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]

[1] Cite as: James JI, AF Shosha, P Gladyshev. (2013) Digital Forensic Investigation and Cloud Computing. K Raun (Ed.), Cybercrime and Cloud Forensics: Applications for Investigation Processes. (pp 1-41). IGI Global. 10.4018/978-1-4666-2662-1.ch001.

REFERENCES

1. (1923). Frye v. United States. F., Court of Appeals, Dist. of Columbia. 293: 1013.

2. (1993). Daubert v. Merrell Dow Pharmaceuticals, US Supreme Court. 509: 579.

3. (1997). General Electric Co. v. Joiner. US, Supreme Court. 522: 136.

4. (1999). Kumho Tire Co. v. Carmichael. US, Supreme Court. 526: 137.

5. ACPO (2008). Good Practice Guide for Computer based Electronic Evidence, ACPO, 7safe.

6. Adelstein, F. (2006). "Live forensics: diagnosing your system without killing it first." Commun. ACM 49(2): 63-66.

7. ADF. (2011). "ADF Solutions." Retrieved 31 Jan., 2011, from http://www.adfsolutions.com/.

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

9. Amazon. (2011). "Amazon Elastic Compute Cloud (Amazon EC2)." Retrieved 15 Feb., 2011, from http://aws.amazon.com/ec2/.

10. Armbrust, M., A. Fox, et al. (2009). Above the Clouds: A Berkeley View of Cloud Computing, EECS Department, University of California, Berkeley.

11. Arms, W. (2000). "Digital Libraries." Retrieved 10 Feb., 2011, from http://www.cs.cornell.edu/wya/DigLib/MS1999/Glossary.html.

12. Barnard, A. (2009) "Could Your Phone Testify Against You?" The New York Times Upfront 142.

13. BBC (2010) "Over 5 billion mobile phone connections worldwide." BBC News.

14. Bilby, D. (2006). Low Down and Dirty: Anti-forensic Rootkits.

15. Brennels. (2010). "Cloud 101 - Recovery as a Service (RaaS) is Here!" Retrieved 16 Feb., 2011, from http://cloudrecovery.info/2010/02/17/cloud-101-%E2%80%93-recovery-as-a-service-raas-is-here/.

16. Brennels. (2010, 8 Feb.). "Cloud 101 - The Four Type of Cloud Services?" Retrieved 14 Feb., 2011, from http://cloudrecovery.info/2010/02/08/cloud-101-the-four-types-of-cloud-services/.

17. Bright, P. (2008). Storms in the cloud leave users up creek without a paddle. Ars Technica. 2011.

18. Brodkin, J. (2008). Gartner: Seven cloud-computing security risks, Network World.

19. Carrier, B. (2003). Open source digital forensics tools: The legal argument. @stake Research Report.

20. Carrier, B. and E. Spafford (2003). "Getting physical with the digital investigation process." International Journal of Digital Evidence 2(2): 1-20.

21. Carrier, B. and E. Spafford (2006). "Categories of digital investigation analysis techniques based on the computer history model." Digital Investigation 3: 121-130.

22. Carrier, B. D. (2006). A hypothesis-based approach to digital forensic investigations. CERIAS. West Lafayette, IN, Purdue University. PhD.

23. Carrier, B. D. (2006, 7 June). "Basic Digital Forensic Investigation Concepts." Retrieved 28 Jan., 2011, from http://www.digital-evidence.org/di_basics.html.

24. Carrier, B. D. (2006). "Risks of live digital forensic analysis." Commun. ACM 49(2): 56-61.

25. Carrier, B. D. (2008, 21 Jan.). "A Brief Introduction To The Computer History Model." Retrieved 2 Feb., 2011, from http://www.digital-evidence.org/hist_model1.html.

26. Casey, E., M. Ferraro, et al. (2009). "Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence." Journal of forensic sciences 54(6): 1353-1364.

27. Civie, V. and R. Civie (1998). Future technologies from trends in computer forensic science. Information Technology Conference, 1998. IEEE.

