A Comprehensive Risk Assessment Framework for Cloud Computing Security

Mahadevan Gomathisankaran
Computer Science and Engineering
University of North Texas
mgmomathi@unt.edu

Krishna Kavi
Computer Science and Engineering
University of North Texas
krishna.kavi@unt.edu

Cloud computing is defined as the delivery of on-demand computing resources; everything from applications to data centers over the Internet on a pay-for-use basis [3]. Its design principle revolve around a custom or an open source cloud operating system that is in charge to control and provision allocated resources throughout the datacenter(s). Cloud computing services are deployed mainly in models such as: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). For example, OpenStack [8] cloud operating system enables developers to design any cloud computing deployment model such as: Public, Private or Hybrid cloud to support any of the cloud computing services.

Assessing security of software services on Cloud is complex because the security depends on the vulnerability of infrastructure, platform and the software services. The recent distributed denial of service cyber-attacks on American Banks websites [7] clearly shows the importance and imminence of cloud vulernability assessment. It was discovered that various cloud services and public Web hosting services had been infected with a form of malware that has existed for years. A cloud based assessment framework could be used to discover this type of vulnerabilities and help to protect banks from being victims of known security vulnerabilities.

In many Cloud systems, the platform or the infrastructure on which the software will actually run may not be known or guaranteed. This implies that the security of the software service must be assured regardless of the underlying infrastructure or platform, requiring a large number of combinations to be tested. Another common trend in Cloud and Service oriented Architecture (SoA) environments is Service composition, whereby new services can be created rapidly by composing existing services. Once again, the component services must be tested for security levels on a large number of platform and infrastructure combinations. We propose to develop a comprehensive risk assessment framework to address these issues of the Cloud computing security. Our framework consists of three components: ontology knowledge base, threat model, and risk estimation.

Ontology knowledge base

We build a Ontology Knowledge Base of known vulnerabilities, attacks, and defenses. A Knowledge base (KB) is a special kind of database of for knowledge management. KB provides a means for information to be collected, organized, shared, searched and utilized. It can be either machine-readable or intended for human use. Examples of current most used type of KB and open source tool are Wikipedia [2] and MongoDB [1]. There is another class of KB known as Semantic Web Knowledge Base (or Ontology Knowledge Base) which is a semantic web repository of data that becomes knowledge. This Ontology Knowledge Base is machine-readable and when visualized is very resourceful where its architecture gives the ability to represent knowledge and facilitate its retrieval and sharing among other applications.

Depending on the security problem addressed, it has been shown that knowledge base that uses the ontological approach enables the security practitioner to not only retrieve data from the KBs but also be able infer new knowledge. Bill and Gritzalis [9] presented a security management framework of an arbitrary

information system (IS) which builds upon knowledge-based resources, such as security ontology (SO) providing reusable security knowledge interoperability, aggregation and reasoning exploiting security knowledge from diverse sources.

We propose to design and implement ontology knowledge bases comprising Vulnerabilities, Attacks and Defenses, to facilitate in the automated risk assessment of the cloud.

Threat modeling

Given an adversary threat model which assumes that any attacker is highly capable, and well motivated; calls for a thorough investigation to identify the areas where any given cloud system is most vulnerable during its design or deployment phase. This way, one can choose the appropriate tools and implement the best design to protect the cloud's assets. To address this challenge, we use Microsoft STRIDE threat model [4] that enables us to classify and rank found threat types for each of the cloud's building block which is made of various shared technologies.

Risk estimation

Risk estimation is a critical task that involves weighting accumulated measurements into a refined indicator, in our case that indicator reflect the risk level of found vulnerabilities, exploits, defenses per threat type generated from threat model. Various risk assessment models such as DREAD [6] and Fenz [5] have been proposed but they all offer either offline, manual or not fully automated evaluations.

The advantage of the Fenz's Bayesian threat probability determination [5] is that it gives the risk manager a methodology to determine the threat probability in a structured and comprehensible way. In addition to the Bayesian calculation schema, this work uses the security ontology to populate the proposed methodology. Using the same methodology, we populate it using our vulnerabilities, attacks and defenses ontology knowledge bases relevant data toward inferring the risk indicator for the given cloud's assets.

In our proposed framework, we bring these useful predictive models and metrics into an automated process, therefore to generate a risk indicator for the given cloud system configuration.

References

[1] Mongodb. `http://www.mongodb.org`.

[2] Wikipedia. `http://www.wikipedia.org`.

[3] IBM Cloud. What is cloud?, 2014.

[4] Microsoft Corporation. The stride threat model, 2014.

[5] Stefan Fenz. An ontology-and bayesian-based approach for determining threat probabilities. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pages 344–354. ACM, 2011.

[6] OWASP. Threat risk modeling, 2014.

[7] NICOLE PERLROTH and QUENTIN HARDY. Bank hacking was the work of iranians, officials say, January 2013. URL: `http://goo.gl/IIXvt`, Last accessed on 01/09/2013.

[8] OpenStack project. Openstack: The open source cloud operating system, 2014.

[9] B. Tsoumas and D. Gritzalis. Towards an ontology-based security management. In *Advanced Information Networking and Applications, 2006. AINA 2006. 20th International Conference on*, volume 1, pages 985–992, 2006.