Exploiting SDN Approach to Tackle Cloud Computing Security Issues in the ATC Scenario

Gabriella Carrozza[1], Vittorio Manetti[1], Antonio Marotta[2], Roberto Canonico[2], and Stefano Avallone[2]

[1] SESM s.c.a.r.l., Via Circumvallazione esterna di Napoli, Giugliano in Campania, 80014 Naples, Italy
Email: gcarrozza, vmanetti {@sesm.it}
[2] University of Napoli Federico II, Dipartimento di Elettronica e Tecnologie dell'Informazione, Via Claudio, 21 - 80125 - Napoli, Italy
Email: stavallo, roberto.canonico, antonio.marotta {@unina.it}

Abstract. Cloud Computing has been receiving great attention in the last few years due to the benefits it provides in terms of flexibility, scalability, virtualization and service provision. Nevertheless, many companies remain reluctant to such a cutting-edge technology due to the serious security issues affecting virtualized environments, especially in critical application scenarios where high safety and dependability levels are required. This work is aimed at discussing and presenting the main security threats for cloud computing infrastructures, as well as proposing a novel architecture in charge of reacting to security attacks in Infrastructure as a Service platforms. The basic idea is to migrate the attacked virtual appliance and to reconfigure the network by means of Software Defined Networking approach. The paper presents the architecture we have in mind and that will be deployed and validated against a real world distributed Air Traffic Control system, for which missing dependability and security targets would result in huge business and human losses.

1 Introduction

Cloud Computing (CC) is a model for enabling flexible and ubiquitous network access to a pool of shared computing resources. The Infrastructure as a Service (IaaS) service model has paved its way as a scalable, efficient and flexible solution since it allows consumers to deploy virtual resources such as networks, storage and virtual machines without any dependence on the physical infrastructure. In the case of private clouds, the cloud infrastructure and the shared resources are operated solely for a given organization which can even let cloud maintenance to third parties. By using the cloud, critical systems could be tested and reproduced, thus improving their dependability. Also, they can be rapidly reconfigured in case of failure by leveraging resources redundancy which characterizes any

cloud infrastructure, with a direct return on business. Notwithstanding these incomparable benefits, CC adoption in critical industry is hampered by the security pitfalls it still exhibits, as well as by the the lack of mechanisms intended at increasing isolation and protection from internal and external threats. Cloud security issues have been widely studied by researchers in the last few years, in order to find effective solutions that can encourage critical systems industries to move towards such architectures. This work comes from an industrial experience in the Air Traffic Control (ATC) field, in which a private cloud testbed has been set up according to the IaaS service model to reproduce real systems in house, as well as to investigate the possibility of interconnecting remote ATC centers through the cloud. It presents a novel architecture for detecting malicious activities and automatically implementing recovery strategies in the cloud infrastructure, when one of the virtual nodes is compromised. The idea is to define and realize mechanisms based on the so-called Software Defined Network (SDN) paradigm, thanks to which the forwarding plane is decoupled from the control plane, and the network behaviour can be easily programmed through a global view of the network itself. By automatically migrating virtual resources from the compromised node in a remote datacenter we are confident to increase the overall system security level. The rest of the paper is organized as follows. Section II formalizes some of the most relevant cloud security issues, while section III briefly introduces the Software Defined Networking (SDN) approach and one of its implementation, namely the OpenFlow protocol. Section IV presents the state of the art and discusses the main related works that propose the use of such an approach for security purposes. Section V illustrates the proposed architecture for anomalies detection and for the implementation of the mitigation strategies. Last, section VI describes the real world critical system representing the case study for the architecture.

