¿Recuerdas al niño que siempre te copiaba en el examen mirando sobre tu hombro? ¡Ha vuelto! Pero esta vez está usandoGoogle Glass, y lo que busca es el PIN de tu iPad.

Expertos ciberforenses de la Universidad de Massachusetts en Lowell han desarrollado una manera de robar las contraseñas introducidas en un teléfono inteligente o una *tablet* usando el video de las gafas de Google y otros dispositivos para grabar video. El ladrón puede estar a casi tres metros de distancia y ni siquiera necesita poder leer la pantalla.

Los investigadores de seguridad crearon un *software* que mapea las sombras de las yemas de los dedos que tocan la *tablet* o *smartphone.* Su algoritmo luego convierte esos puntos de contacto en las teclas reales que fueron tocadas, permitiéndoles a los investigadores descifrar el código de acceso.

El algoritmo fue probado en contraseñas introducidas en una iPad de Apple y en una Nexus 7 de Google, así como en un iPhone 5.

¿Por qué debería preocuparnos? “Podríamos obtener la contraseña de tu cuenta bancaria”, advirtió el investigador Xinwen Fu.

El *software* puede aplicarse al video grabado en una variedad de dispositivos: Fu y su equipo experimentaron con las Google Glass, el vídeo del teléfono celular, una cámara web y una cámara de vídeo. El sistema funcionó incluso con una videocámara que grababa a una distancia de 40 metros.

Por supuesto, apuntar a un desconocido con una cámara de video podría despertar cierta suspicacia, pero el auge de la tecnología portátil es lo que a este enfoque realmente viable. Un *smartwatch,* por ejemplo, podría grabar con disimulo a una persona tecleando en su teléfono en una cafetería sin llamar mucho la atención.

Fu señala que Google Glass facilita enormemente este tipo de vulnerabilidad. “Lo más importante aquí es el ángulo. Para que este ataque tenga éxito el atacante debe poder ajustar el ángulo para tomar un mejor vídeo… ven tus dedos, y roban la contraseña”, explica.

CNNMoney puso su *software* a prueba. Instalamos dentro de nuestra cafetería corporativa a un investigador de seguridad portando las gafas Google Glass a 2.5 metros de distancia de nuestra pizarra iPad.

Fu y sus colegas dijeron que podían identificar la contraseña con una certeza del 100% si grababan el proceso de inicio de sesión (el momento en que introduces el código) tres veces. También probaron el *software* con las gafas de Google en un robot, por si el movimiento de la cabeza del investigador era motivo de sospecha.

En menos de 10 minutos fueron capaces de identificar con precisión nuestra contraseña, 5-1-2-0. (Por lo general toma menos tiempo, pero la corresponsal de CNNMoney Tech Laurie Segall tiene las uñas cortas, lo que creaba menos sombra a fin de que su *software* la analizara. Pero con todo pudieron descifrarla.)

La principal vulnerabilidad detectada por la gente de Fu es que las teclas están siempre en el mismo lugar en el teclado. Existen herramientas que pueden aleatorizar la ubicación de las teclas en el teclado, de modo que un «9» podría aparecer donde usualmente se ubica un «1», pero no son muy comunes. El objetivo de este tipo de trabajo es hacer que esa clase de protecciones sean más usadas.

La investigación será presentada el próximo mes en la conferencia de seguridad cibernética Black Hat.

Fuente: cnnexpansion