Towards Enabling Behavioral Trust among Participating Cloud Forensic Data Center Agencies

Sean Thorpe[1], Tyrone Grandison[2], Indrajit Ray[3], Abbie Barbir[4]

[1] University of Technology, Kingston, Jamaica
[2] IBM Research, York Town Heights, NY, USA
[3] Colorado State University, Fort Collins, USA
[4]Bank of America
[1]*thorpe.sean@gmail.com,*
[2] *tyroneg@us.ibm.com,*
[3]*indrajit@cs.colostate.edu*
[4]*abbie.barbir@bankofamerica.com*

Abstract. In this position paper, the authors present some of the concerns with respect to monitoring and managing the behavioral trust of participants in a forensic cloud data center environment. The basic idea of the approach is to view the interaction process of collaborating forensic cloud data centers overseeing an existing investigation or a set of such investigations across distinct jurisdictions. This work is an important first step to support the need for enabling trustable cloud digital investigations among participating law enforcement agencies.

1 Introduction

While cloud forensics is a field that is still in its infancy, it is gaining traction in the face of proliferate criminal actors taking advantage of the insecurity of these abstract domains. By definition a virtual cloud domain represents the service oriented architecture (SOA) based technology that unlocks the economies of scale gained from leveraging traditional web hosted services. In other words, the cloud as a service model offers on-demand, elastic and scalable provisions to its networked end users.

The cloud deployment model is categorized using networked communities of public, private and hybrid domains of users. Underlining these cloud service deployment models is the fact that each deployment has a generic set of service layers, namely the Infrastructure as a Service (IAAS), Platform as a Service (PAAS) and Software as a Service (SAAS) layers. To date, vendors like Amazon with its Elastic Cloud Provisions (EC2) and Google are major IAAS providers. Windows Azure, VMWare and Xen Citrix represent the major PAAS and SAAS providers [1]. These service layer designs however inherently lack any trusted Forensics and Security constructs within the existing virtualization stack, and this has unfortunately become an urgent need by law enforcement.

Cloud forensics at this point still does not have a universally accepted definition, but current practices borrow heavily from the existing digital forensics literature in how information retrieval can be supported within these logical domains [15]. To ground the theories that this paper puts forward, a suitable definition for cloud forensics would be one based on Casey's definition of forensics as "a characteristic of evidence that satisfies its suitability for admission as fact and its ability to persuade based upon proof (or high statistical confidence)" [2].

As an elastic service model, cloud computing environments are ideally open distributed domains similar to Grid computing and main frame environments [3]. These data clouds are composed of autonomously participating groups that interact with each other using specific mechanisms and protocols to offer and/or use services (e.g. computation, storage, and bandwidth). The difference between the grid and the cloud however is in the elastic, on-demand nature of the resources available across private, as well as public, domains. For the purposes of managing a trustable cloud forensic investigation where participating forensic cloud data centers can be located in any independent set of geographic jurisdictions, one realizes that such participation may not have sufficient knowledge about their interaction partners in the environment; particularly those in a public cloud domain setting. As a result, the authors see trust management mechanisms as a promising solution for strengthening the confidence quality of the interaction between forensic cloud data centers established to act as oversight agencies in the daily operations of large scale cloud computing investigations. We define trust in a Cloud Forensics environment as "the extent to which every participating digital investigative datacenter is willing to interact with each other, at a specific moment in time, with evidence of relative security regarding the identity and the behavior of their counterparts"; even though unexpected negative outcomes could result from the entire interaction process.

This definition extends on the views by Papalilo et.al. [3] and we adopt that this trust permeates all layers of the virtualization stack. We extend the principles in [3] to suggest the need to have a probabilistic cloud forensic data center trust model for both the identity and the behavior of the interaction parties. In this paper, we present the conceptual views for managing the trust of these participatory cloud forensic data centers. Ideas of quality assurance for identifying the "real" behavior of a participant during an interaction and for "keeping" the behavior of the participants "in control" are also presented. If the behavior of a cloud forensic data center participant is "out of control", then this participant's reliability and dependability are called into question, which translates to either:

- The participant not being used as an interaction partner for certain applications, because the expected behavior and trust requirements were not met but the participant could still be considered for other applications with moderate trust requirements OR
- The participant not being considered anymore for further interactions, independent of the expected behavior and trust requirements of applications

The rest of the paper is organized as follows. In section 2, an explanation of the trust behavior of cloud forensic data center participants is provided. In section 3, our view on how behavior trust can be established and managed among cloud participants

is given. Section 4 presents the considerations for managing (behavioral) trust in cloud forensic environments. In Section 5 concludes and provides discussion on future work.

