Buongiorno io sono Orioli Stefano,

quello di cui vi parlerò oggi è riassunto nei seguenti punti:

inizierò con una breve introduzione alla tecnologia bluetooth low energy con un accenno ai principali campi di applicazione ed agli utilizzi più comuni, ponendo particolare attenzione alle tematiche della sicurezza di tipo informatico che riguardano questi dispositivi. Vedremo poi il sistema nano versione 2 della società RedBear e come può essere utilizzato per creare uno Sniffer multicanale di pacchetti BLE. Infine vi parlerò di cosa è stato effettivamente realizzato e come il progetto può evolvere in futuro.

Il bluetooth low energy è una tecnologia di comunicazione wireless a corto raggio ed a ridotto consumo energetico che opera nella banda di frequenza ISM a 2,4 GHz. La specifica Low Energy è stata introdotta nella versione 4.0 dal SIG, ovvero lo Special Interest Group, che è l’organizzazione che sovraintende lo sviluppo di questa tecnologia. In queste frequenze di trasmissione coesistono molte comunicazioni anche di altri standard trasmissivi, come per esempio il più comune Wi-FI ed è quindi soggetta a interferenze. Per ridurre queste interferenze e per avere quindi un canale che sia il più pulito possibile, il bluetooth low energy divide la banda trasmissiva in 40 canali ed utilizza un canale trasmissivo diverso per ogni pacchetto che invia, fino a 1600 volte al secondo. Inoltre, grazie alla funzionalità di Adaptive Frequency Hopping, questo cambio di canale è adattivo, cioè va ad escludere quei canali che sono troppo disturbati da altre comunicazioni.

Come sappiamo il bluetooth è largamente implementato nei dispositivi che utilizziamo tutti i giorni, dagli smartphone ai dispositivi dell’IoT, e ogni giorno se ne fa un uso sempre maggiore in svariati campi applicativi. È lecito quindi domandarsi se queste comunicazioni sono sicure e se i dati che scambiamo con esse sono protetti da ascoltatori indesiderati. Da qui nasce la necessità di accertarne la sicurezza mediante la creazione di un dispositivo di test, che sia il più economico possibile e che quindi permetta di mostrarne le vulnerabilità sfruttabili anche da quegli attaccanti con scarsità di risorse utilizzabili.

Per queste motivazioni è stato utilizzato il prodotto di punta della RedBear, il Nano versione 2, con un costo che si aggira attorno ai 30$. Questo dispositivo, nonostante il costo ridotto, Integra il System On a Chip della Nordic, l’nRF52832 che dispone un processore ARM a 32 bit ed è uno dei migliori presenti sul mercato che supporta il protocollo BLE. Viene fornito dotato di un programmatore chiamato DAPLink, che tramite un’interfaccia USB permette di programmare facilmente il Nano, utilizzando un PC, e di dialogare con quest’ultimo tramite HW dedicato, come UART e SPI per lo scambio dati in modalità seriale.

Lo sviluppo dello sniffer è stato effettuato in ambiente UNIX utilizzando Ubuntu versione 17 ed Eclipse come IDE di supporto alla scrittura del codice in linguaggio C. Sono state utilizzate anche altre periferiche a supporto dello sviluppo, come USRP B210 o il Frontline BPA Low Energy, dispositivi molto più costosi del nano ma che si sono rivelati necessari per analizzare nel dettaglio come i pacchetti sono trasmessi.

I primi pacchetti ad essere catturati sono stati quelli di Advertise, ovvero quei pacchetti che un dispositivo bluetooth usa per notificare la propria presenza ai dispositivi vicini; essi sono trasmessi solo in 3 canali, il 37 38 e 39 e quindi sono più facili da catturare. Questi pacchetti, anche se molto contenuti come dimensioni, danno parecchie informazioni sulle intenzioni del dispositivo: notificano la disponibilità o meno ad una connessione da parte del dispositivo, l’indirizzo del dispositivo che li invia, e altre informazioni contenute nel payload che possono essere di varia natura, dal semplice nome del dispositivo, ad una panoramica dei servizi offerti. Analizzando uno dei primi pacchetti di advertise catturati, possiamo ricavare ad esempio dal primo Byte, del valore di 42 esadecimale, che è un Advertise di tipo NonConnectable, ovvero che non è disponibile ad una connessione, e che trasmette un indirizzo privato. Possiamo quindi già dedurre che sia un dispositivo di tipo Beacon, ovvero utile per dare informazioni in broadcast a tutti i dispositivi vicini, come ad esempio la vicinanza a qualche punto di interesse. Il secondo Byte indica la lunghezza del payload, ovvero le informazioni contenute nel pacchetto, che in questo caso vale 0C, quindi 12 Byte di lunghezza. Dopodiché si ha l’indirizzo dell’Advertiser stesso, lungo 6 Byte, che sappiamo da prima essere privato, ovvero non il reale indirizzo della periferica Bluetooth ma uno generato pseudo-casualmente, per ragioni di sicurezza.

Dopodiche, con il valore di 5 si ha un’ulteriore campo length, che questa volta indica la lunghezza del campo dati del pacchetto, che contiene quelle informazioni che l’Advertiser vuole fornire a tutti in broadcast. Il valore FF specifica il tipo dei dati comunicati, che ad esempio in questo caso sono del tipo Manufacturer Specific Data, e infine gli ultimi 4 Byte contengono i dati veri e propri.

La vera sfida è stata catturare il pacchetto di CONNECT\_REQ, ovvero quel pacchetto che da avvio ad una connessione e che contiene le informazioni necessarie per poter catturare tutti i pacchetti della stessa. I campi fondamentali di questo pacchetto sono L’access Address, che è il primo campo di 4 Byte del payload, ed il campo CRCInit con il quale dovrà essere inizializzato il calcolo del CRC dei pacchetti della connessione. Il campo Interval regola le tempistiche con cui effettuare il salto del canale e la costante di Hop, contenuta negli ultimi 5 bit del pacchetto, regola il numero di canali da saltare per ogni pacchetto inviato.

Dopo essere riusciti a catturare ed analizzare questo pacchetto, si è potuto saltare con le tempistiche corrette tra i vari canali ed intercettare così tutti i pacchetti di una connessione.

Un esempio di cattura di una connessione è mostrato nella slide, in cui la comunicazione inizia nel canale 37 con l’invio del pacchetto di connection Request da parte del master; si entra poi nello stato di connessione e quindi ci si sposta fra i vari canali, dapprima il canale 14 passando per il 28 e così via. Si nota che per ogni canale vengono inviati almeno 2 pacchetti, uno dal master che è sempre il primo a parlare in una comunicazione e la risposta dello Slave, necessaria per mantenere la connessione.

Con questo lavoro di tesi è stato quindi creato uno Sniffer multicanale economico, ma che riesce ad ascoltare anche la fase di connessione tra due dispositivi. Questo Sniffer può essere utilizzato in futuro per implementare vari attacchi volti a testare la sicurezza del Bluetooth Low Energy, come l’attacco Man in the Middle che consente ad un attaccante di rubare e/o modificare le informazioni scambiate o l’attacco di Relay del segnale a lunga distanza, che fa credere a 2 dispositivi di essere vicini e in grado di comunicare, anche se in realtà sono molto distanti fra loro.

Io ho concluso, grazie per l’attenzione.