harald Blatand "Bluetooth", Re della Danimarca agli inizi del X secolo. Mentre i popoli nordici erano in guerra, egli riuscì a unificare la Danimarca e parte della Norvegia. Harald fu ucciso nel 986 a.C durante una battaglia dal figlio. Anche se non riuscì a unificare tutte le nazioni nordiche, il suo nome è diventato sinonimo di una tecnologia senza fili orientata alla comunicazione mobile.
Il logo che contraddistingue la tecnologia è ispirato a simboli runici riguardanti appunto la leggenda di Harald Bluetooth.

1) PRESENTAZIONE TECNOLOGIA

E' una tecnologia che consente la realizzazione di comunicazioni wireless a corto raggio (sia per dati che per voce) tra qualsiasi tipo di dispositivo elettronico. Questa comunicazione avviene senza l'intervento manuale esplicito dell'utente; indipendentemente dal dispositivo abilitato a Bluetooth individuato da un altro dispositivo dello stesso tipo, i due dispositivi si sincronizzano automaticamente, dando luogo ad un tipo di rete wireless istantanea.

La tecnologia Bluetooth è specificatamente progettata per realizzare la comunicazione senza fili per apparecchi di piccole dimensioni. Il concetto chiave ispiratore di questa tecnologia è quello di eliminare completamente i cavi necessari alla comunicazione fra apparecchi.

Questa tecnologia utilizza segnali di radiofrequenza (**RF**), per stabilire trasmissioni di voce e dati di tipo punto a punto e punto a molti punti, nel raggio di 10 metri. La tecnologia che supporta Bluetooth è definita in una Specifica Bluetooth di 1500 pagine; tutti i dispositivi che incorporano la tecnologia devono essere conformi ai dettagli descritti nella specifica.

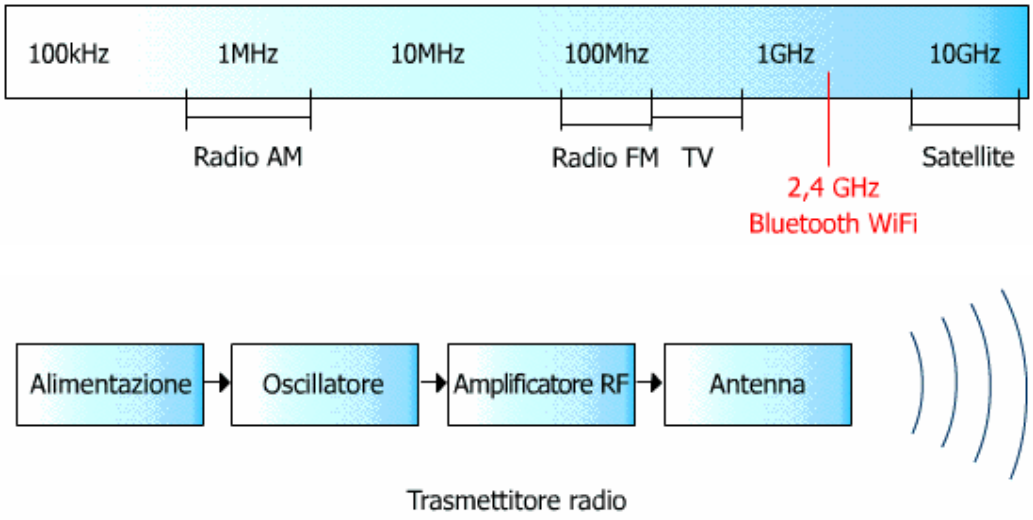
Il Bluetooth Special Interest Group (**SIG**) ha proposto una nuova versione del Bluetooth che offrirà trasferimenti a velocità più alte utilizzando meno energia. La versione attuale di questo standard wireless a corto raggio è popolare in Europa e sta iniziando a prendere piede in USA. Bluetooth **EDR** (Enhanced Data Rate) sarà significativamente più veloce del Bluetooth 1.2. Offrirà trasferimenti dati fino a 2,1 Mbps, che è quasi tre volte più veloce degli attuali 721 Kbps. Fortunatamente, i dispositivi che saranno dotati di questo nuovo standard saranno retro-compatibili con gli altri standard Bluetooth. Si utilizzerà ancora lo stesso metodo per collegare i dispositivi e trasferire i pacchetti, ma sarà possibile immagazzinare più dati in ogni pacchetto. Questo incremento di velocità non significa che il Bluetooth richiederà più energia. In effetti sarà il contrario. La prossima generazione di dispositivi Bluetooth dovrebbe funzionare per un tempo doppio rispetto a quelli attuali. Il Bluetooth SIG si aspetta che le specifiche EDR vengano finalizzate durante l'autunno del 2004, con i primi prodotti dipsonibili nel 2005.

Affinché due dispositivi possano comunicare tra loro, entrambi i dispositivi devono contenere una radio Bluetooth. Questa radio è di dimensioni estremamente ridotte (essa è incorporata in un chip, che contiene a sua volta un Link Controller, che stabilisce e gestisce le singole connessioni) e consuma una quantità di energia minima.

2) TRASMISSIONE

Un'onda radio è un impulso di energia elettromagnetica ed è generata quando un trasmettitore oscilla ad una frequenza specifica. Quanto è più rapida l'oscillazione, tanto più elevata è la frequenza. Per amplificare e trasmettere il segnale radio a grandi distanze, viene utilizzata un'antenna e per ricevere un segnale radio, è necessario un ricevitore radio. Il ricevitore viene sintonizzato su una frequenza specifica, per ricevere i segnali che oscillano a tale frequenza; se il ricevitore non viene sintonizzato a tale frequenza, le onde radio passano oltre. Le trasmissioni RF sono diffuse su un vasto intervallo di frequenze e sono misurate in cicli al secondo (Hz).

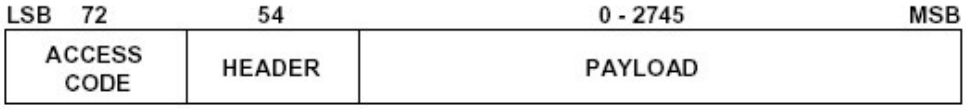
A differenza delle trasmissioni ad infrarossi, che si servono di onde luminose e richiedono la sistemazione dei dispositivi connessi lungo una linea visiva senza ostacoli, le onde radio non detengono necessità di questo tipo e possono, in effetti, passare attraverso gli oggetti solidi. Questo significa che un dispositivo radio Bluetooth può trasmettere segnali RF dall'interno di una ventiquattrore, o attraverso le pareti di un ufficio.
Le comunicazioni Bluetooth (sia per voce sia per dati) si servono di una banda RF senza licenza, nel campo di azione che si estende da 2,4 a 2,48 GHz.



Trasmettitore radio

Questa banda di frequenza ISM (Industrial, Scientific and Medical) può essere utilizzata da chiunque, per qualsiasi finalità. Si tratta di un aspetto positivo perché può essere usata a costo zero, e di un aspetto negativo perché lo spazio all'interno della banda è limitato ed esistono diversi altri tipi di dispositivi che si servono anch'essi di questa banda.
Proprio per questo si può dar luogo a delle interferenze reciproche tra i vari dispositivi pena il rallentamento delle trasmissioni di dati. Per evitare ciò i dispositivi radio di Bluetooth si servono di una tecnica chiamata **HOPPING di frequenza a largo spettro:** Esso è una tecnica piuttosto comune **FHSS** (Frequency Hopping Spread Spectrum), in cui un segnale passa rapidamente da una frequenza all'altra, nel corso di una singola trasmissione. Il risultato è che le trasmissioni Bluetooth non rimangono su una singola frequenza per un tempo sufficiente per essere colpite da interferenze, all'interno di tale frequenza. Nelle trasmissioni il segnale radio passa rapidamente tra 79 frequenze comprese tra 2,4 GHz e 2,48 GHz compiendo 1600 hps (salti di frequenza al secondo), ad intervalli di 1 MHz. La sequenza dei salti è determinata dall'orologio di sistema di un'unità master di una rete che sincronizza i timer di tutte le unità slave ad essa connesse.

I segnali radio contenenti dei dati si servono generalmente di una tecnologia definita **a pacchetti**. Con questa trasmissione, i dati sono suddivisi in piccoli blocchi o pacchetti prima di essere inviati. Ogni pacchetto può essere inviato in diversi percorsi a diverse frequenze, poi, al termine della ricezione di tutti i pacchetti di un messaggio, questi vengono ricompilati nell'ordine originale.
I segnali vocali al contrario, si servono di una tecnologia definita **a circuito**; con essa i messaggi non sono suddivisi in pacchetti, ma viene stabilito un canale (o circuito) dedicato, per tutta la durata della trasmissione. La trasmissione a pacchetti è un metodo efficace per trasmettere dati binari a causa del suo ritardo variabile e non prevedibile (ritardo di coda, perdita pacchetti, mentre quella a circuito è ideale quando le comunicazioni devono avvenire in tempo reale.