28. Clede, B. (1993). "Investigating Computer Crimes." Law and Order 41(7): 99-102.

29. CNN. (2009). ”CNN: Her name was Neda.” from http://www.youtube.com/watch?v=b5KBrsz

30. Collier, P. A. and B. J. Spaul (1992a). ”A forensic methodology for countering computer crime.” Artificial Intelligence Review 6(2): 203-215.

31. Collier, P. A. and B. J. Spaul (1992b). ”Forensic Science Against Computer Crime in the United Kingdom.” Journal of the Forensic Science Society 32(1): 27-34.

32. Connery, E. M. and S. B. Levy (1979). ”Computer Evidence in Federal Courts.” Commercial Law Journal 84: 266-276.

33. DarkReading (2008) ”Tech Insight: Digital Forensics and Incident Respose Go Live.”

34. DeHetre, J. D. (1975). ”Data Processing Evidence-Is It Different?” Chicage-Kent Law Review 52: 567-599.

35. DFRWS (2001). DFRWS Technical Report: A Road Map for Digital Forensic Research. Digital Forensic Research Workshop. G. Palmer. Utica, New York.

36. Duffy, J. (2009, 12 May). ”Cisco unveils cloud computing platform for service providers.” Retrieved 10 Feb., 2011, from http://www.infoworld.com/d/cloud-computing/cisco-unveils-cloud-computing-platform-service-providers-113.

37. Economist (2008) ”Getting wired.” The Economist.

38. Ellison, L. (2009). Why Larry Ellison hates Cloud computing, TechPulse360.com.

39. Eucalyptus (2010). Eucalyptus User Guide, Eucalyptus Systems, Inc. 1.6.

40. Eucalyptus. (2010). ”Resources.” Retrieved 9 Feb., 2011, from http://www.eucalyptus.com/res myths-dispelled#q2.

41. Eucalyptus. (2011). ”Eucalyptus: The Open Source Cloud Platform.” Retrieved 27 Feb., 2011, from http://open.eucalyptus.com/.

42. Farmer, D. and W. Venema (2005). Forensic Discovery, Addison-Wesley Professional.

43. Feliz, T. (2010). Cloud Computing, 10 Web Operating Systems. admixweb, AdmixWeb.com. 2011.

44. Foster, I., Y. Zhao, et al. (2009). Cloud computing and grid computing 360-degree compared. Grid Computing Environments Workshop, 2008. GCE'08, IEEE.

45. Garfinkel, S. L. (2010). "Digital forensics research: The next 10 years." Digital Investigation 7(Supplement 1): S64-S73.

46. Garfinkel, T. and M. Rosenblum (2005). When virtual is harder than real: Security challenges in virtual machine based computing environments, USENIX Association.

47. Gellman, R. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, World Privacy Forum.

48. Giannelli, P. (2006). Judicature - Scientific Evidence.

49. Gladyshev, P. (2004). Formalising event reconstruction in digital investigations. Computer Science and Informatics. Dublin, University College Dublin. PhD: xi, 212 p.

50. Gladyshev, P. and A. Almansoori (2010). Reliable Acquisition of RAM dumps from Intel-based Apple Mac computers over FireWire. Second International Conference on Digital Forensics and Cyber Crime (ICDF2C). Abu Dhabi, UAE, ICST.

51. Gladyshev, P. and A. Patel (2004). "Finite state machine approach to digital event reconstruction." Digital Investigation 1(2): 130-149.

52. Gogolin, G. (2010). "The Digital Crime Tsunami." Digital Investigation 7(1-2): 3-8.

53. GoGrid (2008). Cloud Computing Explained.

54. Goss, J. (2010). Forensic Triage: Managing the Risk. Computer Science and Informatics. Dublin, University College Dublin. Master fo Science: 51.

55. Gutheil, T. G. and H. J. Bursztajn (2005). "Attorney Abuses of Daubert Hearings: Junk Science, Junk Law, or Just Plain Obstruction?" Journal of the American Academy of Psychiatry and the Law 33(2): 150-152.

56. Halderman, J., S. Schoen, et al. (2009). "Lest we remember: cold-boot attacks on encryption keys." Communications of the ACM 52(5): 91-98.

