Universidad Latinoamericana de Ciencia y Tecnología

Facultad de Ingeniería

Escuela de Ingeniería Informática

Trabajo Final para optar por el Grado de Licenciatura en Informática con Énfasis Redes y Sistemas Telemáticos

Tema

Seguridad en Tecnologías Bluetooth

Sustentante: Manuel Ulate Obando

Cédula: 1-1203-0895

Tutor: Lic. Miguel Pérez Montero

III Cuatrimestre 2009

Contenido (Seguridad Bluetooth)

Resumen ejecutivo

Para adentrarnos en el tema de *bluetooth* y sus características es importante decir que esta tecnología busca como fin principal la facilidad y eficacia en la comunicación inalámbrica siendo su objeto de uso en redes personales dando como resultado el trasiego de información.

Bluetooth nace como una necesidad de los usuarios por conseguir mayores niveles de operatividad e integración de la creciente demanda de dispositivos que día con día aparecen en el mercado de las tecnologías.

Sin embargo como toda tecnología que surge, viene acompañada de vulnerabilidades y es un blanco latente para los *hackers*[1], quienes buscan las brechas de seguridad para atacar, ya sean dispositivos como celulares, manos libres y cualquier aparato que contenga este tipo de tecnología de comunicación. Es por esta razón que este proyecto busca aclarar no solo las especificaciones de la tecnología IEEE 802.15.1 de *bluetooth* si no mostrar los niveles de inseguridad de los cuales desconocemos a la hora de manipular terminales con *bluetooth*.

En el documento se detallan las especificaciones con las que cuenta *bluetooth*, los servicios que brinda, entre los cuales está facilitar las comunicaciones además de una gran gama de dispositivos que manejan esta tecnología y los niveles de seguridad con los que se debe contar para un mayor aprovechamiento de uso.
Al final la manipulación y seguridad correcta de *bluetooth* impedirá estar en el círculo latente de ataques.

[1] En la actualidad se usa de forma corriente para referirse mayormente a los criminales informáticos, debido a su utilización masiva por parte de los medios de comunicación desde la década de 1980. Tomado de: http://es.wikipedia.org/wiki/Hacker

Abstract

To go into in the bluetooth topic and their characteristics it is important to say that this technology looks for as main the easiness and effectiveness in the wireless communication being its use object in personal nets giving the transmission of information as a result.

Bluetooth is born like a necessity of the users to get bigger operability levels and integration of the growing demand of devices that day with day appears in the market of the technologies.

However as all technology that arises, it comes accompanied by vulnerabilities and it is a latent target for the hackers who look for the breaches of security to attack, be already devices like cellular, free hands and any devices that it contains this type of communication technology.

It is for this reason that this project looks for to not clarify alone the specifications of the technology IEEE 802.15.1 of bluetooth also to show the levels of insecurity of which we ignore when manipulating terminals with bluetooth.

In the document the specifications are detailed with those that count bluetooth, the services that it toasts, among which to facilitate the communications besides a great range of devices that they manage this technology and the levels of security with those that it should be counted for a bigger use it.

At the end the manipulation and correct security of bluetooth will prevent to be in the latent circle of attacks.

Frases descriptoras

- Seguridad Bluetooth
- Ataques bluetooth
- Tecnología Bluetooth
- Estándar Bluetooth
- Estándar IEEE 802.15.1

Introducción

La necesidad de interconexión ha avanzado de manera agigantada, dando así el surgimiento de las tecnologías de vanguardia como bluetooth.

Las tecnologías inalámbricas tipo bluetooth son facilitadores en el tema de transferencia de datos, voz y video, sin embargo como redes de área personal acarrean un nivel de seguridad muy importante, el cual se omite en la mayoría de casos en su aplicación y usos, este proyecto pretende no solo mencionar aspecto de conceptos, debilidades, fortalezas y ventajas, sino mas bien evidenciar los agujeros de seguridad que perjudican la integridad de los datos y el trasiego de información.

Bluetooth es hoy en día un estándar basado en radiofrecuencia, esto permite la transmisión inalámbrica, siendo así un aliado muy eficaz en la interoperabilidad de dispositivos para y hacia diferentes equipos, como por ejemplo los celulares o móviles personales que se conectan y trasladan datos de manera inalámbrica a una computadora, además de otros aparatos como manos libres que facilitan una conversación de manera libre y a su vez concentrarse solo en el manejo de un vehículo por ejemplo.

Ahora bien, básicamente para adentrar el concepto de bluetooth es en su esencia una tecnología que permite la conexión, enlace y comunicación sin necesidad de cables a corto alcance teniendo presente que su uso genera un bajo consumo de energía pero que aun así pasa datos, audio y video además de su bajo costo.