2 Security Issues in IaaS Cloud Computing Environment

A lot of papers in the literature propose interesting countermeasures to the most common security flaws in the IaaS Cloud Computing environments. One of the most discussed and well-known issues is data protection and availability: when the user entrusts his data to the cloud, he is not aware of the location where they will be stored and the way they will be treated. Different ways to use encryption are proposed, such as the one based on attributes: the decision of which users can decrypt a ciphertext is taken on the basis of the attributes and policies associated with the

message and the user.
Although the great advantages that come along with the application of cloud computing, new security challenges related to the virtualization must also be taken into account. One of the most serious problem in the cloud infrastructure is related to the VMs image management risk: before even securing the running VM and the customer data, it is needed to be sure about the integrity of the virtual image which is about to be spawned in the cloud infrastructure. If an insider attacker gets access to the location where the VM images are stored, he has the chance to modify the way VMs will behave according to his malicious intention. That is why VMs images should be patched for security reasons and scanned with the aim of finding malicious software. Another important task is the verification of the running VMs integrity and the behaviour of the components of the platform. The cloud infrastructure gives the chance to the end user to orchestrate, provision and manage all the implemented services through a set of APIs, that constitute the unique entry point for users to interact with the platform. Nevertheless, if the exposed APIs are vulnerable, there may arise lots of security threats, such as: clear text authentication, anonymous access, reusable token and weak access controls. In this work, the focus is on a private cloud IaaS for which dependability and security issues are fewer than in public clouds. Here, indeed, network and data are stored and managed by third parties and off premises, differently from a private cloud environment. However, there still arise internal security threats: in this case, insider attacks come from the cloud platform users or the administrator himself.

3 OpenFlow and Software Defined Networking

Software Defined Networking (SDN) paradigm, which has rapidly changed the perspective of doing network research, is based on a sharp distinction between the infrastructure layer, composed by network devices, and the control layer where the network intelligence is deployed (the OpenFlow Controller). Using this approach, the forwarding plane is decoupled from the control plane, and the network behaviour can be easily programmed through a global view of the network. The OpenFlow Protocol constitutes the interface between the two layers, allowing to control and to define traffic management strategies to be performed by the switch devices in the infrastructure. OpenFlow is also attracting lot of interest in cloud computing platforms as a leading technology for implementing Networking as a Service. The need to have fully-virtualized networks becomes the

main focus of the cloud computing community: being the hypervisor the heart of hardware-virtualization, it is needed to find solutions allowing to reach the same level of abstraction with physical network resources. Indeed OpenFlow can be used to guarantee the programmability of the networking level for the VMs. Concerning security requirements, the dynamic nature of CC systems makes the traditional solutions inefficient rising the need to find new approaches for protecting the infrastructure from different kind of attacks. OpenFlow can be considered as a leading technology for implementing an architecture that is aware of dynamic application security policies at a low cost.

4 Related Work

Some recent works propose OpenFlow as an effective solution for security and introduce OpenFlow-based platforms for implementing several security techniques. In [5], authors argue that the SDN paradigm can make the implementation of traffic anomaly detection easier by using the well-known NOX [6] OpenFlow controller in SOHO (small office/home office) networks. They implement four different anomaly detection algorithms as applications on the controller and point out that SDN allows to implement line-rate detection of network vulnerabilities exploitation and also risk mitigation.

Braga *et al.* [7] face a well-known security issue, which is the Distributed Denial of Service. Their proposal aims at minimizing the overhead due to the extraction of network features used in the detection process, by requesting the flows to the OF switches.

Wang *et al.* [8] suggest a flexible security management architecture for large-scale production networks to overcome the drawbacks of the existing static solutions, by considering the peculiarities of data center networks. The architecture they propose is composed by a control component having the view of both the global state of the network, and the designed security policies, besides one or more security elements which are responsible for detecting anomalies in the traffic patterns. The programmability of the network flows enables the check of the global security policies and the fast reaction to alarms. However, such a distributed architecture requires a deep analysis to verify if the introduced latency (caused by the presence of the security elements) does affect user experience.

This work differs from the ones proposed in the literature, in the sense that it proposes an architecture in which the SDN paradigm is used to

implement mitigation and recovery strategies in case of disasters and security breaches.

