A Vision for Intrusion Analysis and Digital Forensics in Cloud

Dr. Kazi Zunnurhain
Assistant Professor
Northern Kentucky University
Highland Heights, KY 41099
+1 859 572 4753
zunnurhaik1@nku.edu

ABSTRACT
Cloud computing is gaining in popularity and complexity. As more companies move their platforms, services and infrastructure to the cloud, security becomes an increasingly important and daunting task. This paper is aimed at exploring improvements to secure authentication and encryption as well as focusing on the changes to intrusion analysis and digital forensics when moving to the cloud, with a future intention to propose a consolidated platform to support rigid authentication and encryption in cloud with support of digital forensics technologies.

Keywords
Cloud computing, digital forensics, authentication, encryption.

1. INTRODUCTION
Cloud computing has become a very widespread and popular technology. Forbes reported that cloud computing was a $56.6 billion dollar industry in 2014 and predicts continuous growth in the future [1]. Cloud computing has been defined in several ways and one of the most common definitions is from the National Institute of Standards and Technology (NIST): “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

Authentication, encryption, and intrusion analysis are important aspects for the future of cloud security. The 2015 data breach investigations report published by Verizon Enterprises noted that credentials were used to gain access to over half of the systems breached in the year 2014 [7]. As threats to computer systems and the cloud are evolving, so should our methods of securing them. In Section 2, alternate forms of authentication are presented as a method for securing the cloud. In Section 3 the need for cloud security for forensic intrusion analysis is introduced. Section 4 discusses the future directions and concludes the paper with our future intention.

2. AUTHENTICATION
Authentication is one of the most prominent feature of security triads (among Confidentiality, Integrity and Authentication). With authenticity the privilege of a user is determined in a system. In this section we will analyze different approaches of authentication mechanism, such as: improving passwords, alternatives of authentication.

2.1 Improving Passwords
Passwords are hard for humans to remember and the typical text based passwords are too easy for computers and our adversaries to guess. There are measures that system administrators can consider to increase the complexity, such as how often the user must change the password or limiting the reuse of previous passwords. One study showed that over 30% of participants wrote the password down on a piece of paper or stored it electronically in clear text [8]. Passwords are also a single point of failure in most systems; if hackers learn a user’s password they can access everything the user is authorized to access on that system.

2.2 Authentication Alternatives
There are multiple authentication methods aimed at replacing or augmenting password usage to increase security. These methods individually have not been proven as feasible replacement for passwords but if combined with passwords or other authentication methods, can provide a much higher level of security than passwords alone. There are several categories of authentication methods that exist today.

2.2.1 Single Sign On
Federated single sign on is an authentication method that allows users to create a single identity through an identity management system and the other service providers trust the identity provider (IDP) to authenticate the user and validate credentials. An example of this is Google OAuth 2.0 or Facebook Connect where users login with their Google or Facebook credentials and connect to other websites or applications with similar identity [9].

2.2.2 QR code
QR code authentication uses either a smartphone or a piece of paper and a webcam, the user proves identity through possession of the token on screen or on paper. On a smart phone a user identifies himself using an app that scans a QR code to validate the user for login based on an identity setup on first use of the phone[9].

2.2.3 Biometrics
Biometric authentication uses a human related characteristic to identify and authenticate users. Common forms are
fingerprints, facial recognition, voice recognition, and retinal scanners. Unique characteristics of each user are used to initially identify the user and allow them to use that characteristic to authenticate them in the future.

3. FORENSIC INCIDENT ANALYSIS

In conjunction with authentication and encryption, intrusion analysis is an important topic of cloud computing security. The NIST definition of cloud computing forensic is "the application of scientific principles, technological practices, and derived and proven methods to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation, and reporting of digital evidence" [2].

The 2015 data breach investigations report published by Verizon Enterprises noted 79,790 reported security incidents in the year 2014 [7]. Cloud computing forensics is in its infancy, and different environments introduced by the cloud created issues for the traditional forensic process. The issues facing cloud forensics are highly documented in many studies, but currently there are only theoretical architectural framework and auditing solutions to address the issues of cloud computing forensics [2], [3].

In an effort to create standard for forensic analysis NIST researched, analyzed, and summarized seventy studies on cloud computing forensics, some of those categories will be discussed in the following sections.

3.1 Cloud Architecture

One of the biggest challenges to cloud forensics is the cloud architecture itself. Each environment is completely different from the other. The physical amount of data that could reside in the cloud can pose a problem for an investigator because if collected data needs to be stored. The data itself can be virtual, volatile, or stored on a hard drive, hence the removal of data will become an issue. If the space is reused then the questions of access to the data, imputed evidences, and data modification are raised.

Security needs to be defined with boundaries in multi-tenant environments. This security would help an investigator from breaching the confidentiality of the other users residing in the same environment. The cloud also needs access control security to assist the investigator in documenting anyone who had access to the data as well as the possibility of contaminated data.

3.2 Collection of Data

Data collection in the cloud environment is also affected by the architecture. Existing forensic techniques would seize storage media or computers and peripherals, but in a cloud environment that is not possible. Locating and isolating all of the data and its copies is a monumental task within itself because of the global aspect of the cloud and since only a real time collection can be performed. Real time data collection and recovery of deleted data has issues due to the volatility of the data in the cloud environment, and the use of live forensic tools cause environmental changes in the system [5].

3.3 Laws and Jurisdiction

The global nature of a cloud environment creates a challenge on how to bring all of the contributors involved in the cloud environment to work together in the collection and validation of digital evidence. This collaboration can cross global and legal jurisdictional boundaries and lead not only to technical challenges, but also to legal and organizational challenges [2]. Security in the cloud would have to include the creation of international laws that will work equally across the global infrastructure of the cloud. It would also have to encompass a form of timely international communication and cooperation so that forensic investigations and requests for data are consistent.

4. FUTURE DIRECTIONS AND CONCLUSION

Research is continuing in the areas of operating system including encryption and memory encryption to prevent security breaches such as the cold boot attacks [15]. One of the technologies called PRIME is being developed to support multiple RSA keys. At the software level there is a plan to redesign system programming languages to allow users more control over the register allocation process [12]. Solutions like PRIME, which uses an infrastructure that protects RSA private keys, and software solutions work to prevent stacks such as the cold boot attack [14]. These approaches will not solve all potential security issues, but can be used in conjunction with other types of security to improve the security.

Currently the development of standards and guidelines for cloud computing forensics is being led by NIST at the request of the Federal Chief Information Officer. NIST is working with the private sector to create the standards so they are cost-effective while meeting forensic requirements. This work has to be thorough, timely, and adaptable so it does not become obsolete as technology advances like the current set of forensic standards did [2]. The standards also have to be applicable to a global environment while not putting a financial or performance burden on the suppliers of cloud resources. Finally, standards also have to ensure personally identifiable information and proprietary information.

In future we would like to propose a concrete model to support authentication with the replacement of passwords for clients in cloud system with a promise to sustain integrity. Most of the IDS and Password authentication protocol do not consider the laws and jurisdictions based on diverse geographic location. Hence in our extended model we will support the SLA to be consolidated based on local laws and restrictions to avoid unexpected breaches or disputes. Future of cloud should be globally supported throughout any application with efficient security and authentication.

5. REFERENCES