Existen un gran diferencia de uso con respecto a tecnologías de comunicación como lo es IrDa, (tecnología de comunicación infrarrojo) que necesitan una comunicación visual directa para poder transferir, bluetooth es más panorámico ya que se comunica a cortas distancias pero en radios no directos necesariamente, o sea que permite una comunicación entre dispositivos que se encuentren en diferentes espacios físicos dentro del área de cobertura.

Bluetooth como la mayoría de protocolos de comunicación son blanco fácil para los ataques a dispositivos con esta tecnología, debido a las vulnerabilidades que se van desarrollando en el proceso de su uso.

Historia y Origen

Ilustración 1 Logo que identifica la tecnología Bluetooth

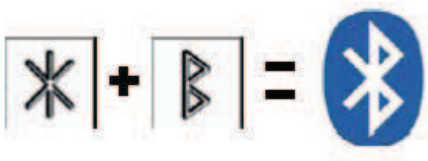
Bluetooth, por Bluetooth, 2009, recuperado el 22 de setiembre de 2009 de http://spanish.bluetooth.com/bluetooth/

En el año 1994 fue desarrollado bluetooth; por la compañía de telecomunicaciones Telefonaktiebolaget (Ericsson) como una idea o proyecto de poder comunicar dos móviles comunes.
Seguido a esto en el año 1998 se conformó un grupo interesado en crear las especificaciones técnicas con respecto a bluetooth, el cual se llamó para ese entonces Bluetooth Special Interest Group y desarrollaron bluetooth 1.0 donde se tomaron en cuenta para las descripciones dos patrones decisivos para su implementación que fueron; desarrollar un perfil principal donde su función sería la de brindar la pautas para la interoperabilidad de sistemas bluetooth y de igual forma un eje principal con detalles como lo son el diseño, nivel de transporte, servicios, medio de transferencia, compatibilidad con otros protocolos de interconexión y capas.

Para dar sentido a la palabra bluetooth es importante aclarar que el término proviene del siglo 10, en honor al rey danés Harald Blatand que se le dio gran importancia por su aporte en la guerra de Dinamarca, Noruega y Suecia al unirlos por medio de un proceso de cristianismo de los vikingos.

Por lo tanto bluetooth pretende conectar y unir dispositivos móviles; de ahí que se le dio el homenaje al rey, traduciendo su apellido a bluetooth.

Pero para saber el origen del logo solo basta con recurrir a las runas[2] nórticas donde la sumas de dos de sus signos del abecedario crean el sello de bluetooth de la siguiente manera:



[2] Alfabetos que se usaron para escribir en lenguas germánicas en la antigüedad y en la edad media, durante el cristianismo principalmente en Escandinavia y las islas británicas. Tomado de : http://es.wikipedia.org/wiki/Alfabeto_r%C3%BAnico

Bluetooth

Esta tecnología como otras ha nacido con la idea de facilitar las comunicaciones y sincronización de datos o información entre personas y/o dispositivos, además permite la movilización con conexión de bajo consumo, utilizando radio de corto enlace debido a su tecnología de bajo consumo de banda y transmisión, aun así permite una excelente comunicación aunque existan pequeños límites como paredes, ventanas u otros obstáculos entre distancias cortas.

Bluetooth ha crecido y por ende se hizo necesaria la creación de estándares y especificaciones para dar mayor control de aplicación y uso.

Estándar

Esta tecnología opera bajo un estándar, el IEEE[3] 802.15.1 para redes inalámbricas, que básicamente funciona a una frecuencia o banda de 2.45 GHz para su transmisión de envió y recepción de datos y en el caso de voz se caracteriza por poseer canales de 64 kbit/s de interconexión.

Cuando se produce una comunicación entre dispositivos su enlace es único y es de 48 bits, para garantizar una transmisión segura y rápida.

Descripciones del Estándar Bluetooth

Teniendo en cuenta el concepto y funciones de la tecnología bluetooth, de ser un estándar que permita la comunicación sin cables basada en radio frecuencias en ambientes móviles, es importante describir las especificaciones, es por esa razón que a continuación se mencionan:

- Bluetooth por su capacidad de uso debe ser una plataforma de comunicación segura y confiable, ya que la mayoría de periféricos que usan este sistema son de uso personal y de bolsillo.
- Este estándar es de bajo costo y adquisición, gracias a que es una tecnología universal.
- El bluetooth es un sistema universal que permita una comunicación sin problemas de compatibilidad con cualquier dispositivo o periférico que posee esta característica.

