Intercepción de tráfico en aplicaciones móviles

Fabian A. Gibellini[1], Leonardo R. Ciceri [1], Juliana M. Notreni [1], German N. Parisi[1], Analia L. Ruhl[1], Ninfa M. Zea Cardenas [1], Marcelo J. Auquer[1], Ileana M. Barrionuevo[1], Federico Bertola[1], Sergio R. Quinteros[1], Ignacio J. Sanchez Balzaretti[1]

[1] Universidad Tecnológica Nacional – Facultad Regional Córdoba
Maestro M. López esq. Cruz Roja Argentina, Ciudad Universitaria, Córdoba, Argentina
{fabiangibellini, leonardorciceri, julinotreni, germannparisi, analialorenaruhl, milyzc, marcelo.auquer, ilebarrionuevo, fedebertola, ser.quinteros, ignaciojsb}@gmail.com

Resumen. El creciente uso de los dispositivos móviles conlleva una mayor utilización de aplicaciones móviles tanto para la búsqueda de datos, uso de redes sociales como para realizar transacciones bancarias, compras, etc. Esto ha generado un nuevo mercado para los delincuentes informáticos. La mayoría de estas aplicaciones se comunican con servidores para enviar datos. Esta comunicación es la que se busca analizar cuando se llevan a cabo auditorías de seguridad o actividades forenses en una aplicación móvil. A su vez, esta comunicación depende, entre otras cosas, del sistema operativo sobre el que se ejecuta la aplicación, el lenguaje de la aplicación, las librerías implementadas, los tipos de cifrado aplicados y el protocolo de comunicación. Al momento de analizar el tráfico de una aplicación móvil, es necesario un marco de trabajo que permita agilizar estas tareas de configuración y otorgue a los pentesters más tiempo de análisis al tráfico de datos, ya que actualmente, el pentester se encuentra con inconvenientes debido a la diversidad de técnicas que debe probar para efectivizar la intercepción de tráfico. Esta es la razón por la que las herramientas actuales no llegan a cubrir esta necesidad.

Palabras Claves: ciberseguridad, pentest, intercepción de tráfico.

Abstract. The growing use of mobile devices leads to a greater use of mobile applications both for data search, use of social networks for banking transactions, purchases, etc. This has provided a new market for computer criminals. Most of these applications communicate with servers to send data. This communication is the one that is sought to be analyzed when carrying out security audits or forensic activities in a mobile application. In turn, this communication depends, among other things, on the operating system on which the application runs, the language of the application, the libraries implemented, the types of encryption applied, and the communication protocol. When analyzing the traffic of a mobile application, a framework is necessary that allows speeding up these configuration tasks and gives pentesters more time to analyze data traffic, since currently, the pentester has problems due to the diversity of techniques that must be tried to make the interception of traffic effective. This is the reason why current tools do not meet this need.

Keywords: cybersecurity, pentest, traffic interception.