Ogni pacchetto è costituito da tre parti fondamentali:

- **Access Code** (72 bit): è utilizzato per distinguere le trasmissione nelle diverse piconet e come sincronismo. Ci sono tre tipi di Access Code: Channel Access Code (CAC) che identifica univocamente una piconet, Device Access Code (DAC) usato per il paging (richiesta e risposta di connessione), Inquiry Access Code (IAC).
- **Header** (54bit): contiene informazioni per la comprensione del pacchetto, quali numerazione dei pacchetti, controllo di flusso, indirizzo dello slave e error check.
- **Payload** (0-2745 bit): può contenere campi "voice" o "data" o entrambi.

In ogni slot, un pacchetto può essere scambiato tra l'unità master e una delle unità slave. Ogni pacchetto ha una lunghezza in bit fissata e comunque sempre con una sequenza di 72 bit di access code che caratterizza l'identità dell'unità master e quindi del canale.

Ogni unità slave, prima di ricevere il payload in ogni pacchetto confronta l'access code col proprio codice di piconet. Se i due non coincidono essa ignora il contenuto di pacchetto, altrimenti lo accetta. Dopo l'access code c'è il packet header. Esso contiene importanti informazioni di controllo, e andando per ordine si suddivide in:

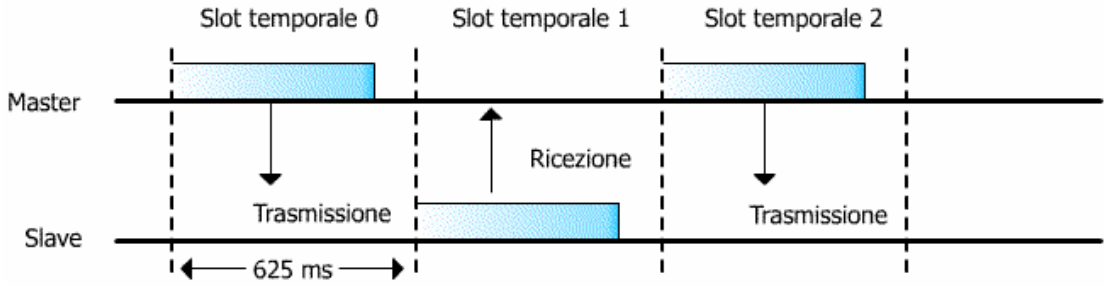
- 3-bit per l'indirizzo di ogni slave in stato attivo.
- 4-bit per il tipo di pacchetto.
- 1-bit per il controllo di flusso.
- 1-bit per ARQ (Automatic Retrasmission Query).
- 1-bit per l'ordine dei pacchetti.
- 8-bit per HEC (Header-Error-Check) meccanismo di check d'errore.

Il successo o meno della consegna di un pacchetto è mostrato nell'header di quello di ritorno e precisamente nel bit di ARQ che mostra al trasmittente se il payload precedentemente inviato è stato ricevuto correttamente o no. Quindi dopo aver analizzato tale bit l'unità di trasmissione stabilisce se ritrasmettere o meno l'ultimo pacchetto dati. Siccome trascorre un tempo di soli

220us., tra la ricezione dell'ultimo bit del payload e la trasmissione del successivo, l'algoritmo CRC di check sul contenuto deve essere molto rapido, quasi in tempo reale. Infine c'è il payload che ha una lunghezza variabile da 0 a 2745 bit e si verifica che un solo pacchetto è sempre mandato su un singolo canale di salto.

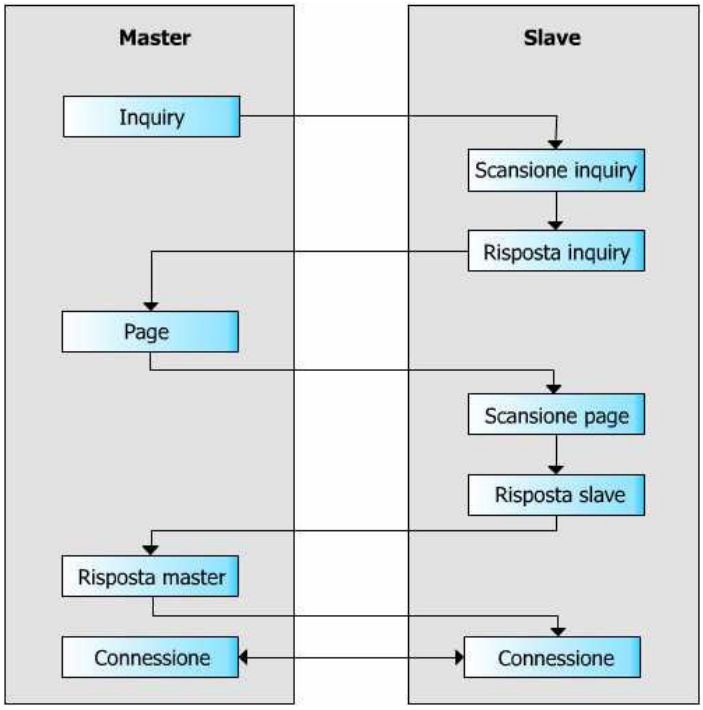
Duplex

Riguarda il flusso di dati in una comunicazione tra dispositivi. Si parla di Full Duplex in caso di trasmissione dei dati in due direzioni, simultaneamente. Half Duplex quando, invece, i dati possono viaggiare in una direzione alla volta. Un telefono è un esempio di dispositivo full duplex perché entrambi gli interlocutori possono parlare contemporaneamente; al contrario, un walkie-talkie è un dispositivo half duplex perché uno dei due interlocutori deve smettere di parlare, prima che l'altro possa iniziare.
Le comunicazioni full duplex sono anche chiamate sincrone e sono dette in gergo orientate alla connessione; mentre le comunicazioni half duplex sono asincrone e sono chiamate senza connessione.
Nella specifica Bluetooth le trasmissioni full duplex si servono di uno schema Time Division Duplex (TDD). In questo schema ogni frequenza e suddivisa in slot temporali di 625 ms ciascuno. TDD assegna slot temporali successivi per trasmissione e ricezione; le unità master trasmettono tramite slot numerati con numeri pari, mentre le unità slave rispondono tramite slot numerati con numeri dispari. Con questo movimento alternato in una singola frequenza, due trasmissioni differenti possono condividere la stessa frequenza e consentire la realizzazione di comunicazioni full duplex.



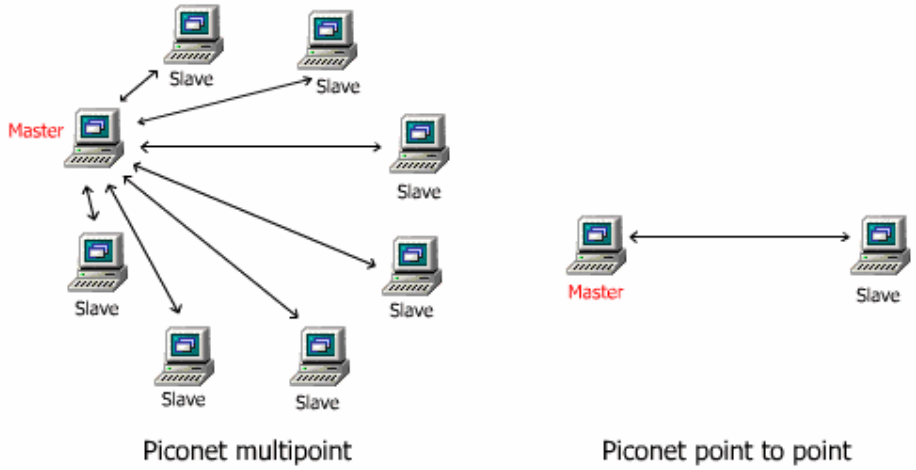
Sequenza di riconoscimento comandi

Tutti i dispositivi Bluetooth non connessi, sono avviati automaticamente in modalità standby, a basso consumo energetico. Quando un'unità riconosce un altro dispositivo in tale area, viene avviata una procedura di connessione. A questo punto, il primo dispositivo assume il ruolo di unità master, in quella che sta per diventare una sorta di rete miniaturizzata.
Un dispositivo Bluetooth può emettere diversi tipi di comandi, per avviare la procedura di connessione. Il primo comando è il comando inquiry. Un comando inquiry viene emesso quando il numero di identificazione o indirizzo, dell'altro dispositivo, non è noto. Quando l'indirizzo del dispositivo è noto, viene emesso un comando page. Il comando page serve per risvegliare l'altra unità e stabilisce una connessione completa tra i due dispositivi.