57. Hannan, M. (2004). To Revisit: What is Forensic Computing? 2nd Australian Computer, Network & Information Forensics Conference. Perth, Australia.

58. Hewlett-Packard. (2011). "Everything as a Service." Retrieved 16 Feb., 2011, from http://www.hp.com/hpinfo/initiatives/eaas/index.html.

59. Higginbotham, S. (2010, 14 Apr.). "Ericsson CEO Predicts 50 Billion Internet Connected Devices by 2020." Retrieved 27 Jan., 2011, from http://gigaom.com/2010/04/14/ericsson-sees-the-internet-of-things-by-2020/.

60. Hobson, E. W. (2010). "What is Cloud Computing?" Retrieved 12 Feb., 2011, from https://sites.google.com/site/cloudinvestigations/whatis.

61. IBM (2010). IBM X-Force 2010 Mid-Year Trend and Risk Report, IBM X-Force.

62. IBTimes (2010) "Number of Internet users in emerging markets to double by 2015: report." International Business Times.

63. IC3 (2009). 2009 Internet Crime Report, Internet Crime Complaint Center (IC3).

64. Ingthorsson, O. (2010). Cloud computing - data privacy and compliance. Cloud Computing Topics. 2011.

65. InternetWorldStats. (2010, 30 June). "Internet Usage Statistics: The Internet Big Picture." Retrieved 27 Jan., 2011, from http://internetworldstats.com/stats.htm.

66. James, J., P. Gladyshev, et al. (2010). "Analysis of Evidence Using Formal Event Reconstruction." Digital Forensics and Cyber Crime 31: 85-98.

67. James, J. I. and P. Gladyshev. (2010). "2010 Report of digital forensic standards, processes and accuracy measurement." Retrieved 22 Dec., 2010, from http://www.forensicfocus.com/2010-digital-forensics-standards-processes-accuracy.

68. Jenkins, M. M. (1975). "Computer-Generated Evidence Specially Prepared for Use at Trial." Chicage-Kent Law Review 52: 600-609.

69. Johnson, B. (2008) "Cloud computing is a trap, warns GNU founder Richard Stallman." Guardian.co.uk.

70. Jones, N. (2004). ”Training and accreditation - who are the experts?” Digital Investigation 1(3): 189-194.

71. Kelman, A. and R. Sizer (1982). Computer in Court - A Guide to Computer Evidence for Lawyers and Computing Professionals.

72. Kent, K., S. Chaevalier, et al. (2006). Guide to Integrating Forensic Techniques into Incident Response, National Institute of Standards and Technology: 121.

73. Koopmans, M. (2010). The Art of Triage with (g)PXE. Computer Science and Informatics. Dublin, University College Dublin. Master fo Science: 51.

74. Mansfield-Devine, S. (2010). ”Fighting forensics.” Computer Fraud & Security(1): 17-20.

75. Martin, A. (2007). ”Firewire memory dump of a Windows XP computer: a forensic approach.”

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

77. McGuigan, B. (2011). ”What is Distributed Computing?” Retrieved 10 Feb., 2011, from http://www.wisegeek.com/what-is-distributed-computing.htm.

78. McKemmish, R. (1999). ”What is forensic computing.” Trends and issues in crime and criminal justice 118.

79. Mell, P. and T. Grance (2009). The NIST Definition of Cloud Computing, National Institute of Standards and Technology.

80. Messmer, E. (2011) ”How one municipality is securing Google Apps, Docs.” CSOnline.

81. Microsoft. (2010). ”Computer Online Forensic Evidence Extractor (COFEE).” Retrieved 4 Feb., 2011, from http://www.microsoft.com/industry/government/solu

82. Microsoft. (2011, 5 Jan.). ”TrojanDropper:Win32/Bohu.A.” Malware Protection Center Retrieved 25 Feb., 2011, from http://www.microsoft.com/security/portal/Th

83. Mislan, R. P., E. Casey, et al. (2010). ”The growing need for on-scene triage of mobile devices.” Digital Investigation 6(3-4): 112-124.

