Un Análisis Preliminar de la Seguridad del Dispositivo IoT VibeEase

Rafael Mantilla, Javier Camargo, y Brahian Rangel

***Abstract*—En el presente documento se expone el análisis realizado al vibrador vestible inteligente VibeEase, el primer vibrador en tener capacidad de integrarse como dispositivo IoT con una aplicación móvil y que permite sincronizarse con música, un audio libro u otras personas a través de internet. El análisis se centra en la seguridad de las comunicaciones que tiene el dispositivo con la aplicación móvil y la nube. En consecuencia, se detalla el protocolo de comunicación entre el dispositivo y la aplicación móvil, así como el intercambio de datos entre la aplicación y la nube de vibease. En general se encontró el uso de algunas buenas prácticas de seguridad y una voluntad del desarrollador por mejorar de forma constante su producto y servicio; sin embargo, también se hallaron algunas vulnerabilidades.**

***Index Terms*—IoT, Seguridad de IoT, BTLE, Vibrador, VibeEase.**

I. Introducción

EL desarrollo en electrónica y en tecnologías de comunicación como BlueTooth han permitido adaptar tecnologías que usen internet hasta en el más mundano de los dispositivos. La interconexión con el internet ha abierto un mercado de posibilidades que se creían inconcebibles. VibeEase es un vibrador que se puede controlar desde el celular y permite generar una experiencia de placer integrada con audio libros, música u otras personas a través del internet. El desarrollo de este producto fue hecho por un *start-up* en un periodo de tiempo muy corto por lo que surgen preguntas sobre la anonimidad y niveles de seguridad que manejan. En este trabajo hacemos un análisis preliminario a la seguridad de las comunicaciones entre el dispositivo y un celular.

II. Descripción de VibeEase

A. Descripción del dispostivo

Women's Health describe a vibease como el futuro de los juguetes sexuales [1]. Vibease inició como un proyecto de crowdfounding en la plataforma indiegogo [2] a través de la cual logró recolectar USD 130.425 de parte de 1402 patrocinadores. El dispositivo es el primer juguete sexual que encaja dentro de las categorías smart y wearable y el motivo de su éxito radicó en convertir un juguete sexual en dispositivo que ofrece una experiencia de sexting multisensorial.

El dispositivo está diseñado para encajar anatómicamente en el "punto dulce" (punto G) del cuerpo femenino, con lo que logra producir una adecuada estimulación del clítoris a la vez que garantiza que el dispositivo permanezca en su lugar de un modo "discreto". Por otro lado, el dispositivo tiene una cobertura de silicona que lo hace resistente al agua e higiénico, por lo que se puede usar en conjunto con lubricantes para permitir sensaciones más placenteras. La figura 1 ilustra la forma y dimensiones del vibrador, así como la forma en la que se ubica en el cuerpo.

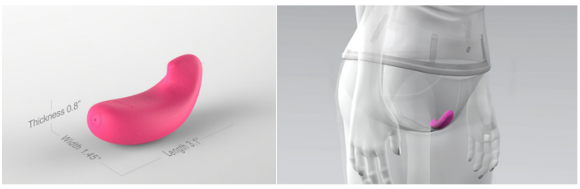

Fig. 1. Forma y dimensiones del dispositivo vestible.

El dispositivo está en capacidad de emitir vibraciones en diferentes intensidades y a diferentes velocidades, personalizables desde la aplicación móvil, lo que le lo hace un dispositivo totalmente manos libre. Asimismo, incorpora una batería que le permite una autonomía de hasta 3 horas de placenteras vibraciones. La batería puede ser recargada cuantas veces sea necesario a través del cable usb suministrado con el vibrador. El vibrador incorpora la tecnología Bluetooth Low Energy (BLE) 4.0 para la comunicación con el teléfono celular, lo que le da la capacidad de hacer uso eficiente de energía y de tener compatibilidad con la mayoría de teléfonos disponibles en el mercado, particularmente dispositivos android y apple, para los que dispone aplicación móvil desde la respectiva tienda de aplicaciones.

B. Descripción de la aplicación

El complemento del dispositivo físico consiste en las aplicaciones móviles disponibles para teléfonos Android, bajo el nombre de " Wireless Remote Vibrator" [3], tanto para teléfonos iOS, bajo el nombre de "Vibease chat" [4]. Es a través de la aplicación móvil que se añade la experiencia multisensorial de vibease, al integrar elementos de audio e imagen.

La aplicación funciona a modo de una red social en donde diferentes usuarios pueden interactuar entre sí. El registro se puede hacer a través de facebook o mediante un correo electrónico y una contraseña; luego de debe configurar nombre de usuario a través del cual los demás usuarios de vibease podrán encontrarle en la red social, además, si un usuario lo desea, puede añadir un código de verificación, caso en el cual quien desee buscar al usuario deberá proporcionar también dicho código Es importante resaltar que no se puede

Este artículo es el trabajo final del curso de Seguridad en IoT de la Universidad de los Andes. Agradecemos a Sandra Rueda y Álvaro Cárdenas.

hacer uso de la aplicación sin antes iniciar sesión. La pantalla principal de la aplicación se concentra en los chats; aquí se puede agregar a nuevos "contactos" (a través del nombre de usuario, e-mail o un enlace que se puede compartir a través de redes sociales), y aceptar las solicitudes de conexión de otros usuarios. Una vez un usuario ha aceptado una solicitud de conexión es posible enviar mensajes de texto, notas de voz, fotografías instantáneas, imágenes de la galería, emoticonos y solicitudes de vibración. Cuando un usuario acepta una solicitud de vibración puede recibir vibraciones cortas o patrones de vibración por parte del compañero autorizado. Asimismo, un usuario puede establecer "compañeros de confianza", los cuales podrán enviar vibraciones sin necesidad de requerir una aprobación. Cada uno de los patrones es personalizable en cuanto a intensidad y duración.