2 Behavioral Trust of Cloud Forensic Participants

2.1 The Problem of Behavior Definition in Clouds

In the literature, the behavior of collaborative parties in cloud environments remains an abstract notion. Participants can be listed either in a "trust list" or "distrust list" [11]. In most cases, "trust list" behavior reflects the expectations of a participant to simply receive a response from another participant involved in an interaction or sometimes to get accurate results. If an interaction party behaves differently from "normal" expectations, it moves to the "distrust list". Participants within a "trust list" exhibit behavior that is considered a part of trusted zones and are thus eligible for future interactions. Participants within a "distrust list" exhibit behavior which may have only minor or no possibility to be considered for further interactions within the participating group. These claims become particularly important to a cloud digital investigation team who may have to be collaborating in participant groups across different geographic jurisdictions and must cooperate with the collaborating parties to unearth potential evidence required in completing a case for court.

To support a flexible behavioral management and classification system of trust for the cloud forensic data center, additional mechanisms are necessary, e.g. splitting behavior into detailed elements, observing them continuously and offering the possibility for evolving behavior classification.

2.2 Behavior Trust and Quality of Service for the Cloud Forensic Data Center

The use of system based logs for a cloud investigation[12,13] in our prior work demonstrates that the forensic data center users must recognize the need for different aspects of Quality of Service(QoS). In the forensic cloud data center environment, usability of data is an important factor as adopted from work done in [5]. Hence, it is meaningful to investigate the relationship between the QoS and the behavior of participants in a cloud forensic investigation, where the participating forensic data center trust groups are from different jurisdictional cloud environments.

QoS refers to the ability of a cloud forensic data center participant to provide network and computation services such that each user's expectations for timeliness, quality and performance are met. There are several dimensions of QoS described in the literature [6], e.g. accuracy, precision and performance. To support a QoS dimension, the cloud forensic investigator request must specify a level of service for one or more of these dimensions, and the underlying control mechanisms should be capable of delivering these services at the requested QoS levels. QoS deals with a range of expected behavior of an individual cloud forensic data center participant, which as a whole defines the completion of the service a forensic team (or forensic

application service) demands. In this context, it is important to map the forensic user's expectations and preferences to the system parameters and capabilities. Hence if the QoS levels are high this can directly influence the trust levels within the data center environments, and the reciprocal is equally true.

From the standpoint of the authors, trust is the most important social element in policing these Internet-supported cloud data systems, as motivated by the earlier work of Grandison and Sloman[14].

3 Establishing Trust among Forensic Cloud Participants

A high degree of trust in a cloud forensic data center participant means that they are likely to be chosen as an interaction partner. Conversely, a low degree of trust suggests that the participant cannot be selected anymore, especially in the case when other, more trusted interaction partners are available. In this way, the trust model aims to guide a participant's decision making process regarding how, when, and who to interact with the others. When an interaction with a new forensic data center is started, i.e. when no information on previous behavior exists, it can use its beliefs about different characteristics of these interaction partners and reason by learning the behavior over a number of interactions. This will act as an enabler in deciding how much trust should be put in each of them. Furthermore, the participant could ask others in the environment about their experiences with the target forensic data center participant(s). If sufficient information is obtained and if this information can be trusted, the participant can reliably choose its interaction partners.

4 Behavioral Trust & Statistical Methods of QOS within a forensic Cloud

Considering different sources for gathering trust information from (self experience, indirect experience, user/application trust requirements), each forensic cloud data center participant sorts out the collaboration partners and starts interacting only with the "most trusted" of them. During the collaboration experiments, the behavioral trust elements are verified either with 100% or with a certain verification frequency. By verification frequency we mean the number of confirmed recommendations issued over time for a party joining the forensic cloud data center trust list or group. We posit that a verification result, assumes that the trust values are updated and influence the decision making process as to whether the collaboration with a certain participant will continue or will be interrupted. The problems start once any deviation from the expected behavior of a collaboration partner is recognized. We can seek to measure behavior deviation in two ways-: either by deviation with the current collaborating cloud forensic data centers, or an observed deviation over time.