5 Description of The Proposed Architecture

Our idea is to design and implement an OpenFlow-based architecture in order to fit the dynamic nature of cloud computing infrastructures. It relies on the OpenvSwitch [9] technology, that is used as the virtual switch to provide connectivity to the virtual guests. OpenvSwitch implements a number of interesting features that led us to choose it since the architecture we are introducing relies on VLANs to guarantee level-2 isolation, and on the use of vNICs in bonding configuration for failover reasons. Moreover, the OpenvSwitch is OpenFlow 1.0 protocol compliant. We also evaluated some of the available open source OpenFlow Controllers and our choice fell on Floodlight [10], a Java event-based Controller. The features we took into account are the modularity of its core functionalities, the availability of REST APIs (which makes it consistent with the CC services provisioning) and its performances compared to the other available controllers.

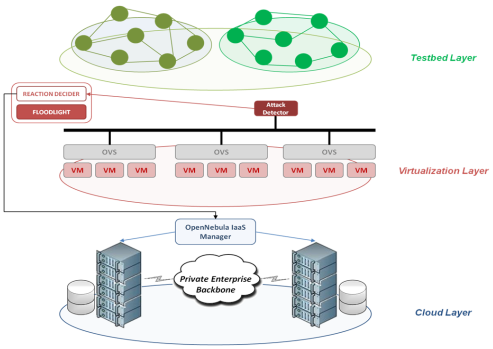

Fig. 1. Different views of the architecture

As shown in Fig. 1, at the switch edge on the virtualization layer we use an Attack Detector agent, which is responsible of sniffing and analysing all the traffic coming from and arriving on the VLANs of the virtual networks. When abnormal activity is detected, the agent sends alerts through a secure channel (a Transport Layer Security socket) to a central Reaction Decider which is implemented on the OpenFlow Controller. The latter is also in charge of programming the flow tables of the

OpenvSwitches and selecting the best countermeasure to adopt in relation to the severity level of the attack and the number of affected nodes. Starting from the assumption that the Cloud infrastructure is made of geographically distributed datacenters (as you can see in the cloud layer), once an attack is detected, a mitigation and recovery strategy for the involved nodes is triggered. Such a strategy consists in dynamically activating a migration of the virtual guests under attack in a remote datacenter belonging to the same cloud infrastructure by interacting with the cloud platform manager. Once the migration process is terminated, the Floodlight Controller is in charge of programming the OpenvSwitches' flow tables in order to redirect the traffic related to the migrated node towards its new location. The aim is to guarantee transparency of the virtual appliance, so that a legitimate user or machine can access the services hosted on the attacked node without being aware of the migration process. Moreover, in order to further increase network security in the connection between the distributed data-centers, we use a mechanism that splits packets into parts and then redirects them to disjoint paths, so that an intruder is not able to reconstruct the flowing traffic. This is done by using a traffic engineering mechanism based on the MPLS (MultiProtocol Label Switching) technology [11]. The confidentiality is guaranteed because if a malicious user is able to intercept the traffic between two nodes of the network passing through different paths, he should be aware of the splitting mechanism in order to reconstruct the original message from the parts he has collected. Besides the mechanism we use is not overhead-heavy compared to the use of end-to-end encryption.

6 Case Study: a Testbed for Air Traffic Control

Air Traffic Control (ATC) are very demanding and software-intensive systems. They are safety critical, highly distributed and hard real time. Among the dimensional architectural requirements of this type of systems there are ultrahigh availability (6 nines), high performance, modifiability, scalability and usability. In the ATC field, ATC centers belonging to the same system are often deployed over different cities in a given country, either for fault tolerance purposes and remote connection needs at country level. For this reason, CC represents the key technology these industries need: first, setting up an extended enterprise private CC platform allows to connect geographically distributed ATC centers for dependability purposes, e.g., by realizing a failover configuration among centers in order to increase overall system availability. Second, it can be leveraged