En cuanto a interactuar con otras redes sociales como facebook y whatsapp, vibease ha añadido la opción de generar links para que otros usuarios descarguen la aplicación y los encuentren para establecer contacto. En este caso, la aplicación no hace publicaciones de forma automática, sino que, cuando un usuario decide compartir la invitación, utiliza las funcionalidades del sistema operativo para generar intents de otras aplicaciones y transmitir el contenido. De este modo, es el usuario el que al final tiene el poder de decisión sobre si comparte un mensaje o publicación y el público con el que lo comparte, ya sea restringiendo la privacidad de la publicación en facebook o los contactos a los que envía el mensaje con el link por medio de whatsapp o messenger. Cabe aclarar en este punto que aunque un usuario puede registrarse haciendo uso del api de Facebook, los demás usuarios no sabrán que está en la red social a menos que él mismo sea quien haga una publicación en esta red social (fig. 3).

En relación a otras funcionalidades sociales, recientemente se incorporó la posibilidad de realizar llamadas de voz y videollamadas, en medio de las cuales es posible enviar vibraciones a la persona que tiene el vibrador. En la figura 2 se muestran algunas de las pantallas que muestra la aplicación para dispositivos Android.

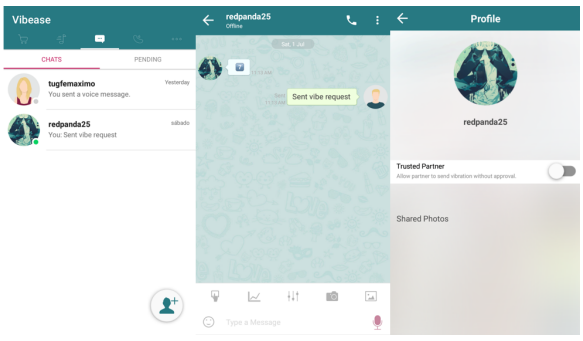

Fig. 2. Funcionalidades de vibease.

En cuanto a la incorporación de experiencias multisensoriales, la aplicación permite la reproducción de música, con la particularidad de emitir vibraciones acorde al ritmo de la misma. Sin embargo, la funcionalidad multisensorial completa se logra por medio de fantasías. Vibease indica que las mujeres que "fantasean" son mucho más satisfechas,

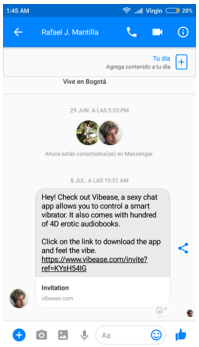

Fig. 3. Invitación a través de Facebook messenger

por lo cual han creado diferentes fantasías que se adecúan a los diferentes estados de ánimo y a través de las cuales permiten a las mujeres ser conducidas a momentos íntimos, emotivos y excitantes [2]. Una fantasía corresponde a una grabación erótica acompañada de vibraciones acordes al relato; así, cuando en el relato se dice "te estoy tocando suave" el vibrador vibra suavemente, mientras que cuando se dice "te estoy tocando fuerte" lo hace más fuerte. Los usuarios tienen acceso una amplia biblioteca de fantasías, las cuales se pueden descargar una vez han sido compradas por medio de créditos (que se compran a través de la aplicación); unas pocas fantasías están disponibles de forma gratuita. Por último,

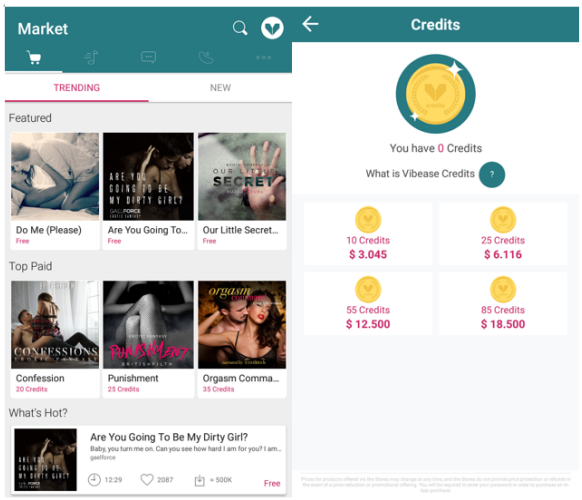

Fig. 4. Tienda de fantasías y de créditos.

la aplicación ofrece un menú en el que se permite establecer la conexión y configurar la vibración por defecto, a la que se accede desde el vibrador mediante un botón físico. Asimismo, ofrece un menú de configuración, en donde se puede agregar una foto de perfil, se puede agregar una contraseña y un pin de seguridad para bloquear la aplicación. Aparentemente se puede desactivar la opción de que vibease realice analiticas sobre los datos recolectados (fig 5).

C. Política de Privacidad y Uso de Datos

La política de privacidad de vibease indica que la compañía recoge una mínima cantidad de datos personales, entre ellos

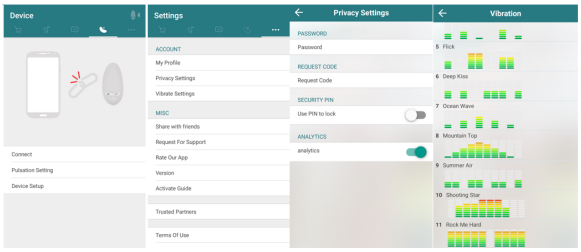

Fig. 5. Ajustes de la aplicación.

se enuncian el nombre, la información de la tarjeta de crédito, los productos o servicios adquiridos, así como otros datos demográficos que no son únicos a un usuario y por tanto no podrían ayudar a identificarle, tales como la edad y el género. No obstante, la política de seguridad asegura de forma explícita que, en un futuro, la compañía podría recopilar otro tipo de información, ya sea de carácter personal o no personal [5].

