Rodolfo Parisio, IW2BSF

Danilo Larizza

Viaggio all'interno del famoso sistema che prende il nome dal re vichingo Harald Bluetooth, che unì Danimarca e Norvegia in un unico stato, passando attraverso l'analisi delle sue rivoluzionarie caratteristiche e dei suoi "bug"

Bluetooth®

Re Harald... modernizzato!

Le tecnologie wireless si stanno evolvendo molto rapidamente, tra queste anche quella denominata Bluetooth. E' il sistema di trasmissione dei dati fra cellulari o dispositivi portatili che utilizza le onde radio invece degli infrarossi come l' IrDA. Sarebbe dovuto essere il più diffuso standard di trasferimento dati a breve distanza, ma probabilmente lo sarà solo nel settore della telefonia mobile. Sta perdendo sempre più terreno nel confronto diretto con l'802.11b Wi-Fi (utilizzata infatti nella nuova tecnologia INTEL CENTRINO), sempre più diffuso come standard di comunicazione senza fili a corto raggio.

Infatti, collegare insieme più dispositivi elettronici non è mai stato semplice specialmente quando si tratta di strumenti realizzati da produttori diversi, che utilizzano sistemi operativi differenti o sono basati su stan-

dard incompatibili o proprietari.
La necessità di rendere comunicanti tra loro questi oggetti - ad esempio PC, computer portatili, PDA, stampanti, videocamere, telefoni cellulari, mouse e tastiere - non è mai stata così impellente. Dato che la tecnologia è parte della vita di ciascuno, è fondamentale che tutto possa coesistere e comunicare in modo affidabile; nel passato, tuttavia, questi dispositivi non hanno praticamente mai avuto a disposizione un linguaggio e una tecnologia universali che permettessero loro di scambiarsi informazioni reciprocamente.
Lo standard Bluetooth è nato per risolvere questo problema offrendo un'interfaccia stabile, uniforme e diretta che i dispositivi compatibili possano adoperare come loro strumento di comunicazione principale.

Bluetooth consente dunque tale connettività tra dispositivi, consentendo di liberarsi nello stesso tempo di cavi perennemente aggrovigliati.

Come funziona
Un dispositivo prima che possa scambiare informazioni elettronicamente con un altro, è necessario che conosca il modo per trasmettere l'informazione e quale protocollo di comunicazione è accettato dall'altro dispositivo; occorre dare una risposta a domande del tipo:

- quale tipo di cavo può connettersi al dispositivo?
- in caso diverso, quale tipo di trasmissione wireless è supportata?
- quali sono i parametri di trasmissione (es. dimensione del pacchetto dei dati trasmessi, etc.)?
- qual è la modalità di presentare i dati? Esiste una cifratura degli stessi?

Le situazioni elencate a volte sono già difficili da risolvere quando i dispositivi sono solo due. Provando ad aggiungerne altri, il quadro si complica ulteriormente - Pc, stampanti, tastiere e telefoni parlano tutti un linguaggio diverso, e i rispettivi produttori sono costretti a implementare metodi proprietari e solitamente costosi perché possano comunicare tra loro.
Ad esempio, la sincronizzazione di un PDA con un PC o un laptop impone spesso il ricorso a un particolare cavo proprietario completo di software specifico; non disponendo del cavo o del software adatti, diventa impossibile effettuare la connessione. Anche il collegamento tramite infrarossi, che non richiede cavi e può rappresentare un mezzo veloce e affidabile nella comunicazione tra dispositivi, ha le sue controindicazioni: la luce viaggia in linea retta, ed è quindi necessario che i dispositivi coinvolti risultino allineati con precisione, senza considerare che questo sistema permette una sola connessione per volta. Bluetooth, valida soluzione a questi e molti altri problemi, è una tecnologia a radiofrequenza a 2,4 GHz che permette a più dispositivi di comunicare senza alcuna necessità di cavi.
La sua implementazione è sovrintesa dal **Bluetooth Special Interest Group** (**SIG**), un consorzio con centinaia di membri che riunisce i più grandi produttori mondiali di apparecchiature elettroniche per l'abitazione e per l'ufficio. Le specifiche Bluetooth sono in continua evoluzione - la versione attuale, la 1.1, è stata introdotta nel 2001. Nonostante le continue modifiche (e le differenti interpretazioni dello standard da parte di vari produttori), la 1.1 è una specifica stabile per comunicazioni wireless che si basa su principi riconosciuti come standard e uniformi. Invece di richiedere cavi o porte infrarossi, le soluzioni compatibili con Bluetooth richiedono solo un semplice e poco

