Investigadores descubrieron un nuevo medio para apuntar a dispositivos controlados por voz mediante la propagación de ondas ultrasónicas por medio de materiales sólidos para interactuar y comprometerlos mediante comandos de voz inaudibles sin el conocimiento de las víctimas.

SurfingAttack, es el ataque que aprovecha las propiedades únicas de la transmisión acústica en materiales sólidos, como tablas, para *«permitir múltiples rondas de interacciones entre el dispositivo controlado por voz y el atacante a una distancia más larga y sin la necesidad de estar en línea».*

Al hacerlo, es posible que un atacante interactúe con los dispositivos utilizando los asistentes de voz, secuestrar códigos de autenticación de dos factores SMS e incluso, realizar llamadas fraudulentas, controlando así el dispositivo de la víctima de forma discreta, según dicen los investigadores en su documento.

La investigación fue publicada por un grupo de académicos de la Universidad Estatal de Michigan, la Universidad de Washington en St. Louis, la Academia de Ciencias de China y la Universidad de Nebraska-Lincoln.

Los resultados se presentaron en el Simposio de Seguridad del Sistema Distribuido de Red (NDSS) el 24 de febrero pasado en San Diego.

Funcionamiento de SurfingAttack

Los micrófonos MEMS, que son estándar en la mayoría de los dispositivos controlados por asistente de voz, contienen una pequeña placa incorporada llamada diafragma, que cuando se golpea con sonido y ondas de luz, se traduce en una señal eléctrica que luego se decodifica en los comandos reales.

El nuevo ataque explota la naturaleza no lineal de los circuitos de micrófono MEMS para

transmitir señales ultrasónicas maliciosas, ondas de sonido de alta frecuencia que son inaudibles para el oído humano, utilizando un transductor piezoeléctrico de 5 dólares que está conectado a la superficie de una mesa.

Para ocultar el ataque de la víctima, los investigadores emitieron una onda ultrasónica guiada para ajustar el volumen del dispositivo lo suficientemente bajo como para que las respuestas de voz no se noten, mientras que aún pueden grabar las respuestas de voz del asistente por medio de un dispositivo de tapping oculto más cerca al dispositivo de la víctima debajo de la mesa.

Una vez configurado, un intruso no solo puede activar los asistentes de voz, sino también generar comandos de ataque (por ejemplo, *«leer mis mensajes» o «llamar a Sam con el altavoz»*), utilizando sistemas de texto a voz (TTS), todos los cuales se transmiten en forma de señales de ondas guiadas por ultrasonidos que pueden propagarse a lo largo de la mesa para controlar los dispositivos.

SurfingAttack se probó con una variedad de dispositivos que utilizan asistentes de voz, como Google Pixel, Apple iPhone, Samsung Galaxy S9 y Xiaomi Mi 8, y se descubrió que cada uno de ellos era vulnerable a los ataques de ondas ultrasónicas. También se descubrió que funciona a pesar de utilizar diferentes superficies de mesa.

Sin embargo, los experimentos vienen con dos casos de falla, incluidos Huawei Mate 9 y Samsung Galaxy Note 10+, el primero de los cuales se vuelve vulnerable al instalar LineageOS. Al observar los sonidos grabados de los comandos de ultrasonido del Galaxy Note 10+, se notaron muy débiles, los investigadores atribuyeron la falla a *«las estructuras y materiales del cuerpo del teléfono».*

Una buena noticia, es que los altavoces inteligentes de Amazon y Google, el Amazon Echo y Google Gome, no se vieron afectados por el ataque.

Hasta ahora no hay indicios de que se haya explotado maliciosamente en la naturaleza el ataque basado en voz, pero no es la primera vez que se descubren ataque de inyección de

este tipo.

De hecho, la investigación se basa en una serie de estudios recientes, de BackDoor, LipRead y DolphinAttack, que muestra que es posible explotar la no linealidad en los micrófonos para entregar comandos inaudibles al sistema por medio de señales de ultrasonido.

Por otro lado, un estudio realizado por investigadores de la Universidad de Tokio de Electrocomunicaciones y la Universidad de Michigan, encontró a finales del año pasado, una serie de ataques denominados Comandos de luz, donde se emplean láseres para inyectar comandos inaudibles en los teléfonos inteligentes y altavoces, y lograr desbloquear puertas, comprar en sitios de comercio electrónico, entre otras acciones.

Aunque este ataque requirió que el rayo láser estuviera en línea directa con el dispositivo objetivo en cuestión, las capacidades únicas de propagación de SurfingAttack eliminan esta necesidad, permitiendo así que un atacante potencial interactúe remotamente con un dispositivo activado por voz y ejecute comandos no autorizados para acceder a información sensible en dispositivos sin conocimiento de la víctima.

Esta última investigación presenta un nuevo vector de ataque que requeriría que los fabricantes de dispositivos recurrieran a nuevas defensas de seguridad para proteger a los dispositivos de ataques basados en voz.