Adicionalmente, la política indica que se hace uso de cookies y otras herramientas para conocer la forma en la que un usuario interactúa con sus sistemas de información, particularmente con su sitio web, con propósitos de analítica y de mercadeo. También informa de la recopilación de datos de navegación, tales como dispositivos, direcciones ip, tiempos de conexión y de servicio, con el objetivo de mejorar los servicios y productos que provee, así como la experiencia del usuario. [5]

Vibease indica que para garantizar la privacidad de los usuarios usa canales seguros para transmisión de la información, tales como SSl, al mismo tiempo que contrata los servicios de Comodo Security Group para mejorar la seguridad de los servicios ofrecidos. No obstante, la compañía "se reserva siempre el derecho de revelar cualquier información si es necesario para adaptarse a cualquier ley, regulación, procedimiento legal o solicitud gubernamental aplicable, o de modificar, rechazar la publicación o eliminar cualquier información o material, en su totalidad o en parte, todo ello a única discreción" [6].

La información que la compañía recolecta se usará para ofrecer servicios y productos, propios o de sus filiales. Asímismo, podrá compartirla con socios confiables con fines estadísticos, para establecer contacto con los usuarios y conocer la opinión acerca de nuevos productos o servicios, brindar soporte al cliente o acordar fechas de entregos o envíos; no obstante, Vibease prohíbe a sus socios compartir o vender la información de sus clientes y le solicita a los mismos mantener la privacidad de la misma. [5]

Por último, vibease establece una política opt-out para eliminar las suscripciones a comunicaciones, en donde por medio de un correo electrónico el usuario podrá solicitar que no se le siga enviando información acerca de los productos o servicios de la compañía. Del mismo modo, asegura que aunque no tiene la responsabilidad de monitorear el material compartido por medio de la aplicación se reserva el derecho de hacerlo y retirar todo aquello que considere que infringe sus términos y condiciones, entre lo que se podría encontrar "información amenazante, falsa, engañosa, difamatoria, invasión a la privacidad, material obsceno, vulgar, profano, pornográfico, hostigador, ilegal o cualquier material que pudiera constituir o alentar una conducta que se consideraría un delito" [6].

D. Permisos de la Aplicación

A nivel de permisos, cabe resaltar que la aplicación no ha sido optimizada para versiones recientes del sistema operativo Android (6.0 o superior), de modo que no se pueden gestionar los permisos de forma independiente, lo que obliga al usuario a otorgar todos los permisos (así no sea claro el motivo de los mismos) si desea usar la aplicación o, en caso contrario, a no hacer uso de ella.

La aplicación solicita acceso a los siguientes servicios sin que sea evidente la razón de su uso, particularmente, cuando la política de privacidad no habla expresamente de ello:

- Lista de contactos.
- Ubicación (exacta y aproximada).
- Consulta de la identidad y estado del teléfono.
- Descarga de archivos sin notificación.
- Mostrarse sobre otras aplicaciones.
- Modificar la configuración segura del sistema.

El acceso a la lista de contactos y la ubicación de los usuarios corresponde a una situación bastante riesgosa, debido al propósito sexual para el que ha sido diseñada la aplicación y el dispositivo. Entre otras cosas, el mal uso de esta información podría desencadenar en algún tipo de amenaza o extorsión al compartir información personal con el círculo social de un usuario, así como revelar los lugares en los que se ha hecho uso del dispositivo vibease, lo que podría conducir a críticas o juicios morales por parte de otras personas. De hecho, estos tres permisos están considerados por Kaspersky como "permisos peligrosos" [7].

Por otra parte, el sitio de seguridad Internet of Dongs ha reportado un exceso de permisos por parte de la aplicación en android, en particular, la de modificar la configuración segura del sistema [18]. Asimismo, el permiso de superponerse sobre otras aplicaciones puede resultar excesivo en tanto que, en primer lugar, la aplicación no tiene burbujas flotantes u otro tipo de interfaz que se ajuste a este tipo de permiso, pero en segundo lugar y más delicado, la aplicación puede visualizar todo aquello que aparece en la pantalla del teléfono (incluso fuera de la aplicación misma) y, como lo indica Kaspersky, le permitiría a la aplicación "mostrar ventanas *phishing* por encima de las aplicaciones legítimas" [7]. En ese sentido, la descarga de archivos en segundo plano sin notificar al usuario podría habilitar la posibilidad de poner archivos maliciosos en los dispositivos.

Respecto al manejo de notificaciones, vibease, a través de estas, muestra información de los elementos enviados y recibidos, así como los títulos y controles de los audios o fantasías que actualmente se están reproduciendo (fig 6). En ese sentido, debido a la naturaleza de la aplicación, es posible que el usuario no quiera que las notificaciones proporcionen mucha información, en cuanto que estas se pueden ver incluso con la pantalla bloqueada, por lo tanto podría considerarse un problema de seguridad, sobre todo porque algunas notificaciones (en Android) no se pueden ocultar, nisiquiera forzando

el cierre de la aplicación. Una de las maneras en las que vibease ha tratado de maximizar la seguridad consiste en la posibilidad de añadir un pin o contraseña para acceder a la aplicación; sin embargo, el pin no se solicita al acceder a la aplicación misma o a algunas funcionalidades, convirtiendo así el pin en algo casi obsoleto que no garantiza la privacidad de la información, además, porque incluso con el pin activado, las notificaciones siguen mostrando toda la información de la aplicación.

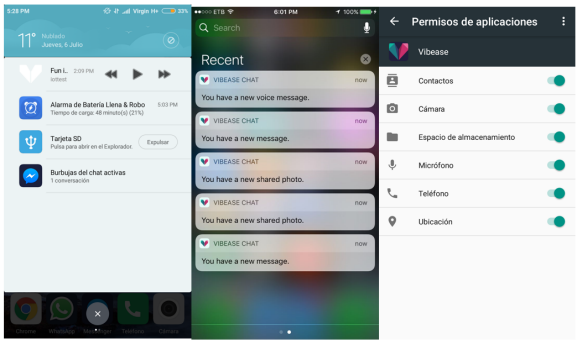

Fig. 6. Notificaciones y permisos de vibease.