[3] Las siglas IEEE son representativas del Instituto de Ingenieros Eléctricos y Electrónicos, que se encargan de la estandarización, para normar distintas actividades ya sean científicas, económicas o industriales, para así garantizar el funcionamiento y uso. Tomado de: http://es.wikipedia.org/wiki/IEEE y http://es.wikipedia.org/wiki/Estandarizaci%C3%B3n

- Bluetooth es un sistema que trabaja y funciona con poco consumo de energía, debido principalmente a que los dispositivos que poseen esta tecnológica usan una fuente de energía de batería, ejemplo: celulares.

Detalles técnicos de la tecnología bluetooth

La tecnología bluetooth divide sus características técnicas en:

a) Frecuencias de Radio

En este caso Bluetooth maneja rangos de frecuencia que van de 2.4 GHZ a 2.48 GHZ, utilizando la banda de ISM[4] lo cual permite utilizar cualquier dispositivo con sistema bluetooth de manera tal que no existan interferencias en el uso y trasferencia de datos, ahora bien hay otros protocolos que pueden utilizar esta banda de ISM sin embargo con bluetooth no existe problema gracias a que funciona con saltos en su trasmisión y uso de frecuencias.

b) Potencia de transmisión y enlace

La potencia es dividida en clases de la siguiente manera:

Clase 1: se maneja en un rango de 100m con una trasmisión de 100 mw en 20 dbm.
Clase 2: se maneja en un rango de 10m con una trasmisión de 2.5 mw en 4 dbm.
Clase 3: se maneja en un rango de 1m con una trasmisión de 1 mw en 0 dbm.

c) Capacidad de transmisión

Antes de mencionar la capacidad con relación a la transmisión es importante citar que existen tres versiones de bluetooth, las cuales son consecutivas por sus características en las velocidades de conexión.

- En el caso de la versión 1.1 trabaja y transmite a 723.1 Kbps

Esta versión se dan las correcciones del manual técnico y del material antes de ser publicadas las especificaciones de la tecnología bluetooth para la versión 1.0 (primera versión).

- En el caso de la versión 1.2 trabaja y transmite a 1 Mbps

Se dan comunicaciones más rápidas en sincronización.
Se dan las conexiones y enlace para sistemas de audio.

[4] Industrial, Scientific and Medical, tomado de: http://es.wikipedia.org/wiki/Banda_ISM

En esta versión se introduce el salto de frecuencia, lo cual mejora no solo la comunicación sino que evita conflictos con otros protocolos de comunicación.

- En el caso de la versión 2.0 trabaja y transmite a 3 Mbps

Para la versión 2.0 fue un logro importante reducir de manera eficaz el consumo de energía teniendo en cuenta que es una versión con más velocidad de transmisión.

Se incrementaron las velocidades hasta 3Mbps, además es una versión compatible con todas las anteriores.

Tipo de Transmisión

La transmisión en la cual se basa la tecnología bluetooth es básicamente omnidireccional, esto gracias a que no requiere un enlace de vista y además trabaja bajo radio frecuencias lo cual permite configuraciones multipunto.

Este tipo de trasmisiones facilita de manera óptima el manejo y movimiento en la disposición de los dispositivos móviles previos a su comunicación con otros de igual tecnología.

Tipos de dispositivos con tecnología bluetooth.

La mayoría de dispositivos personales hoy en día contienen la opción de bluetooth, lo cual ha venido a facilitar el manejo y transmisión de datos además de dispositivos para funciones siempre en el ámbito de comunicación móvil inalámbrica.

Existen varios periféricos con esta técnica de comunicación, los cuales se mencionan a continuación por clases:

Ilustración 2, Dispositivos bluetooth de imagen y video

Seguridad Bluetooth, por Telefónica NET, 2009, recuperado el 30 de setiembre de 2009 de http://www.telefonica.net/web2/telamarinera/docus/PFC.Seguridad.en.Bluetooth.pdf

Ilustración 3, Dispositivos bluetooth periféricos varios

Seguridad Bluetooth, por Telefónica NET, 2009, recuperado el 30 de setiembre de 2009 de http://www.telefonica.net/web2/telamarinera/docus/PFC.Seguridad.en.Bluetooth.pdf

Ilustración 4, Dispositivos bluetooth para automóviles

Seguridad Bluetooth, por Telefónica NET, 2009, recuperado el 30 de setiembre de 2009 de http://www.telefonica.net/web2/telamarinera/docus/PFC.Seguridad.en.Bluetooth.pdf