84. Myslewski, R. (2009, 2 Dec.). ”Intel puts cloud on a single megachip.” Retrieved 10 Feb., 2011, from http://www.theregister.co.uk/2009/12/02/intel_scc/.

85. NationMaster. (2008). "Mobile cellular (per capita)." Retrieved 27 Jan., 2011, from http://www.nationmaster.com/graph/med_tel_mob_cel_percap-telephones-mobile-cellular-per-capita.

86. NIJ. (2008, 14 Apr.). "Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition." Second Edition. Retrieved 2 Feb., 2011, from http://www.ojp.usdoj.gov/nij/publications/ecrime-guide-219941/welcome.htm.

87. O'Connor, T. (2010, 21, Aug.). "Admissibility of Scientific Evidence Under Daubert." Retrieved 26, Jan., 2011, from http://www.drtomoconnor.com/3210/3210lect0

88. OWASP. (2010, 29 Sep.). "Threat Risk Modeling." Retrieved 27 Feb., 2011, from http://www.owasp.org/index.php/Threat_Risk_Modeling.

89. Parallels. (2011). "Hosted Applicaitons - SaaS." Retrieved 16 Feb., 2011, from http://www.parallels.com/eu/spp/apphostingsaas/.

90. Pollitt, M. (1995). Principles, practices, and procedures: an approach to standards in computer forensics.

91. Pollitt, M. (2007). An ad hoc review of digital forensic models, IEEE.

92. Polsson, K. (2011, 1 Jan.). "Chronology of Personal Computers." Retrieved 25 Jan., 2011, from http://www.islandnet.com/ kpolsson/comphist/.

93. Purdy, C. (2010, 11 Aug.). "Industry's First Forensic-base Critical Infrastructure Security Solution." Retrieved 29 Jan., 2011, from https://www.guidancesoftware.co

94. Rekhis, S. and N. Boudriga (2010). Formal Digital Investigation of Anti-forensic Attacks. Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, IEEE.

95. Ristenpart, T., E. Tromer, et al. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. 16th ACM conference on Computer and communications security, ACM.

96. Roberts, J. J. (1974). "A Practitioner's Primer on Computer-Generated Evidence." The University of Chicago Law Review 41(2): 254-280.

97. Rogers, M., J. Goldman, et al. (2006). "Computer forensics field triage process model." Journal of Digital Forensics, Security and Law 1(2): 27-40.

98. Scheier, R. L. (2009) "What to do if your cloud provider disappears." Cloud Computing.

99. Schneier, B. (2010). The Threat of Cyberwar Has Been Grossly Exaggerated. Schneier on Security. 2011.

100. Shinder, D. and M. Cross (2008). Scene of the Cybercrime, Syngress Media.

101. Smith, S. E. (2011). "What is Cyberwar?" Retrieved 28 Jan., 2011, from http://www.wisegeek.com/what-is-cyberwar.htm.

102. Spafford, E. H. and S. A. Weeber (1993). "Software forensics: Can we track code to its authors?" Computers & Security 12(6): 585-595.

103. Stephenson, P. (2003). "Using a Formalized Approach to Digital Investigation." Computer Fraud & Security 2003(7): 17-20.

104. SWGDE (2009). SWGDE/SWGIT Digital & Multimedia Evidence Glossary Version: 2.3, Scientific Working Group on Digital Evidence.

105. Swiderski, F. and W. Snyder (2004). Threat modeling, Microsoft Press Redmond, WA, USA.

106. Tapper, C. (1974). "Evidence From Computers." Rutgers Journal of Computers and the Law 4: 324-406.

107. Teubner, A. L. (1978). "The Computer as Expert Witness: Toward a Unified Theory of Computer Evidence." Jurimetrics Journal 19: 274-297.

108. USDoJ (2002). Prosecuting Computer Crimes. S. Eltringham, United States Department of Justice, Computer Crime & Intellectual Property Section.

109. Vouk, M. A. (2008). Cloud computing-Issues, research and implementations, IEEE.

110. Willassen, S. (2008). Using simplified event calculus in digital investigation. 2008 ACM symposium on Applied computing, ACM.