III. Trabajos Previos

Un punto de partida para este artículo fue el paper de Vibease Smart Massager [17] en el cual se da un primer enfoque respecto a posibilidades de mejora entorno al la seguridad del dispositivo, en este exponen una vulnerabilidad respecto al tema del chat en formato XMPP, situación que no se exploró a profundidad y no se hicieron diversas pruebas para determinar qué información delicada podría enviarse; también se trabajó en primera medida en el manejo de las credenciales bluetooth pero dicha práctica ya fue mejorada por parte de la aplicación y también se relaciono el tráfico wi-fi y btle con cierta actividad de la aplicación. Por otro lado, la página IoD [18] reporta ciertas vulnerabilidades que se han encontrado entorno a la aplicación mobil y el manejo de los usuarios, un ejemplo de estas son las siguientes:

- DVE-2017-10: Solicitud de permisos para WRITE_SECURE_SETTINGS en la aplicación de android, está ya se encuentra solucionada en la versión v2.50.35
- DVE-2017-14: Enumeración de los usuarios para el acceso a la aplicación, podría encontrarse el nombre de otros usuario, ya está solucionada en la actualización de la aplicación. De lo anterior se observa un esfuerzo por parte del fabricante en atender cualquier hallazgo de seguridad y la búsqueda de soluciones, constantemente se trabaja con los usuarios y se incentiva el reporte de estas vulnerabilidades.

IV. Protocolo de Comunicación BLE

Para capturar el tráfico bluetooth se utilizó el dispositivo Bluefruit LE Sniffer ofrecido por Adafruit. El análisis del protocolo de comunicación entre el celular y el vibrador se llevó a cabo luego de ejecutar los siguientes escenarios de conexión:

1) Encendido del vibrador y escaneo desde un celular.
2) Encendido del vibrador en modo pairing y solicitar el emparejamiento desde el celular.
3) Prender el vibrador y el bluetooth del teléfono, permitir que se establezca la conexión.
4) Permitir la conexión entre el vibrador y el teléfono y enviar un comando de vibración constante.
5) Establecer la conexión entre los dos dispositivos y enviar un comando de vibración con un patrón de vibración específico.

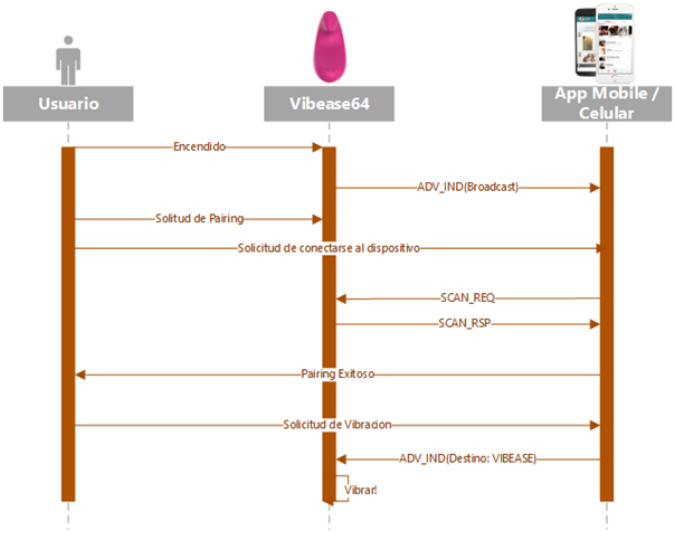

Fig. 7. Resumen del Proceso de Comunicación

Una vez encendido el Vibease empieza a enviar mensajes informando su dirección, estos mensajes se realizan al aire y todos los dispositivos pueden capturarlos.

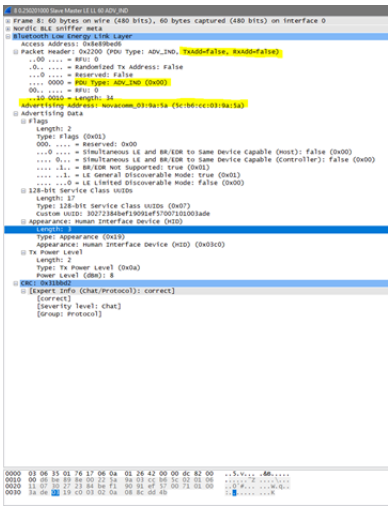

Fig. 8. Paquete Informativo VibeEase

En el paquete informativo de VibeEase se pueden observar las siguinte características:

- **ADV_IND**: El paquete es de carácter informativo, significa que el Vibease está constantemente enviando mensajes Bluetooth esperando que algún dispositivo desee iniciar el pairing
- **TxAdd, RxAdd**: Como estos campos son falsos, significa que la dirección del Vibease que está contenida en el Payload es pública y puede ser visible por otros.
- **Advertising Address**: Como la dirección es pública, en este caso es posible observar la dirección Vibease, se observa que en las diferentes capturas esta dirección es constante.

Si el celular ya ha hecho el proceso de pairing con el Vibease tiene la opción de realizar una conexión automática realizando el proceso de autentificación, de lo contrario es necesario dar inicio al proceso manual que se describió anteriormente.

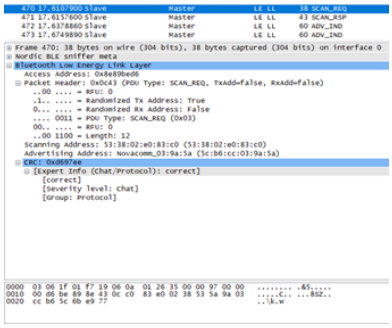

Fig. 9. Mensaje de solicitud de escaneo por parte del celular con la aplicación

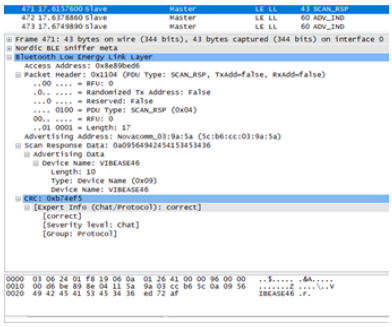

Fig. 10. Repuesta a solicitud de escaneo del VibeEase

Cuando el Vibease acepta la conexión, luego emite un último mensaje aceptado la conexión y menciona el nombre del dispositivo en este caso es VIBEASE64. Con este mensaje se ha finalizado el proceso de pairing, el celular se encuentra conectado al Vibease y ya es posible hacer uso de este. Respecto al dispositivo, este ya no vuelve a emitir ningún tipo de mensaje, queda atado al celular que lo esté utilizando y únicamente recibe los mensajes emitidos por este.

