Abstract

Virtual machine technology has emerged with powerful features, offering several benefits and promising revolutionary outcomes. It is one technology that combines into one package several computing concepts like resource management, emulation, time-sharing, isolation and partitioning. These features have made evidence acquisition and preservation difficult and in some cases unfeasible. The aftermath is that conventional approaches to integrity preservation have not yielded the best results required to facilitate acceptability. Subjects around virtualization forensics, its affiliation with digital evidence integrity, and impacts on admissibility have been decisively examined. A part of this discourse dwelt on recognising potential threats to the integrity and reliability of evidence from a virtual environment; specifically using VMware Virtual Machine Monitor as a case study. A theoretical framework for preserving the integrity of digital evidence from such environments is introduced. This structure highlights guidelines, processes and parameters essential for keeping the accuracy, consistency and trustworthiness of digital evidence, made possible via abstractions from eminent integrity principles of well-formed transactions and separation of duties as proposed by Clark and Wilson. Key parameters in the model include; strength of hash functions, number of evidence attributes, and number of evidence cycle covered; all represented conceptually in a mathematical model. This is further consolidated with the introduction of an integrity rating factor/threshold and the
definition of an integrity enforcement process in line with globally recommended standards. While still working on practical demonstration of the proposed model, the work done so far is seen to open a path for unification and amplification of trust levels required for the admissibility of virtual environment evidence.

References

- Christiaan Beek, "Virtual Forensics," Ten ICT Professionals, Paper n.d.
Safeguarding Forensic Integrity of Virtual Environment Evidence

- FIPS PUB 180-3 NIST, "Secure Hash Standard (SHS)," Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, Technology Standard 2008.

Index Terms

Computer Science

Applied Sciences

Keywords

Evidential Integrity  Virtualisation Machine Forensics  Evidence Reliability  VMware evidence

Integrity Preservation