Los investigadores de seguridad cibernética demostraron lo que llaman *«el primer ataque activo sin contacto contra pantallas táctiles capacitivas».*

GhostTouch, como se le llama, *«utiliza interferencia electromagnética (EMI) para inyectar puntos de contacto falsos en una pantalla táctil sin necesidad de tocarla físicamente»,* dijo un grupo de académicos de la Universidad de Zhejiang y la Universidad Técnica de Darmstadt en un nuevo artículo.

La idea central es aprovechar las señales electromagnéticas para ejecutar eventos táctiles básicos, como toques y deslizamientos en ubicaciones específicas de la pantalla táctil con el objetivo de tomar el control remoto y manipular el dispositivo subyacente.

El ataque, que funciona desde una distancia de hasta 40 mm, depende del hecho de que las pantallas táctiles capacitivas son sensibles a EMI, aprovechándolo para inyectar señales electromagnéticas en electrodos transparentes integrados en la pantalla táctil para registrarlos como eventos táctiles.

La configuración experimental involucra una pistola electrostática para generar una fuerte señal de pulso que luego se envía a una antena para transmitir un campo electromagnético a la pantalla táctil del teléfono, lo que hace que los electrodos, que actúan como antes, capten la EMI.

Esto se puede ajustar aún más al modificar la señal y la antena para inducir una variedad de comportamientos táctiles, como mantener presionado y deslizar para seleccionar, según el modelo de dispositivo objetivo.

En un escenario del mundo real, esto podría desarrollarse de distintas formas, incluyendo deslizar hacia arriba para desbloquear un teléfono, conectarse a una red WiFi no autorizada, hace clic sigilosamente en un enlace malicioso que contiene malware e incluso, responder una llamada telefónica en el teléfono de una víctima en su nombre.

> *«En lugares como un café, una biblioteca, una sala de reuniones o vestíbulos de conferencias, las personas pueden colocar su teléfono inteligente boca abajo sobre la mesa. Un atacante puede incrustar el equipo de ataque debajo de la mesa y lanzar ataques remotamente»,* dijeron los investigadores.

Se encontraron hasta nueve modelos diferentes de smartphones vulnerables a GhostTouch, incluidos Galaxy A10s, Huawei P30 Lite, Honor View 10, Galaxy S20 FE 5G, Nexus 5X, Redmi Note 9S, Nokia 7.2, Redmi 8 y iPhone SE (2020), el último de los cuales se utilizó para establecer una conexión Bluetooth maliciosa.

Para contrarrestar la amenaza, los investigadores recomiendan agregar blindaje electromagnético para bloquear EMI, mejorar el algoritmo de detección de la pantalla táctil e instar a los usuarios a ingresar el PIN del teléfono o verificar sus rostros o huellas dactilares antes de ejecutar acciones de alto riesgo.

> *«GhostTouch controla y da forma a la señal electromagnética de campo cercano e inyecta eventos táctiles en el área objetivo de la pantalla táctil, sin necesidad de contacto físico o acceso al dispositivo de la víctima»,* dijeron los investigadores.