

# ARC '18

مؤتمر مؤسسة قطر  
السنوي للبحوث

QATAR FOUNDATION  
ANNUAL RESEARCH CONFERENCE

البحث والتطوير: التركيز على  
الأولويات، وإحداث الأثر

R&D: FOCUSING ON PRIORITIES,  
DELIVERING IMPACT

20-19 مارس  
19-20 MARCH



مؤسسة قطر  
Qatar Foundation

إطلاق قدرات الإنسان.  
Unlocking human potential.

## Computing & Information Technology - Poster Display

<http://doi.org/10.5339/qfarc.2018.ICTPD998>

### ThreatBased Security Risk Evaluation in the Cloud

Armstrong Nhlabatsi\*, Khaled Khan, Noora Fetais, Rachael Fernandez, Jin Hong, Dong Seong Kim

Qatar University  
\* Armstrong.Nhlabatsi@qu.edu.qa


Research Problem Cyber attacks are targeting the cloud computing systems, where enterprises, governments, and individuals are outsourcing their storage and computational resources for improved scalability and dynamic management of their data. However, the different types of cyber attacks, as well as the different attack goals, create difficulties providing the right security solution needed. This is because different cyber attacks are associated with different threats in the cloud computing systems, where the importance of threats varies based on the cloud user requirements. For example, a hospital patient record system may prioritize the security of cyber attacks tampering patient records, while a media storage system may prioritize the security of cyber attacks carrying out a denial of service attack for ensuring a high availability. As a result, it is of paramount importance to analyze the risk associated with the cloud computing systems taking into account the importance of threats based on different cloud user requirements. However, the current risk evaluation approaches focus on evaluating the risk associated with the asset, rather than the risk associated with different types of threats. Such a holistic approach to risk evaluation does not show explicitly how different types of threats contribute to the overall risk of the cloud computing systems. Consequently, This makes it difficult for security administrators to make fine-grained decisions in order to select security solutions based on different importance of threats given the cloud user requirements. Therefore, it is necessary to analyze the risk of the cloud computing systems taking into account the different importance of threats, which enables the allocation of resources to reduce particular threats, identify the risk associated with different threats imposed, and identify different threats associated with cloud components. Proposed Solution The STRIDE threat modeling framework (short for STRIDE) is

© 2018 The Author(s), licensee HBKU Press. This is an open access article distributed under the terms of the Creative Commons Attribution license CC BY 4.0, which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

دار جامعة حمد بن خليفة للنشر  
HAMAD BIN KHALIFA UNIVERSITY PRESS



Cite this article as: Nhlabatsi A et al. (2018). ThreatBased Security Risk Evaluation in the Cloud. Qatar Foundation Annual Research Conference Proceedings 2018: ICTPD998  
<http://doi.org/10.5339/qfarc.2018.ICTPD998>.



proposed by Microsoft, which can be used for threat categorization. Using the STRIDE, we propose a threat-guided risk evaluation approach for the cloud computing systems, which can evaluate the risk associated with each threat category from the STRIDE explicitly. Further, we utilize seven different types of security metrics to evaluate the risk namely:  $\textit{component}$ ,  $\textit{component-threat}$ ,  $\textit{threat-category}$ ,  $\textit{snapshot}$ ,  $\textit{path-components}$ ,  $\textit{path-threat}$ , and  $\textit{overall asset}$ .  $\textit{Component}$ ,  $\textit{component-threat}$ ,  $\textit{threat-category}$ , and  $\textit{snapshot}$  risks measure the total risk on a component, component risk for a particular threat category, total snapshot risk for a single threat, and the total risk of the snapshot considering all threat categories, respectively.  $\textit{Path-components}$ ,  $\textit{path-threat}$ , and  $\textit{overall asset}$  measure the total risk of components in an attack path, the risk of a single threat category in the attack path, and the overall risk to an asset considering all attack paths, respectively. These metrics makes it possible to measure the contribution of each threat category to the overall risk more precisely. When a vulnerability is discovered in a component (e.g. a Virtual Machine) of the Cloud deployment, the administrator first determines which types of threats could be posed should the vulnerability be successfully exploited, and what would be the impacts of each of those threats on the asset. The impact assignment of each threat type is weighted depending on the importance of the component. For example, a Virtual Machine (VM) that acts a Web Server in a medical records management application could be assigned a higher weighting for  $\textit{denial-of-service}$  threats because if such attacks are successfully launched then the rest of the VMs that are reached through the Web Server will be unavailable. On the other hand, a vulnerability discovered in a VM that hosts a database of medical records would be rated highest impact for  $\textit{information disclosure}$  because if it is compromised confidentiality of the medical history of patients will be violated. By multiplying the probability of successfully exploiting the vulnerability with the threat impact, we compute the risk of each threat type. The variation in the assignment of impact for different threat types enables our approach to compute risks associated with the threats - thus empowering the security administrator with the ability to make fine-grained decisions on how much resources to allocate for mitigating which type of threat and which threats to prioritize. We evaluated the usefulness of our approach through its application to attack scenarios in an example Cloud deployment. Our results show that it is more effective and informative to administrators compared to asset-based approaches to risk evaluation.