costoso chip capace di trasmettere e ricevere un segnale radio che rappresenta l'informazione che si vuole scambiare: un dato da stampare, un protocollo di rete, un output di tastiera o un database di indirizzi. Non occorre dunque portare con sé cavi o docking station: dato che tutti i chip Bluetooth trasmettono e ricevono lo stesso tipo di segnale, ogni dispositivo che ne contenga uno può teoricamente agganciarsi ad ogni altro prodotto - aderente allo standard - senza bisogno di interfacce e software proprietari.
E poiché i chip Bluetooth operano bidirezionalmente, i dispositivi possono connettersi reciprocamente stabilendo uno scambio con un minimo intervento da parte dell'utilizzatore.

Alcuni dei più recenti dispositivi presenti sul mercato che sfruttano la tecnologia Bluetooth" , quali la "chiavetta" elettronica, il SonyEricsson T610 e la Toyota YarisBlue, che permette di interagire con il proprio telefonino senza bisogno di auricolare e senza togliere le mani dal volante, ed il classico auricolare senza fili.

La tecnica

A differenza da altre tecnologie wireless quali il famoso 802.11b (Wi-Fi), che possono trasmettere diversi megabit al secondo (Mbps), lo standard Bluetooth non è progettato per elevati volumi di dati. Ciascuna rete ("piconet") può supportare al massimo 1 Mbps che deve essere condiviso tra tutte le periferiche presenti in rete - al massimo otto, a seconda dell'applicazione. Il modo in cui la trasmissione dati è strutturata dipende dall'applicazione che si utilizza e dal fatto che il trasferimento avvenga in una sola direzione (half duplex) o bidirezionalmente (full duplex). Le applicazioni half duplex come la stampa possono operare fino a 720 Kbps in una direzione; le trasmissioni full duplex hanno velocità ridotta a 64 Kbps nelle due direzioni, comunque più che sufficiente per numerose applicazioni.
Poiché Bluetooth utilizza la medesima banda di altri dispositivi elettronici, sono stati espressi alcuni dubbi riguardanti l'interferenza con sorgenti esterne che potrebbero compromettere le comunicazioni Bluetooth, e viceversa. Bluetooth è stato tuttavia specificamente progettato per evitare questo problema, utilizzando una tecnica di trasmissione a banda larga con salti di frequenza (FHSS): dopo aver trasmesso un pacchetto di dati su una certa frequenza, il dispositivo commuta immediatamente su un altro dei 78 canali disponibili (vengono utilizzate in totale 79 frequenze). I due componenti del collegamento, trasmettitore e ricevitore, sono sincronizzati tra di loro ed effettuano il cambio di frequenza 1.600 volte al secondo, rendendo altamente improbabile il rischio di interferenza: se anche questo dovesse verificarsi, il problema sarebbe limitato ad una piccolissima frazione di secondo, senza effetti percepibili dall'utente.
Come abbiamo gia' visto utilizza la stessa banda ISM del sistema Wi-Fi, da 2,4 a 2,5GHz ma a differenza di quest'ultimo la potenza in uscita da un modulo Bluetooth e' di soli 1 mW RF,quindi consentendo al ricetrametitore di comunicare a distanze massime di circa 10 metri!

