Ataque bluebugging en dispositivos móviles Bluetooth

Libia Malla
MGTI. Student, FIS
Escuela Politécnica Nacional
Quito, Ecuador
johannlibi@hotmail.com

Diana Yacchirema
Departamento FIS
Escuela Politécnica Nacional
Quito, Ecuador
diana.yacchirema@epn.edu.ec

Resumen— **En este documento se describe los modos de seguridad proporcionados por la tecnología de comunicación inalámbrica Bluetooth, así como también los diferentes tipos de ataques que se realizan para detectar las vulnerabilidades existentes en dispositivos que incorporan dicha tecnología. El propósito de este trabajo es exponer la realización del ataque informático bluebugging a teléfonos celulares, para ello se ha desarrollado una aplicación en .Net C#. Esta aplicación permite realizar varias acciones en el teléfono atacado tales como: Leer mensajes, escribir mensajes, llamar y transferir llamadas. También se presentan algunos resultados de las pruebas realizadas para la ejecución del ataque y las conclusiones a las que se ha llegado.**

Keywords- Bluebugging , Bluetooth, Seguridad

I. INTRODUCCIÓN

Bluetooth es una de las tecnologías de redes inalámbricas de Área personal (WPAN) más utilizada en los últimos años, en la actualidad la mayor parte de dispositivos como computadoras, ratones, teclados, impresoras, cámaras y en especial dispositivos móviles como PDAs y teléfonos celulares ya integran esta tecnología. Con el crecimiento de la telefonía móvil se puede acceder a dispositivos inteligentes cuyas aplicaciones permiten navegar por Internet, acceder a correo electrónico, editar y transferir archivos con mejor administración de la información; tales aplicaciones requieren confidencialidad, integridad y disponibilidad para mantener la privacidad del usuario. Sin embargo al igual que en otras tecnologías inalámbricas los riesgos son inherentes y la comunicación puede estar amenazada ya que los mensajes pueden ser fácilmente interceptados, por lo tanto la seguridad en Bluetooth es un factor primordial.

II. ELEMENTOS DE SEGURIDAD EN BLUETOOTH

Para garantizar la seguridad de la información en la transferencia de datos, la tecnología Bluetooth incorpora varios mecanismos de seguridad. El perfil de Acceso Genérico Bluetooth define tres modos de seguridad.

- Modo de seguridad 1: modo no seguro
- Modo de seguridad 2: Seguridad a nivel de servicio
- Modo de seguridad 3: Seguridad a nivel de enlace

Cada dispositivo Bluetooth puede operar en un solo modo de seguridad en un momento particular [1]

El modo 1 es no seguro debido a que los dispositivos bluetooth no inician ningún mecanismo de seguridad, la funcionalidad de autenticación y cifrado son completamente ignorados, aunque para dispositivos que funcionan a este nivel la autenticación puede ser opcional permitiendo conexiones desde cualquier dispositivo Bluetooth hacia él.

En el modo 2, la seguridad se da a nivel de servicio en la capa de protocolo de adaptación y control de enlace lógico (L2CAP), estos mecanismos se utilizan una vez establecido el canal de comunicación. El acceso de los dispositivos a los diferentes servicios se controla a través de un gestor de seguridad, así es posible conceder el acceso a algunos servicios sin proporcionar acceso a otros, en función de su nivel de confianza; en otras palabras el proceso de decidir si al dispositivo A se le permite tener acceso a un servicio X se le conoce como autorización.

Por lo general, los dispositivos intentarán verificar otros dispositivos que está tratando de acceder a los servicios por medio de un Número de Identificación Personal (PIN) Bluetooth [2]

En el modo 3, se proporciona seguridad a nivel de la capa de protocolo de administración de enlace (LMP) para lo cual los mecanismos de seguridad se utilizan antes de establecer el canal de comunicación, estos mecanismos de seguridad son: autenticación, autorización y cifrado de datos. Cuando un dispositivo desea establecer una conexión con otro dispositivo Bluetooth activado, este envía una solicitud de conexión al LMP que se encarga del establecimiento de la conexión y negociación de parámetros, estableciendo sincronización con el segundo dispositivo. Antes de enviar la información se debe asegurar que todas las precauciones de seguridad se han tomado y esto se logra con la autenticación y cifrado de datos. Si algún requisito no se ha cumplido habrá error de autenticación [3].