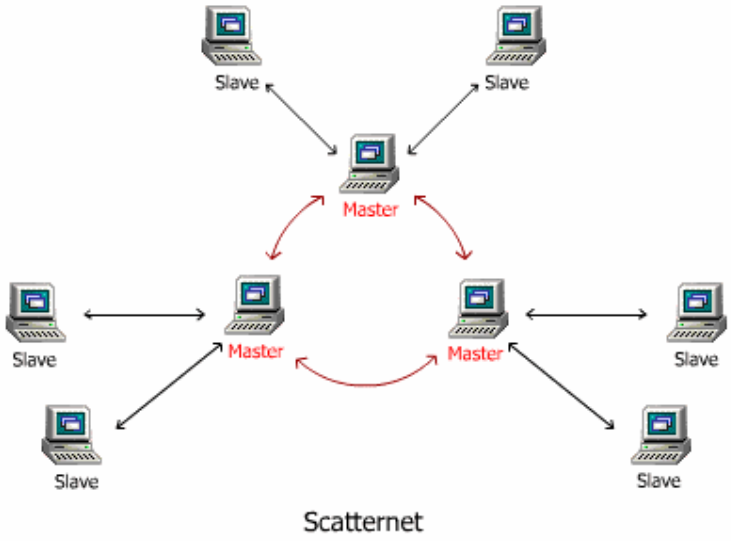

Master
Slave
Inquiry
Scansione inquiry
Risposta inquiry
Page
Scansione page
Risposta slave
Risposta master
Connessione
Connessione

3) COLLEGAMENTI

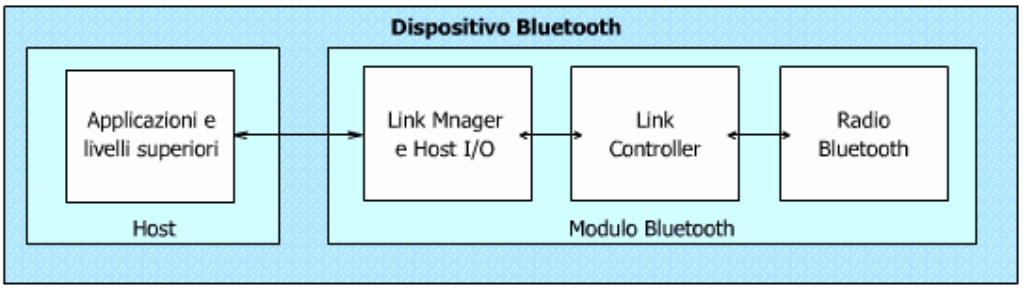
Quando due dispositivi Bluetooth stabiliscono una connessione, creano un tipo di rete personale definita **PICONET**. Ogni piconet può contenere fino ad otto dispositivi Bluetooth dove uno di essi funge da master, mentre gli altri sette fungono da slave. Tutti i dispositivi condividono lo stesso canale di passaggi di frequenza, che è determinato dagli slave, che sincronizzano i propri orologi interni con quello dell'unità master.



Poiché diverse piconet hanno identità differenti, basate su diversi canali di passaggi di frequenza, più piconet possono condividere lo stesso spazio fisico, senza interferire reciprocamente.
Per collegare più di otto elementi bisogna unire più piconet per formare una **SCATTERNET**. In essa tutte le comunicazioni tra le diverse piconet sono filtrate attraverso i singoli dispositivi master delle piconet. In una singola scatternet è possibile includere fino a 10 piconet, oltre questo numero la rete si satura, poiché Bluetooth si serve solo in totale di 79 frequenze.



4) ARCHITETTURA



Architettura di un dispositivo Bluetooth

In un dispositivo Bluetooth la parte non Bluetooth viene definita **host** mentre tutti i componenti Bluetooth sono combinati nel **modulo**. Le comunicazioni tra host e modulo sono gestite dal software **Link Manager** e dall' **Host Controller** del modulo.
L' **Host Controller** è la parte di modulo che gestisce tutte le comunicazioni ed interazioni, tra il modulo ed il dispositivo host. Esso interpreta i dati ricevuti dall'host e li dirige verso il componente o i componenti del modulo Bluetooth. Inoltre, interpreta i dati provenienti dal modulo e li invia verso la funzione adeguata nel dispositivo host.
Il software **Link Manager** si occupa di impostazioni, autenticazione, configurazione dei collegamenti e di altre attività necessarie, per stabilire un collegamento tra i dispostivi Bluetooth. In pratica, LM identifica la presenza di altri dispositivi che eseguono lo stesso software LM e comunica con questi, tramite il Bluetooth Link Manager Protocol (LMP). Per eseguire queste operazioni, il L.M. deve impiegare i servizi forniti dall'hardware **Link Controller** che facilita l'invio e ricezione di dati, l'impostazione delle connessioni ed altre attività correlate. I messaggi inviati tra queste due unità prendono la forma di quelle che vengono definite **Protocol Data Units (PDU)**. Esse rappresentano un linguaggio comune, qualsiasi dispositivo Bluetooth comprende e risponde immediatamente ad una PDU inviata da un altro dispositivo.
Poi c'è la **radio** che è un dispositivo che trasmette sulla banda RF 2,4 GHz, utilizzando le tecnologie hopping di frequenza a largo spettro impiegando la tecnica **FHSS** (Frequency Hopping Spread Spectrum). La radio può funzionare in un raggio di 10 metri. Essa interfaccia direttamente con il Link Controller che a sua volta interfaccia con l'Host Controller che collega il modulo al dispositivo Host.

5) PROTOCOLLI

Protocollo di base

I protocolli di base sono impiegati nel fornire funzioni di gestione per trasmissione e collegamenti, in qualsiasi applicazione.

Baseband

Consente la connessione RF fisica tra due o più unità B. che formano una piconet. Questo protocollo sincronizza anche le frequenze di trasmissione per il processo di hopping e per gli orologi dei singoli dispositivi di una piconet. Il protocollo Baseband fornisce due diversi tipi di collegamenti fisici: con un collegamento Syncronous Connection-Oriented, i pacchetti possono contenere una combinazione di audio e dati, o solo audio; con un collegamento Asyncronous Connection-less, i pacchetti sono riservati esclusivamente alla trasmissione di dati.

Link Manager Protocol (LMP)

Immediatamente sopra il livello del protocollo Baseband, responsabile dell'inizializzazione tra dispositivi, si occupa dell'impostazione e controllo del collegamento tra due o più dispositivi Bluetooth. Questo implica numerose questioni di sicurezza, come autenticazione e codifica, nonché controllo e negoziazioni di dimensioni dei pacchetti Baseband.

Logical Link Control and Adoption Protocol (L2CAP)

L2CAP funziona in parallelo con LMP, per trasferire I dati di livello superiore relative al livello Baseband. Ha capacità di multiplexing di diversi canali, cioè L2CAP riesce a distinguere a quale protocollo superiore si riferiscono i pacchetti. L2CAP è definito solo per connessioni ACL e non supporta connessioni SCO.

La grande differenza tra L2CAP e LMP è che il primo fornisce servizi al livello superiore, cosa che il secondo non è in grado di fare. L2CAP supporta solo collegamenti ACL.

Service Discovery Protocol (SDP)

Il protocollo SDP permette alle applicazioni di capire che servizi sono implementati in un dispositivo bluetooth remoto. SDP fornisce informazioni sui servizi (e sui loro attributi) ma non l'accesso a questi.

Questi servizi consentono a due dispositivi differenti di riconoscere e stabilire connessioni reciproche e forniscono le basi per ogni singolo profilo B. SDP fornisce ad un dispositivo la possibilità di effettuare una query sulle informazioni, servizi e caratteristiche dell'altro dispositivo. Inoltre, consente di stabilire una connessione tra tali servizi.

Protocollo di sostituzione cavo

RFCOMM

E' un protocollo che emula una connessione seriale RS-232 tra due dispositivi. In altri termini, si tratta del protocollo di sostituzione cavo. Consente di emulare i segnali RS-232 di dati e controllo, nella Baseband di Bluetooth; inoltre, fornisce abilità di trasmissione per servizi di livello superiore, che in caso contrario, utilizzerebbero una connessione seriale come meccanismo di trasmissione.

Protocolli di controllo telefonico

Questi protocolli consentono ai dispositivi di gestire voce e dati, provenienti da dispositivi abilitati a Bluetooth. Affinché un dispositivo B. possa funzionare come telefono o modem, è necessario implementare uno dei due protocollo di controllo telefonico.

Telephony Control Specification-Binary (TCS-BIN)

Definisce il segnale di controllo di chiamata, necessario per stabilire chiamate di voce e dati tra dispositivi. Esso definisce anche le procedure di gestione della mobilità, impiegate per gestire gruppi di dispositivi B.

AT Commando (ATC)

Questi comandi sono utilizzati per controllare tutte le funzione che possono essere eseguite da un telefono o un modem dati, e sono comuni tra molti dispositivi e produttori. Questi comandi sono impiegati quando un profilo richiede che un dispositivo B. funga da telefono o modem, nel collegamento ad una lineari terra o ad un sistema di telefonia cellulare.

Protocolli di trasmissione

Oltre ai protocolli precedenti, nella serie di protocolli B., sono stati adottati numerosi protocolli stabiliti in altri settori. Questo permette alle applicazioni più vecchie di funzionare anche con la nuova tecnologia B., ed ai dispositivi B, di collegarsi a reti di comunicazione globali.

