Seguridad en redes

PEC3

Pablo Riutort Grande

22 de diciembre de 2019

1.

1.1. Signal

1. Esta vulnerabilidad permite a un atacante hacer una llamada y que esta sea "contestada" por el receptor sin que este intervenga estableciendo así una escucha no autorizada.

2. Al ser Signal una aplicación de mensajería instantánea de código abierto, cualquiera que desarrolle un cliente especial para esta aplicación puede explotar la vulnerabilidad.

3. La vulnerabilidad permite a un cliente de la aplicación efectuar una llamada a un objetivo, en el momento en que hay tono de llamada, si el atacante pulsa el botón de silencio en su terminal fuerza al receptor a contestar la llamada. Esto se debe a que Signal utiliza el protocolo RTP (*Real-time Transport Protocol*) para establecer las llamadas y procesa estos paquetes antes de que la llamada sea contestada. De esta forma, el atacante puede explotar la vulnerabildad de la aplicación con un cliente modificado y aceptar la llamada de manera remota sin interveción del receptor.

4. Poca, el atacante solo necesita que el receptor pueda recibir llamadas y que le de tiempo a aceptarla sin que intervenga el receptor.

5. Según las declaraciones del creador de Signal la vulnerabilidad parece quedar resuelta. Concretamente, vemos los siguientes cambios en el repositorio oficial de la aplicación que hacen referencia a la principal función de la vulnerabilidad.
   En el mismo report del bug existe un comentario de un miembro del proyecto donde se afirma que dicho bug está solventado.

1.2. WhatsApp

1. La vulnerabilidad permite al atacante ejecutar código de manera remota (*RCE* (*Remote Code Execution*))o efectuar un ataque DoS sin necesidad de autenticarse.

2. Esta vulnerabilidad se puede explotar por cualquier atacante que envíe un mensaje específico a la víctima.

3. Mandando un archivo MP4 creado especialmente para explotar esta vulnerabilidad, al parsear el flujo de metadatos del archivo y se puede efectuar un buffer overflow en el WhatsApp de la víctima efectuando así un RCE, DoS o robar datos del terminal.

4. En este caso, la víctima debe confiar de alguna forma en la identidad o en el mensaje que el atacante envía. Por tanto, la ingeniería social puede jugar un papel crucial puesto que si se trata de un contacto desconocido el atacante debería ganarse la confianza de la víctima sobre la legitimidad del mensaje.

5. Facebook afirma que la vulnerabilidad solo afecta a dispotivos cuya versión sea anterior a una específica. No se han econtrado evidencias de que este bug haya sido resuelto en versiones anteriores.

2.

1. En el enfoque de las redes DTN, las comunicaciones ocurren a nivel de capa de aplicación y, por tanto, se sitúa por encima de cualquier combinación de redes existente.
   Las capas inferiores a DTN pueden ser de cualquier familia de protocolos y coexistir varios algoritmos de encaminamiento. Estos pueden ser prefijados en los nodos o referenciados en los propios mensajes que recibe cada nodo. La dificultad estriba en ponerse de acuerdo en qué algoritmo implementar en cada nodo o en cada mensaje.
   Tanto AODV como OLSR son algortimos de encaminamiento de redes Ad Hoc y, por tanto, podrían ser protocolos que se utilizasen en la capa inferior a DTN.

2. En un esquema basdo en IBC se utiliza la identidad del usuario para obetener la clave pública y las claves privadas son obtenidas a través de una tercera entidad de confianza. Esta arquitectura requiere de una entidad indepediente, el PKG, cuya capacidad de generar las claves privadas es crítica para esta aplicación y puede incurrir en un coste adicional puesto que la comunicación con esta entidad tiene que ser de total confianza. Además, los atributos necesarios para generar la clave pública son también críticos, pudiendo suplantar una identidad si no se escogen adecuadamente y son tratados de manera segura.
   En cambio, en un esquema de establecimiento de claves a partir de una clave maestra de corto plazo se utiliza un protocolo de descubrimiento de nodos vecines y posteriormente establecer las claves de enalce en el despliegue inciial. Este esquema está pensado para aprovechar la naturaleza estática de las redes de sensores, es decir, que la vecindad entre nodos no es muy variable y que los cambios en estas son muy esporádicos. Además, en este esquema la clave maestra se carga en los nodos y cada uno calcula su clave de nodo de manera independiente, es decir, todos los nodos parten de la misma clave para calcular las suyas.
   Dada la naturaleza del *car pooling* y su semejanza en este esquema donde hay usuarios estáticos con pocos cambios en la vecindad de la red el esquema de estableciemiento de claves a partir de una clave maestra es un mejor esquema que el IBC para lleva a cabo la arquitectura de la aplicación.

3. El cifrado homomórfico permite aplicar una función algebraica de igual forma sobre un texto a su equivalente cifrado. Es decir, permite operar sobre datos crifados sin necesidad de descifrarlos primero.
   En esta aplicación, la votación del precio (puja) puede ocurrir de manera cifrada sin necesidad de que ninguno de los usuarios (pasajeros o conductor) necesite desencriptar estos datos para introducir una votación en el sistema creando así un sistema de pujas seguro y mucho más eficiente.