La connessione tra dispositivi

Si basa sull'idea di individuabilità - la capacità del dispositivo di individuare o di essere individuato. Molti dispositivi sono capaci di rintracciare e di essere rintracciati; i telefoni mobili Bluetooth sono per esempio in grado di rilevare la presenza di un PDA per scambiare un contatto o l'agenda. Altri dispositivi non sono in grado di effettuare ricerche di questo tipo: le stampanti, per esempio, devono essere costantemente a disposizione dei sistemi che possono

decidere di inviarvi i loro dati. Quando i dispositivi entrano nel reciproco campo d'azione, si instaura tra essi una "conversazione" via radio. Quando due dispositivi si sono individuati a vicenda, essi devono accordarsi su come comunicare e quali funzionalità ciascuno metta a disposizione dell'altro. Alcuni dispositivi richiedono la condivisione dei dati, mentre altri richiedono semplicemente il controllo del dispositivo individuato; per un mouse o una tastiera, ad esempio, è richiesta solamente la trasmissione di comandi verso un computer. Per semplificare la realizzazione di dispositivi capaci di compiere particolari funzioni attraverso connessioni Bluetooth, è stato introdotto pertanto il concetto di "profilo".

Un profilo non è altro che un set di istruzioni finalizzato a svolgere particolari compiti, come la stampa o la sincronizzazione di dati. Per far si che due dispositivi svolgano la medesima funzione, occorre che entrambi possiedano lo stesso profilo; diversamente, non saranno in grado di comunicare nella maniera richiesta, anche qualora rientrino nel raggio del segnale e possano quindi "vedersi" a vicenda. Si può pensare a Bluetooth come se fosse una grossa tubatura invisibile nella quale possono essere inseriti tanti cavi - i profili - altrettanto invisibili: ciascun cavo collega diversi dispositivi e consente loro di svolgere un'attività specifica.

Molti dispositivi includono più di un profilo. Come minimo, ciascuno deve includere il profilo GAP, perché definisce i processi di individuazione: in sua mancanza, un dispositivo non è in grado di rilevarne nessun altro. Oltre a questo, ogni dispositivo ha bisogno del profilo adatto a supportare la funzione per cui è stato costruito: un telefono cordless Bluetooth, per dare un'idea, deve comprendere il profilo HP. Nonostante questo sistema sembri semplice e diretto, non tutti i produttori fanno il medesimo uso dei profili per compiere la medesima funzione. Per esempio, molti PDA utilizzano il profilo SPP per emulare una porta seriale scambiando dati allo stesso modo dei palmari collegati via cavo, piuttosto che ricorrere a profili di sincronizzazione più complessi: questo può creare problemi di configurazione all'utente. Diversi nuovi profili sono in attesa di adozione ufficiale nella specifica Bluetooth. Molti di essi sono già usati in alcuni prodotti, sebbene non siano ancora formalmente completi né garantiscano il 100% di compatibilità con gli altri prodotti Bluetooth; è il caso del BPP (Basic Printing Profile),

per esempio, già disponibile su alcune stampanti Bluetooth. Il profilo Human Interface Device, concepito per mouse e tastiere, è stato adottato a fine maggio 2003.