Ilustración 5, Dispositivos bluetooth de audio

Seguridad Bluetooth, por Telefónica NET, 2009, recuperado el 30 de setiembre de 2009 de http://www.telefonica.net/web2/telamarinera/docus/PFC.Seguridad.en.Bluetooth.pdf

Ilustración 6, Dispositivos bluetooth para computadoras personales

Seguridad Bluetooth, por Telefónica NET, 2009, recuperado el 30 de setiembre de 2009 de http://www.telefonica.net/web2/telamarinera/docus/PFC.Seguridad.en.Bluetooth.pdf

Ilustración 7, Dispositivos bluetooth para servicios de telefonía

Seguridad Bluetooth, por Telefónica NET, 2009, recuperado el 30 de setiembre de 2009 de http://www.telefonica.net/web2/telamarinera/docus/PFC.Seguridad.en.Bluetooth.pdf

Topología Bluetooth

Existe una gran ventaja de uso con respecto a las tecnologías que utilicen redes PAN y por ende protocolos IEEE 802.15, ya que no importa el lugar donde se encuentren los dispositivos con la tecnología bluetooth, lo único que importa es que estén en el mismo sitio y a una distancia relativamente cerca teniendo en cuenta el radio de cobertura necesario, esto quiere decir que si se hallan dos celulares en un helicóptero y poseen bluetooth; perfectamente se pueden transferir archivos de un celular a otro.

Bluetooth permite, además de la facilidad que brinda el protocolo IEEE 802.15, que en el radio de cobertura se puedan conectar hasta un máximo de 8 dispositivos con esta tecnología, poder comunicarse y transferir datos entre ellos, produciendo así un *Piconet*, como detalle importante si hubiera varios conjuntos de *piconets* se le llamaría *scatternet*.

En una conexión tipo *piconet*, se dan dos tipos de involucrados, los maestros, quienes se encargan de iniciar el enlace y a su vez el envío o transmisión de datos, por otro lado tenemos los esclavos, estos son los dispositivos conectados al maestro del piconet con tecnología bluetooth.

El dispositivo bluetooth maestro no solo es único en un *piconet*, si no que es quien controla y sincroniza las acciones de comunicación para todos los dispositivos.

Bluetooth por sus especificaciones anteriores permite crear estructuras *scatternet*, esto porque no solo se basa en comunicación punto a punto, si no multipunto a punto, es por esta razón que una topología completa de bluetooth es un conjunto de *piconets*, sin embargo en una *scatternet* las *piconets* manejan distintos saltos o tiempos de sincronización.

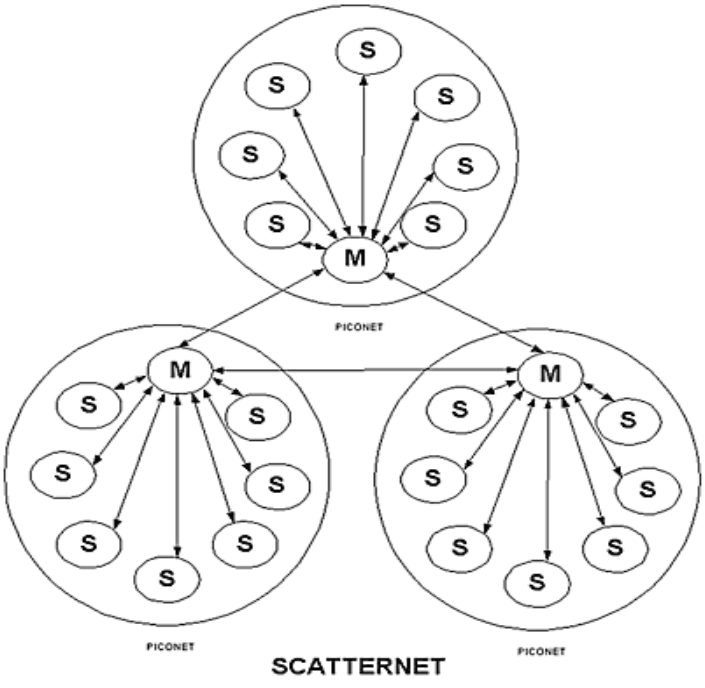


Ilustración 8, conjunto de dispositivos bluetooth conectados *piconet* y *scatternet*

Kasperky, por google imágenes, 2009, recuperado el 6 de octubre de 2009 de http://images.kaspersky.com/sp/vlpub/0602_sapronov_bt_pic1.gif

Ambientes bluetooth

Para el trasiego de datos, bluetooth posee una gran cantidad de escenarios posibles donde las conexiones se dan con facilidad gracias a los dispositivos que tenga esta tecnología, como los son los siguientes:

Transmisión de datos por medio de dispositivos personales.

