# Foreword

Understanding technological change is really not that difficult. It is a repeated cycle of research, experience, adjustment, and examination. Research, combined with past experience and new infrastructures, leads to new technologies. When those new technologies offer lower cost or better features (or both), they become popular. Once deployed, those technologies are refined and eventually considered for evolution or replacement. It is not always obvious what a particular set of winning combinations and features may be, but therein lies the ongoing challenge for researchers, developers, and entrepreneurs.

Cloud computing is one example of such a technology advancement. Computing centers have been around for many decades, thus providing a long baseline of experience. Research in academia and experience with commercial systems—c.mmp/Hydra and Grapevine in the 1970s; Eden, ISIS, Clouds[1], and Apollo/Domain in the 1980s; RAID, NFS, Amoeba, Banyan, and Novell in the 1990s and beyond; and development of virtual environments and multicore systems in the 2000s—all laid the groundwork for current "cloud computing" to emerge. It required a special mix of hardware cost/performance, platform mix, and network bandwidth coupled with the experience from those earlier systems to make "cloud computing" economical and dependable enough for everyday use; it was not an "overnight" development.

There are opportunities with technology advancements applied to existing areas of endeavor. That is certainly the case with cloud computing and digital forensics. For example, one of the biggest problems for many researchers and investigative organizations is keeping copies of all of the images of systems that might be under investigation, and copies of all the various bits of malware, tools, and contraband that are used for comparison. Cloud computing offers the promise of vast storage, and better sharing of commonly used resources. Some research will need to be conducted to handle issues of integrity of evidence, and ensuring the authenticity of references, as well as how to ensure that there are usable backups of material, but approaches to these issues are not impossible to envision.

Another potential benefit of cloud computing is "Platform as a Service" or PaaS. This provides an opportunity to collect a "reference library" of possible system configurations, and load them as needed as remote, cloud-based images. Investigators can use these images for comparison, testing of software, tool benchmarking, hypothesis testing of malicious activity and code, and a number of other possibilities, all without the expenses and labor involved in having local machines. Furthermore, by having it "in the Cloud," other researchers can share the technology . . . and results.

There are potentially a host of other services that could be based "in the Cloud"—either public clouds or private clouds, or a hybrid combination—that could aid investigators and researchers. Having access to large amounts of storage, software, and virtual machines that would be too expensive or labor-intensive to maintain locally may open up many new possibilities for researchers and investigators alike.

However, some of the opportunities provided by new technologies are not what the designers of those technologies intended. Usually, the early development of any technology is oriented towards making the technology work—reliably—and then in reducing their cost. Issues of security, privacy, and compliance monitoring are often secondary thoughts . . . for the designers. There are those who see new technologies as new platforms for fraud, abuse, and the furtherance of illicit activities. The dual nature of new technologies is not limited to computing, either, but as a relatively new area of endeavor, we have less experience in coping with the associated complications. Cloud computing is certainly an example of note. Computers have brought us computer viruses, email has enabled spam, the WWW supports phishing, and networks enable all sorts of APT-style threats. We have yet to see what kinds of problems cloud computing might enable.

Digital forensics, as a field, is only slightly more than two decades old; consideration of what is available to us for local computing systems reveals gaps in our investigative methods for the Cloud. For example, crimes committed using virtual machines in PaaS-type environments are extremely unlikely to leave system residue (or images) that can be analyzed. As another example, shutting down a running cloud service to perform an investigation on petabytes (or larger) of storage is simply not feasible, both because of available methods and because of the potential for disruption of many innocent third parties.

There is often a small window of opportunity between the growing acceptance of a new technology and the emergence of associated threats. The key problem is getting a head start on the fixes (if possible) and countermeasures given that those who are concerned are usually not those who own the technologies and infrastructure where the threats will be manifest. This is where vision and creativity are critically important.

This volume is focused on the potential of "the Cloud"—both its promises and potential downsides. Herein you will find some foundational thinking about how to apply digital forensics in cloud computing environments. The coverage includes essays on everything from structure of an investigation, to data and tools, to legal requirements, to as-yet-unmet needs, to some methods of using the cloud paradigm itself to support digital investigations.

Cloud computing is here, and we cannot control its spread even if we wanted to. We can anticipate ways in which it may be used to support our activities, as well as how it may be used in furtherance of criminal activities, or abused within the confines of an organizational set of prohibitions. We can, and should, start thinking of how we might deploy those services to support our research and investigations. We also need to start thinking about how to investigate cloud-based incidents to gather the necessary digital evidence to identify with certainty the perpetrators and inform appropriate reactions to their deeds. Thus, if we are to try to stay ahead of the "bad guys" we need to start thinking about new methods of investigation, research, and forensics using cloud computing.

The editor and authors of these chapters have started that process. They have not yet solved all the challenges, but they have made significant steps toward defining the problems and setting forth how to address them. The problems that remain present a new set of challenges for practitioners, developers, and researchers. The cycle continues. Good luck with your portions of it!

*Eugene H. Spafford*
*Purdue University, USA October 2012*

**Eugene H. Spafford** *is a Professor of Computer Sciences at Purdue University, and is the founder and Executive Director of the Center for Education and Research in Information Assurance and Security (CERIAS). His research and education over three decades has contributed to many of the technologies used in modern computing system protection. Spaf's current research interests are in information security, cybercrime, software engineering, professional ethics, and security policy. Dr. Spafford is a Fellow of the ACM, AAAS, IEEE, ISC2, is a Distinguished Fellow of the ISSA, and has received many other awards for service, scholarship, and education.*

## ENDNOTES

[1] Yes, there was a distributed, boundary-less computing system named Clouds, developed at Georgia Tech in the 1980s. My Ph.D. dissertation was on building the prototype kernel for it. New ideas in the computing marketplace are not that new to researchers!