CERIAS

The Center for Education and Research in Information Assurance and Security

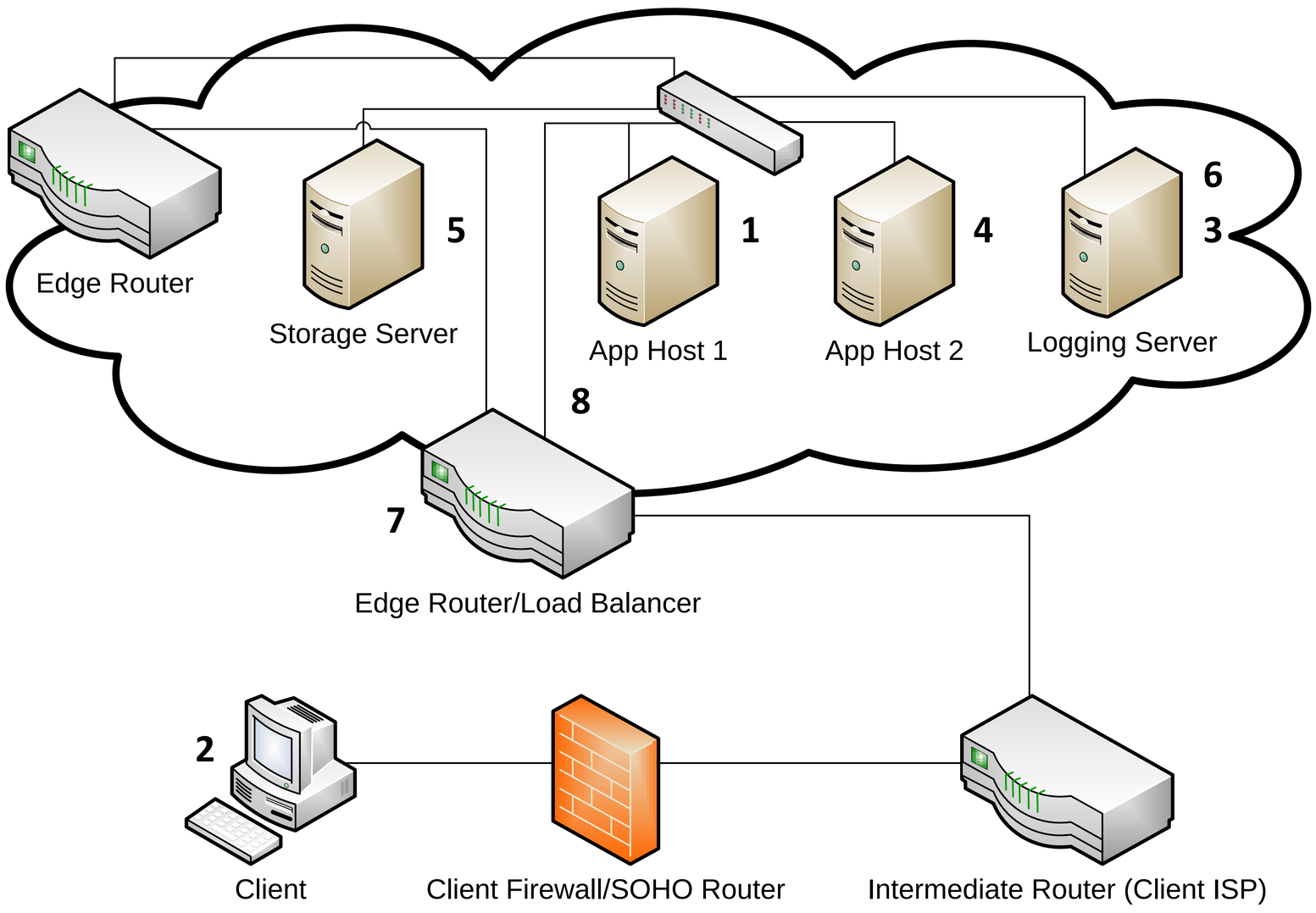
SaaS Incident Response: Evidence Provenance in a Cloud Service

Jake Kambic, Dr. Samuel Liles

Abstract

The purpose of this project was to analyze the origins of evidence in a cloud service, specifically targeting the Software as a Service (SaaS) business model. Due to the high volatility of cloud services, their abstract nature, and the physically dispersed infrastructure upon which they are based, forensic collection and analysis in the cloud is not realistically feasible. However, techniques for gathering evidence which can produce reasonably accurate results do exist. For this reason, an analysis of Incident Response in the cloud was undertaken, with the expressed purpose of identifying places where evidence is located in an SaaS cloud environment and the determining the level of effort required to acquire that evidence.

Typical SaaS Environment [Simplified]



Methods

In order to identify where evidence resides within the cloud environment, two approaches were taken. A combination of literature review and technical overview of cloud network architectures and the devices involved helped to reveal where evidence has been sought in the past and a general idea of where evidence is capable of being located. This was then cross-referenced with various known attacks on SaaS cloud services to ascertain if where responders look for the evidence is also where the best possible evidence lies.

Evidence Provenance

1. **Application logs**
2. **Client Machines** – often forgotten is that a large portion of any cloud transaction is the client and data on a client is typically less volatile
3. **Infrastructure billing documentation**
4. **Virtualization layer acquisition** – acquiring virtual machine images and memory if available
5. **Infrastructure Backups**
6. **Infrastructure Server Monitoring & Performance logs**
7. **Network Devices** – volatile transactional data can reside in network devices which may aid in attribution
8. **Network Capture** – Evidence can be extracted directly from network captures if available

CERIAS

PURDUE UNIVERSITY