Point to Point Protocol (PPP)

Il protocollo Point to Point definisce le modalità di trasmissione dei dati IP, in collegamenti seriali di tipo punto a punto. Questo protocollo viene generalmente impiegato in connessioni Internet di tipo dial-up, o in accessi ad un router di rete in una linea dedicata.
Nel mondo Bluetooth il PPP viene eseguito con il protocollo RFCOMM, per stabilire connessioni di tipo p2p, tra dispositivi. Il PPP si trova nei profili Accesso Lan, Dial-up Networking e Fax.

Transport Control Protocol (TCP)

Il Trasfer Control Protocol comprende un servizio orientato alla connessione ed un servizio di trasferimento affidabile dei dati. Prevede una fase preventiva chiamata handshaking tra client e server permettendo loro di prepararsi per l'arrivo massiccio dei pacchetti. Dop la fase precedente si dice che esiste una connessione TCP fra i socket dei due processi. La connessione è di tipo full-duplex perché i due processi possono inviare messaggi l'uno all'altro, contemporaneamente sulla connessione. Il TCP garantisce il recapito di tutti i dati spediti senza errori e nell'ordine appropriato. C'è anche un altro meccanismo di controllo che è detto di congestione che garantisce il corretto funzionamento di Internet piuttosto che per un diretto vantaggio dei processi di comunicazione strozzando un processo quando la rete è congestionata.

User Datagram Protocol (UDP)

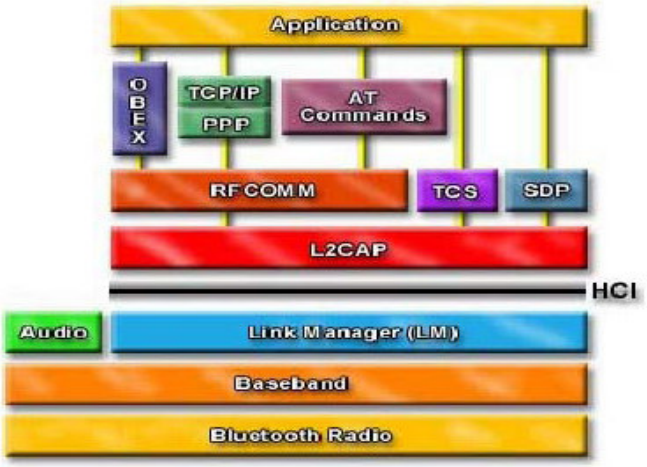
E' senza connessione, quindi non c'è handshake prima che i due processi inizino a comunicare. Fornisce un servizio di trasferimento dati non affidabile, cioè, quando un processo spedisce un messaggio in un socket UDP, l'UDP non garantisce che il messaggio raggiungerà il socket ricevente. Inoltre i messaggi che arrivano al socket ricevente possono non arrivare in ordine. Esso non comprende un controllo di congestione, così un processo che spedisce può pompare dati nel socket dell'UDP a qualsiasi velocità.

Internet Protocol (IP)

Il primo componente del protocollo della rete, che definisce l'indirizzamento dello strato di rete. L'IP identifica univocamente la nostra connessione in quel preciso momento, per renderci visibili e rintracciabili. Ogni IP è unico ed identifica un host name, cioè il computer che sta usando la connessione per navigare, e viceversa ad ogni host name in rete corrisponde un IP, anche se può cambiare ogni volta. L'IP può essere statico, se ci viene assegnato una volta per tutte quando apriamo il nostro account, oppure dinamico, cioè cambia ogni volta che ci colleghiamo alla rete. L'IP è un numero di 32 bit, rappresentato nella forma xxx.xxx.xxx.xxx, dove le xxx indicano la codifica dei quattro byte (gruppi di 1 byte, ovvero 8 bit) in numeri decimali, compresi tra 0 e 255. Si usa anche la forma xxx.xxx.xxx.xxx:yyyy, per intendere un indirizzo IP su una certa porta (yyyy).

In definitiva i protocolli si possono raggruppare in due categorie:

- **Trasport protocols:** sono i protocolli specifici Bluetooth essenziali per la comunicazione tra due o più dispositivi
- **Middleware protocols:** comprendono protocolli sviluppati per il Bluetooth e non; abilitano determinati servizi in base all'applicazione che si vuole usare per trasmissione dati.



6) PROFILI

Un profilo Bluetooth definisce le procedure ed i protocolli necessari per implementare una specifica applicazione o modello di utilizzo. Oltre ai protocolli di identificazione, ogni profilo definisce procedure e messaggi che devono essere usati per implementare una specifica applicazione. E' stata realizzata una serie di specifiche per implementare le applicazioni: i profili.

Profili generali

Chiamati generali perché sono essenziali per tutte le comunicazione B.

GAP (Generic Access Profile)

Definisce le modalità e le procedure comuni a tutti gli altri profili. In Pratica, GAP è la base su cui sono costruiti tutti gli altri profili.

In generale, GAP è associato a tre tipi di voci: dizionario: raccolta di termini e delle relative definizioni, in modo che i produttori utilizzino la stessa terminologia, connettività: operazioni che permettono ad un dispositivo di connettersi e di autenticarsi con altri dispositivi, personalizzazione: elementi che identificano e personalizzano singoli dispositivi B. Il GAP definisce il tipo di dispositivo ed i tipi di servizi supportati da tale tipo di dispositivo. Inoltre permette ai dispositivi di avere nomi semplici per gli utenti con una lunghezza massima di 248 byte, benché alcuni dispositivi, per limitazione di display, potrebbero non essere in grado di visualizzare il nome completo. Poi stabilisce che l'utente del dispositivo potrebbe immettere un numero di identificazione personale (PIN) da usare nella procedura di autenticazione.

Questo profilo sfrutta: Obex, Rfcomm, Sdp, L2cap, lmp, Baseband.

SDAP (Service Discovery Application Profile)

Metodo per localizzare I servizi registrati in altri dispositivi, raccogliere informazioni su di essi e farne uso con l'utilizzo di SDP. Anche SDAP è progettato per essere incorporato virtualmente in qualsiasi dispositivo Bluetooth. Il dispositivo che inizializza il processo di scoperta del servizio è etichettato come dispositivo locale; invece quello che risponde è remoto. Tale processo assegna al locale il ruolo del client in un processo client/server, mentre il dispositivo remoto è incaricato di servire le informazioni su se stesso al dispositivo di inizializzazione.

Questo profilo sfrutta: Sdp, L2cap, Lmp, Baseband.

Profili della porta seriale

Essi definiscono le specifiche per le applicazioni che devono trasferire dati da un dispositivo all'altro.

SPP (Serial Port Profile)

Per implementare soprattutto il modello di utilizzo del desktop cordless. Definisce i ruoli di parità tra i dispositivi per la comunicazione seriale. In questo tipo di comunicazione la relazione master/slave non esiste e tutti i dispositivi sono uguali quando sono previste delle comunicazioni seriali. Si emula la porta seriale RS-232.

Questo profilo sfrutta: Rfcomm, Sdp, L2cap, Lmp, Baseband.

GOEP (General Object Exchange Profile)

Definisce il modo in cui I dispositivi implementano I modelli di utilizzo che integrano una qualche forma di trasferimento dati, come per esempio I modelli di trasferimento file, dal sincronizzatore automatico e altri modelli correlati. Questo profilo funziona su un modello client/server, piuttosto che su un modello p2p. Il dispositivo che inizializza la connessione è definito come client, mentre l'altro dispositivo è identificato come il server.

Questo profilo sfrutta: Obex, Rfcomm, Sdp, L2cap, Lmp, Baseband.

Profili di telefonia

Si basano sulle generali funzioni della telefonia. Integrano la trasmissione di segnali vocali ed è probabile che siano usati ampiamente nei dispositivi B. prodotti dalle società di telecomunicazioni.

CTP (Cordless Telephony Profile)

Per implementare il modello di utilizzo del telefono tre in uno. Questo profilo consente di usare un ricevitore cordless per chiamare, tramite una stazione base vocale, la rete di telefonia fissa e di connettersi direttamente ad una rete di telefonia mobile. Questo profilo permette di

implementare il servizio CLIP che consente a sua volta agli utenti di identificare il numero di telefono della parte chiamante prima di rispondere al telefono.

INTP (Intercom Profile)
Scritto per implementare il modello di utilizzo del telefono tre in uno. Spiega come un ricevitore telefonico cordless può connettersi direttamente ad altri ricevitori come walkie-talkie.
Questo profilo sfrutta: Sdp, L2cap, Lmp, Baseband.
HSP (Headset Profile)
Scritto per implementare il modello di utilizzo del kit di auricolari e consente la connessione wireless di un kit di auricolari ad un ricevitore telefonico, ad una stazione base o ad un pc.
Questo profilo sfrutta: Rfcomm, Sdp, L2cap, Lmp, Baseband.

