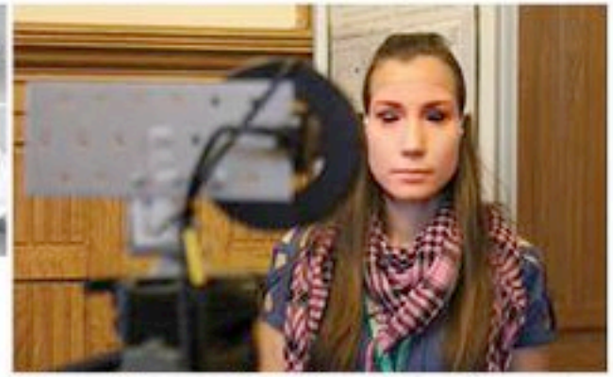
LA ÚLTIMA BATALLA CONTRA LOS SUPLANTADORES

INVESTIGADORES EUROPEOS BUSCAN MEJORAR LA SEGURIDAD DE LOS SISTEMAS DE RECONOCIMIENTO BIOMÉTRICO



Obtener una copia de una cara en tres dimensiones cuesta menos de 300 euros y se puede pedir por Internet. Las máscaras reproducen el rostro a partir de una fotografía.

SI LA POLICÍA ENTRARA en este salón, pensaría que está ante una convención de impostores. Alrededor de la mesa hay una serie de personas en actitudes de lo más pintorescas: un tipo que hace gestos delante del ordenador con una máscara, un grupo que ha fabricado huellas dactilares y una chica que muestra la fotografía de un ojo para confundir al lector de iris. Pero los especialistas aquí reunidos no son peligrosos *hackers*, sino expertos en seguridad biométrica venidos de todo el mundo para probar sus sistemas. Ellos son los que diseñan las herramientas para que nadie pueda hacerse pasar por nosotros. Este "Desafío de Suplantación" *(Spoofing Challenge)* formó parte de la Conferencia Internacional de Biometría celebrada en Madrid y sirvió para comprobar si la seguridad de sus sistemas era robusta.

"Se trataba de encontrar modos de detectar ataques, de manera que podamos defendernos de ellos", asegura a *Quo* Sebastian Marcel, coordinador del proyecto *Tabula Rasa*, donde la Unión Europea ha invertido 4,4 millones de euros y en el que participan doce organizaciones de siete países europeos.

Los expertos prevén que pronto viviremos en un mundo sin contraseñas, donde las máquinas nos reconozcan y den acceso por nuestras características físicas, pero ¿será suficientemente fiable?

La seguridad de los sistemas biométricos volvió a estar en tela de juicio tras la presentación hace unos meses del último modelo de *iPhone*, que incorporaba el reconocimiento de huellas dactilares. Los usuarios no tardaron ni 24 horas en burlar la seguridad mediante moldes de silicona. "Fue un gesto valiente de Apple", asegura Julián Fiérrez, investigador de la Universidad Autónoma de Madrid que participa en *Tabula Rasa*, "pero el teléfono no está preparado para detectar huellas de goma".

La clave para evitar que alguien engañe a la máquina es que sea capaz de identificar si lo que tiene delante es la persona que busca y si está viva. En el caso de las huellas dactilares, explica Fiérrez, la idea es capturar algunas señales como las pulsaciones, la sudoración y la capacidad eléctrica. La compañía Morpho, por ejemplo, ha comercializado un sistema que escanea el patrón de las venas de la mano, para aumentar la seguridad. Estas mejoras en el detector resultan demasiado caras para un teléfono, y la forma de abaratarlas es desarrollar un software que encuentre patrones matemáticos. "En la impronta de un dedo real", explica Fiérrez, "hay ciertos detalles, como la distorsión elástica, que nos permiten distinguir un dedo falso". Si estas medidas de seguridad nos parecen poco relevantes, pensemos en lo fácil que resultaría obtener nuestra huella de un vaso, sacar un molde y acceder a nuestros equipos. O peor: poner las huellas en el escenario de un crimen.