En este caso pueden ser equipos portátiles, PDA's, o celulares inteligentes, donde bluetooth permite la transferencia de archivos o datos gracias a su versatilidad y flexibilidad, así se puede transferir desde un celular a una computadora de escritorio.

Muchas empresas han optado por este método ya que se les facilita el intercambiar y actualizar datos importantes referentes a compras, pagos o estados financieros desde una handhelp o PDA que utilice algún proveedor de la empresa.

Ilustración 9, transferencia de datos vía handhelp

Seguridad bluetooth, por google imágenes, 2009, recuperado el 6 de octubre de 2009 de http://www.appsmashups.com/wp-content/uploads/2009/06/imagen-6.png

Gracias a la facilidad que da bluetooth por medio de sus radiofrecuencias de corto alcance agiliza la búsqueda de dispositivos con tecnología inalámbrica de este tipo, permitiendo así un mejor tiempo de respuesta y envió.

La gran cantidad de dispositivos bluetooth hace una vida más fácil y accesible tecnológicamente hablando, esto porque por ejemplo hoy en día existen aparatos que reciben algún dato y lo pueden procesar, así es el caso de una foto que se desee imprimir desde un celular, de esta manera se puede enviar la misma vía bluetooth a la impresora con la misma tecnología para así imprimirla esto se puede lograr por medio de la computadora o con impresoras con bluetooth.

Ahora bien los manos libres también tienen un gran aporte a las necesidades de los usuarios para sus conversaciones facilitando por ejemplo el manejo de un vehículo evitando así posibles accidentes o daños graves, también permiten facilidad de movimiento ya que cuentan con una interfaz de entrada y salida de voz.
Es importante no dejar de lado los beneficios que trae bluetooth con respecto a *GPS*, esto porque desde un celular se pueden enviar coordenadas de ubicación y así los demás equipos visualizar los datos actualizados según su posición global.

Seguridad en la tecnología bluetooth

La seguridad en los sistemas bluetooth es ignorada por muchos de nosotros, sin embargo este protocolo por sus especificaciones es una tecnología con un grado de seguridad importante, que bien utilizado puede evitar pérdida de información, robos, daños en aplicaciones, ataques, problemas de identidad cibernética e inconvenientes de confidencialidad.

El tema de seguridad para todos los dispositivos con bluetooth es omitido, podría ser por no generar temor en los compradores, lo cual bajaría sustancialmente las ventas de, por ejemplo, celulares, sin embargo el *hackeo* por medio de la violación de acceso en las tecnologías bluetooth cada vez se hace más grande, no solo por el crecimiento de dispositivos con este tipo de protocolo si no porque un alto porcentaje de los usuarios desconoce siquiera que poseen algún aparato con bluetooth.

Las prevenciones en el uso de bluetooth, no son muy complicadas, basta con activar o desactivar el servicio pero, aunado a esto es importante ponerle *password* o clave para que los usuarios o terminales que se vayan a conectar al dispositivo que inicia la conexión deban ingresar la misma clave y así sean aceptados para poder intercambiar y transferir información.

Importante no dejar de lado las autentificaciones en transmisión, las cuales es recomendado aplicarlas de la siguiente manera:

- Para el caso de entradas, seria autenticar y autorizar.

- Para el caso de salidas, sería importante solo autenticar.

Niveles de seguridad de enlace bluetooth

Los niveles de seguridad, están determinados y clasificados por métodos de nivel de enlace como lo son la autentificación, encriptación y autorización, además de niveles de banda base los cuales se mencionan a continuación:

Autentificación

La autentificación es un proceso básico de seguridad, ya que su naturaleza es la de confrontar un aparato con tecnología bluetooth con otro para así consolidar de manera fiel la conexión y a su vez poder ingresar a los servicios que este último ofrece, esta autentificación se basa en claves para los enlaces.

Sin embargo es importante aclarar que la autentificación solo valida dispositivos y no así usuarios.

A manera de explicar el proceso de enlace, sería de la siguiente manera:

1. Generar una clave de acceso común para los dispositivos bluetooth involucrados.
2. Cada usuario introduce un código de enlace para la comunicación pero debe ser igual en los dos dispositivos asociados. Con longitudes de hasta 16 bits para el código.
3. Cuando se dan las dos confirmaciones iguales de claves o códigos por parte de los usuarios; entonces la conexión está en curso esto porque los dos códigos son correctos y son los mismos para las dualidades en cuestión.