Tanto la autenticación, autorización y cifrado de datos son mecanismos de seguridad por los cuales los dispositivos Bluetooth acceden a los servicios de otros. Se debe tener en cuenta que cada dispositivo Bluetooth está identificado por una dirección única de 48 bits denominada BD_ADDR (dirección MAC). Hay varias claves diferentes que se utilizan para

establecer y autenticar la conexión entre dispositivos. La clave de autenticación privada es una clave que se utiliza durante el proceso de autenticación cuya longitud de 128 bits. La clave privada de cifrado es una clave utilizada para el cifrado y puede variar entre 8 y 128 bits de largo. Por último, hay un número aleatorio producido por los dispositivos Bluetooth individuales y es 128 bits de largo en longitud [4].

III. TECNICAS DE ATAQUE A LA SEGURIDAD BLUETOOTH

Es evidente que con el transcurso de los años los fabricantes de dispositivos móviles en especial de teléfonos celulares fueran implementando los distintos modos de seguridad a nivel de enlace, debido a que existieron varias vulnerabilidades que afectaban la seguridad de la información del dispositivo; es por ello que los nuevos teléfonos Smartphone disponen del modo 3 de seguridad, esto ocurrió porque se descubrió que era posible acceder a servicios protegidos utilizando como nexo los servicios no protegidos. Sin embargo diferentes tipos de ataques en Bluetooth han ido evolucionando ya que se siguen detectando vulnerabilidades en los teléfonos móviles que traen consigo la perdida de confidencialidad de los recursos del teléfono y de la información del usuario.

En la siguiente sección se describen algunos procesos que permiten hackear los teléfonos móviles con tecnología Bluetooth incorporada:

A. Ataque Bluesnarf

Este ataque consiste en la extracción de archivos de un teléfono móvil Bluetooth a través del perfil de carga de objetos (OBEX object push) sin autorización del usuario propietario. El programa de software bluesnarfing intenta conectarse al dispositivo Bluetooth a través del perfil de Bluetooth OBEX Push, pero utiliza el "pull" en lugar de la función "Push" con la cual se obtienen los datos almacenados en el dispositivo [5].

Los atacantes tienen acceso a los datos almacenados e incluso a la zona restringida de la memoria, incluyendo la agenda, fotos, configuraciones, mensajes y los números de teléfono de serie. Con esta información se puede llegar a clonar el teléfono celular, donde otro teléfono celular puede hacer llamadas telefónicas de la cuenta atacada. Esto es posible sólo cuando el estado de bluetooth del dispositivo atacado se cambia a modo "detectable" o "Visible", aunque se pueden desarrollar herramientas que hacen el ataque posible incluso en modo "invisible" [6].

B. Ataque Bluejacking

Es un secuestro temporal del teléfono celular de otra persona mediante el envío de mensajes no solicitados a través de Bluetooth, se utiliza la función OBEX "push" y no se requiere autenticación. Este ataque no implica la eliminación o modificación de los datos desde el dispositivo, sin embargo los Bluejackers que son quienes realizan este tipo de ataques, lo hacen con el fin de ver la reacción del usuario enviando mensajes publicitarios o bromas, aunque pueden utilizarlo para actividades maliciosas.

Con el fin de llevar a cabo un bluejacking, los dispositivos de envío y recepción deben estar dentro de 10 metros el uno del otro [7]

C. Ataque BlueBuggins

Este es uno de los ataques más peligrosos que puede sufrir un teléfono móvil y que tiene mayor impacto en el usuario. Esta vulnerabilidad es causada por un error en la implementación de la pila de protocolos Bluetooth gracias al cual es posible conectarse al puerto serie RFCOMM del teléfono móvil y enviar comandos AT que serán ejecutados en el terminal GSM sin necesidad de autenticación, si el dispositivo no está protegido [8].