L'identificazione automatica

Timori, dubbi e diatribe hanno fatto il loro tempo. Bluetooth e Wi-Fi, al di là di operare nella stessa banda di frequenze, hanno ben poco in comune, al più si possono considerare complementari. In proposito è categorico il sito ufficiale www.bluetooth.org: "La tecnologia wireless Bluetooth è designata a sostituire i cavi fra telefoni cellulari, laptop e altri dispositivi elettronici operanti nel raggio di 10 metri. Wi-Fi è wireless Ethernet: fornisce un'estensione al cablaggio di rete o sostituisce lo stesso per dozzine di computer". Circa il problema della potenziale interferenza reciproca, lo stesso sito esprime totale tranquillità, anzi viene dato rilievo allo scenario più critico, in cui cioè i due sistemi trasmissivi, Bluetooth e Wi-Fi, coesistono ed operano nello stesso dispositivo: esempio probante di una collaborazione che assicura garanzia di robustezza e di performance. Infatti, dopo le prime integrazioni della tecnologia Bluetooth nei dispositivi di lettura (pistole laser e simili), già da qualche mese sono disponibili terminali mobili che dispongono di entrambe le tecnologie di trasmissione, a cui spesso se ne aggiunge una terza, verosimilmente quella GSM/GPRS. La presenza della tecnologia Bluetooth sui terminali impiegati nei processi logistici, siano essi veicolari o palmari, combinati con i lettori dotati della stessa tecnologia, spalanca una finestra su nuove interessanti soluzioni.

Niente male per la "cenerentola" del wireless!

rodolfo.parisio@elflash.it

GLOSSARIO

USB: Universal Serial Bus. Porta di comunicazione utilizzata nel mondo informatico.

MAC ADDRESS: Media Access Control. Sistema di identificazione dei dispositivi di rete tramite un numero assegnato dal produttore in modo permanente e univoco.

WARDRIVING: Tecnica di hacking delle reti wireless

WIRELESS: Senza fili: apparecchiature che sfruttano radiofrequenza o raggi infrarossi per connettere due o più dispositivi evitando l'uso di scomodi cavi di connessione.

Bluetooth si…

Nelle pagine precedenti l'amico Parisio ha elencato egregiamente le peculiarità del sistema di trasmissione senza fili Bluetooth. E' comodo… è utile… è simpatico… insomma ci piace! Ormai lo troviamo di serie su moltissime diavolerie elettroniche presenti in commercio… dal cellulare al forno a microonde passando dall'automobile e alla lavatrice.

Lo scopo principale è quello di permettere la connessione tra piccoli dispositivi elettronici (palmari , auricolari, notebook ,stampanti , cellulari …ed altri). A differenza del wi-fi (utilizzato solo per in ambito informatico) questa tecnologia è utilizzata da qualsiasi tipo di dispositivo elettronico. Unica limitazione sta nel numero. Non possiamo superare le otto apparecchiature interconnesse tra loro. Nel wi-fi abbiamo la LAN… qui abbiamo una piconet.

Ecco un po' di specifiche per i lettori dal saldatore facile :

Frequenza di lavoro: **2400 – 2483 MHz**

Potenza: **classe3 = 1mW**
classe2 = 2,5mW
classe1 = 100mW

Numero massimo di connessioni contemporanee: **8 (piconet)**

Banda passante : **circa 1Mbit/s**

Tutto bellissimo direte voi… W la tecnologia. Ma come siamo messi a sicurezza?

Bluetooth no…

Nei mesi scorsi abbiamo parlato di "WARDRIVING". Un utente smaliziato munito di portatile e scheda wireless andava in giro a scovare ed esplorare le reti altrui con la possibilità di fare danni , sferrare attacchi o semplicemente navigare su internet a spese nostre. E con il Bluetooth? Anche qui siamo nella stessa situazione. Il mezzo di comunicazione e' lo stesso (l'aria) e quindi lo stesso utente smaliziato può sferrare attacchi

"Falle , sevizie e trucchetti che girano intorno al mondo del Bluetooth"

È proprio il caso di dire che il destino dei vecchi telefoni sia "appeso ad un filo". Tra qualche tempo, infatti, sarà sempre più difficile vederne modelli che utilizzino i vecchi ed obsoleti fili. È la tecnologia che lo "impone".

al nostro cellulare sfruttando le falle ormai da molti conosciute.

Analizziamo il procedimento

Uscite dal negozio di telefonia con il vostro nuovo cellulare munito di bluetooth. Che bello l'ho pagato un milione di euro quindi lo accendo… se poi lo uso o no… non ha importanza.