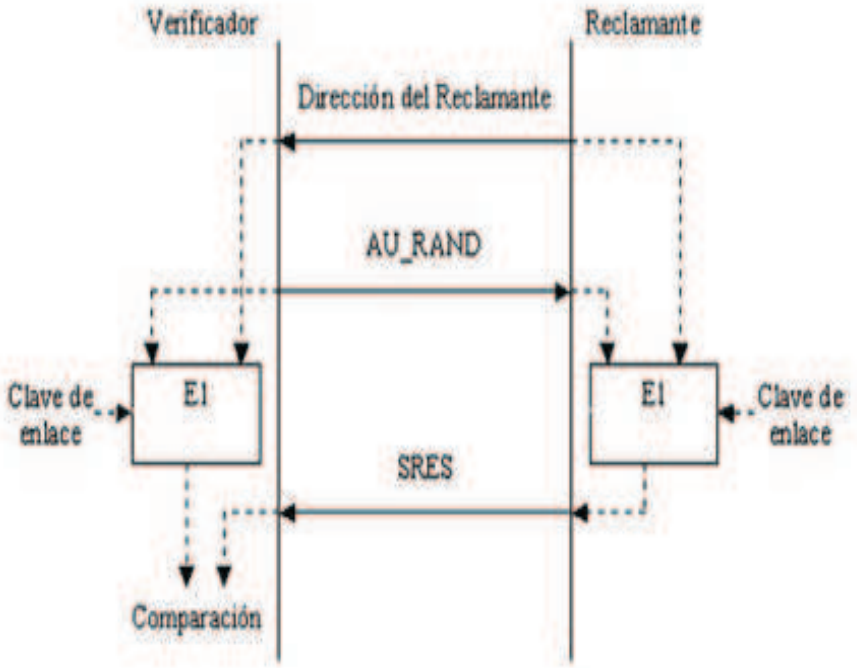


Ilustración 10, proceso de autentificación entre dos dispositivos bluetooth

Bluetooth, por seguridad Mobile, 2009, recuperado el 10 de octubre de 2009 de http://www.seguridadmobile.com/bluetooth/seguridad-bluetooth/Temp/E1.jpg

Encriptación

Como método de seguridad es muy importante la encriptación, esta simplemente es un acuerdo de ambas partes (Maestro y esclavo) con dispositivos bluetooth para establecer directrices de envío y tamaños de claves (longitudes), además la encriptación se da después de que la autorización y autentificación se den.

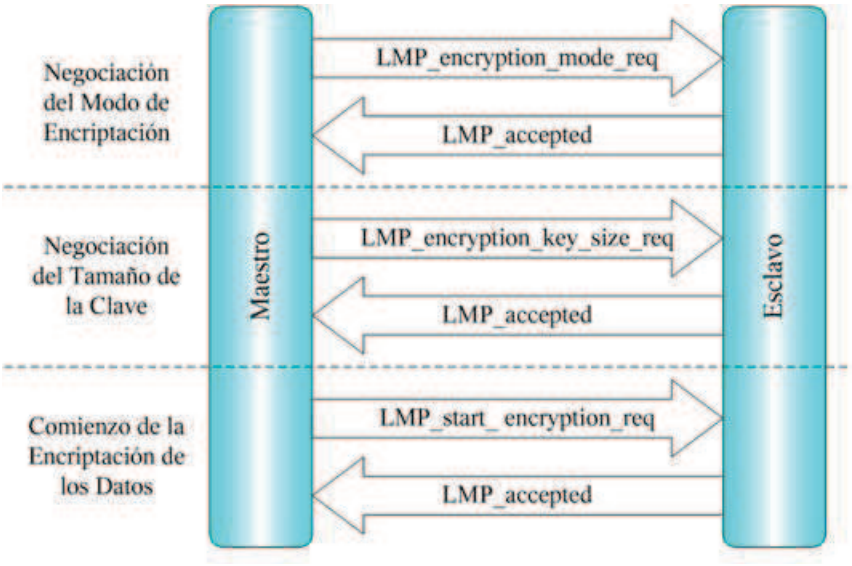


Ilustración 11, proceso de negociación para la encriptación entre dos dispositivos bluetooth

Encriptación, por bing, 2009, recuperado el 10 de octubre de 2009 de http://www.bing.com/images/search?q=Proceso+de+encriptacion+bluetooth&form=QBIR#

Autorización

En el caso de las autorizaciones, son permisos y derechos para ingresar a distintos servicios, avalados por el dispositivo maestro, además de establecer ciertos parámetros de privilegios a los distintos usuarios, así se comparten servicios con derechos totales, restringidos o nulos.

