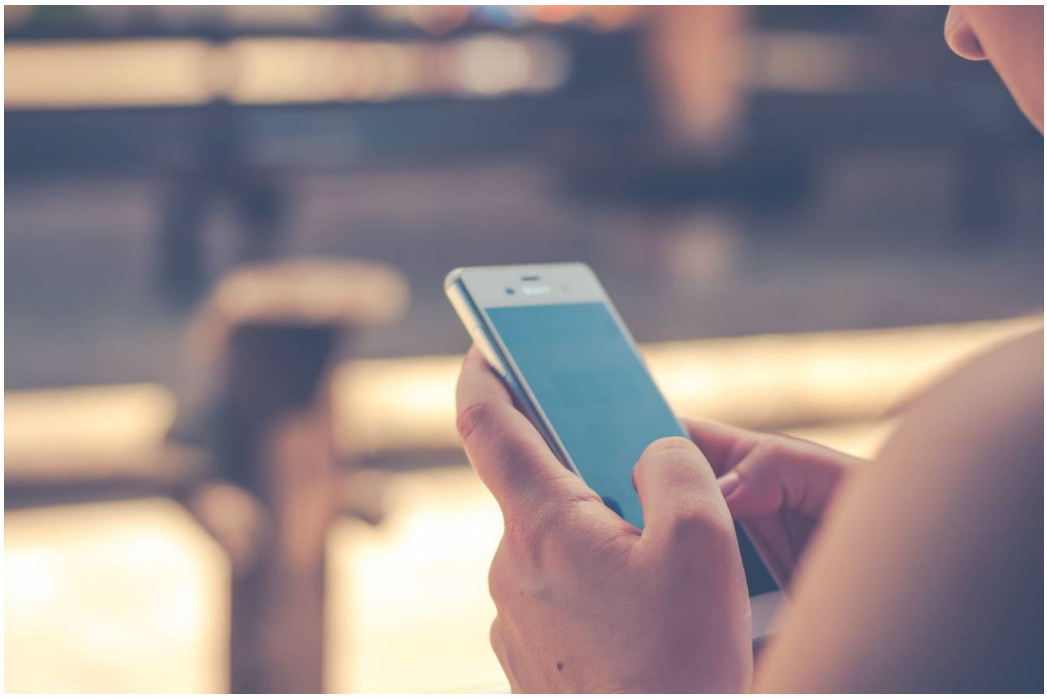
Las ‘app’ de salud ponen en riesgo millones de datos personales

Un estudio europeo en el que han participado investigadores de la Universitat Rovira i Virgili ha detectado graves problemas de seguridad después de analizar las veinte ‘app’ Android de salud mejor valoradas y con una puntuación más alta. Ocho de cada diez no cumplen con los estándares para evitar el uso de datos sensibles de los usuarios.

SINC 14/2/2018 10:03 CEST



El estudio ha analizado las 20 aplicaciones con más descargas y mejor puntuación / Universitat Rovira i Virgili

El 80% de las aplicaciones de salud más populares disponibles para Android no cumplen con muchos de los estándares destinados a evitar el uso y la divulgación de datos sensibles de los usuarios. Así lo demuestra un estudio europeo, iniciado en 2016, en el que ha participado Agustí Solanas, jefe del Grupo de Investigación en Salud Smart, del Departamento de Ingeniería Informática y Matemáticas de la Universitat Rovira i Virgili (URV), junto con investigadores de la Universidad del Pireo (Grecia) liderados por Constantinos Patsakis.

La investigación ha puesto en evidencia graves problemas de seguridad en estas aplicaciones, las veinte más populares de la red. El trabajo ha consistido en analizar y poner en conocimiento de los desarrolladores los problemas de seguridad detectados, y comprobar posteriormente si se habían resuelto.

Las aplicaciones seleccionadas por los investigadores tenían de 100.000 a 10 millones de descargas cada una y una calificación mínima de 3,5 de 5. Para analizar su funcionamiento, los investigadores interceptaban, almacenaban y monitores los datos privados de los usuarios, como problemas de salud, enfermedades o agendas médicas.

Un 50% de las aplicaciones compartía con terceros datos personales, tanto de texto como multimedia

Los investigadores analizaron las comunicaciones de las aplicaciones, como almacenaban la información o qué permisos requerían para poder funcionar, así como la manera en que se administraban los datos. Los resultados demostraron la existencia de graves problemas de seguridad en la gestión de los datos de los usuarios.

Solo un 20% de las aplicaciones almacenaba los datos en los teléfonos inteligentes de los usuarios, y una de cada dos solicitaba y administraba las contraseñas de inicio de sesión sin utilizar una conexión segura.

Los investigadores también detectaron que un 50% de las aplicaciones compartía con terceros datos personales, tanto de texto como multimedia, así como imágenes de rayos X, por ejemplo. Otro dato: más de la mitad transmitió datos de salud de los usuarios a través de enlaces HTTP, lo que conlleva que cualquier persona que tenga acceso pueda disponer de estos datos.

De las aplicaciones sometidas a estudio, un 20% no transmitía al usuario ninguna política de privacidad o el contenido no estaba disponible en inglés, el idioma de la aplicación. Otros pedían acceso a la geolocalización,

micrófonos, cámara, lista de contactos, tarjeta de almacenamiento externo o Bluetooth de los usuarios, aunque el buen funcionamiento de la aplicación no dependía del acceso a estos datos.

Información a las empresas

Una vez finalizado el análisis, los investigadores pusieron en conocimiento de las empresas desarrolladoras de las aplicaciones todos los problemas de seguridad detectados. Pasado un tiempo, volvieron a evaluarlas con los mismos parámetros que en el estudio inicial. Aunque detectar que algunas de las carencias se habían resuelto, como transferencias de datos de salud inseguras o la posibilidad de identificar a los usuarios debido a transferencias de datos inseguras a terceros; otros problemas, como las filtraciones de datos de uso de la aplicación, no se habían corregido.

Este trabajo ha sido parcialmente financiado por el proyecto europeo Operandi (del programa H2020) y también ha recibido financiación del programa Cooperación en Ciencia y Tecnología, a través de la Acción Cryptacus.

Referencia bibliográfica:

"Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice". A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, C. Patsakis. *IEEE Explore*. DOI: 10.1109/ACCESS.2018.2799522

Derechos: **Creative Commons**

Creative Commons 4.0
Puedes copiar, difundir y transformar los contenidos de SINC. Lee las condiciones de nuestra licencia

La ciencia es noticia