Profili di rete

LAP (Lan Access Profile)
Scritto per implementare il modello di utilizzo accesso LAN. In questo profilo, più terminali di dati utilizzano un punto di accesso LAN come connessione wireless ad una rete locale. Una volta connessi, i terminali di dati funzionano come se fossero connessi alla LAN tramite una tradizionale connessione di accesso remoto e possono accedere a tutti i servizi forniti dalla rete.
Questo profilo sfrutta: Tcp, Udp, Ip, Ppp, L2cap, Lmp, Rfcomm, Lmp, Baseband.
DUNP (Dial-Up Networking Profile)
Scritto per implementare la componente di accesso remoto del modello di utilizzo del bridge internet. In questo profilo, un telefono cellulare o un modem cordless,agisce come modem per un pc, fornendo capacità di accesso remoto senza una concreta connessione dedicata.
Questo profilo sfrutta: Ppp, Rfcomm, Sdp, L2cap, Lmp, Baseband.

Profili di scambio oggetti

I tre profili si riferiscono alla trasmissione e ricezione di oggetti di dati, tipicamente sotto forma di file di computer. Tutti e tre i profili integrano il Serial Port Profile, dato che i file dei computer sono tradizionalmente trasmessi tramite porta seriale del pc.
FTP (File Trasfer Protocol)
Per implementare diversi modelli di utilizzo: trasferimento file. Definisce come trasferire oggetti da un dispositivo all'altro. Qui non c'è il p2p ma la relazione client/server.
Questo profilo sfrutta: Obex, Rfcomm, Sdp, L2cap, Lmp, Baseband.
SP (Synchronization Profile)
Scritto per implementare il modello di utilizzo del sincronizzatore automatico. Questo profilo fornisce un sincronizzazione da dispositivo a dispositivo del tipo di informazioni che si trovano tipicamente nel software PIM, compresi nominativi, indirizzi, numeri di telefono… Il processo di sincronizzazione richiede che le informazioni siano trasferite ed elaborate da vari tipi di dispositivi che utilizzano un protocollo ed un formato di dati comune.
Questo profilo sfrutta: Obex, Rfcomm, Sdp, L2cap, Lmp, Baseband.
OPP (Object Push Profile)
Scritto per implementare uno specifico sottoinsieme del modello di utilizzo trasferimento file, la semplice operazione di scambio di informazioni digitali tra due dispositivi. Questo profilo si riferisce alla capacità di inviare dati da un dispositivo ad un altro e di ricevere dati in senso contrario. (scambio biglietti da visita).
Questo profilo sfrutta: Obex, Rfcomm, Sdp, L2cap, Lmp, Baseband.

7) SICUREZZA

Un sistema di telecomunicazioni deve essere dotato di meccanismi di protezione dei dati, a qualunque livello esso operi; tale esigenza è resa ancora più stringente, nel caso di bluetooth, dalla sua natura di interfaccia wireless: un sistema di comunicazione senza fili è per definizione più sensibile agli attacchi rispetto a un impianto cablato a causa delle propagazioni di onde radio che, a vantaggio della comodità di utilizzo, devono essere in qualche misura isotrope, cioè rivolte a direzioni non precise.

CHIAVI E SICUREZZA

La tecnologia Bluetooth, come detto finora, permette comunicazioni di tipo peer to peer a dispositivi che risiedono in un' area limitata.
Allo scopo di fornire protezione e confidenzialità ai dati, il sistema prevede misure di sicurezza sia a livello applicazione, che a livello link.
A livello link, la sicurezza è garantita per mezzo di quattro entità: **un indirizzo pubblico**, unico per ciascun dispositivo, **due chiavi segrete** e un **numero casuale** differente per ogni nuova transazione. Nella figura sono indicate le loro lunghezze:

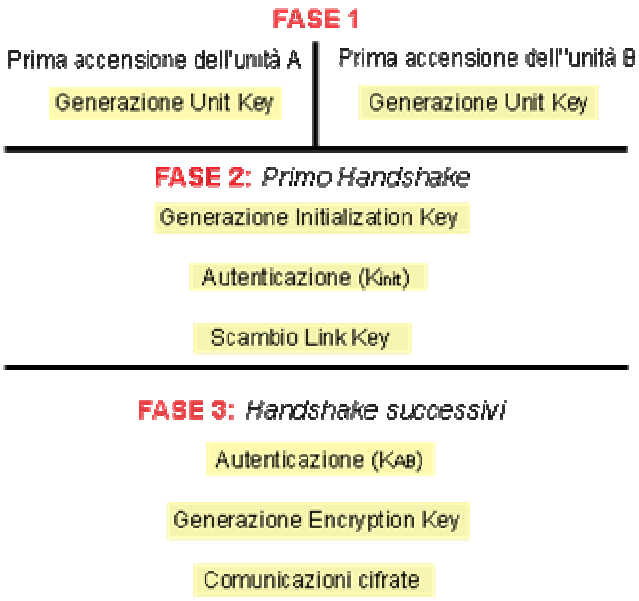
Entità	lunghezza
BD_ADDR	48 bit
Chiave privata per l'autenticazione autentication key	128 bit
Chiave privata per la cifratura encryption key	da 8 a 128 bit
Numero casuale	128 bit

L'indirizzo Bluetooth di un dispositivo (**BD_ADDR**) è un indirizzo IEEE a 48 bit, unico per tutti i dispositivi. Le chiavi segrete sono derivate durante il processo di inizializzazione.
Normalmente, **l'encryption key** tra due dispositivi è ottenuta dalla **chiave di autenticazione**, che coincide con la chiave associata al loro link, detta link key, con lunghezza 128 bit.
In casi particolari, quando il dispositivo master della piconet vuole trasmettere contemporaneamente a più slave le stesse informazioni, allora l'encryption key è calcolata da una link key temporanea, detta master key, generata dal master e con la quale sono sostituite temporaneamente le link key già fissate tra il master e ogni slave.
Per l'algoritmo di autenticazione, la lunghezza della chiave è di 128 bit, ma per quello di cifratura può variare da un minimo di un ottetto ad un massimo di 16 ottetti.
La taglia della chiave di cifratura è configurabile per due motivi. In primo luogo, disponendo di un algoritmo la cui è chiave di cifratura è variabile in lunghezza, è possibile superare le limitazioni imposte da alcuni stati sull'esportazione degli algoritmi di cifratura. La seconda ragione è legata alla possibilità di aggiornare facilmente nel tempo la lunghezza della chiave senza dover ridisegnare l'algoritmo di cifratura.
La chiave di cifratura è totalmente differente dalla chiave di autenticazione.
Ogni qualvolta la cifratura è attivata, una nuova chiave è generata. Perciò il tempo di vita della chiave di cifratura non necessariamente coincide con il tempo di vita della chiave di autenticazione.
Ogni dispositivo Bluetooth possiede un **generatore pseudo-casuale** per la generazione dei numeri casuali necessari alle funzioni legate alla sicurezza.
Idealmente un generatore di numeri casuali dovrebbe essere basato su un processo fisico intrinsecamente casuale, ma per ragioni pratiche è utilizzato un generatore pseudo-casuale.

La sicurezza è garantita dall'esecuzione di vari passi che possiamo dividere in **3 fasi**: Supponiamo di avere 2 soli dispositivi che vogliono comunicare:

- **Prima fase** i due dispositivi generano ciascuno una unit key. Questa chiave è generata da un dispositivo al momento della sua prima accensione ed è poi memorizzata in una propria memoria non volatile, per essere utilizzata anche in futuro.
- **Seconda fase** inizia con il primo handshake tra i due dispositivi. In essa avviene la generazione dell'initialization key, l'autenticazione dei dispositivi sulla base di questa chiave e lo scambio della link key da usare nelle iterazioni successive.
- **Terza fase** è caratterizzata da ulteriori handshake che permettono ai due dispositivi di trasmettere successivamente solo informazioni cifrate.

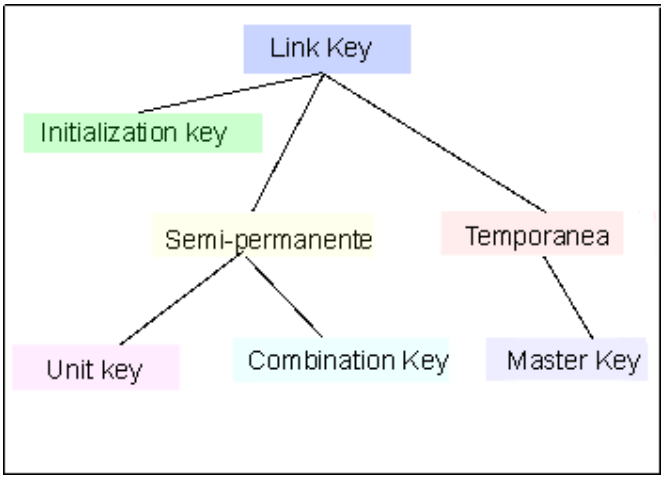
Le operazioni di questa fase sono l'autenticazione sulla base della chiave K_{AB} e la generazione della encryption key usata per cifrare tutte le comunicazioni tra i due dispositivi.



