Poster: Multi-Layer Threat Analysis of the Cloud

Salman Manzoor
Lancaster University
United Kingdom
s.manzoor1@lancaster.ac.uk

Antonios Gouglidis
Lancaster University
United Kingdom
a.gouglidis@lancaster.ac.uk

Matthew Bradbury
Lancaster University
United Kingdom
m.s.bradbury@lancaster.ac.uk

Neeraj Suri
Lancaster University
United Kingdom
neeraj.suri@lancaster.ac.uk

ABSTRACT

A variety of Threat Analysis (TA) techniques exist that typically target exploring threats to discrete assets (e.g., services, data, etc.) and reveal potential attacks pertinent to these assets. Furthermore, these techniques assume that the interconnection among the assets is static. However, in the Cloud, resources can instantiate or migrate across physical hosts at run-time, thus making the Cloud a dynamic environment. Additionally, the number of attacks targeting multiple assets/layers emphasizes the need for threat analysis approaches developed for Cloud environments. Therefore, this proposal presents a novel threat analysis approach that specifically addresses multi-layer attacks. The proposed approach facilitates threat analysis by developing a technology-agnostic information flow model. It contributes to exploring a threat's propagation across the operational stack of the Cloud and, consequently, holistically assessing the security of the Cloud.

CCS CONCEPTS

• **Security and privacy** → *Formal security models*; *Security services*; **Information flow control**.

1 INTRODUCTION

The Cloud offers access to a pool of geo-distributed resources (e.g., network, storage, compute) that can be provisioned dynamically at run-time to satisfy the user/application requirements. Additionally, multiple technologies/services co-exist in the Cloud to provide functionality and flexibility in resource management, making the Cloud a complex environment with a complex threat landscape. This is evidenced by the increasing number of attacks and security breaches targeting the Cloud. For example, some attacks led to the leakage of users' confidential information [3] while other attacks have targeted the availability of the Cloud [9].

The process of threat analysis is advocated to identify a system's exposure to threats. Therefore, multiple threat analysis approaches for the Cloud have been proposed to explore threats targeting a specific component in the Cloud [1, 10]. Alternate techniques, such as attack trees/graphs, have also been utilized to explore potential attack paths in the Cloud [2].

Existing approaches perform effective threat analysis [2, 5]. However, they are either limited to identifying threats in the targeted asset or assume that the system under consideration is a static environment. Therefore, the applicability of existing schemes to dynamic environments, e.g., the Cloud, is hindered due to these limitations. We address these challenges by proposing a novel threat analysis approach that facilitates Cloud providers in exploring threats and their propagation, considering the inherent elasticity of the Cloud. Furthermore, the proposed approach is technology-agnostic to the underlying Cloud technologies, enabling the analysis of the impact of multiple threats across different layers and services in the Cloud. To develop a threat analysis scheme that is technology-agnostic, a new information flow model is proposed that captures the functional behavior of the Cloud.

Differing from contemporary models, our emphasis is on the interconnection among the services and information flow rather than performance measurements. The information flow model is based on rules that describe the baseline behavior of the Cloud. First, the functional behavior of the Cloud is validated to enumerate baseline operations, and thereafter, threats are inserted to determine their impact on the Cloud behavior. It reveals the changes in the sequence of the transitions, which supports exploring the propagation of threats across the Cloud.

Overall, the main contributions are:

(1) A functional Cloud model capable of representing the operations of a Cloud by abstracting the services from real-world Cloud deployments.
(2) A technology-independent information flow model capturing the dynamic service interactions and consequently representing the functional behavior of the Cloud.
(3) A path-illustrative approach to profile the flow of threats and analyze their impact on targeted services.

2 METHODOLOGY

The proposed approach is developed as a progression of three building blocks as depicted in Figure 1. An overview of each of these blocks is presented in the following subsections.

