Hace unas semanas publicamos un artículo sobre investigaciones relacionadas con la recopilación de datos confidenciales por más de 1300 aplicaciones de Android, aún cuando los usuarios denegaron explícitamente los permisos necesarios.

Dicha investigación se centró principalmente en cómo los desarrolladores de aplicaciones abusan de múltiples formas para la recopilación de datos de ubicación, identificadores de teléfono y direcciones MAC de sus usuarios mediante la explotación de canales ocultos y laterales.

Ahora, un equipo separado de investigadores de seguridad cibernética demostró con éxito un nuevo ataque de canal lateral que podría permitir que las apps malintencionadas escuchen la voz que sale de los altavoces de su smartphones sin necesidad del permiso del usuario en el dispositivo.

Abuso del acelerómetro de Android para capturar datos de los altavoces

Este ataque, apodado como Spearphone, se beneficia de un sensor de movimiento basado en hardware, llamado acelerómetro, que se integra en la mayoría de los dispositivos Android y al que se puede acceder sin restricciones desde cualquier app instalada, aunque no tenga ningún permiso.

Un acelerómetro es un sensor de movimiento que permite que las aplicaciones interactúen dependiendo de la inclinación del teléfono, sacudida, rotación o balanceo, midiendo la tasa del tiempo de cambio de velocidad con respecto a la magnitud o dirección.

Debido a que el altavoz incorporado de un teléfono inteligente se coloca en la misma superficie que los sensores de movimiento integrados, produce reverberaciones de voz en la superficie y áreas en el cuerpo del teléfono inteligente cuando el modo de altavoz está habilitado.

Descubierto por un equipo de investigadores de seguridad (Abhishek Anand, Chen Wang, Jian

Liu, Nitesh Saxena, Yingying Chen), el ataque puede desencadenarse cuando la víctima pone una llamada de teléfono o video en modo de altavoz, o intenta escuchar a los medios de comunicación.

Como prueba de concepto, los investigadores crearon una app para Android, que imita el comportamiento de un atacante malicioso, diseñada para registrar las reverberaciones del habla con el acelerómetro y enviar los datos capturados a un servidor controlado por el atacante.

Los investigadores dicen que el atacante remoto podría entonces examinar las lecturas capturadas, de forma fuera de línea, utilizando el procesamiento de la señal junto con técnicas de aprendizaje automático «*listas para usar*» para reconstruir las palabras habladas y poder extraer la información relevante acerca de la víctima.

Según los investigadores, el ataque con Spearphone puede utilizarse para conocer el contenido del audio reproducido por la víctima, seleccionado de la galería del dispositivo por medio de Internet, o notas de voz recibidas a través de las aplicaciones de mensajería instantánea como WhatsApp.

> *«El ataque propuesto puede espiar las llamadas de voz para comprometer la privacidad del habla de un usuario final remoto en la llamada. La información personal como el número de seguridad social, fecha de nacimiento, edad, datos de tarjetas de crédito, detalles de cuentas bancarias, entre otros, consiste de forma principal en dígitos numéricos. Por lo tanto, creemos que la limitación del tamaño de nuestro conjunto de datos no debe restar importancia al nivel de amenaza percibido de nuestro ataque»,* explicaron los investigadores.

Los investigadores también probaron su ataque contra los asistentes de voz inteligentes del teléfono, incluidos Google Assistant y Samsung Bixby, y capturaron con éxito la respuesta a una consulta del usuario por medio del altavoz del teléfono.

Los investigadores creen que al usar técnicas y herramientas conocidas, su ataque con Spearphone tiene *«un valor significativo, ya que puede ser creado por atacantes de bajo perfil».*

> *«Por ejemplo, un atacante puede saber si una persona en particular estuvo en contacto con el propietario del teléfono en un momento dado»,* dijeron los investigadores.

Nitesh Saxena confirmó a THN que el ataque no se puede utilizar para capturar la voz de los usuarios específicos o sus alrededores debido a que *«eso no es lo suficientemente fuerte como para afectar los sensores de movimiento del teléfono, especialmente teniendo en cuenta las bajas tasas de muestreo impuestas por el sistema operativo»,* y por lo tanto, tampoco interfiere con las lecturas del acelerómetro.

Para más detalles, puedes leer el documento de investigación completo, bajo el título *«Spearphone: Una explotación de Privacidad del Discurso a través de Reverberaciones Sensibles por Acelerómetro de Altavoces para Smartphone».*

En el documento también se pueden observar algunas posibles técnicas de mitigación que pueden ayudar a prevenir estos ataques, así como algunas limitaciones, como la baja tasa de muestreo y la variación en el volumen máximo y la calidad de voz de diferentes teléfonos que podrían afectar negativamente las lecturas del acelerómetro.