Engañando a los sistemas biométricos
Roberto Gómez

Uno de los mecanismos de autenticación que se han puesto de moda son los biométricos. Los hemos visto aparecer en series de televisión y en películas de espionaje. Son varias las organizaciones que los utilizan para autenticar a sus empleados o para verificar la asistencia y puntualidad de sus trabajadores. Sin embargo se ha demostrado que estos mecanismos tan sofisticados pueden ser engañados.

Los mecanismos biométricos verifican la identidad de una persona midiendo digitalmente determinados rasgos de alguna característica física, comparándolos con los patrones de referencia guardados en un archivo, en una base de datos o algunas veces en una tarjeta inteligente. Varios trabajos de investigación han demostrado las debilidades de este tipo de mecanismos.

En enero del 2002 el equipo del investigador japonés Tsutomu Matsumoto presento el trabajo Impact of Artificial "Gummy" Fingers on Fingerprint Systems. En dicho artículo demostraron que es posible engañar a los dispositivos biométricos basados en huellas dactilares, utilizando elementos caseros, con un costo de 10 dólares y un poco de ingenio. Los investigadores presentaron dos métodos, en el primero recrean la huella digital directamente de un dedo y en el otro la recrean partir de huellas obtenidas en diferentes objetos.

En el primer de los casos usaron plástico para moldeado (35 gramos de freeplastic) y gelatina (30 gramos de gelatine leaf). El plástico para moldear se pone en agua caliente para suavizarlo, después se presiona el dedo sobre el plástico y se obtiene un molde del dedo (la misma técnica usan los escultores para obtener el molde de una cara). Por último se vierte la gelatina sobre el molde, se mete al refrigerador y tiempo después se retira del molde, obteniendo un dedo de gelatina con las huellas dactilares del dedo original.

Si no se cuenta con el dedo original, es posible obtener la huella de algún objeto. En esto caso se usa una cinta adhesiva de cianocrilato para tomar la muestra del objeto (p.e. un vaso). Después se toma una foto digital de la huella, con PhotoShop se afinan detalles y se imprime la huella en una diapositiva. La diapositiva se usa para grabar la huella sobre el cobre de una tarjeta de circuito impreso foto-sensible (PCB), disponible en la mayor parte de las tiendas de componentes electrónicos, transformando la impresión en un modelo tridimensional. Por ultimo se usa gelatina para obtener un dedo artificial a partir de la impresión en la tarjeta de circuito impreso,

El equipo de Matsumoto probo lo anterior con 11 productos comerciales, pudiendo engañar a los dispositivos en un 80% de los casos. Los dedos de gelatina se pueden usar en presencia de guardias. Simplemente se pone el dedo artificial sobre el dedo original y se presiona sobre el dispositivo. Después de entrar, el intruso puede comerse la evidencia.

Las dos técnicas presentadas solo atacan sistemas biométricos basados en huellas dactilares. En junio del 2002 un equipo de investigadores alemanes probaron diferentes dispositivos biométricos, no solo aquellos basados en huellas digitales. Sus resultados se describen en el artículo “Body Check: Biometrics Defeated”, de la revista alemana c’t. Los investigadores alemanes analizaron once sistemas presentados en CeBITs 2002, nueve dispositivos basados en huellas digitales, uno de reconocimiento del rostro y sistema de scaneo de iris. Otros sistemas, como reconocimiento de voz, medida de la geometría de la mano o reconocimiento de firma, no fueron tomados en cuenta ya que cuentan con un bajo porcentaje de ventas. A continuación presentamos las técnicas usadas.

Para engañar a los dispositivos de reconocimiento de rostro, se toma una fotografía digital de un usuario autorizado y se almacena en una notebook. Las fotos se colocan frente al dispositivo de captura (webcam) y la autenticación se lleva a cabo. Otra opción es utilizar un video (.avi) donde aparezca el rostro del usuario autorizado.

Una forma de engañar a los dispositivos de huellas digitales, consiste en intentar reactivar las huellas que un usuario autorizado haya dejado. Por ejemplo, una vez que la persona autorizada se autenticó el intruso puede aspirar encima del dispositivo de captura. En algunos dispositivos el calor del aliento reactivará la huella que

quedo impresa. También es posible reactivar las huellas poniendo una bolsa delgada rellena de agua caliente en la superficie del dispositivo.

Otra forma de engañar al dispositivo es con la ayuda de un kit de huellas digitales. Se polvorea la superficie de un objeto que contiene la huella digital y con la ayuda de una cinta adhesiva se recupera la huella. Después se coloca la cinta sobre el dispositivo, se presiona y la autenticación se lleva a cabo. Otra opción es pegar la cinta con la huella sobre una bolsa de plástico rellena de agua caliente.

El engañar a los dispositivos de reconocimiento de iris es más complicado. Se toma una "fotografía" de la iris del individuo autorizado. Para evitar la sobre-exposición de la foto, debido a la luz usada por el dispositivo para realizar el reconocimiento, se imprimen las imágenes digitales de la iris sobre un papel que cuenta con un pequeño hoyo donde se verá la pupila del atacante. Se coloca el papel en el ojo, poniéndose de frente al dispositivo para ser autenticado.

Vale la pena aclarar que, de acuerdo a los fabricantes de los dispositivos probados, ninguno de ellos fue diseñado para ser usado ambientes de alta seguridad. También es necesario comentar que no todos los dispositivos probados fueron engañados.

Los resultados obtenidos por los dos equipos son contundentes. La buena noticia es que varios dispositivos biométricos están diseñados para prevenir ataques como los arriba mencionados, pero la mala noticia es que estos productos son mas costosos. Por otro lado, mucha gente ignora las debilidades de los productos más baratos. También es posible combinar los mecanismos biométricos con otros tipos de autenticación como tarjetas inteligentes o passwords para disminuir el riesgo de sufrir una usurpación de personalidad. Es tarea de los responsables de seguridad el tomar las medidas necesarias para que no se vean afectados.