Con esto es posible utilizar el teléfono para iniciar llamadas, enviar/leer mensajes sms, conectarse a servicios de datos como Internet, e incluso monitorear las conversaciones en las cercanías del teléfono. El acceso Bluetooth sólo es necesario durante unos segundos con el fin de establecer la llamada o desviar la misma a otro destinatario, con ello se puede interceptar llamadas y también robar la identidad mediante suplantación de la víctima.

El ejecutar comandos AT en el teléfono móvil, permitirá al atacante llevar a cabo varias acciones en el terminal hackeado como: obtener información básica de la marca, modelo, IMEI; revisar la agenda de contactos (leer, escribir, borrar); acceso a la agenda de llamadas: últimas llamadas, llamadas perdidas, recibidas o realizadas. Gestión de mensajes SMS: leer, escribir y enviar, borrar [9].

D. Ataque BlueMAC Spoofing

Este tipo de ataque le permite a un atacante suplantar la identidad de un dispositivo de confianza llamado así porque previamente se auténtico y solicito autorización para acceder a los servicios que ofrece un sistema y pasa a ser parte de una lista de dispositivos que pueden acceder a cualquier servicio que requiera autenticación y/o autorización. Con ello el atacante utiliza sus credenciales para acceder a los servicios. Cómo se reviso en la sección II, cada dispositivo bluetooth tiene una dirección MAC única que no puede ser cambiada, razón por la cual se hace una suplantación de esta dirección denominada BD_ADDR y con ello acceder a los servicios que requieren autorización como por ejemplo el Perfil de carga de Objetos (OBEX Push) que se encuentra implementado en la mayor parte de teléfonos móviles [10].

E. Ataque Backdoor

Este tipo de ataque se basa en el ataque BlueMac Spoofing ya que una vez que se suplantó la dirección BD_ADDR el dispositivo que pertenece a la lista de dispositivos de confianza, se borra de la lista una vez que está conectado para que cuando vaya a acceder a un servicio no se quede registrado en la lista de dispositivos emparejados, y así proceder al ataque sin ser observado por el dueño del dispositivo. El atacante es capaz de continuar el acceso para llamar por teléfono libremente con el privilegio de una relación de confianza, también acceder a la Internet, WAP o GPRS y no solo a datos almacenados en el teléfono [11].

IV. EJECUCIÓN DEL ATAQUE BLUEBUGGING

La utilización de dispositivos móviles que incorporan en gran medida la tecnología Bluetooth como teléfonos celulares, PDAs y Tablet PCs; proporcionan herramientas para explotar nuevas vulnerabilidades que permitan atacar a otros dispositivos Bluetooth [12]. Las ventajas de su uso radican en que se puede estar más cerca del otro dispositivo a ser atacado sin levantar sospechas y otras son las capacidades mejoradas de procesador y memoria que actualmente disponen estos dispositivos móviles para ejecutar cualquier tipo de aplicación que puede ser desarrollada en entornos embebidos a través de SDKs (Software Development Kits) como Visual C++ o J2ME.

Para la ejecución del ataque se desarrollo una aplicación desarrollada en .Net C# llamada "BlueBugg" con el objetivo de ejecutar ataques a algunos teléfonos móviles, mediante la ejecución de comandos AT en el dispositivo comprometido y con ello obtener el control total del dispositivo. La implementación de comandos AT es específica del terminal GSM y no depende del canal de comunicación a través del cual sean enviados, estos comandos permiten acciones como realizar llamadas, gestionar mensajes de texto SMS, además de otras opciones de configuración del terminal.

La aplicación Bluebugg fue instalada en un teléfono celular marca Samsung I637 con un sistema operativo Windows Mobile 6.1, funciona en la red inalámbrica GSM a 850/900/1800/1900 MHz y también en UMTS a 2100 MHz; al ser un terminal GSM posee un juego de comandos AT específico que sirve como interfaz para configurar y proporcionar instrucciones a otros terminales. La aplicación BlueBugg permite llevar a cabo ataques Bluebugging, a través de la conexión por Bluetooth a otros dispositivos mediante conexiones RFCOMM emuladas sobre puerto COM virtuales.

La primera fase para iniciar el ataque consiste en realizar el emparejamiento con otro teléfono celular que tenga el Bluetooth activado, para lo cual se inicia la aplicación Bluebugg instalada en el teléfono celular, la cual muestra el estado inicial del dispositivo Bluetooth del teléfono indicando que el Bluetooth se encuentra desconectado, tal como se puede observar en la figura 1.

Figure 1. Estado inical del dispositivo

Una vez que activamos el Bluetooth podemos iniciar un descubrimiento de dispositivos móviles a los cuales se les enviará mensajes para iniciar el emparejamiento con aquel dispositivo que responda a la conexión. Al ser un mensaje proveniente de un desconocido es posible que los dispositivos a atacar no respondan al mensaje, razón por la cual se enviarán mensajes comerciales para evitar sospechas.

Cuando el dispositivo acepta el mensaje se establece la conexión Bluetooth y los dispositivos quedan emparejados, mediante la aplicación se emula un puerto serial virtual para poder ejecutar los comandos AT en el dispositivo atacado; en el menú principal se encuentran varias acciones que permiten suplantar la identidad de la víctima como por ejemplo leer mensajes, escribir, llamar y transferir, como se muestra en la figura 2.

Figure 2. Menú principal de la aplicación

Una vez que se ha establecido la conexión se puede empezar a ejecutar el ataque, las acciones que se pueden llevar a cabo, se ejecutan en la aplicación de forma automática ya que se han programado los comandos AT para poder realizar las acciones antes mencionadas, a continuación se revisara cada fase de suplantación de identidad:

A. *Fase "Leer mensaje"*

La aplicación permite leer los mensajes almacenados en la bandeja de entrada del celular, el comando AT utilizado es AT+CMGR= < índice >, <estado>, <número>. En el menú escogemos leer mensaje y nos aparecerá un recuadro donde debemos poner el numero de mensaje que queremos leer, esto corresponde al índice, el estado representa a si el mensaje fue leído o no, esto se muestra en la figura 3.

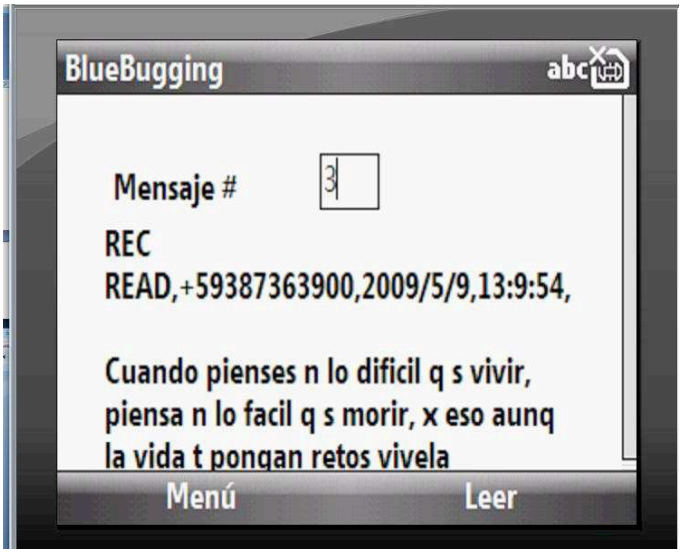

Figure 3. Menú leer mensajes SMS

B. *Fase "*Realizar llamadas*"*

Uno de los ataques más importantes y que permiten utilizar la identidad de la víctima es realizar llamadas, ya que se utiliza su propia línea del teléfono para efectuar llamadas; para ello se configuró el comando ATD (Dial Command); la aplicación permite ingresar el número al cual se desea llamar, como se observa en la figura 4.

