Publicado en 28003 el 11/10/2013

Los sistemas de verificación biométricos y sus problemas, según Kaspersky Lab

Cuando hablamos de plataformas móviles, en entornos externos inestables, la luz y la vibración aumentan el margen de error y, por este motivo, el reconocimiento facial de Android, por ejemplo, falla en el 30 ó 40% de los casos. Los sistemas biométricos utilizan "esqueletos" que pueden reconstruirse para imitar la muestra original.

Todos los días, millones de equipos se enfrentan y resuelven el mismo problema: verificar si tú eres quien dices ser. La herramienta más utilizada para conseguirlo es la contraseña. No obstante, éste es un método que se puede robar u olvidar. Debido a los problemas surgidos con las claves de acceso, ha sido imprescindible desarrollar otros sistemas para verificar la identidad de los usuarios.

Una de estas vías alternativas es la verificación biométrica, que puede utilizar nuestras huellas o nuestra voz, y de la que se ha hablado mucho en las últimas semanas tras el incidente de Apple con su sistema de seguridad biométrico Touch ID. Según los expertos de Kaspersky Lab, existe un gran problema: las técnicas biométricas bien desarrolladas necesitan herramientas muy complejas y tienen un coste muy alto.

¡Peligro! Extraños a la vista

La mayor diferencia entre un sistema ordinario de contraseñas y un sistema biométrico es que la muestra original y la muestra a verificar nunca coinciden a la perfección. No se pueden obtener dos huellas dactilares totalmente idénticas del mismo dedo y la situación empeora si usamos el rostro humano. Los rasgos faciales dependen de la luz, la hora del día, el maquillaje y, por supuesto, la edad. La voz, a su vez, también se ve afectada por múltiples factores como por ejemplo, un simple resfriado. Bajo estas condiciones, es realmente difícil desarrollar un sistema que permita el acceso al propietario; negándoselo, a su vez, a los extraños.

Para resolver el problema, los sistemas biométricos intentan limpiar las muestras escaneadas de cualquier elemento que interfiera en el proceso de verificación, utilizando solo las características fácilmente reconocibles. Sin embargo, este "esqueleto" debe coincidir con el original según unos parámetros matemáticos. Para un sistema de seguridad medio, se asume como normal un margen de error de un extraño por cada 10.000 intentos y el bloqueo del usuario legítimo cada 50 casos. Cuando hablamos de plataformas móviles, en entornos externos inestables, la luz y la vibración aumentan el margen de error y, por este motivo, el reconocimiento facial de Android, por ejemplo, falla en el 30 ó 40% de los casos.

Una contraseña para toda la vida

Si olvidas o te roban tu contraseña, la puedes cambiar. Si pierdes las llaves, puedes cambiar la

cerradura de tu casa. Pero ¿qué harías si tu cuenta bancaria utiliza la palma de la mano como clave de acceso y alguien roba la base de datos que contiene dichas huellas?

Las huellas dactilares no se pueden cambiar, sin embargo este problema se puede solucionar, parcialmente, con el resto de huellas dactilares. Las malas noticias son que los sistemas biométricos utilizan “esqueletos” que pueden reconstruirse para imitar la muestra original.

Estos mecanismos tienen algunos problemas de privacidad. Las “contraseñas” biométricas identifican al usuario como el propietario legítimo, haciendo imposible que una misma persona tenga dos cuentas diferentes en la misma plataforma online. Además, aunque cada individuo tenga miles de rasgos indistinguibles, gracias a la ayuda del Geo-IP y otros metadatos, es posible crear un perfil de usuario único para cada persona. Si alguien consigue implementar este sistema en cada servicio web, entonces será muy fácil rastrear la actividad online de los usuarios.

Biometía en la vida real

Dejando a un lado a las películas de ciencia ficción y la investigación militar, para Kaspersky Lab existen dos casos en los que encontramos con sistemas biométricos en la vida real. Algunas entidades bancarias están realizando pruebas con escáneres que analizan las palmas de las manos en cajeros automáticos o la voz en los servicios móviles. Otro ejemplo verídico son los escáneres instalados en los dispositivos electrónicos como ordenadores o smartphones. La cámara frontal se puede usar para la verificación facial, un sensor puede reconocer las huellas dactilares o incluso se pueden utilizar los altavoces para el reconocimiento de voz.

Los sistemas de reconocimiento facial, rara vez, pueden distinguir un rostro real de una foto. En cambio, cuando usamos un mecanismo de estas características en nuestro móvil, éste es realmente exigente con las condiciones de luminosidad y el entorno en general, así que no será necesario configurar sistemas adicionales. Sin embargo, es importante tener una contraseña robusta para desbloquear el móvil en mitad de la noche.

La mayoría de desarrolladores de sistemas de verificación de voz afirman que estos son capaces de detectar voces falsas, grabaciones, etc. En realidad, algunos investigadores afirman que un software de alteración de voz puede engañar a dichos sistemas en el 17% de los casos. Además, los ataques man-in-the-middle son especialmente peligrosos para los sistemas de voz, porque es más fácil obtener una muestra de voz que de otra parte del cuerpo.

Tanto los problemas prácticos como los riesgos en seguridad han evitado que los sistemas de verificación biométricos reemplacen a las contraseñas tradicionales o a los tokens electrónicos. Una verificación de identidad biométrica, hoy en día, solo es posible en ciertas condiciones muy controladas como las aduanas en los aeropuertos o el puesto de control de un edificio. Sin embargo, no funcionan con calidad en lugares más arbitrarios como los smartphones, que usamos a diario.

Datos de contacto:

Redacción

Nota de prensa publicada en: 28003

Categorías: Telecomunicaciones E-Commerce Ciberseguridad