C14 Examining the Impact of Garbage Collection and Process States in Userland Memory Forensics

Sneha Sudhakaran, MTech, Louisiana State University, Baton Rouge, LA 70803; Aisha Ali-Gombe, PhD, Towson University, Towson, MD 21252; Golden G. Richard III, PhD, Louisiana State University, Baton Rouge, LA 70808*

Learning Overview: After attending this presentation, attendees will understand the effect of some critical external factors of the mobile runtime environment that impact userland memory forensics. The research primarily aims to highlight the impact of Garbage Collection(GC) and process states on the reliability of memory analysis as a crucial and important forensics technique.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by illustrating the effect of critical runtime activities in the acquisition of memory and recovery of important evidence.

An efficient memory dump acquisition technique is required for useful memory analysis. Android™ GC can impact the availability of evidence as it is an automatic process that removes unused objects from memory. This research will demonstrate how GC and process states can affect data recovery by identifying different combinations of GC and process states introduced by Android™ Runtime (ART). The GC states include GC triggered and GC not triggered. Android's™ different process states are foreground, background, visible, service, and empty.[1] This research predominantly focuses on the foreground and background process states. First, the foreground state is the state when the user interacts with the application. Then, the background process state is when the application under execution is not visible to the user, but the runtime maintains the application in a dynamic list containing processes that are in execution.[1] The various combinations of GC and process states include: foreground and no GC triggered; foreground and GC triggered; background and no GC triggered; and background and GC triggered. This research acquired the real-time application dump for each combination and identify differences in data recovery.

In newer Android™ versions, ART allocates objects using RegionSpace and LargeObjectSpace allocators that trigger the GC for efficient memory utilization. The RegionSpace allocator allocates small objects like primitive objects, and the LargeObjectSpace allocator allocates large objects like multimedia in memory.[2,3] If the application creates many objects, then the Android™ Runtime environment triggers GC frequently.[2] As a result, the number of objects allocated and deleted during the runtime is unknown to a forensic analyst or the user. Thus the impact of GC and the process state changes triggered by the runtime is the primary focus of this research.

Acquired memory dumps were evaluated with tools like DroidScraper and VCR in recovering objects from RegionSpace and LargeObjectSpace.[2,3] In this work, the memory dumps acquired from the same application in different combinations of GC and process states are analyzed in depth with the tools mentioned above to monitor the number of objects retrieved. The results demonstrated differences in objects retrieved for certain combinations; for example, more objects retrieved when GC did not trigger, and process state was the background. Hence, a hypothesis opens a new research dimension to explain which objects get removed and when they are removed to illustrate the effect of external factors on the reliability and accuracy of memory forensic tools on a multi-app platform such as Android™.

Reference(s):

1. https://learncswithandroid.blogspot.com/2017/12/android-process-states.html.
2. Ali-Gombe, A., Sudhakaran, S., Case, A., and Richard III, G.G. (2019). DroidScraper: A Tool for Android In-Memory Object Recovery and Reconstruction. In: *22nd International Symposium on Research in Attacks, Intrusions, and Defenses* ({RAID} 2019) (pp. 547-559).
3. Saltaformaggio, B., Bhatia, R., Gu, Z., Zhang, X., and Xu, D. (2015, October). VCR: App-agnostic recovery of photographic evidence from Android device memory images. In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 146-157).

Garbage Collection, Process State, Userland Memory Forensics

*Presenting Author