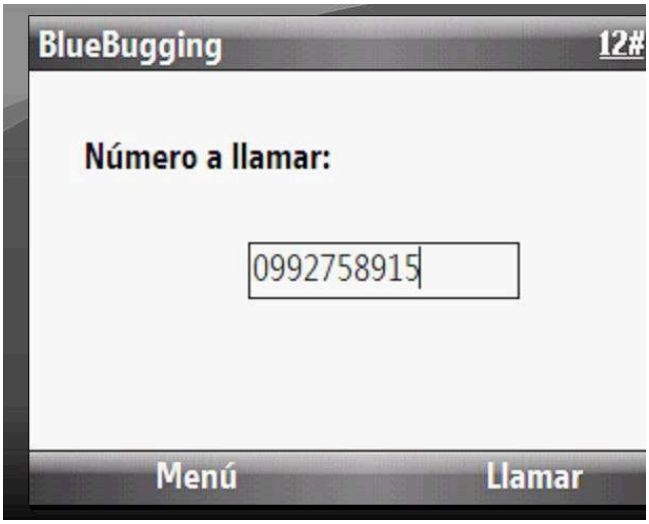

Figure 4. Menú realizar llamadas

V. RESULTADOS

Las pruebas realizadas con la aplicación sé las llevo a cabo en varios lugares donde existe mayor concurrencia de personas como centros comerciales, medios de transporte (buses) y universidades; con el objetivo de verificar el número de personas que disponen de dispositivos móviles con Bluetooth activado y que son vulnerables al ataque bluebugging.

Para empezar se realizaron varias búsquedas de dispositivos Bluetooth, determinando que de cada 20 personas con teléfonos celulares, por lo menos el 40% tienen el Bluetooth activado.

Para establecer conexión con los dispositivos encontrados se envió varios mensajes, entre ellos un mensaje comercial con el nombre "Movistar" para no levantar sospechas, de todos los intentos de conexión se pudo determinar que el 37.5% de usuarios aceptaron el mensaje.

Una vez que el usuario acepto el mensaje, mediante la aplicación se pudo acceder a los servicios del teléfono y efectuar el ataque; la lectura de mensajes y contactos en el dispositivo atacado se realizó con éxito; los resultados del ataque realizado con la aplicación se muestran en la tabla I.

TABLE I. RESULTADOS DE LAS PRUEBAS

	Busquedas realizadas			
	Búsqueda 1	**Búsqueda 2**	**Búsqueda 3**	**Búsqueda 4**
Total usuarios aproximados	25	30	18	40
% teléfonos con Bluetooth activado	24% 6 usuarios	15% 4 usuarios	27% 4 usuarios	20% 8 usuarios
% de usuarios que aceptan el mensaje	50% 3 usuarios	50% 2 usuarios	25% 1 usuario	50% 4 usuarios
Ataque realizado	Lectura de SMS	Llamada de voz	Lectura de contactos	Lectura de contactos

Los resultados obtenidos muestran la factibilidad de realizar un ataque bluebugging a diferentes teléfonos celulares, el número de usuarios que acepta un mensaje en cuatro búsquedas nos lleva a concluir que mediante ingeniería social se puede lograr con mayor facilidad que diferentes personas sean vulnerables a diferentes tipos de ataques.

VI. CONCLUSIONES

Se ha desarrollo la aplicación BlueBugg en lenguaje .Net #C que funciona en una plataforma móvil para realizar el ataque bluebugging, esta herramienta ha sido capaz de automatizar el proceso de explotación de una vulnerabilidad, permitiendo al atacante obtener información sensible y comprometer la privacidad de los usuarios de los teléfonos celulares.

