Digital Forensic Investigation and Cloud Computing

Joshua I. James, Ahmed F. Shosha, Pavel Gladyshev
Digital Forensic Investigation Research Group
University College Dublin
Belfield, Dublin 4
Ireland

Abstract

This chapter aims to be a high-level introduction into fundamental concepts of both digital forensic investigations and cloud computing for non-experts in one or both areas. Once fundamental concepts are established, this work begins to examine cloud computing security-related questions, how past technological and methodological flaws are inherited by cloud computing models, as well as the new security issues that are unique to the cloud. By looking at security related issues, attack vectors will be generally defined, and the effectiveness of current digital forensic practices will be analyzed against these situations. Finally, a threat assessment model will be proposed that allows the mapping of threats in cloud computing to evidentiary traces, allowing a model for digital investigators and security engineers to identify and understand what threats can and cannot be investigated in their organization using current digital forensic investigation techniques.¹

REFERENCES


8. AFP (2011) ”Number of Internet users worldwide reaches 2 bln: UN.”


29. CNN. (2009). "CNN: Her name was Neda." from http://www.youtube.com/watch?v=b5KBrsz1


76. McAfee (2010). A Good Decade for Cybercrime. Santa Clara, California, McAfee, Inc.


111. Williams, C. (2011) ”Cybercrime gang ‘responsible for a third of all data thefts’.” The Telegraph.


ADDITIONAL READING

Definitions

Digital Forensic Investigation Process Models

Cloud Computing and Digital Investigations
Legal Aspects of Digital Investigations


Threats/Cases/Proof of Concept Exploitation


Cloud Providers and Software


Key Terms

Digital Forensic Investigation; Digital Crimes; Formal Digital Forensics; Cloud Computing Investigations; Cloud Threat Modeling; Extended STRIDE Model; Risk Analysis and Cloud Computing; Global Digital Investigation Collaboration