Constantemente el celular envía mensajes al Vibease, utilizando los canales 37, 38 y 39, de tipo ADV_INV con los campos TxAdd, RxAdd con valor falso; estos se encuentran cifrados, por parte del celular su dirección es posible observar que va cambiando constantemente, por el contrario el VIBEASE siempre utiliza la misma dirección. También se observa que la aplicación móvil envía mensajes cada 0.3

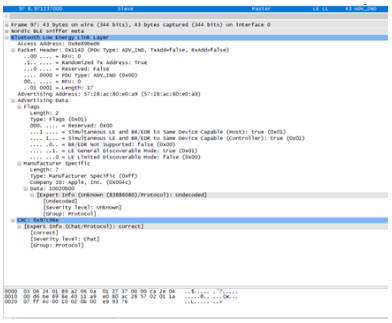

Fig. 11. Envío de vibración del celular a VibeEase

segundos al Vibease, lo que tiene un fuerte impacto en el consumo de batería del teléfono del usuario.

El contenido de estos mensajes suele ser de muy baja variación, en particular hay dos bloques de información (4c:00:10:02:0b:00 y 4c:00:10:02:07:00) que se repiten gran parte del tiempo. En la figura 12 obsrervamos la cantidad de paquetes enviados a través de una sesión de prueba. En esta sesión se mandaron diferentes frecuencias de vibración y en la mitad de la sesión se apagaron las vibraciones. Debido a la frecuencia donde aparecen tenemos la hipótesis de que uno de los paquetes (el de color azul en la figura 12) aumenta la vibración y el otro la detiene. Sin embargo en ningún punto de la captura fue posible encontrar una diferencia fundamental en los paquetes que se pueda asociar a la fuerza de la vibración, por lo que nos quedamos con la duda de cómo logra el dispositivo regular esto.

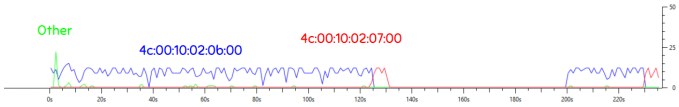

Fig. 12. Tráfico BLE a través del tiempo colorado según su contenido

V. Hallazgos de Seguridad

A. *Tráfico dirigido a terceros*

Como precedente se utilizó la información de la página Internet of Dongs respecto al nivel de seguridad que utilizaban los sitios web asociados a diversos juguetes sexuales IoT, en la figura 13 se encuentra la clasificación del vibease.

URL	Jan 22nd	Feb 25th	Notes
api.imtoy.com	F	F	IMtoys has not replied to the IoD project yet
api.missvvsmystery.com	F	A	Fixed after IoD communication of the problem
api.ohmibod.com	A	A	Dec 20 test was F, fixed after IoD communication of the problem
apps.lovense.com	A	A	Work in progress, some legacy code to deprecate
api.vibease.com	A	A	Cert mismatch due to redirect, non-issue
content.sic-apps.net	A	A	Part of We-Vibe
im1.lovense.com	F	F	Work in progress, scheduled to be fixed within 30 days
mm.sic-apps.net	A-	A-	Part of We-Vibe
secure.vibease.com	A	A	
tools.sic-apps.net	A	A	Part of We-Vibe
vibrato-prod.herokuapp.com	A	A	For Mysteryvibe

Fig. 13. Valoración de seguridad por Internet of Dongs [18]

En este estudio se evaluó el estado del SSL/TLS con ayuda del sitio *SSLlabs.com* [10] que otorga una calificación en

función de ciertas vulnerabilidades conocidas y la seguridad de la página respecto a estas. En el caso del Vibease, la calificación fue de A y no se encontro ningun tipo de problema, este referente es un indicio del estado de la aplicación respecto a los servidores con los que se comunica.

Con base en lo anterior, se va a intentar realizar una exploración con la técnica de man in the middle utilizando la herramienta de Charles Proxy. Para poder utilizar esta herramienta es necesario configurar el celular y el computador que se utilizara de hotspot para que este haga la negociación de los certificados con las páginas a las que se conecta la aplicación y conocer mejor el tráfico que esta genera. Respecto a este análisis, no fue posible que la aplicación

Fig. 14. Configuración *Man in the Middle*

confiara en Charles proxy al momento de realizar el envío de su información, a pesar de utilizar certificado de raíz en el celular y en el computador que corre Charles proxy [8], la aplicación de Vibease no permite el envío de paquetes, ya que al momento de la comunicación Vibease realiza una validación de los certificados a utilizar y tiene una base de datos de los aceptados, por consiguiente cuando se intenta utilizar el certificado de charles proxy este es rechazado. Por

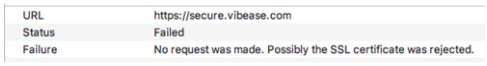

Fig. 15. Mensaje de *Charles Proxy*

otro lado mediante la configuración de un proxy tanto en el celular como en el Hotspot es posible analizar el tráfico que utiliza la aplicación web.

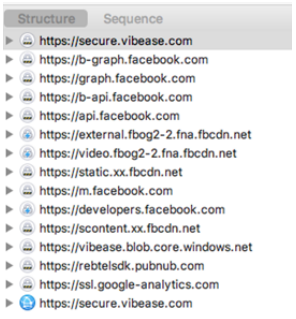

Fig. 16. Sitios utilizados por la aplicación.

De la figura 16, en su mayoría, los sitios consultados corresponden a la autenticación de facebook y se resalta el uso de graph, en este dominio de facebook es donde se utiliza el servicio para obtener la imagen de perfil correspondiente a un usuario. Respecto a la aplicación, la mayoría del tráfico esta dirigo a los dominios de secure.vibease.com y rebelsdk.pubnub.com, el primero dominio es el de la aplicación, corresponde a la ip 104.45.239.70 y esta en el hosting de Microsoft en California; la segunda dirección corresponde a un servicio para comunicaciones de VoIp pero solo fue consultada una vez.