The first type of deviation has a more immediate effect on the current collaboration and the validity of the data being processed. If a 100% verification strategy is applied, it is easy to tell that until that specific moment, no other deviation has happened. On

the contrary, if a verification frequency is applied, it is not possible to tell that no more deviations occurred except those verified and where confirmed to have existed.

5 Conclusions

In this position paper, the authors have presented some of the concerns with respect to monitoring and managing the behavioral trust of participants in a forensic cloud data center environment. The basic idea of the approach is to view the interaction process of collaborating forensic cloud data centers overseeing an existing investigation or a set of such investigations across distinct jurisdictions. Ongoing work explores the hardening and verification of a suitable family of trust formalisms and the development of a proof of concept simulation. This cloud simulator environment is similar to Gridsim [4] and explores the use of four (4) enterprise cloud service providers (CSP) including the University of Technology - Jamaica as the participatory cloud forensic groups. We expect to achieve from this ongoing work a qualification of the identifiable trust elements that should be considered, together with more complex scenarios. The aim is to evaluate the effects that trust has in determining how forensic cloud data center groups collaborate as well as to ascertain the performance of every single participant within the groups as a function of the efficiency of designing a sustainable trust model. We believe this is very important, in the face of elevated and intensive threats that inadvertently could compromise the security of forensics within these logical domains.

References

1. P.Mell, T. Grance. NIST Definition of Cloud Computing.
   Retrieved from:
   http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, September 2009.
2. E. Casey. Digital Evidence and Computer Crime. Academic Press, San Diego, CA, second edition, 2004.
3. E. Papalilo, T. Friese, M. Smith, B. Freisleben: "Trust Shaping: Adapting Trust Establishment and Management to Application Requirements in a Service-Oriented Grid Environment". In *Proceedings of the 4th International Conference on Grid and Cooperative Computing (GCC), Beijing, China*, pp.47-58, 2005.
4. GridSim. Online at : http://www.gridbus.org/gridsim.
5. I. Foster, C. Kesselman: *The Grid2: Blueprint for a New Computing Infrastructure*, Morgan Kaufmann, 2004.
6. A.S. Ali, O. Rana, D.W. Walker: "WS-QoC: Measuring Quality of Service Compliance". In *Proceeding of the Second International Conference on Service-Oriented Computing Short Papers (ICSOC),New York, USA*, pp. 16-25, 2004.
7. P. Lindstrom: "Attacking and Defending Web Services".
   In *http://www.forumsystems.com/papers/AttackingandDefending_WS.pdf*. 2004.
8. D. De Roure, N. Jennings, N. Shadbolt: "Research Agenda for the Semantic Grid: A Future E-Science Infrastructure". Online at : *www.semantic grid.org/v1.9/semgrid.pdf*, 2001.

9. I. Foster, H. Kishimoto, A. Savva, D. Berry, A. Djaoui, A. Grimshaw, B. Horn, F. Maciel, F. Siebenlist, R.Subramaniam, J. Treadwell, J. Von Reich: "The Open Grid Services Architecture".
Online at: *http://www.gridforum.org/documents/GWD-I-E/GFDI .030.pdf*, 2005.
10. E.Papalilo, B. Freisleben: "Combining Incomparable Public Session Keys and Certificateless Public Key Cryptography for Securing the Communication between Grid Participants". In *Proceedings of International Conference on Grid Computing, High-Performance and Distributed Applications (GADA'07), Vilamoura, Algarve, Portugal. R. Meersman and Z.Tari et al. (Eds.): OTM 2007, Part II, Springer Verlag,LNCS 4804*, pp. 1264–1279, 2007
11. S .Thorpe. Modeling Trust in a Cloud Computing Context. *Proceedings of the ACM CIKM/PIKM, October 2010.*
12. S. Thorpe, I. Ray. Detecting Temporal Inconsistency in Virtual Machine Activity Timelines. *Proceedings of Journal of Information Assurance and Security (JIAS), Volume 7. No.1, May 2012.*
13. S. Thorpe, I. Ray. File Timestamps in a Cloud Digital Investigation. Journal of Information Assurance and Security. ISSN1554-1010 Volume 6 Issue 2, pp. 495–502, December 2011.
14. T. Grandison and M. Sloman, "A survey of trust in Internet applications," *IEEE Communications Surveys& Tutorials*, Vol. 3, No. 4, 2000.
15. D.Riley, C.Wren, T.Berry, "Cloud Forensic Challenges for Law Enforcement proceedings", Proceedings of the International Conference For Internet Technology and Secured Transactions, London, UK ,Nov. 2010.