Como el nombre lo indica en el caso de los derechos totales, permiten el ingreso completo y de uso directo a los servicios previamente compartidos por el dispositivo bluetooth; los restringidos, permiten ingresar a ciertos servicios y con previas limitaciones de uso; y por último los nulos, no permiten ni el ingreso a los servicios compartidos ya que no cuentan con la confianza del dispositivo maestro.

Seguridad de banda base bluetooth

Como se mencionó en el estándar, bluetooth opera con una frecuencia de 2.4GHz en la banda asignada, esto estandarizado para todos los países, sin embargo, y debido a que existen muchas tecnologías que utilizan la misma banda específica, bluetooth trabaja con un método que se basa en saltos de frecuencias, esto permite dividir la banda en cuestión para así poder transmitir sin ningún problema de interferencias.

Ataques a equipos bluetooth

La mayoría de la integración de servicios bluetooth está determinada por celulares o dispositivos móviles de uso personal.

Las vulnerabilidades han estado latentes siempre solo que en menor cantidad, esto porque en un principio bluetooth no entró al mercado de redes personales inalámbricas con una idea de quedarse, sin embargo fueron los mismos usuarios que solicitaron mejorías y niveles de seguridad en esta tecnología para aprovechar al máximo sus propiedades de transferencia de datos y conservar la fiabilidad de la información.

Ahora bien Bluetooth por si solo es un estándar con un nivel de seguridad idóneo y eficaz, pero no es aquí donde las vulnerabilidades nacen; sino mas bien en los *comandos tipo AT,* ya que pueden facilitar la entrada a los dispositivos bluetooth y manipular el mismo directamente para extraer datos como contactos, mensajes de texto (privados), datos de llamadas, fotos, videos y demás información confidencial para el afectado.

Como dato importante las empresas que iniciaron el uso de bluetooth para sus celulares fueron Nokia y Motorola, sin embargo contaban con un grado bajo de seguridad esto porque no iniciaban la seguridad de enlace de autentificación ni autorización.

Con el tiempo surgieron los modos de seguridad aumentando su grado conforme su nombre *modo 1, modo 2 y modo 3,* así hoy en día los modelos de celulares o dispositivos con tecnología bluetooth se encuentran con el modo 3 el cual controla de manera más sencilla y eficiente el enlace de datos para la transmisión dando mayor seguridad al trasiego y a la protección de datos de manera tal que el modo 3 se focaliza en la mitigación de; robo de información básica del dispositivo, realización de llamadas y/o desvió de las mismas, control de agenda de contactos, control de mensajería en fin la manipulación total de los involucrados en el ataque.

Modos de Seguridad Bluetooth

Los modos de seguridad son definidos para apoyar la seguridad de enlace de datos donde la encriptación, autentificación y autorización son la base principal para iniciar los procesos de confirmación en la transferencia de cualquier dato u archivo.

A continuación se describen los tipos de modos de seguridad:

Modo 1 o Ausencia de seguridad:

En este caso los niveles de seguridad están deshabilitados u omitidos en la transferencia por lo que no era seguro conectarse a cualquier dispositivo con tecnología bluetooth, sin embargo su mayor vulnerabilidad latente era que los aparatos con bluetooth estaban en un modo en el que cualquier dispositivo podía conectarse a él ya que estaba encendido y por ende los datos no era cifrados.

Modo 2 o seguridad en algunos servicios:

En este caso se cuenta con un grado importante de seguridad, además es efectivo solo cuando la comunicación ya ha sido establecida, por lo tanto existía un riesgo previo a la transferencia de datos.

Sin embargo una vez establecida la comunicación; contaba con niveles de acceso dependiendo de la confianza configurada.

Modo 3 o seguridad a niveles LMP:

En este caso LMP es un nivel previo de seguridad a la comunicación con el canal.

A diferencia del modo 2 brinda mayor seguridad ya que no permite ningún tipo de transferencia sin una previa autorización inicial.
Además requiere que se de un enlace pero con clave compartida con los dispositivos involucrado.

Es así como el modo 3 es el nivel latente con mayor confianza de uso, y que hoy por hoy se encuentra en todos los dispositivos de vanguardia con bluetooth.

Conclusiones

Durante la investigación de seguridad en tecnologías bluetooth, se mencionaron las vulnerabilidades latentes a la hora de manipular este tipo de red personal inalámbrica, el artículo pretende evidencia no solo el uso de estas técnicas si no sus debilidades, que son producto de la falta de implementación de mecanismos de seguridad por parte de los fabricantes y diseñadores de la tecnología bluetooth sin embargo sigue siendo una red personal inalámbrica muy robusta y eficiente que permite la comunicación y la trasmisión de datos por medio de los enlaces de autentificación y encriptación existentes.