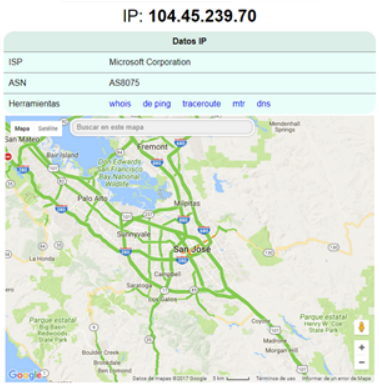

Fig. 17. Información de la ip asociada al dominio de secure.vibease.com.

Respecto al servicio de graph de facebook, no es claro por qué se utiliza sin en ningún momento fue autorizado el uso de alguna imagen de perfil, después de navegar la aplicación, se observa que la imagen de perfil es utilizada en el perfil de esta. Tal vez por el tipo de aplicación no es deseable que se utilice esta foto de perfil, a lo mejor es conveniente preguntarle al usuario sobre el uso que se hará con su información de facebook, muchos usuarios no consideran agradable que este proceso sea automático.

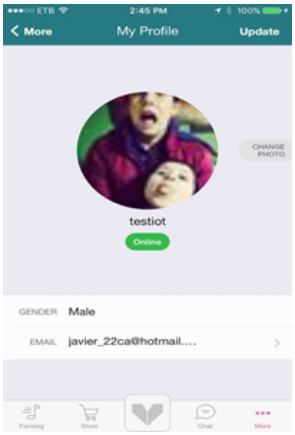

Fig. 18. Imagen del Perfil de Facebook en el perfil de la aplicación de Vibease.

B. Capturas de tráfico de la aplicación

En cuanto al tráfico de la aplicación con sus servidores se puede observar que la mayoría del tráfico va dirigido a las URL *secure.vibease.com* y una URL interna de *pubnub.com*, un IaaS en tiempo real que ofrece servicios de *Data Stream Network*. Todo el tráfico viaja encriptado y usa TLSv1.2, por lo cual es imposible escanear el contenido de estos paquetes. Cabe anotar que para las funcionalidades básicas de Vibease no es necesario estar conectado a internet.

Para el uso de la mensajería interna de la aplicación se envía el tráfico a través del protocolo XMPP (*Extensible Messaging and Presence Protocol*) [11]. Este protocolo permite transmitir

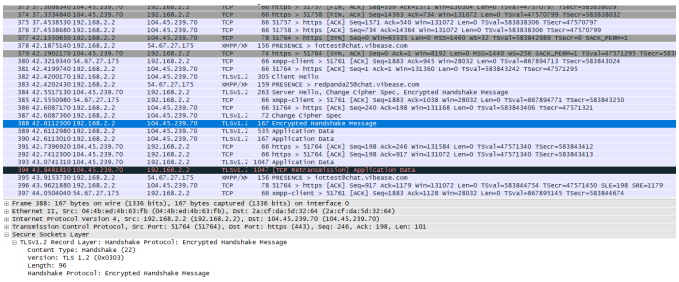

Fig. 19. Captura de paquetes Wi-Fi mostrando el uso de TLS.

XML e información de presencia en tiempo real, usa TLS para encriptar los XML y SASL para la autenticación [13]. En el caso de la aplicación se puede ver en la figura 20 que el servidor soporta Autenticación usando OAUTH2.0 y PLAIN. Inmediatamente el cliente responde que desea usar el modo PLAIN [12], garantizando que la autenticación viaja en texto plano.

Fig. 20. Protocolo de autenticación SASL de Vibease

Gracias al mal manejo de SASL y la ausencia total de TLS para usar XMPP es posible extraer la siguiente información de los mensajes:

- El nombre de usuario dentro de la aplicación de Vibease de ambas personas participando en la comunicación.
- El contenido del mensaje en texto plano.
- Las imágenes, video y micrófono no viajan a través de XMPP, sin embargo es posible identificar cuándo se han enviado con un ID interno a la base de datos de Vibease.
- Cuando la aplicación le permite a un usuario delegarle al otro el control sobre la vibración de su Vibease es posible ver esta autorización y los patrones de vibración enviados (esto incluye la intensidad de la vibración y frecuencia en milisegundos).

Un ejemplo de esta extracción se puede ver en la figura 21.

C. Tráfico Bluetooth

1) Pairing BTLE: Para emparejar el dispositivo con la aplicación móvil es necesario oprimir un botón de emparejar que

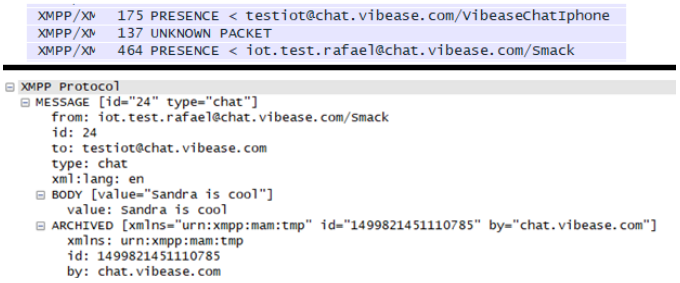

Fig. 21. Extracción del nombre de usuario y texto plano de la conversación

identifica el dispositivo dentro de la aplicación. Sin embargo, es posible emparejar el dispositivo fuera de la aplicación y como se evidencia en la figura 22 cualquier dispositivo que pueda escanear Bluetooth puede intentar emparejarse con el Vibease incluso fuera del modo *pairing*. Note que al momento de escanear dispositivos aparece el nombre 'VIBEASE', lo cual puede ser una preocupación grande para la privacidad del usuario.

