A Generic Logging Support Architecture for Infrastructure as a Service (IaaS) Cloud

Winai Wongthai, Francisco Liberal Rocha, and Aad van Moorsel
School of Computing Science, University of Newcastle upon Tyne
email winai.wongthai@ncl.ac.uk
phone 07868239952

1. Conclusion
To mitigate a lack of trust in IaaS from consumers’ point of views, this paper proposed a Generic Logging Support Architecture (GLSA) and described its components. We then identified the appropriate Logging System (LS) to mitigate spam activities in a customer virtual machine (VM) by demonstrating how to 1) use the GLSA as a template to design, implement, deploy a LS, and 2) evaluate management and security of this new built LS. This evaluation is used as keys to effectively and efficiently monitor IaaS to mitigate a lack of trust in IaaS.

2. Introduction
The CSA Top Threats to Cloud Computing report [1] can be a concrete indicator of a lack of trust in IaaS. Monitoring [2,3], which actually has a LS as a core, the IaaS can be an ideal solution. Moreover, critical components of a LS are a logging process (LP) and logging files (LFS). However, evaluation of management and security of the LP(s) and the LFS themselves is a crucial challenge. Therefore, a clear architecture of monitoring/logging and the detail of its components in the IaaS environment are necessary.

3. Aim
To mitigate a lack of trust in the IaaS by using monitoring/logging solutions.

4. Research Questions
✓ What is a GLSA to monitor the IaaS?
✓ In order to mitigate CSA threat 1 (Abuse and Nefarious Use of Cloud Computing such as spam activities in an IaaS), how can we use the GLSA to identify an appropriate LS and how to evaluate its management and security?

5. Method

6. Results
1). A GLSA and the appropriate, new built LS in IaaS environment

2). To mitigate CSA threat 1: a case study of identification of an appropriate LS that is in a management domain (dom0); and this LS can obtain spam activities-related data from a customer/dimU such as the spam subject that sent to, and email address of the victim.

7. Discussion
✓ With a GLSA, we can have an appropriate LS which can be deployed in the IaaS real world with its management and security concerns.
✓ One key component in the LS is the open source library (libVMI [4]) that can access the main memory of a customer VM to obtain spam activities-related data. However, this memory accessing is violation of customer’s privacy. We plan to address this issue in our future work through the evaluated LS.

8. References
4. B. Payne, vmitools, Virtual machine introspection tools.