Un equipo de investigadores del Instituto Federal Suizo de Tecnología en Zurich (ETH Zurich), encontró una vulnerabilidad de seguridad en el protocolo sin contacto EMV de Visa, que podría permitir a los hackers realiar ataques de omisión de PIN y cometer fraude con tarjetas de crédito.

Normalmente, existe un límite en la cantidad que se puede pagar por bienes o servicios utilizando una tarjeta sin contacto. Una vez que se supera el límite, la terminal de la tarjeta solicitará una verificación mediante el PIN.

La nueva investigación, titulada «*The EMV Standard: Break, Fix, Verify*«, demostró que un delincuente que puede tener en sus manos una tarjeta de crédito podría explotar la falla para compras fraudulentas sin tener que ingresar el PIN, aún en los casos en que se haya excedido la cantidad límite.

Los investigadores demostraron cómo se puede llevar a cabo el ataque utilizando dos teléfonos Android, una tarjeta de crédito sin contacto y una aplicación de prueba de concepto de Android que desarrollaron especialmente para este propósito.

> *«El teléfono cerca de la terminal de pago es el dispositivo emulador de tarjeta del atacante y el teléfono cerca de la víctima es el dispositivo emulador POS del atacante. Los dispositivos del atacante se comunican entre sí a través de WiFi, y con el terminal y la tarjeta a través de NFC»*, explicaron los investigadores, agregando que su aplicación no requiere ningún privilegio de root para funcionar.

«El ataque consiste en una modificación de un objeto de datos de la tarjeta, los Calificadores de Transacciones de Tarjetas, antes de entregarlo a la terminal», dice la descripción del ataque, con la modificación que indica a la terminal que no se necesita una verificación de PIN y que el titular de la tarjeta ya fue verificado por el dispositivo del consumidor.

Los investigadores probaron su ataque de bypass de PIN en uno de los seis protocolos sin contacto EMV (Mastercard, Visa, American Express, JCB, Discover, UnionPay). Sin embargo,

creen que también se podría aplicar a los protocolos Discover y UnionPay, aunque no se probó en la práctica.

EMV, el estándar de protocolo internacional para el pago con tarjeta inteligente, se utiliza en más de 9 mil millones de tarjetas en todo el mundo, y a diciembre de 2019, se utilizaba en más del 80% de todas las transacciones con tarjeta presente a nivel mundial.

Cabe mencionar que además de probar el ataque en condiciones de laboratorio, los investigadores lograron hacerlo exitosamente en tiendas reales, utilizando tarjetas Visa Credit, Electron y V Pay.

El equipo también mencionó que sería difícil para un cajero darse cuenta que algo fraudulento está ocurriendo, ya que se ha convertido en un hecho habitual para los clientes pagar productos con sus teléfonos inteligentes.

Además, con la investigación se descubrió otra vulnerabilidad, que involucra transacciones sin contacto fuera de línea realizadas con una tarjeta Visa o Mastercard antigua. Durante el ataque, el pirata informático modifica los datos producidos por la tarjeta, denominados *«Criptograma de transacción»*, antes de que se entreguen a la terminal.

Sin embargo, estos datos no pueden ser verificados por la terminal, sino por el emisor de la tarjeta, es decir, el banco. Entonces, para cuando ocurre esto, el ladrón ya se habrá ido con la mercancía.