Le **link key** utilizzate in Bluetooth sono numeri casuali a 128 bit. Queste chiavi sono condivise da due o più dispositivi e sono alla base della sicurezza delle loro transazioni. Sono utilizzate sia in fase di autenticazione, che per la generazione dell'encryption key.

E' possibile dividere le link key in due classi: link key semipermanenti e link key temporanee. Una link key **semipermanente**, una volta generata, è memorizzata in una memoria non volatile e può essere utilizzata anche dopo che la corrente sessione è terminata; quindi anche in più fasi di autenticazione. Le link key **temporanee**, invece, hanno un tempo di vita che è limitato da quello della sessione in cui sono state generate.
A seconda del tipo di applicazione, le link key possono essere:

- unit key, K_A;
- combination key, K_{AB};
- master key, K_{master};
- initialization key, K_{init}.

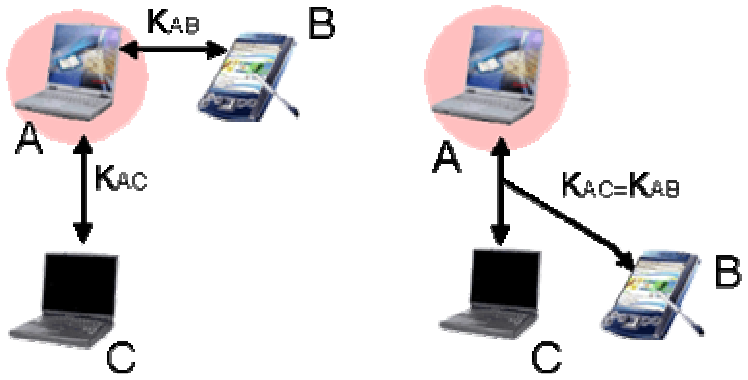


Una **unit key**, K_A, è generata da un dispositivo A, quando è avviato per la prima volta. Una volta creata, è memorizzata in una memoria non volatile ed è modificata solo in casi eccezionali.
Una **combination key**, K_{AB}, è ottenuta da informazioni prodotte da due unità, A e B. Questa chiave è generata per ogni coppia di dispositivi quando è necessaria maggiore sicurezza. L'uso di queste chiavi comporta un maggiore spreco di memoria in quanto ciascun dispositivo dovrà memorizzare una combination key per ogni sua connessione.
Una **initialization key**, K_{init}, è usata come link key durante il processo di inizializzazione, quando non è stata ancora definita e scambiata una unit key o una combination key, da usare come link key, oppure nel caso in cui una link key precedente è stata persa.
Una tale chiave è necessaria quando due dispositivi entrano in contatto per la prima volta, in modo da garantire la protezione dei parametri fondamentali dell'inizializzazione.
Una **master key**, K_{master}, è usata quando il dispositivo master vuole trasmettere contemporaneamente a vari dispositivi. Una chiave di questo tipo sostituisce momentaneamente la link key della corrente sessione.

ATTACCHI ALLA SICUREZZA

Attacchi all'autenticazione

Per mezzo dell'autenticazione, due dispositivi possono verificare che entrambi condividono una stessa link key.
Se la link key è una initialization key, allora l'unica informazione segreta usata nella sua generazione è il PIN. Questo codice normalmente è un parola chiave di 4 numeri decimali. Quindi sono possibili solo 10.000 valori diversi e un attacco di forza bruta è realizzabile a tutti gli effetti.
Diversi problemi possono sorgere se i dispositivi hanno una limitata capacità di memoria. Infatti, in una tale situazione, il dispositivo con limitata capacità usa la propria unit key come link key.
In questo scenario, se un dispositivo A comunica prima con un dispositivo B e poi con un altro C, e in entrambi i casi è usata come link key la unit key di A, allora i tre dispositivi usano la stessa chiave e possono impersonare uno qualunque dei tre ed intercettare la comunicazione tra gli altri due.



Attacchi alla cifratura

Per riuscire a decifrare correttamente una comunicazione tra due dispositivi, un attaccante deve per prima cosa conoscere la chiave usata per la cifratura, la cui lunghezza può variare da 8 a 128 bit, in base al grado di sicurezza richiesto.
In genere, la lunghezza minima della chiave è stabilita dallo strato applicazione allo scopo di evitare che l'uso di una chiave troppo corta possa pregiudicare la sicurezza delle informazioni trasmesse.
Una volta che l'attaccante è entrato in possesso della chiave di cifratura non può automaticamente decifrare una trasmissione, deve infatti riuscire a sincronizzarsi con il clock del master.
Dal momento che la sola informazione segreta su cui è calcolata la chiave di cifratura è la link key, perchè i numeri casuali sono sempre trasmessi in chiaro sul canale, la conoscenza della link key e l'intercettazione di tutte le trasmissioni durante la fase di autenticazione sono sufficienti per decifrare le informazioni scambiate dai dispositivi.
Un altro tipo di attacco sfrutta la debolezza introdotta da codici PIN troppi corti. In genere la lunghezza dei PIN utilizzati è di 4 numeri decimali. Da qui, se un attaccante inizia ad intercettare le comunicazioni dal primo handshake, potrebbe con un attacco di forza bruta sul PIN, riuscire a dedurre tutti i parametri utilizzati per la generazione della chiave di inizializzazione K_{init}.

Attacchi alla comunicazione

Un primo attacco che si può compiere alla comunicazione è legato alla possibilità di riuscire a impersonare un altro dispositivo. Il frame di un pacchetto Bluetooth può essere modificato in tre parti:

- i tre bit del member address;
- il bit di acknoledgement;
- gli otto bit dell'error check per l'header.

Modificando questi 3 campi di un pacchetto un attaccante può inviare un pacchetto ad un altro dispositivo impersonandone un terzo.
Altri comuni attacchi includono la possibilità di compiere intercettazioni e la modifica di bit. Con uno scanner, se la chiamata è non cifrata l'attaccante può ascoltare tutta la trasmissione tra due dispositivi. Con la modifica di bit invece un attaccante non entra in possesso di alcuna informazione trasmessa da un altro dispositivo, ma è grado di impedire ad esso qualunque trasmissione di informazione.
Un altro possibile attacco in Bluetooth è un attacco di replay in cui un dispositivo attaccante registra una conversazione tra due dispositivi in un certo istante e la ritrasmette successivamente impersonando chi l'ha trasmessa.
Per esempio, se le informazioni trasmesse sono da un PDA, A, ad un router wireless, B, di una banca e riguardano una transazione bancaria, un attaccante potrebbe prendere una copia bit per bit dell'informazione inviata da A a B e reinviarla alla banca multiple volte portando quest'ultima a eseguire più volte la stessa operazione.
Per un attacco di questo tipo, l'attaccante deve essere, però, in grado di riuscire a registrare le informazioni trasmesse da A su tutti e 79 i canali utilizzati in Bluetooth.
In realtà un attacco di questo tipo è tutt'altro che semplice.
Per prima cosa le apparecchiature che permettono di monitorare contemporaneamente 79 canali sono poche diffuse, inoltre anche se l'attaccante disponesse di una registrazione parallela di tutti i canali gli resterebbe comunque il gravoso compito di stabilire in ogni slot su quale canale è avvenuta la trasmissione delle informazioni della transizione.

Attacchi al canale

Sebbene un attacco ad uno schema di comunicazione, basato su salti di frequenza sia estremamente difficile, in Bluetooth è possibile trovare a tale riguardo punti deboli.
Le parti fondamentali di uno schema di comunicazione basato sui salti di frequenza sono:

- il clock;
- la capacità di trasmissione di un dispositivo in ogni direzione;
- il sistema di trasmissione radio.

Ogni dispositivo Bluetooth possiede un clock a 28 bit che non è mai né spento né modificato. La frequenza del clock è di 3.200 tick per secondo, cioè un tick si verifica ogni 312 msec che corrisponde ad un clock rate di 3.2 KHz.
Un attaccante usando un laser a bassa energia (LEL) o impulsi elettromagnetici (EMP) può disturbare il clock del dispositivo rendendo impossibile sia la trasmissione che la ricezione di informazioni. Entrambi gli attacchi sono estremamente rari e i rischi ad essi legati sono abbastanza limitati.
I dispositivi che operano in reti wireless sono capaci di trasmettere informazioni in ogni direzione.
Le potenzialità offerte da una propagazione in ogni direzione è anche un punto di debolezza dei sistemi che la utilizzano. Infatti, se da un lato essa permette ad un dispositivo di trasmettere in modo semplice informazioni ad altri dispositivi, dall'altra presenta lo svantaggio di estendere anche il campo d'azione di un attaccante.
Come si sa le onde radio si propagano oltre le porte, le pareti, le finestre degli edifici e danno di conseguenza la possibilità ad un attaccante di intercettare trasmissioni, acquisire informazioni sulla rete rimanendo a debita distanza dalla rete anche per molto tempo. Contromisure per questo tipo di attacco si basano sull'imporre limitazioni alla potenza di trasmissione dei dispositivi oppure a porre limiti fisici tra la rete e un potenziale attaccante.

Interferenze agli schemi di gestione della potenza di trasmissione possono compromettere il funzionamento del modulo per la selezione della frequenza usata (FSM Frequency Selection Module), con conseguente interessamento di tutte le funzioni della piconet. Dispositivi in uno stato connesso possono modificare la potenza di trasmissione nella piconet, per un certo link e chiedere al dispositivo all'altro capo del collegamento di modificare la propria potenza di trasmissione in base alla qualità del link di comunicazione. Se un attaccante è in grado di danneggiare o disturbare il sistema di gestione della potenza di uno qualunque dei dispositivi, allora può porre la piconet in uno stato di caos. Senza la corretta potenza il FSM non può operare correttamente e il sistema di salto della frequenza è ostacolato o degradato nelle sue funzioni.

VULNERABILITA' IN BLUETOOTH

Per valutare il grado di sicurezza offerto da reti Buetooth, è possibile utilizzare a tale scopo la tecnica **VERDICT** (Validation Exposure Randomness Deallocation Improper Conditions Taxonomy) con la quale è possibile scoprire le vulnerabilità presenti in un sistema e quindi risolverle nella progettazione dei dispositivi.
Questa tecnica valuta un sistema, analizzandone quattro caratteristiche fondamentali:

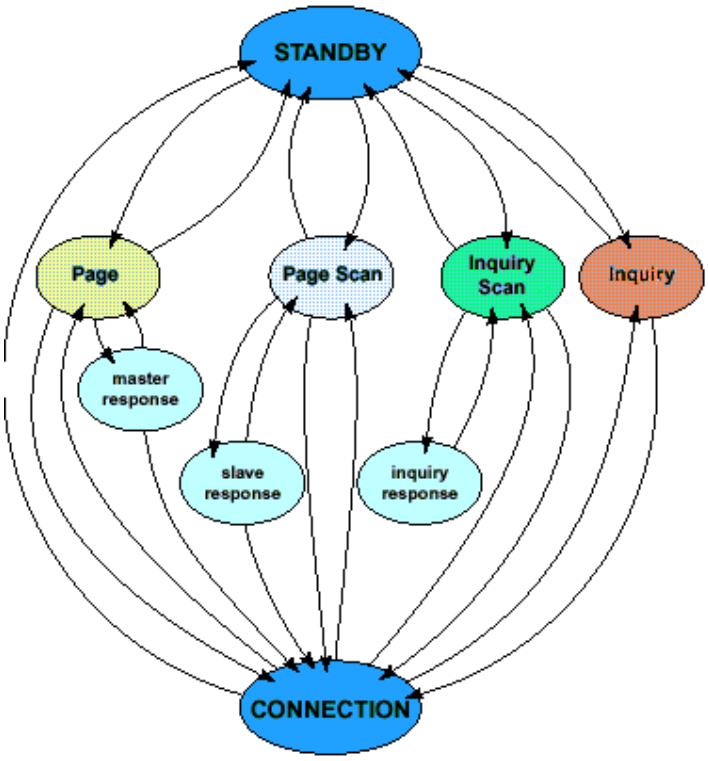
- convalida;
- esposizione;
- casualità;
- deallocazione.

La **convalida** di un codice garantisce che nessuna operazione in un sistema possa portare ad un buffer overflow. A tale scopo vanno controllate tutte le condizioni critiche ed i particolari input che si possono ricevere.
L'**esposizione** permette ad un sistema la rivelazione dei dispositivi presenti in una rete. Un'esposizione impropria può essere sfruttata da un attaccante per agire impropriamente in una rete da una opportuna distanza di sicurezza.
La **casualità** è un altra importante caratteristica per i computer e per i protocolli di sicurezza, in quanto numeri casuali sono spesso utilizzati nella generazione di chiavi e sono parte integrante di molti schemi di sicurezza. Per tale motivo, i numeri casuali dovrebbero essere sempre generati da semi sufficientemente casuali.
La **deallocazione** è un aspetto importante della sicurezza. Un sistema deve essere sempre in grado di deallocare le risorse impegnate in precedenti utilizzi.

Convalida impropria

La maggior parte delle vulnerabilità presenti sia in reti tradizionali che wireless è causata dalla presenza di convalida impropria. Vediamo in dettaglio a tale riguardo le vulnerabilità presenti in Bluetooth.

- **Convalida degli indirizzi dei dispositivi**. Un dispositivo Bluetooth è identificato univocamente da un indirizzo a 48 bit. Il suo formato è simile a quello degli indirizzi IEEE 802.3 ed a quelli usati nelle reti Ethernet. Se un utente è in grado di modificare l'indirizzo Bluetooth di un proprio dispositivo, allora è possibile avere in una piconet due dispositivi con uno stesso indirizzo e quindi un attacco simile all'IP spoofing.
- **Stati invalidi (Link Control)**. Per il link control di un dispositivo Bluetooth sono previsti 9 stati dei quali 2 sono stati principali: STANDBY e CONNECTION e 7 sono sottostati: page, page scan, inquiry, inquiry scan, master response, slave response, inquiry response. Per rappresentarli è sufficiente un bit per i due stati principali e 3 per gli altri 7. Chi progetta sistemi Bluetooth deve garantire che l'ottavo possibile stato, non associato ad alcun effettivo stato, non sia mai raggiunto e se è raggiunto per una qualche ragione, allora deve essere prevista anche una transizione in uno stato sicuro. Infatti, se ciò non accadesse, allora sarebbe possibile per un attaccante condurre il sistema in uno stato di instabilità sfruttandone i comportamenti errati.



- **Stati invalidi (Modalità di cifratura)**. Se un dispositivo slave ha ricevuto una master key, allora ci sono 3 possibili combinazioni per la cifratura. In questo caso tutte le unità usano una stessa link key, la master key. E' possibile rappresentare i 3 stati con due bit anche se è possibile rappresentarne un quarto. Il quarto stato non dovrebbe mai essere raggiunto, perché in esso tutto il traffico broadcast è cifrato prima della trasmissione, ma quello point-to-point è inviato sul link in chiaro.

STATO	Traffico Broadcast	Traffico Unicast
1	Non cifrato	Non cifrato
2	Non cifrato	Cifrato
3	Cifrato	Cifrato
4	Cifrato	Non cifrato

- **Chiavi di cifratura.** Secondo la specifica Bluetooth il dispositivo master di una piconet non può usare differenti chiavi di cifratura per messaggi broadcast e unicast. Il master può indicare a vari dispositivi slave di usare una comune link key e quindi indirettamente di usare una comune chiave di cifratura. Questo può rendere possibile l'ascolto delle trasmissioni di tutti i dispositivi.

Esposizione impropria

Nel protocollo Bluetooth sono presenti due esposizioni improprie. La prima riguarda la non segretezza della link key, la seconda la possibilità per un dispositivo di passare dal ruolo di master a quello di slave di una piconet:

- **Non segretezza della link key**: Attacchi all'autenticazione.
- **Switching Master-Slave**: la seconda vulnerabilità è legata alla capacità di un dispositivo di compiere lo switching (MS switching) dal ruolo di master al ruolo di slave. Ci sono tre situazioni in cui è necessaria una tale operazione. La prima si ha quando un'unità compie il paging sul dispositivo master di un'esistente piconet, perché vuole entrare a fare parte di tale rete. Per definizione l'unità che esegue l'operazione di paging è il master di una particolare piconet, composta dallo stesso dispositivo e dal master coinvolto. La seconda situazione si ha quando un dispositivo vuole creare una nuova piconet di cui esso è master e il corrente master sia suo slave. Questo caso comporta per il master di una piconet un doppio ruolo; master della sua piconet e slave di un'altra. La terza situazione riguarda la possibilità per un dispositivo slave di riuscire a prendere il controllo completo di un'esistente piconet. Una tale operazione comporta per tutti gli slave il passaggio alla nuova piconet, quindi notevole spreco di tempo nella sicronizzazione di tutti gli slave. La vulnerabilità introdotta dall'operazione di switching è legata al blocco della cifratura di qualunque trasmissione ogni qualvolta un MS switching è avviato. Ciò significa, che se dei dispositivi stanno ancora trasmettendo al master della piconet, mentre un dispositivo attaccante si presenta come un dispositivo, che vuole prendere possesso della corrente piconet, questo sarà in grado di ascoltare tutto il traffico sulla rete per tutto il tempo richiesto dal master per trasferire le informazioni di sincronizzazione.

