Chapter 15
Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics

George Grispos
University of Glasgow, Scotland

Tim Storer
University of Glasgow, Scotland

William Bradley Glisson
University of Glasgow, Scotland

ABSTRACT

Cloud computing is a rapidly evolving information technology (IT) phenomenon. Rather than procure, deploy, and manage a physical IT infrastructure to host their software applications, organizations are increasingly deploying their infrastructure into remote, virtualized environments, often hosted and managed by third parties. This development has significant implications for digital forensic investigators, equipment vendors, law enforcement, as well as corporate compliance and audit departments, amongst other organizations. Much of digital forensic practice assumes careful control and management of IT assets (particularly data storage) during the conduct of an investigation. This paper summarises the key aspects of cloud computing and analyses how established digital forensic procedures will be invalidated in this new environment, as well as discussing and identifying several new research challenges addressing this changing context.

INTRODUCTION

Cloud computing technologies have significant potential to revolutionise the way organizations provision their information technology (IT) infrastructure. Migration to cloud computing involves replacing much of the traditional IT hardware found in an organization's data centre (including servers, racks, network switches and air conditioning units) with virtualized, remote, on-demand software services, configured for the particular needs of the organization. These services can

DOI: 10.4018/978-1-4666-4006-1.ch015

be hosted and managed by the user organization (on a reduced hardware base), or by a third-party provider. Consequently, the software and data comprising the organization's application may be physically stored across many different locations, potentially with a wide geographic distribution.

There have been several predictions of substantial market growth in cloud services over the next few years. Gens has speculated that spending on cloud services will grow by 30% in 2011 (Gens, 2010). A Gartner press release forecast cloud service worldwide revenue to reach $68.3 billion in 2010, an increase of 16.6% from the 2009 revenue of $58.6 billion, and goes on to claim that cloud service revenues will reach $148.8 billion in 2014 (Pring et al., 2010). A study at the end of 2010 predicted that within the next three years, approximately 40% of Small and Medium Businesses (SMBs) expect to be using three or more cloud services and will have migrated their data into the cloud (Kazarian & Hanlon, 2011). There is some speculation that new and SMBs will benefit the most in the coming years, with cloud computing allowing these organizations to utilize appropriately scaled IT infrastructure that was previously only accessible to larger corporations (Schubert, Jeffery, & Neidecker-Lutz, 2010).

The use of cloud computing has potential benefits to organizations, including increased flexibility and efficiency. Virtualized services provide greater flexibility over an in-house physical IT infrastructure, because services can be rapidly re-configured or scaled to meet new and evolving requirements without the need to acquire new and potentially redundant hardware. Complementary to this, the use of cloud computing can reduce the costs of providing IT services, by eliminating redundant computing power and storage, reducing support requirements and reducing fixed capital commitments. Khajeh-Hosseini et al. found that a 37% cost saving could be obtained by an organization who chose to migrate their IT infrastructure from an outsourced data-centre to the Amazon Cloud (Khajeh-Hosseini, Greenwood, & Sommerville, 2010).

However, the use of cloud computing presents significant challenges to the users of clouds (both individuals and organizations), as well as regulatory and law enforcement authorities. It has been estimated that cybercrime will cost the British economy £27 billion per year in the coming years, with businesses accounting for nearly £21 billion of losses, largely due to the theft of intellectual property and espionage (Detica, 2011). It is likely that users of cloud computing services and technologies will be exposed to similar risks. The security of confidential corporate and private data remains one of the greatest concerns organizations have when they consider cloud computing (Butler, Heckman, & Thorp, 2010). Recent reports have noted Botnet attacks on Amazon's cloud infrastructure (Amazon Web Services, 2009). The compromise of the Gmail email service by (alleged) Chinese hackers (Blumenthal, 2010) illustrates that cloud computing platforms are already a target for malicious activities.

When security breaches, attacks or policy violations occur, it may be necessary to conduct a digital forensic investigation. However, existing digital forensic principles, frameworks, practices and tools are largely intended for off-line investigation. In particular, these approaches assume that the storage media under investigation is completely within the control of the investigator. Conducting investigations in a cloud computing environment presents new challenges, since evidence is likely to be ephemeral and stored on media beyond the immediate control of an investigator. This paper raises the awareness on the challenges posed by cloud computing technologies for digital forensics through an analysis of the applicability of the Association of Chief Police Officers (ACPO) digital forensics principles and the Digital Forensics Research Conference (DFRW) Investigative Process