EN EL FUTURO, LAS MÁQUINAS NOS PEDIRÁN QUE REALICEMOS GESTOS PARA DEMOSTRAR QUIÉNES SOMOS Y QUE ESTAMOS VIVOS

El 80% del mercado de la seguridad biométrica gira alrededor de las huellas dactilares. Estos sistemas son especialmente importantes para la identificación forense. Basta un molde de goma para suplantar cualquier huella.

CON EL RECONOCIMIENTO DEL IRIS pasa lo mismo. La tecnología que vemos en las películas consta de sofisticados láser, pero la que se usa en la realidad sigue siendo fotográfica y fácil de engañar. "La única diferencia", matiza Fiérrez, "es que utiliza luz infrarroja para resaltar la textura del iris y evitar que la pupila se dilate". Para impedir que nos suplanten con una fotografía, los expertos han desarrollado algoritmos que encuentran pequeñas diferencias, como la manera en que se refleja la luz en la córnea. También se recurre a la estrategia denominada "desafío-respuesta", que consiste en pedir al usuario que haga una serie de gestos para comprobar que está vivo. Una especie de *captcha* gestual para que la máquina compruebe si está ante un ser humano.

Engañar a un sistema de reconocimiento facial es un proceso parecido. Además de fotografías y vídeos, en el *Spoofing Challenge* se usaron máscaras de resina. La reproducción de una cara en tres dimensiones cuesta menos de 300 euros y se puede comprar por internet, nos explica Marcel. "Probamos 17 máscaras de 17 personas distintas", asegura "y el resultado fue muy dispar: algunas eran muy eficaces y otras no lo eran nada". La máscara es mejor para burlar los sistemas que analizan el rostro en 3D, pero el método más eficaz, para sorpresa de todos, fue el más casero. La investigadora Antitza Dantcheva, de la Universidad de Michigan, engañó al sistema haciéndose pasar por un hombre mediante maquillaje, incluyendo un bigote. "El maquillaje es especialmente bueno para burlar la llamada detección de vida", explica Antitza a *Quo*. "Sigues teniendo una cara natural y puedes hacer los gestos que el sistema te pida."

ENGAÑAR CON MAQUILLAJE

En el reciente *Spoofing Challenge* celebrado en Madrid, la investigadora Antitza Dantcheva, del Departamento de Ingeniería y Ciencias de la Computación de la Universidad de Michigan, ganó el "desafío de suplantación" maquillándose la cara y haciéndose pasar por un hombre. El método es más eficaz que usar una máscara, porque la cámara detecta una cara viva.

LA LLAMADA DEL CIBORG. En la película *Terminator 2* hay una escena en la que el androide T-1000 se hace pasar por la madre del protagonista imitando su voz por teléfono. Esto no está lejos de ser posible en un futuro, según el especialista en reconocimiento de audio Nick Evans, que investiga para Eurecom. "Yo podría conseguir tu voz, grabar esta conversación y generar un discurso que sonara exactamente como tú", asegura. Dentro de *Tabula Rasa*, su equipo trabaja en encontrar las señales que delatan a una voz sintetizada y evitar que alguien se haga pasar por otro.

El último sector en el que trabaja el español Javier Acedo es aún más futurista. El sistema que desarrolla Starlab identifica al usuario por su señal cerebral única o por su electrocardiograma. "Puede servir para que un médico controle si el paciente está haciendo el tratamiento", asegura, "para sistemas de telepresencia en los que alguien podría hacerse pasar por ti y para dispositivos militares en los que una única persona está autorizada para manejar un equipo". Así, engañar a la máquina cuando se toman tantos datos será casi imposible para los suplantadores. "El uso masivo de los sistemas biométricos", advierte Sebastian Marcel, "dependerá de si la gente los considera útiles. En cambio, nadie los usará si los ve como una fuente de problemas", asevera.

Para Nick Evans, aún estamos arañando la superficie. "Hay mucho que hacer todavía para poder afirmar que los sistemas son seguros", concluye, "pero tenemos que ser responsables y no exagerar: en este momento los ataques más exitosos son de alta tecnología, y eso no está al alcance de cualquiera". ■