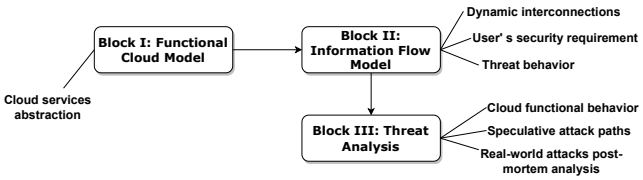

Figure 1: Blocks of the proposed methodology

2.1 Functional Cloud Model

A considerable body of research exists for modeling the application in the Cloud to analyze its behavior and investigate security and performance issues [4, 8]. However, ascertaining threat progression in the Cloud requires modeling the functionality of the Cloud that captures interactions among services. Thus, we define an abstract model for the Cloud emphasizing the interactions of services during the life cycle of a VM [7]. The Cloud model shown in Figure 2 illustrates a generalized 3-layered (Control, Infrastructure, and Storage) architecture. The primary function of the control layer is to authenticate users, allowing them access to their VMs and enabling

them to request new VMs. The infrastructure layer binds virtual resources to the physical hosts and provides a coherent view of the resources to the user by linking resources belonging to the same user. The storage layer provides storage capabilities for the data.

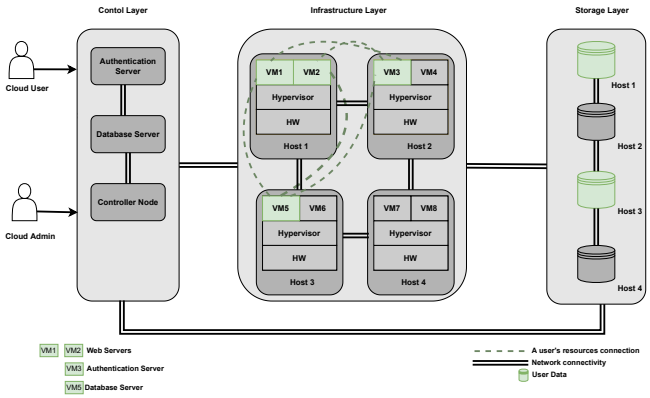

Figure 2: Multi-layer architecture of the Cloud

The services and their interactions during the VM life cycle are translated into a technology-agnostic information flow model. The information flow model forms the basis for understanding the interplay between services' interactions and the progression of the threat in the Cloud.

2.2 Information Flow Model

This building block of the methodology focuses on developing a technology-agnostic information flow model. Among the primary function of the Cloud is running a VM. Therefore, the information flow among the service during the VM life cycle is specifically targeted. The model is shown in Figure 3. The basic premise is developing a model independent of the vendor and technological characteristics. Additional specifications for the information flow model are: (a) the model should represent the functional behavior of the Cloud and the specified threats, and (b) identify violations from the sequence of transitions caused by the threats by determining any modifications in the proper functioning of the Cloud. The model is developed using Petri Nets, designed explicitly for concurrent and distributed systems. Specifically, each transition in the Petri Nets is enabled and fired locally, i.e., as soon as the local precondition is satisfied, the transition is fired without considering the global state of the system. For instance, the authentication is triggered as soon as the user enters the credentials. If the credentials are valid, the users are transitioned to the next state, where they can access VMs associated with them.

We have described the first two building blocks of the proposed methodology, i.e., modeling the Cloud functionality and developing an information flow model. The final block in the methodology is to perform threat analysis which is explained in the following section.

2.3 Threat Analysis

The third block of the proposed methodology targets assessing the impact of threats on the services of the Cloud. We evaluate the effects of threats at multiple services to identify their potential to (a) propagate in the Cloud and (b) the possibility of exploiting a combination of threats to violate a user's security requirement.

To perform threat analysis, the relevant preconditions of the threats are inserted into multiple transitions. These transitions are fired if a threat's condition is satisfied and we identify any modifications in the Cloud behavior. To explore the progression of the threat in the Cloud, CPN tools [6] are used to simulate the Cloud model. By inserting threats across the different layers of the Cloud, we can investigate the cause-effect relationship between threats and services. The proposed methodology can be used to perform speculative threat analysis using vulnerabilities reported in publicly available databases, e.g., NVD, to identify attack paths. An example of the generated attack graph from the publicly disclosed vulnerabilities is shown in Figure 4.

Path 1: A successful exploitation of vulnerabilities in this path leads to obtaining resources from inactive users. To achieve this, either vulnerability CVE-2013-4222 or CVE-2012-4457 is exploited, enabling attackers to access an authorization token to authenticate themselves and access the victim's resources.