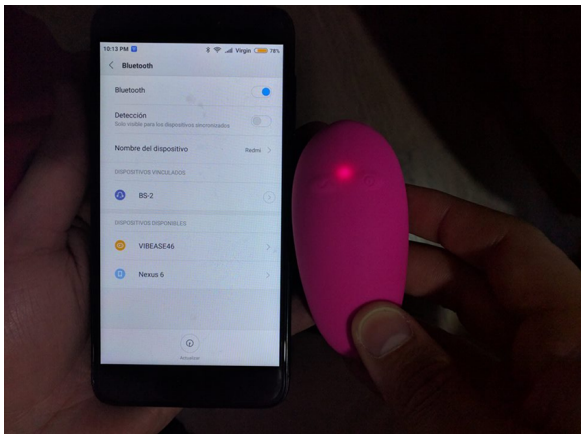

Fig. 22. El dispositivo aparece visible para cualquier celular sin estar en modo emparejamiento.

2) Encripción: Al momento de realizar el Pairing el Vibease es posible que se expongan las credenciales dado que utiliza este proceso está basado en el estándar de Security Manager Protocol para comunicación de BTLE. Este protocolo prevé el siguiente proceso para establecer un canal de comunicación segura para el envío de cualquier tipo de mensaje, bajo este protocolo estos mensajes son vistos como un advisor de low energy pero en realidad cuando se conoce la llave con que están encriptado ya revelan su verdadero tipo y respectivo mensaje asociado. En el caso de Vibease cuando se utilizó la herramienta del Uberthooth a comparación del Adafruit la cantidad de paquetes capturados era mucho mayor, en esta ocasión se visualizó todo el proceso, pero no aparecían este tipo de mensajes: en otro experimento, cuando se hizo el pairing de manera rápida sin oprimir el botón del Vibease, en este tráfico fue posible observar el intercambio de llaves para la creación del canal seguro, en trabajos anteriores se menciona que este proceso únicamente es posible cuando se interfiera la conexión y se forza a una nueva negociación pero en este caso fue posible observar este proceso mediante la

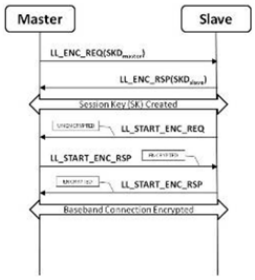

Fig. 23. Security Manager Protocol utilizado en la comunicación BTLE del Vibease al momento del pairing.

escucha de paquetes de btle. De la captura en la figura 24

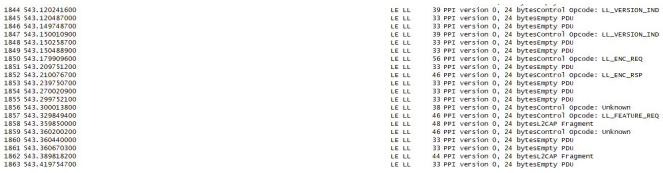

Fig. 24. Captura del Vibease donde se evidencia el Security Manager Protocol.

adicionalmente se observa el intercambio de paquetes respecto a la versión utilizada y los mensajes con la característica del Empty PDU, que en este caso es dada por la presencia de un protocolo de encriptación. Con ayuda de herramientas como Crackle [14] es posible utilizar la información anterior para determinar el pin de pairing utilizado en la comunicación, muchas veces otros dispositivos utilizar pines comunes como 000000, 123456 entro otros. En el caos de Vibease utiliza una combinación de mayor complejidad y dado que este valor está con un padding de 128 requiere una gran capacidad de cómputo encontrarlo, si se cuenta con la tecnología para lograr encontrar este tipo de pin sería posible encontrar la llave utilizada para el intercambio de mensaje y con esta es posible desencriptar el tráfico de la aplicación al Vibease y detectar qué mensajes está enviando.

3) Dirección MAC: El Vibease al momento de transmitir la los ADV_INV siempre utiliza la misma dirección, una vez hecho el pairing, es posible ver la direccionde destino en los mensajes y en ningún momento se utiliza una dirección diferente a la del VIbease, en este caso la dirección es 5c:b6:cc:03:ga:5a, adicionalmente en la información de estos advisor es posible observar el nombre del dispositivo, por consiguiente cualquier persona que tenga encendido el bluetooth y el Vibease no haya hecho pairing es posible que identifique que alguien está utilizando el dispositivo y rastrearlo de acuerdo a la intensidad de la señal.

D. Ingeniería Inversa

En la red se encuentra un sitio web denominado HackApp. El portal web ofrece una funcionalidad gratuita de escaneo de vulnerabilidades de aplicaciones móviles para android a partir del proceso de ingeniería inversa, así como otras características premium de auditoría de seguridad y continuo monitoreo de seguridad [16]. Aunque el servicio de escáner de vulnerabilidades pueda indicar algunos hallazgos, el portal es enfático al indicar que cada uno de dichos hallazgos debe ser verificado de forma manual por el equipo desarrollador, con la finalidad de detectar que efectivamente se trata de una vulnerabilidad.

El análisis asociado a vibease[[16]] muestra los siguientes resultados:

- Es posible la ejecución de código remoto (CRE) por medio de WebView.
- La implementación para validación de certificados SSL corresponde a una implementación propia que, de no estar correctamente implementada, podría permitir ataques de tipo Man In The Middle.
- Dentro de la aplicación se usa código del estilo 'Runtime.getRuntime().Exec()', lo que puede significar una puerta para la ejecución de código malicioso.

Estos resultados, aunque no son muy profundos, podrían ser considerados por los desarrolladores para adoptar prácticas de programación más seguras, que conlleven a garantizar la seguridad y privacidad de la información de sus usuarios.

E. Vibease Bug Bounty

Una de las principales preocupaciones del equipo Vibease se centra en la seguridad de la información de sus clientes. En ese sentido, dispone de un micrositio [19] en donde expone su preocupación y el proceso para reporte de fallas y vulnerabilidades asociados a sus servicios. Para dar solución a este tipo de reportes cuenta con un equipo técnico que está en la disposición de reproducir los errores y evaluar el impacto de los mismos. Por otra parte, aunque vibease no maneja un programa de recompensas por el reporte de errores y vulnerabilidades, puede considerar la entrega de una cuando se trate de una vulnerabilidad considerada crítica; sin embargo, siempre agradecerán de forma pública (a través de su micrositio de seguridad) el reporte de estos incidentes, a menos que quien los reporta desee permanecer en el anonimato.