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

112. Wilsdon, T. and J. Slay (2005). Digital forensics: exploring validation, verification & certification. First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05), IEEE.

113. Wolski, R. (2010). Top 5 Questions Posted on "Cloud Computing" [Part 1/3]. Eucalyptus. 2011.

114. Xen. (2011). "Xen Hypevisor - Leading Open Source Hypervisor for Servers." Retrieved 10 Feb., 2011, from http://www.xen.org/products/xenhyp.html.

115. Zittrain, J. (2009). Lost in the Cloud. The New York Times. Cambridge, Mass., The New York Times Company.

ADDITIONAL READING

Definitions

Armbrust, M., A. Fox, et al. (2009). Above the Clouds: A Berkeley View of Cloud Computing, EECS Department, University of California, Berkeley. NIST. (2010, 27 Aug.). "Cloud Computing." Retrieved 27 Feb., 2011, from http://csrc.nist.gov/groups/SNS/cloud-computing/.

Digital Forensic Investigation Process Models

Carrier, B. and E. Spafford (2003). "Getting physical with the digital investigation process." International Journal of Digital Evidence 2(2): 1-20. Carrier, B. D. (2006). A hypothesis-based approach to digital forensic investigations. CERIAS. West Lafayette, IN, Purdue University. PhD. Home Office (2010). Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System. F. S. Regulator, Crown Copyright: 55. Pollitt, M. (2007). An ad hoc review of digital forensic models, IEEE.

Cloud Computing and Digital Investigations

Hobson, E. W. (2010). QinetiQ White Papers: Digital Investigations in the Cloud. Higgins, K. J. (2011, 25 Jan.). "Proposed Nonprofit Would Bridge Law Enforcement, Enterprise Security Worlds." Retrieved 27 Feb., 2011, from http://www.darkreading.com/smb-security/167901073/security/news/229100238/proposed-nonprofit-would-bridge-law-enforcement-enterprise-security-worlds.html. Zimmerman, S. and D. Glavach (2011). "Cyber Forensics in the Cloud." IAnewsletter 14(1): 4-7.

Legal Aspects of Digital Investigations

CoE (2001). Concention on Cybercrime. Budapest, Council of Europe. Gellman, R. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, World Privacy Forum. USDoS. "U.S. Department of State Freedom of Information Act (FOIA)." Retrieved 27 Feb., 2011, from http://www.state.gov/m/a/ips/.

Threats/Cases/Proof of Concept Exploitation

CSA (2010). Cloud Security Alliance Top Threats to Cloud Computing v1.0, Cloud Security Alliance (CSA). Dhanjani, N., B. Rios, et al. (2009). Hacking: The Next Generation. Sebastopol, CA, O'Reilly Media, Inc. Gustin, S. (2011) "GFail: Google 'Very Sorry' After The Cloud Eats 150,000 Gmail Accounts." Wired. Thomas, K. (2010) "Microsoft Cloud Data Breach Heralds Things to Come." PCWorld Business Center.

Could Providers and Software

Amazon. (2011). "Amazon Elastic Compute Cloud (Amazon EC2)." Retrieved 27 Feb., 2011, from http://aws.amazon.com/ec2/ Eucalyptus. (2010). "Eucalyptus Community." Retrieved 27 Feb., 2011, from http://open.eucalyptus.com/. Feliz, T. (2010). Cloud Computing, 10 Web Operating Systems. admixweb, AdmixWeb.com. 2011. Finley, K. (2010) "5 Cloud-Oriented Operating Systems Available Now." ReadWrite Cloud. Google. (2011). "Top ten advantages of Google's cloud." Retrieved 28 Feb., 2011, from http://www.google.com/apps/intl/en/busines OpenNebula. (2011). "The Open Source Toolkit for Cloud Computing." Retrieved 27 Feb., 2011, from http://opennebula.org/ Xen. (2011). "Xen Cloud Platform." Retrieved 27 Feb., 2011, from http://www.xen.org/products/cloudxen.html

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