in pre-operational phases by setting up testbed platforms in the cloud to perform distributed testing campaigns on complex systems from different premises, to reproduce real world scenarios in house and to validate the system in a number of operational use cases.
The use case scenario in which we intend to test and evaluate the proposed OpenFlow-based architecture is a Private Enterprise CC Infrastructure that hosts an Area Control Center (ACC), the main operative center in an ATC system. ACC is the infrastructure responsible for controlling aircraft in a particular volume of airspace at high altitudes between airport approaches and departures. By using this case study, we aim at validating our architecture on a very complex real world system which is one of the main industrial assets. In order to perform a preliminary assessment of the whole architecture, we implemented a proof of concept deploying an ACC (accounting for a total of 32 nodes) on a Private IaaS Infrastructure realized by using the OpenNebula [14] OpenSource solution. We simulated some Distributed Denial of Service attacks and used the Snort [12] Intrusion Detection system to trigger the mitigation strategy already presented. We are now investigating the presence of vulnerabilities of the testbed nodes which can be exploited as an attack surface. To this aim we exploited a linux-based distribution, namely Backtrack [13], which is widely used for penetration testing and security assessment.

7 Conclusions and Future Work

CC perfectly fits IT companies' needs for elasticity and scalability by extremely reducing CapEx/OpEx costs and datacenter start-up time. Anyway there are still open research issues about the security level and performances achievable when moving services in the cloud. In this work we built a private Enterprise CC platform to host an entire Air Control Center and then we designed an architecture with the aim of automatically reacting to attacks towards the ACC nodes. For the proof of concept, we used a simple DDoS attack which is detected by the agent and the raised alarm is sent to a central decider, which is in charge of triggering the mitigation strategy. The decider is implemented on an OpenFlow Controller which has a global view of the network and it interacts with the cloud manager in order to activate the migration of the attacked node in a remote data-center. In the connection between the two data-centers, confidentiality is guaranteed thanks to the use of an MPLS-based splitting mechanism which makes the eavesdropping of the packets very hard to possible attackers. Finally, the Controller can then reconfigure traffic

flows in order to guarantee the transparency of the location of the node after the mitigation process. Our future work consists in an evaluation of the proposed architecture and the use of classical anomaly detection with other mechanisms aimed at identifying malicious patterns on a per-user or per-application basis.

8 Acknowledgements

This work has been partially supported by MIUR under Project "SVEVIA" (PON02_00485_3487758) of the public-private Laboratory "COSMIC" (PON02_00669).

References

1. Nick McKeown et al., *OpenFlow: Enabling Innovation in Campus Networks*, ACM SIGCOMM Computer Communication Review archive, Volume 38 Issue 2, April 2008. Pages 69 - 74
2. Gundeep Singh Bindra et al., *Cloud Security: Analysis and Risk Management of VM Images* . 2012 International Conference on Information and Automation (ICIA), 6-8 June 2012. Page(s): 646 - 651
3. Flavio Lombardi, Roberto Di Pietro, *Secure Virtualization for Cloud Computing*. Journal of Network and Computer Applications. Volume 34 Issue 4, July 2011. Pages 1113 - 1122
4. Ting-ting Yu, Ying-Guo Zhu, *Research On Cloud Computing And Security*. 2012 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science (DCABES), 19-22 Oct. 2012. Pages 314 - 316
5. Mehdi et al., *Revisiting Traffic Anomaly Detection Using Software Defined Networking*. Proceedings of the 14th International Symposium, RAID, 20-21 September 2011. Pages: 161 - 180
6. Nox Controller, `http://www.noxrepo.org/`
7. Rodrigo Braga et al., *Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow*. 2010 IEEE 35th Conference on Local Computer Networks (LCN), 10-14 Oct. 2010. Pages: 408 - 415
8. Kai Wang et al., *LiveSec: Towards Effective Security Management in Large-scale Production Networks*. 2012 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW), 18-21 June 2012. Pages: 451 - 460
9. `http://openvswitch.org/`
10. Floodlight Controller, `http://floodlight.openflowhub.org/`
11. Avallone Stefano et al., *A Splitting Infrastructure For Load Balancing And Security in an MPLS Network*. 3rd International Conference on Testbeds and Research Infrastructure for the Development of Networks and Communities, 21-23 May 2007. Pages: 1 - 6
12. Roesch M. *Snort, Lightweight Intrusion Detection For Networks*. In 13th USENIX Systems Administration Conference (LISA 99), Seattle, WA, Nov. 1999.
13. `http://www.backtrack-linux.org/`
14. `http://opennebula.org/`