Path 2: This path demonstrates combining different vulnerabilities to create a larger impact on the Cloud. For example, the attackers can exploit the vulnerability (CVE-2014-5251) at the control service to bypass access control restrictions and identify restricted projects. To retain access to these restricted projects, an attacker exploits the vulnerability (CVE-2018-14432), enabling the attacker to access the projects with an expired authorization token.

Path 3: In path 3b, a combination of CVE-2014-9623 with CVE-2014-0134 at the hypervisor results in either reading the computer host file (breaching the confidentiality of the user) or potentially causing the VM to migrate. In the latter case, new attack surfaces are exposed to attackers, e.g., exploiting CVE-2018-04635 during VM migration can be used to intercept network traffic. This path depicts that the inherent elasticity of the Cloud can open new attack surfaces at run-time.

3 CONCLUSION

We have presented a threat analysis methodology that furthers the state-of-the-art gap by incorporating the Cloud's elasticity into the threat analysis process. Our methodology can be used to explore threats considering the operations of the Cloud, e.g., VM migration. Furthermore, it is independent of the underlying Cloud technologies. NVD threats have been used to demonstrate the capability of the methodology in performing threat analysis.

ACKNOWLEDGMENTS

This research was supported, in part, by EC H2020 CONCORDIA GA No. 830927 and by the UKRI Trustworthy Autonomous Systems Node in Security [EPSRC grant EP/V026763/1].

