C3 The Recreation and Visualization of Runtime Objects Relationship From Process Memory Images

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 have gained an understanding of an app-agnostic technique for the recreation and visualization of process execution paths and the in-memory object relationship network. The goal of this presentation is to illustrate how these relationships can aid cybercrime investigations and malware analysis.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by illustrating a novel effort in userland memory analysis that aids investigators in piecing together the context of valuable forensics evidence to determine its provenance, execution path, and overall scope within the application trace. Similar to the field of archaeology, where historical human activities are determined by recovering and piecing together material from a culture, this presentation will demonstrate the reconstruction of object relationships from process memory images without prior knowledge of the application semantics.

As userland memory forensics continues to be a practical and crucial alternative to kernel-level memory forensics and traditional disk forensics in program analysis and cybercrime investigations, there is a need to develop techniques that go beyond simple data recovery. Specifically, more sophisticated semantic analysis capabilities that reconstruct the state of a system under investigation from the volatile memory image are needed. In recent years, various application-specific memory analysis techniques that recover forensically interesting artifacts from well-known applications such as Facebook®, default messaging apps, and Telegram®, were presented in the literature.[1-5] Although these techniques are useful and often adopted by practitioners to provide forensics evidence, their methodologies are conceived based on an individual app's specific logic. Hence, their resulting recovery algorithm cannot be generalized to other applications or even different versions of the same app. Thus, this research presents a post-execution and app-agnostic semantic analysis approach designed to help investigators establish concrete evidence by exploring application execution paths and recreating the relationships between in-memory objects in a process memory image. The technique utilizes DroidScraper to find all the objects allocated in the process heap.[6] Then, treating each object as a node, it utilizes Heap Context Points-to analysis to establish the graph edges (representing the relationships between the graph nodes). In Heap Context Points-to analysis, object relationships are determined by finding the allocation site for each object, which is within its allocator's field data. Walking the chain of the allocator's predecessors and successors, a concrete network is established for all the associated objects that reside in the process image. The evaluation of the proposed approach on real applications shows the reconstruction and visualization of the object allocation network can aid investigators in finding the context for forensically interesting data such as deleted Whatsapp messages and malware data leaks.

Reference(s):

1. Levinson, Alex, Bill Stackpole, and Daryl Johnson. Third party application forensics on apple mobile devices. In *2011 44th Hawaii International Conference on System Sciences*, pp. 1-9. IEEE, 2011.
2. Ali-Gombe, Aisha Ibrahim. *Volatile Memory Message Carving: A "per process basis" Approach.* (2012). Master's thesis, University of New Orleans, LA.
3. Grispos, George, William Bradley Glisson, and Tim Storer. Recovering residual forensic data from smartphone interactions with cloud storage providers. *arXiv preprint arXiv:1506.02268* (2015).
4. Anglano, Cosimo, Massimo Canonico, and Marco Guazzone. Forensic analysis of telegram messenger on Android smartphones. *Digital Investigation* 23 (2017): 31-49.
5. Choi, Jusop, Jaewoo Park, and Hyoungshick Kim. Forensic analysis of the backup database file in KakaoTalk messenger. In *2017 IEEE International Conference on Big Data and Smart Computing (BigComp)*, pp. 156-161. IEEE, 2017.
6. Ali-Gombe, Aisha, Sneha Sudhakaran, Andrew Case, and Golden G. Richard III. 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. 2019.

Memory Forensics, Android™, Visualization

*Presenting Author