Casualità impropria

Come già detto nella sezione 3, in Bluetooth l'unica richiesta per i numeri casuali è che essi siano non repeteating e randomly generated. A tale scopo i progettisti hardware dovrebbero garantire che i semi utilizzati nella generazione di numeri casuali siano sufficientemente casuali.
Una vulnerabilità legata ai numeri casuali è dovuta al trasferimento in chiaro di numeri casuali usati nella generazione di chiavi e in procedure di autenticazione.

Deallocazione impropria

La deallocazione impropria di risorse utilizzate in precedenza può agevolare un attaccante in successivi attacchi.
Consideriamo il caso dell' autenticazione dopo la cifratura. Il comando HCI Authentication Requested è usato per tentare di autenticare un dispositivo remoto associato con uno specificato Connection Handle. Un Connection Handle è un identificatore a 12 bit che è usato per indirizzare unicamente una connessione dati/voce da un dispositivo Bluetooth ad un altro. Un Connection Handle può essere immaginato come un identificatore che identifica un canale che connette due dispositivi Bluetooth. Purtroppo o il master o lo slave potrebbero non pubblicizzare tale comando con un Connection Handle corrispondente ad un link cifrato.
Nel caso di fallimento nell'autenticazione, l'Host Controller o il Link Manager potrebbero non eliminare automaticamente il link con un'operazione di Disconnect. Da qui un attaccante potrebbe non autenticarsi dopo un attacco di spoofing su un link cifrato ed essere agevolato nell'attacco.

Possibili soluzioni:

- Garantire in qualche modo che gli utenti scelgano i propri PIN spesso a caso.
- Aumentare la lunghezza dei PIN in modo da essere più sicuri.
- Adottare metodi di sicurezza basati sui certificati.
- Sviluppare una migliore forma di copertura fisica, per evitare agli estranei di intercettare segnali provenienti da dispositivi Bluetooth.

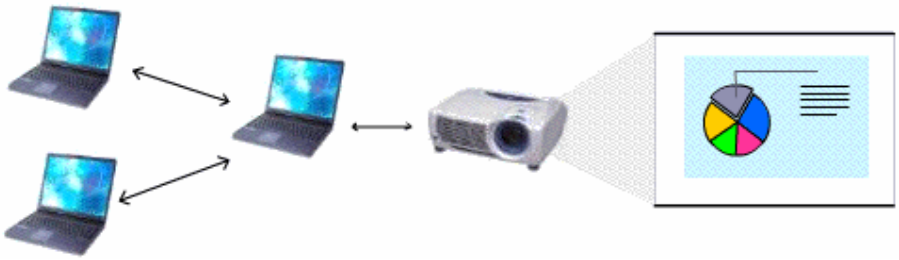
9) APPLICAZIONI PRATICHE

Bluetooth a casa.

La nostra casa potrebbe diventare una casa del futuro grazie a varie applicazioni di Bluetooth. Ad esempio possiamo connettere qualsiasi tipo di periferica al nostro computer di casa senza l'ausilio di cavi; tutte le periferiche come mouse, tastiera, stampante ecc. utilizzando il Bluetooth si connetteranno al pc senza cavi automaticamente e potranno essere disposti nella stanza in qualunque posizione.

Ad esempio gli elettrodomestici sono collegati in una PICONET Bluetooth. La macchina del caffè comunica con il tostapane ("il caffè si sta riscaldando è ora di iniziare a tostare il pane"), il tostapane comunica con il frigorifero ("sono appena state usate due fette di pane: è necessario aggiornare l'inventario") e il frigorifero comunica con noi ("sta per terminare il pane") attraverso il nostro portatile trasmettendo l'elenco dei contenuti attualmente disponibili per poi regolarci per la spesa.

Bluetooth al lavoro.



In una **conferenza interattiva** tutti i partecipanti alla riunione sono connessi tramite tecnologia wireless per lo scambio istantaneo di dati. Inoltre c'è il controllo di un Pc principale che è collegato a sua volta ad un proiettore che visualizza le informazioni trasmesse per una presentazione. In qualsiasi istante è possibile trasmettere dati da un computer agli altri.

Bluetooth al negozio.

Percorrendo i vari reparti di un negozio troviamo un articolo di nostro interesse e ne leggiamo il prezzo; non contenti prendiamo il cellulare che legge le informazioni incorporate elettronicamente e si connette ad internet per un confronto immediato dei prezzi. Successivamente il telefonino si illumina per indicarci altri negozi che vendono lo stesso articolo. E' possibile, tramite PDA cercare un reparto di un supermercato visualizzandone la mappa.

Bluetooth in automobile.

E' possibile avere una configurazione personale dell'automobile. Programmando il nostro cellulare con il dispositivo Bluetooth della macchina una volta entrati in essa l'automobile, percependo il nostro arrivo, adegua automaticamente la posizione del sedile, accende il condizionatore e sintonizza l'autoradio sulla nostra stazione preferita. Inoltre il cellulare si connette ad un microfono ed un altoparlante installati nel cruscotto per fungere da viva voce senza che esso sia estratto dal taschino.

Bluetooth in valigetta.

Ci troviamo in strada con il portatile in valigetta e ci arriva un messaggio di posta elettronica sul cellulare. Il cellulare si collega al nostro portatile emettendo un suono che ci avverte dell'arrivo di messaggi di posta elettronica. All'apertura del portatile potremo visualizzare tutti i messaggi di posta in arrivo.

Bluetooth e auricolari.

Ci sono degli auricolari senza fili che permettono la piena libertà di movimento. Sono particolarmente utili perché sono utilizzabili con qualsiasi tipo di telefono (cell, cordless, fisso). Sono molto importanti per chi lavora con il telefono perché le radiazioni emesse sono di gran lunga inferiori rispetto a quando si porta un telefonino all'orecchio: 3 watt contro 1milliwatt.

Gioielli digitali.

Infine c’è da citare l’imminente arrivo dei gioielli digitali; Saranno probabilmente dispositivi indossati come anelli o girocolli contenenti un piccolo dispositivo radio Bluetooth che forniscono informazioni a chi li indossa, cambiando colore o emettendo un determinato segnale. Potrebbero magari segnalare l’arrivo di posta elettronica cambiando colore.

9) CURIOSITA'

Il sistema di connessione a breve distanza dei cellulare è sempre più usato per "agganciare" partner occasionali in bar o metropolitane.

Dall'inglese to tooth, rosicchiare, la nuova moda impazza tra i giovani lavoratori inglesi alla ricerca di sesso mordi-e-fuggi.
Basta avere un cellulare Bluetooth, una buona dose di coraggio e un pizzico di fortuna: il flirt è dietro l'angolo, anche in Italia. Ormai presente su quasi tutti i nuovi cellulari e palmari, il Bluetooth permette di «vedere» altri terminali nelle vicinanze e contattarli.
Treni e metropolitane sono il luogo ideale per il flirt wireless: il toother annoiato cerca utenti nei paraggi e quando ne trova uno, invia un messaggio di invito. «**Toothing**?» è la parola d'ordine per capire che aria tira e se dall'altra parte la risposta è positiva, ha inizio il balletto di messaggi, che in alcuni casi può concludersi con un focoso incontro.
«Il toothing è una forma di sesso anonimo praticato con estranei generalmente su mezzi di trasporto o in particolari occasioni come convegni e seminari».

Nel Regno Unito i toother siano migliaia, certamente sono centinaia i visitatori del suo blog che si scambiano consigli e raccontano le proprie avventure.
Spuntano come funghi le comunità di toother, in Francia come in Danimarca, in Olanda come negli Stati Uniti. Yahoo! ha dedicato una directory e cercando toothing in Google sono quasi 32 mila i risultati, segno che la mania dilaga. In Italia, la prima comunità del toothing è raggiungibile all'indirizzo www.togatoga.it.

Per il toothing, non è necessario stabilire una connessione tra due cellulari, può essere sufficiente inviare un messaggio anonimo sotto forma di biglietto da visita, con una tecnica chiamata Bluejacking.
I biglietti da visita inviati con il **Bluejacking** sono ricevuti da tutti i dispositivi con Bluetooth attivo. Per evitare di essere disturbati, è possibile disattivare la connessione Bluetooth oppure mettere il telefonino in modalità «invisibile».
Per scambiarsi file, contatti, rubrica e note è invece necessario stabilire una connessione diretta tra i due terminali, chiamata pairing (accoppiamento). Bisogna assegnare un «nome» al terminale, attivare la connessione Bluetooth e la modalità «visibile».
Una volta «accoppiati» i due terminali, è possibile accedere da un cellulare ai dati personali (rubrica, note) memorizzati sull'altro cellulare.
Un'operazione delicata per la privacy: il **Bluesnarfing** è proprio il furto dei dati memorizzati sul cellulare dopo il pairing. È stato Adam Laurie a scoprire alcuni problemi di sicurezza del Bluetooth, ed elencando i cellulari vulnerabili (Nokia 6310i e 8910i, Ericsson T39, R520 e T68, Sony Ericsson T68i, T610, T630 e Z600). Per non correre rischi con questi modelli, è sufficiente attivare la modalità invisibile.