El artículo también se menciona de manera clara los fines de los ataques y la forma en que los atacantes extraen información confidencial de equipos con esta tecnología inalámbrica.

La idea no es solo documentar todo lo básico sobre bluetooth, si no de igual forma crear conciencia a los usuarios para que tomen las medidas necesarias y así cuidar y resguardar sus datos, por esa razón se mencionaron ejemplos de dispositivos como manos libres y teléfonos celulares donde la necesidad de seguridad hacia los mismos ha creado herramientas que se encarguen de controlar y mitigar las vulnerabilidades evitando así que los ataques sean materializados y puedan captar y adueñarse de los datos privados de los usuarios.

Las tecnologías de redes personales de corto alcance se han convertido en un importante aliado en la comunicación social brindando no solo transferencias más rápidas y sencillas de datos si no también en la facilidad de manejo y control de información para los usuarios.

Las recomendaciones de uso básicos harán más efectivo el resguardo de información sensible e importante, como lo es el asignar nombre y clave a los aparatos con tecnología bluetooth diferente al nombre y marca del mismo, así también utilizar claves de al menos 5 caracteres y por ultimo no aceptar enlaces con dispositivos desconocidos.

Así al final tendremos un panorama general y básico de qué es bluetooth, sus características, sus vulnerabilidades y su importancia en la comunicación actual de la sociedad en la que vivimos donde la necesidad de transmitir hace más fácil la vida de todos.

Referencias Bibliográficas

Blueback. (2009). *Seguridad Bluetooth*. Recuperado el 5 noviembre de 2009, de http://bluehack.elhacker.net/proyectos/bluesec/bluesec.html

Bluetooth. (2009). *Bluetooth*. Recuperado el 22 de setiembre de 2009, de http://spanish.Bluetooth.com/Bluetooth/

Bluetooth. (2009). *Sitio oficial Bluetooth*. Recuperado el 15 noviembre de 2009, de http://www.Bluetooth.com/Bluetooth/

Bluetooth, por *Bluetooth*, 2009, recuperado el 22 de setiembre de 2009 de http://spanish.bluetooth.com/bluetooth/

Bluetooth, *por seguridad Mobile*, 2009, recuperado el 10 de octubre de 2009 de http://www.seguridadmobile.com/bluetooth/seguridad-bluetooth/Temp/E1.jpg

El arcón de consejos. (2009). *Los peligros del Bluetooth*. Recuperado el 15 noviembre de 2009, de http://elarcondeconsejos.blogspot.com/2009/06/los-peligros-de-el-Bluetooth.html

Encriptación, *por bing*, 2009, recuperado el 10 de octubre de 2009 de http://www.bing.com/images/search?q=Proceso+de+encriptacion+bluetooth&form=QBIR#

Gamermafia. (2009). *Todo sobre Bluetooth*. Recuperado el 28 de setiembre de 2009, de http://gamersmafia.com/tutoriales/show/432

Kioskea. (2009). *Introducción a la tecnología Bluetooth*. Recuperado el 22 de setiembre de 2009, de http://es.kioskea.net/contents/Bluetooth/Bluetooth-intro.php3

Kasperky por *google imágenes*, 2009, recuperado el 6 de octubre de 2009 de http://images.kaspersky.com/sp/vlpub/0602_sapronov_bt_pic1.gif

PaloWireless. (2009). *Fuentes Bluetooth*. Recuperado el 18 noviembre de 2009, de http://www.palowireless.com/Bluetooth/

Seguridad Bluetooth. (2009). *Bluetooth*. Recuperado el 22 de setiembre de 2009, de http://www.uberbin.net/archivos/mobile/seguridad-en-Bluetooth.php

Seguridad Bluetooth, por *Telefónica NET*, 2009, recuperado el 30 de setiembre de 2009 de http://www.telefonica.net/web2/telamarinera/docus/PFC.Seguridad.en.Bluetooth.pdf

Seguridad bluetooth, *por google imágenes*, 2009, recuperado el 6 de octubre de 2009 de http://www.appsmashups.com/wp-content/uploads/2009/06/imagen-6.png

Suite 101. (2009). *Origen de la palabra Bluetooth*. Recuperado el 3 de octubre de 2009, de http://movilescelulares.suite101.net/article.cfm/que_significa_Bluetooth

Taringa. (2009). *Sobre tecnología Bluetooth*. Recuperado el 5 noviembre de 2009, de http://www.taringa.net/posts/info/1104205/Todo-Sobre-La-Tecnoligia-Bluetooth.html