ISSA 2015:14th International Information Security for South Africa Conference, Rosebank, Johannesburg, South Africa, 12-13 August 2015

Playing hide-and-seek: detecting the manipulation of android timestamps

Pieterse, H

Olivier, M

Van Heerden, R

DOI:10.1109/ISSA.2015.7335065

ISBN: 978-1-4799-7754-3

Abstract

Mobile technology continues to evolve in the 21st century, providing users with improved capabilities and advance functionality. The current leader of this evolution is Android, a mobile operating system that continuously elevates existing features and offers new exciting applications. Such improvements allowed Android to gain popularity worldwide. A combination of Android's advance technology and increasing popularity allow smartphones supporting this operating system to become a rich source of trace evidence. Traces found on Android smartphones form a significant part of digital investigations, especially when the user of the smartphone is involved in criminal activities. A key component of these traces is the date and time, often formed as timestamps. These timestamps allow the examiner to relate the traces found on Android smartphones to some real event that took place. Knowing when events occurred in digital investigations is of great importance to the overall success of the investigation. This paper introduces a new solution, called the Authenticity Framework for Android Timestamps (AFAT) that establishes the authenticity of timestamps found on Android smartphones. Currently the framework determines the authenticity of timestamps found in SQLite databases by following two individual methods. The first method identifies the presence of certain changes in the Android file systems, which are indications of the manipulation of the SQLite databases. The second method subsequently focuses on the individual SQLite databases and the identification of inconsistencies in these databases. The presence of specific file system changes as well as inconsistencies in the associated SQLite databases indicates that authenticity of the timestamps might be compromised. The results presented in the paper provide preliminary evidence that the suggested approach, Authenticity Framework for Android Timestamps, shows potential.