Un grupo de académicos ha desarrollado un *«ataque de canal lateral acústico basado en aprendizaje profundo»* que puede ser empleado para clasificar las pulsaciones de teclado de una laptop registradas mediante un teléfono cercano con una precisión del 95%.

> *«Al ser entrenado con las pulsaciones de teclado grabadas utilizando el software de videoconferencia Zoom, se logró una precisión del 93%, estableciendo un nuevo récord en esta área,»* indicaron los investigadores Joshua Harrison, Ehsan Toreini y Maryam Mehrnezhad en un reciente estudio publicado la semana pasada.

Los ataques de canal lateral se refieren a una categoría de vulnerabilidades de seguridad que buscan obtener información de un sistema al monitorear y medir sus efectos físicos durante el procesamiento de datos sensibles. Algunos de los efectos físicos observables comunes incluyen el comportamiento en tiempo de ejecución, el consumo de energía, la radiación electromagnética, la acústica y los accesos a la caché.

Aunque no existe una implementación completamente libre de canales secundarios, los ataques prácticos de esta naturaleza pueden tener consecuencias perjudiciales para la privacidad y la seguridad de los usuarios, ya que podrían ser utilizados por un actor malicioso para obtener contraseñas y otros datos confidenciales.

> *«La amplia presencia de las emanaciones acústicas del teclado no solo las convierte en un vector de ataque fácilmente disponible, sino que también lleva a las víctimas a subestimar (y, por lo tanto, no intentar ocultar) su salida. Por ejemplo, al ingresar una contraseña, las personas a menudo ocultan su pantalla, pero hacen poco para disimular el sonido de su teclado»*, afirmaron los investigadores.

Para llevar a cabo el ataque, los investigadores realizaron primero experimentos en los que utilizaron 36 teclas de un Apple MacBook Pro (0-9, a-z), y cada tecla fue presionada 25 veces consecutivas, variando la presión y el dedo utilizado. Esta información fue registrada tanto a

través de un teléfono en proximidad física cercana a la laptop como a través de Zoom.

La fase siguiente involucró el aislamiento de las pulsaciones individuales de teclado y su conversión en un mel-espectrograma, en el cual se aplicó un modelo de aprendizaje profundo llamado CoAtNet (pronunciado «coat» nets y que significa redes de convolución y autoatención) para clasificar las imágenes de las pulsaciones de teclado.

Como medidas de respuesta, los investigadores sugieren cambios en el estilo de escritura, el uso de contraseñas aleatorias en lugar de contraseñas que contengan palabras completas, y la incorporación de pulsaciones de teclado falsas generadas al azar para enfrentar ataques basados en llamadas de voz.