Por último cabe mencionar que vibease ha sido uno de los dispositivos analizados por al web de modo que han realizado ajustes constantes en la aplicación móvil con el objetivo de mejorar la seguridad de la información.

VI. Resumen del análisis de seguridad

Característica	**Nivel de Seguridad**
Política de protección y recopilación de datos	LEVE: Ambigua y permisiva
Integración con redes sociales	MODERADA: A excepción del uso de la foto de perfil de facebook en la aplicación, el usuario es consciente de cómo y qué está publicando en las redes sociales

Permisos de la aplicación	LEVE: Excesivos y sin relación aparente con el servicio ofrecido
Manejo de notificaciones	LEVE: Revelan demasiada información
Saber si un usuario está dentro de la aplicación	MODERADA: El usuario necesita revelar cuál es su nickname para que otros puedan buscarlo. Cuando se generan enlaces éstos no tienen fecha de caducidad ni restricción de acceso, por lo que pueden ser retransmitidos entre otros usuarios sin el consentimiento del usuario inicial.
Fingerprinting del dispositivo	LEVE: Si el dispositivo está encendido pero el teléfono al que está asociado no está activo, independientemente a que no esté en modo de emparejamiento, siempre responde a los SCAN_REQUESTs. Anuncia su nombre de forma clara. Mantiene una dirección MAC estática.
Protocolo de emparejamiento	ALTO: El cifrado del intercambio de llaves se hace utilizando el Security Manager Protocol.
Probabilidad de suplantación de servidor y alteración de paquetes	ALTA: El SSL que utiliza la aplicación es considerado seguro. La aplicación valida que los certificados provenientes del servidor se encuentren dentro de los certificados de confianza.
Protocolo de intercambio de mensajes	NULA: Los mensajes van en texto plano, esto expone información como el nombre de usuario, el contenido del chat, el id de imágenes enviadas y mensajes de voz, el uso del modo de delegación de vibración y la frecuencia de vibración usada.

REFERENCES

[1] Rooney Erin, *A New Wearable Sex Toy Can Sync To Audio Erotica*, Australian Women's Health, Oct 2016. Disponible en: https://www.womenshealth.com.au/article/sex-love/wearable-sex-toy-sync-audio-erotica

[2] Vibease, *Vibease Wearable Smart Vibrator that brings Fifty Shades of Fantasy to life.* IndieGoGo, 2014. Disponible en: https://www.indiegogo.com/projects/vibease-wearable-smart-vibrator-that-brings-fifty-shades-of-fantasy-to-life/#/

[3] Vibease, *Wireless Remote Vibrator.* Google Play Store, 2014. Disponible en: https://play.google.com/store/apps/details?id=com.vibease.ap3

[4] Vibease, *Wireless Remote Vibrator.* iTunes Store, 2014. Disponible en: https://itunes.apple.com/us/app/swinger-safari-2-0/id933024993?mt=8

[5] Vibease, *Privacy policy"*, Vibease.com [online]. Disponible en: https://www.vibease.com/policy

[6] Vibease, *Terms of Use*, Vibease.com [Online]. Disponible en: https://www.vibease.com/terms

[7] Roman Unuchek, *Todo sobre los permisos de las aplicaciones de Android*. Kaspersky Lab Daily 9 de Febrero del 2017. Disponible en: https://latam.kaspersky.com/blog/android-permissions-guide/8921/

[8] "Charles Web Debugging Proxy • HTTP Monitor / HTTP Proxy / HTTPS & SSL Proxy / Reverse Proxy", Charlesproxy.com, 2017. [Online]. Available: https://www.charlesproxy.com/. [Accessed: 22- Jul- 2017].

[9] "Información de la dirección IP", Es.infobyip.com, 2017. [Online]. Available: https://es.infobyip.com/. [Accessed: 22- Jul- 2017].

[10] SSL Server Test (Powered by Qualys SSL Labs)", *Ssllabs.com*, 2017. [Online]. Available: https://www.ssllabs.com/ssltest/. [Accessed: 22- Jul- 2017].

[11] P. Saint-Andre, Ed. *RFC 3921: Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence* Jabber Software Foundation. October 2004. Disponible en https://xmpp.org/rfcs/rfc3921.html

[12] K. Zeilenga, Ed. *RFC: 4616 The PLAIN Simple Authentication and Security Layer (SASL) Mechanism*. OpenLDAP Foundation. Agosto 2006. Disponible en: https://tools.ietf.org/html/rfc4616

[13] Prof. Richard Sinn, Vanita Mohite y Sudhir Sharma. *An Analysis of XMPP Security*. CMPE 209 – Network Security, Fall 2008 Semester, San Jose State University. 28th October, 2008 Disponible en: http://openloop.com/education/classes/sjsu_engr/engr_networksecurity/fall2008/preso/AnAnalysisofXMPPsecurity.pdf

[14] *mikeryan/crackle*, GitHub, 2017. [Online]. Available: https://github.com/mikeryan/crackle. [Accessed: 22- Jul- 2017].

[15] *Pairing*, Fte.com, 2017. [Online]. Available: http://fte.com/WebHelp/BPA600/Content/Documentation /WhitePapers/BTLE/Pairing.htm. [Accessed: 22- Jul- 2017].

[16] HackApp, Online Security Scanner. *Wireless Remote Vibrator*. Disponible en: https://hackapp.com/report/d7f9587361a793f9adadfe392c0b0dcd

[17] Ryan Kao, Kyle Tillotson y Matthew Wynn. *Vibease Smart Massager* Artículo preliminar para el curso CS6324.001 — INFORMATION SECURITY 1 en UTDallas. 2017

[18] "*Vibease DVE Reports*", The Internet Of Dongs Project, 2017. [Online]. Available: https://internetofdon.gs/vibease/. [Accessed: 22- Jul- 2017].

[19] Vibease, *Security*. Disponible en: https://www.vibease.com/security