Forensic Analysis of Software-as-a-Service Cloud Providers Metadata

Subject: Master of Science in Engineering
Thesis advisor: Prof. Dr. Emmanuel Benoist
Expert: Prof. David Billard

The main topic of our thesis is IT forensic related to cloud environments. In particular we focussed our attention to the cloud platforms Google Drive and Dropbox and we developed a web platform able to analyze the metadata of users' account. This analysis is made possible by another software that runs on the suspect machine and decrypt credentials found in Chrome or Firefox password databases in order to access later to the metadata of the user.

Introduction

With the time, a steady increase of users involved with the cloud has opened the doors for new concepts regarding how cyber crime should be handled. The sharing of data between different users in different locations has seen a dramatic increase, due to the ease of use of new cloud platforms. In addition cyber criminals are encouraged to use the computation power offered by modern cloud computing providers to distribute malware or perform other actions. To fight against this new kind of threat, the term «cloud forensics» has been coined. This new branch of IT forensic aims to explore and give answers to crimes committed in highly dynamic environments like the cloud.

IT Forensic Overview

IT forensic refers to the science of finding legal evidence on a digital level. More in detail we try to identify, preserve, analyze and present to the public useful information about digital information. This information could later be used in front of a court in order to establish if a suspect if guilty or not. The type of evidence involved in digital forensic can assume different forms, like browser history or memory dump. The evidence should be gathered using scientific methods (e.g. digital signatures) in order to assure the impartiality of the evidence.

Cloud Computing

The paradigm of cloud computing has became a new trend during these last years. In a cloud environment everything happens in the internet and not on the local machine of the user so we gain in flexibility. Nowadays everything can live in the cloud: data, applications or servers are some examples of what we can access. There exists 3 different models of cloud computing:

- Infrastrucutre-as-a-Service: the user controls the operating system
- Platform-as-a-Service: the user controls the application
- Software-as-a-Service: the user uses a service offered by a provider in the cloud

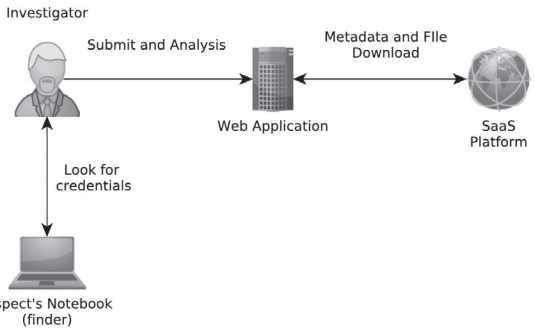
During our thesis we focussed on the Software-as-a-Service model.

Finder and Web Application

To perform forensic analysis tasks over the data in the cloud, we developed two pieces of software. One is the finder and the other is the web platform responsible of the analysis itself.

The finder is the first component we have developed. Its main task is to look for users' credentials like password and username and decrypt them in order to give the possibility to the investigator to access users' account on the cloud platform. The look up of password take place in the browser's databases of Firefox and Chrome and since they store passwords using symmetric cryptography it is possible to obtain the clear text password by using the key previously stored by these browsers.

The second component we developed is the web application. The web application takes as input the passwords found previously, logs in into the suspect account and download the file and the metadata for further analysis.
The investigator would be able then to download the file form Dropbox or Google Drive and analyze the metadata and other information. The important point is that the evidence we download are always signed by a third party so that anyone can verify that the application is not cheating.



Interaction between the investigator, the finder, the web application and the cloud provider.

Giuseppe Scalzi