Dokumenttyp: Konferenzbeitrag

Art des Konferenzbeitrags: Vortrag / Präsentation

Autor(en) des Beitrags: Taubmann, Benjamin and Huber, Manuel and Wessel, Sascha and Heim, Lukas and Reiser, Hans Peter and Sigl, Georg

Titel des Beitrags: A Lightweight Framework for Cold Boot Based Forensics on Mobile Devices

Abstract: Mobile devices, like tablets and smartphones, are common place in everyday life. Thus, the degree of security these devices can provide against digital forensics is of particular interest. A common method to access arbitrary data in main memory is the cold boot attack. The cold boot attack exploits the remanence effect that causes data in DRAM modules not to lose the content immediately in case of a power cut-off. This makes it possible to restart a device and extract the data in main memory. In this paper, we present a novel framework for cold boot based data acquisition with a minimal bare metal application on a mobile device. In contrast to other cold boot approaches, our forensics tool overwrites only a minimal amount of data in main memory. This tool requires no more than five kilobytes of constant data in the kernel code section. We hence sustain all of the data relevant for the analysis of the previously running system. This makes it possible to analyze the memory with data acquisition tools. For this purpose, we extend the memory forensics tool Volatility in order to request parts of the main memory dynamically.
from our bare metal application. We show the feasibility of our approach by comparing it to a
traditional memory dump based analysis using the Samsung Galaxy S4 mobile device.

Stichworte: Cold Boot, Digital Forensics, Mobile Device Security, Smartphones, Virtual Machine
Introspection

Dewey Dezimalklassifikation (Liste): 620 Ingenieurwissenschaften

Kongress- / Buchtitel: The 10th International Conference on Availability, Reliability and Security (ARES) 2015

Kongress / Zusatzinformationen: Toulouse, France

Datum der Konferenz: 24.-28.08.2015

Jahr: 2015

Quartal: 3. Quartal

Jahr / Monat: 2015-08

Monat: Aug

Sprache: en

WWW: http://www.ares-conference.eu/conference/

Occurences: Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle
und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2015

entries: