Una nueva investigación realizada por un grupo de académicos de la Universidad de California en San Diego, reveló por primera vez que las señales de Bluetooth pueden tomarse mediante huellas dactilares para rastrear teléfonos inteligentes, y por lo tanto, personas.

La identificación depende de las imperfecciones en el hardware del conjunto de chips Bluetooth introducido durante el proceso de fabricación, lo que da como resultado una *«huella digital de capa física única».*

«Para realizar un ataque de huellas dactilares en la capa física, el atacante debe estar equipado con un rastreador definido por software: un receptor de radio capaz de registrar señales de radio IQ sin procesar», dijeron los investigadores en el artículo llamado Evaluación del seguimiento de ubicación BLE de capa física para localizar ataques a dispositivos móviles.

El ataque es posible gracias a la naturaleza ubicua de las balizas Bluetooth Low Energy (BLE) que se transmiten de forma continua por dispositivos modernos para habilitar funciones cruciales como el rastreo de contactos durante emergencias de salud pública.

Los defectos de hardware, por otro lado, se derivan del hecho de que los componentes WiFi y BLE a menudo se integran juntos en un *«chip combinado»* especializado, lo que somete efectivamente a Bluetooth al mismo conjunto de métricas que se pueden usar para identificar dispositivos WiFi de forma única: compensación de frecuencia portadora y desequilibrio IQ.

La toma de huellas dactilares y el seguimiento de un dispositivo implica la extracción de imperfecciones de CFO e I/Q para cada paquete mediante el cálculo de la distancia de Mahalanobis para determinar *«qué tan cerca están las características del nuevo paquete»* de su huella dactilar de imperfección de hardware previamente registrada.

> *«Además, debido a que los dispositivos BLE tienen identificadores temporalmente estables en sus paquetes, podemos identificar un dispositivo en función del promedio de varios paquetes, lo que aumenta la precisión de la identificación»,*

> dijeron los investigadores.

Entonces, existen varios desafíos para realizar un ataque de este tipo en un entorno adversario, el principal de ellos es que la capacidad de identificar de forma única un dispositivo depende del conjunto de chips BLE utilizado, así como de los conjuntos de chips de otros dispositivos que están en proximidad física al objetivo.

Otros factores críticos que podrían afectar las lecturas incluyen la temperatura del dispositivo, las diferencias en la potencia de transmisión de BLE entre los dispositivos iPhone y Android, y la calidad de la radio rastreadora utilizada por el atacante para ejecutar los ataques de huellas dactilares.

> *«Al evaluar la practicidad de este ataque en el campo, particularmente en entornos concurridos como cafeterías, descubrimos que ciertos dispositivos tienen huellas dactilares únicas, y por lo tanto, son particularmente vulnerables a los ataques de rastreo, otros tienen huellas dactilares comunes, a menudo serán mal identificados»,* agregaron los investigadores.

> *«BLE presenta una amenaza de rastreo de ubicación para dispositivos móviles. Sin embargo, la capacidad de un atacante para rastrear un objetivo en particular es esencialmente una cuestión de suerte».*