Le modalità sono di solito tre:

Acceso e raggiungibile: il cellulare ha il bluetooth acceso e dice a tutti gli altri dispositivi nel raggio di qualche metro: "Ehiiii… sono quiiii… ci sono… mi chiamo Pippo!"

Acceso e non raggiungibile: il cellulare ha il bluetooth acceso ma non dice niente a nessuno… della serie: "comunico con te solo se sai che ci sono".

Spento: bluetooth spento e cellulare non raggiungibile.

Sappiate che se un cellulare è nelle prime due modalità è attaccabile. Preoccupatevi :)

Ecco come funziona. Ogni cellulare o dispositivo bluetooth in genere è identificato da un numero esadecimale di 12 cifre molti simile al "mac address" delle schede di rete dei Pc e da un "nome" dato da voi e modificabile dai vari menù di configurazione.

Ok! prendo un portatile con una penna bluetooth connessa via USB, lancio il mio bel programmino (costruito appositamente e scaricabile liberamente da internet) e vedo l'elenco di tutti i dispositivi disponibili (e raggiungibili) nella zona. Nel caso in cui ne trovassi un paio devo solo prendere nota del loro indirizzo.

Ogni cellulare offre una serie di servizi connessi al bluetooth identificati da un bel numeretto decimale. Esempio (non reale) l'audio è connesso al numero 1, il fax al numero 2, la rubrica e gli sms al numero 3. Sono come delle porte alle quali possiamo collegarci per utilizzare quel determinato servizio.

A questo punto ci serve un altro programmino che, inserito l'indirizzo del cellulare da attaccare, ci elenca tutti i servizi disponibili e le rispettive porte. Prendo nota anche di questo :)

Arriviamo alla fine… la parte più

bella… i signori del bluetooth hanno messo a disposizione un bel protocollo che si chiama **RFCOMM** (**Radio Frequency Communications**). Sapete cosa fa questo protocollo? Permette di emulare la porta seriale RS232 via buetooth! Pausa di riflessione… Avete capito bene??? Il protocollo fa sì che l'utente a 10mt di distanza (munito di portatile, programma giusto e esperienza) risulti collegato al mio cellulare come se stesse usando il cavetto fornito in dotazione all'acquisto! Immaginate cosa possa fare? No??? Vi faccio un elenco?
Scaricare la mia rubrica telefonica, scaricare i miei sms, inviare sms.

Continuo?
Scrivere messaggi che compariranno sul mio display, editare la mia rubrica e, magia delle magie, inserirsi tra il cellulare e il mio auricolare bluetooth ascoltando le mie telefonate. E infine il top… INVIARE UN MP3 A TUTTO VOLUME NELL'AURICOLARE MENTRE STO SCHIACCIANDO UN PISOLINO SUL TRENOOOOO! Fantasia??? Purtroppo no… REALTA'. Ma non c'è il Pin???? Diranno alcuni? Pin...??? Parlate di quel "robustissimo" codice pin di quattro cifre!!!!!!! quattro cifre che vanno da 0 a 9??? Fate due moltiplicazioni e vedrete che un computer la combinazione giusta la scova in pochi secondi :) Paura????

Conclusioni
Non ho potuto spiegare le tecniche in maniera più particolareggiata per ovvi motivi. Ma da buoni utenti di internet… se aprite il vostro bel browser, il vostro motore di ricerca preferito e scrivete bluetooth… troverete sicuramente quello che cercate :)
Dopo questa breve lettura vi invito a tenere il bluetooth spento quando non serve… anche perché grava moltissimo sulla durata delle batterie.
Tranquillizzo i più spaventati dicendo che queste tecniche non sono né istantanee, né alla portata di tutti. Fortunatamente per sferrare un attacco del genere devono coincidere un bel po' di cose e bisogna avere il cellulare giusto (non tutti i cellulari sono attaccabili facilmente).
Saluti a tutti.

danilo.larizza@elflash.it