Se ha logrado determinar las vulnerabilidades que tiene la tecnología Bluetooth a nivel de la capa RFCOMM mediante la utilización de comandos AT una vez que se lleva a cabo el emparejamiento con otro dispositivo Bluetooth. Con este desarrollo se propone continuar con el estudio de vulnerabilidades en los nuevos dispositivos Bluetooth, esta aplicación queda abierta a ejecutar el resto de comandos AT como por ejemplo: AT+CPBR=<indice> este comando permite leer una entrada de la agenda de contactos; AT+CPAS ese comando informa el estado de actividad del teléfono; AT+CCFC este comando gestiona el desvío de llamadas, entre otros que se pueden encontrar en juegos de comandos AT GSM.

El ataque BlueBugging es una de las vulnerabilidades más peligrosas y con mayor impacto en los usuarios de dispositivos móviles Bluetooth ya que se puede acceder a la información del usuario violando su privacidad y por ende suplantando su identidad mediante el envío de mensajes y realizando llamadas desde su propio número ocasionando el consumo de saldo de la víctima.

Para evitar este tipo de vulnerabilidades se podría restringir el acceso a los comandos AT desde la interfaz Bluetooth, pero no se lo puede realizar debido a que los propios fabricantes desarrollan aplicaciones para sincronizar el dispositivo móvil con una PC, también los dispositivos Bluetooth como los manos libres requieren el control del teléfono para colgar o iniciar una llamada y esto lo hacen a través de comandos AT.

Algunas medidas que se pueden poner en práctica para evitar ser víctima de este tipo de ataques por medio de dispositivos Bluetooth se recomienda y que le dan buen uso a la tecnología Bluetooth, como por ejemplo: activar el Bluetooth solo cuando sea necesario para realizar algún tipo de comunicación con otro dispositivo de confianza y apagarlo cuando no se vaya a utilizar; también se puede configurar el dispositivo en modo oculto con esto se disminuyen las probabilidades de que un atacante detecte la presencia del dispositivo al realizar una búsqueda de los mismos. Además se puede configurar el dispositivo para que utilice la función de cifrado en todas las comunicaciones y por último se recomienda no aceptar bajo ningún concepto conexiones entrantes de dispositivos desconocidos, así sean mensajes comerciales de alguna marca conocida.

REFERENCES

[1] V. María , C. José, "Evaluación de las vulnerabilidades de la tecnología Bluetooth en stacks libres", febrero 2005.

[2] H. Stephanie, N. Brian and W. Frank, "Security Analysis of Bluetooth Enabled Mobile", IEEE, pp. 1,2, 2006.

[3] IEEE, «Bluetooth Doc, Specification of the Bluetooth,» 2004. [En línea]. Available: http://grouper.ieee.org/groups/802/15/Bluetooth/profile_10_b.pdf. [Último acceso: 12 junio 2012].

[4] k. T. a. O. L, "Wireless network security", Bluetooth and handheld devices , 2002.

[5] D. Browning, «Bluetooth Hacking: A Case Study,» Champlain College Center for Digital Investigation, pp. 4,5, 2008.

[6] Annalee Newitz, "They've Got Your Number…Wired", IEEE, pp. 3,4, 2004.

[7] Bluejacking Tools, «bluejackingtools,» 27 enero 2009. [En línea]. Available: http://www.bluejackingtools.com. [Último acceso: 24 junio 2012].

[8] K. Munir, "Bluesnarfing tools", ZDNet U, pp. 4,5, 2006.

[9] M. T. Alberto, "Seguridad en Bluetooth", Madrid: Universidad Pontificia Comillas, 2006.

[10] W. Stephen, J. Wan and A. Saddlier, "Bluetooth Security", Madrid, 2005.

[11] J. Alfaiate, "Bluetooth security analysis for mobile phones", IEEE PERVASIVE computing, pp. 3,4, 2003.

[12] P. McFedries, "Bluetooth Cavities", IEEE Spectrum , p. 1, 2002.