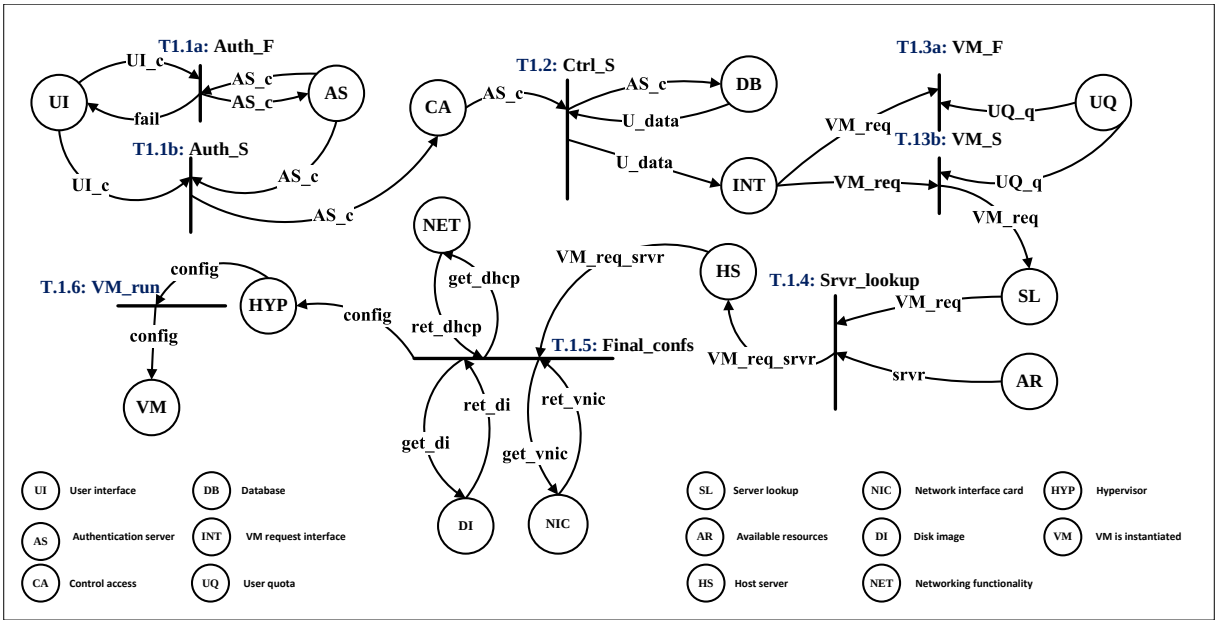

Figure 3: Information flow model using Petri Nets

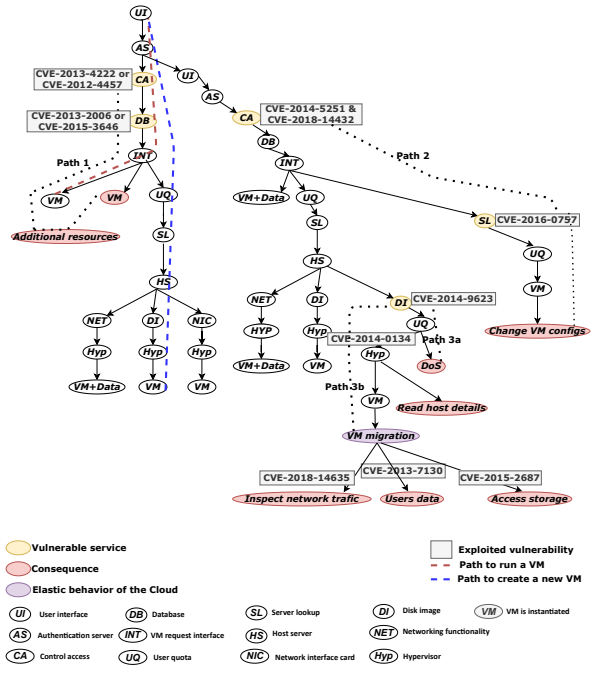

Figure 4: Attack paths based on the selected vulnerabilities

REFERENCES

[1] Hesham Abusaimeh. 2020. Security Attacks in Cloud Computing and Corresponding Defending Mechanisms. *International Journal of Advanced Trends in Computer Science and Engineering* 9 (2020), 4141–4148. https://doi.org/10.30534/ijatcse/2020/243932020

[2] Nawaf Alhebaishi, Lingyu Wang, Sushil Jajodia, and Anoop Singhal. 2016. Threat Modeling for Cloud Data Center Infrastructures. In *International Symposium on Foundations and Practice of Security*. Springer International Publishing, Québec City, Québec, Canada, 302–319. https://doi.org/10.1007/978-3-319-51966-1_20

[3] Benjamin Edwards, Steven Hofmeyr, and Stephanie Forrest. 2016. Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity* 2, 1 (12 2016), 3–14. https://doi.org/10.1093/cybsec/tyw003 arXiv:https://academic.oup.com/cybersecurity/article-pdf/2/1/3/26672851/tyw003.pdf

[4] Archana Ganapathi, Yanpei Chen, Armando Fox, Randy Katz, and David Patterson. 2010. Statistics-driven Workload Modeling for the Cloud. In *International Conference on Data Engineering Workshops*. IEEE, Long Beach, CA, USA, 87–92. https://doi.org/10.1109/ICDEW.2010.5452742

[5] Shareeful Islam, Moussa Ouedraogo, Christos Kalloniatis, Haralambos Mouratidis, and Stefanos Gritzalis. 2018. Assurance of Security and Privacy Requirements for Cloud Deployment Models. *IEEE Transactions on Cloud Computing* 6 (2018), 387–400. https://doi.org/10.1109/TCC.2015.2511719

[6] Kurt Jensen and Lars Kristensen. 2009. *CPN ML Programming*. Springer Berlin Heidelberg, Berlin, Heidelberg, Chapter 3, 43–77. https://doi.org/10.1007/b95112_3

[7] Xin Jin, Qixu Wang, Xiang Li, Xingshu Chen, and Wei Wang. 2019. Cloud Virtual Machine Llifecycle Security Framework based on Trusted Computing. *Journal of Tsinghua Science and Technology* 24 (2019), 520–534. https://doi.org/10.26599/TST.2018.9010129

[8] Fumio Machida, Ermeson Andrade, Dong Kim, and Kishor Trivedi. 2011. Candy: Component-based Availability Modeling Framework for Cloud Service Management Using SysML. In *Proceedings of the International Symposium on Reliable Distributed Systems*. IEEE, Madrid, Spain, 209–218. https://doi.org/10.1109/SRDS.2011.33

[9] Mohammad Masdari and Marzie Jalali. 2016. A Survey and Taxonomy of DoS Attacks in Cloud Computing. *International Journal of Security and Communication Networks* 9 (2016), 3724–3751. https://doi.org/10.1002/sec.1539

[10] Daniele Sgandurra and Emil Lupu. 2016. Evolution of Attacks, Threat Models, and Solutions for Virtualized Systems. *Comput. Surveys* 48 (2016), 1–38. https://doi.org/10.1145/2856126