Srinivas Naik, Rajesh Adepu / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 3, May-Jun 2013, pp.762-765

Focus on Nefarious Behavior threats in Cloud

Srinivas Naik*, Rajesh Adepu**
*(Department of Computer Science, Princeton College of Engineering, Hyderabad- 501 301)
** (Department of Computer Science, Princeton College of Engineering, Hyderabad – 501 301)

ABSTRACT

Computing over cloud is emerging into internet space with virtual platform based applications and attracting users with its effortless deployments. This enhanced features of cloud computing has withdrawn attention of intruders and has made prone to threats due to which it has lead to security concerns. As more services migrate to cloud architecture the cloud will become a more appealing target for cyber criminals. This journal discusses current threats to cloud computing as well as summarizing the currently available detection systems for malware in the cloud.

Keywords – *Cloud threats, Malware, Security, Threat Detection,*

INTRODUCTION

Cloud Computing is emerging as the de facto service model for modern enterprises. Cloud Services such as Apple's iCloud, and established products, such as Dropbox, have proven that remote storage and seamless access to data across multiple devices are popular features among consumers. In the future we will see an increase in the reliance of cloud computing as more and more consumers move to mobile platforms for their computing needs.

Cloud technologies are made possible through the use of virtualization in order to share physical server resources between multiple virtual machines (VMs) and resources as in FIG 1. The advantages of this approach include an increase in the number of clients that can be serviced per physical server and the ability to provide infrastructure as a service (IaaS).

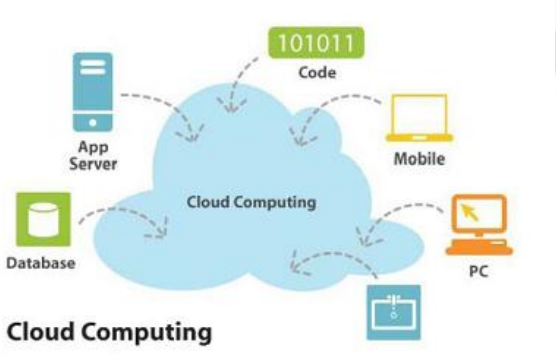

Fig 1

Disadvantages include a more complex software stack and a relatively small understanding of security issues. The security issues of regular operating systems (OSs) are well known due to decades of testing and experience in this area. Security breaches now commonly occur at the application level and are less commonly due to a flaw in the OS itself. Exceptions to this are usually due to the inclusion of new features into an OS kernel either to provide new functionality or to support new hardware. Virtualisation is not only subject to the security issues of applications and operating systems, but also introduces new security issues that are not as well understood, such as the sharing of hardware resources between VMs.

Clouds themselves are composed of a number of virtualized environments which are networked together. The compact topology of this network and the high probability of relative homogeneity across VMs create an ideal environment for rapid malware propagation. Protecting against malware in the cloud therefore requires a certain level of coordination between virtualized environments if threats are to be reliably detected and dealt with.

In this journal we review previous work on malware detection, both conventional and in the presence of virtualization in order to determine the best approach for detection in the cloud. We also argue the benefits of distributing detection throughout the cloud and present a novel approach to coordinating detection across the cloud. Below phases provides background to the research area, specifically: cloud technologies, security in the cloud, malware detection and detection in the cloud. Further phase will focuses on malware detection at the hypervisor level and introduces our work in this area.

BACKGROUND

A. Cloud Technologies

Cloud computing is an umbrella term for services that offer offsite computing and storage. There are three main types of cloud computing: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). Not all of these require virtualisation, SaaS for example could be implemented as a typical client/server service, but virtualisation allows hardware to be better utilised and enables the infrastructure itself to be hired out, as is the case in IaaS.

There are various implementations of virtualisation, but they areall built on the concept of virtual machines (VMs). The VMs exist as a virtual computer system and each have their own operating system (OS) and applications. The VMs are managed by a virtual machine monitor (VMM), which is sometimes referred to as a hypervisor.
Virtualization products such as VM Ware ESXi, Xen Hypervisor, KVM Hypervisor, etc are examples of bare-metal hypervisors. Another form of virtualization exists at application level within an OS, known as hosted hypervisors. Basically referring it as type-I and type-II hypervisors respectively. Type-I hypervisors are focused in this journal due to their use for cloud services.

The cloud itself is usually composed of many physical server machines, or hardware nodes. These nodes each have their own VMM hosting some VMs. There are a number of reasons for having multiple hardware nodes, the first being limited resources. It is important not to run too many VMs on a single hardware node because of the limited size of RAM and disk space available. With more than one physical machine it is possible to load balance based on CPU, RAM or network utilisation. Another reason for multiple hardware nodes is redundancy. If a fault is detected on a server the VMs can be migrated to another server before it goes down. This is achieved in the same way as load balancing, but solves a slightly different problem.

B. Security in the Cloud

Previous work on cloud security has suggested that there are a number of security issues associated with cloud computing. Below are the following threats to cloud computing:
Threat 1: Data Breaches
Threat 2: Data Loss or Leakage
Threat 3: Account or Service Hijacking
Threat 4: Insecure Interfaces and APIs
Threat 5: Denial of Service
Threat 6: Malicious Insiders
Threat 7:Abuse and wicked Use of Cloud Computing
Threat 8: Unknown Security Profile
Threat 9: Shared Technology Issues

Of these, threats 3, 4 and 9 are directly related to malware. Account and Service Hijacking can be targeted by XSS malware for example to perform unauthorized activities. Insecure Interfaces and APIs would allow malware running on one VM to execute code or access data on another VM. Shared Technology Issues include the sharing of physical memory between multiple VMs.
This could lead to a new form of worm that, instead of spreading via networks, could spread by writing to the memory owned by another VM. This kind of propagation would be unique to virtualized environments. Few Threats could be indirectly related to malware, for example in the deployment of malware by malicious individuals. Few vulnerabilities fall into Denial of Service (Threat 5) when a specific input gets triggered. Malicious Insiders (Threat 6) is a similar threat, but instead of being customers the malicious individuals are instead employees of the cloud providers. Abuse and Nefarious Use of Cloud Computing (Threat 7) is possible due to the relative anonymity of cloud subscription. Malicious organizations could use cloud space as a platform to launch attacks.

Account Hijacking (Threat 3) is a common threat throughout the Internet and would allow malicious individuals to perform similar actions to threats 1 and 4. Threats 2 and 8 are not related to malware and are concerned with data loss, which is a natural occurance in computer systems, and the opacity that is inherent in the cloud. Data Loss or Leakage is exacerbated in virtualised environments because the system as a whole is more complicated than a single OS computer system. Unknown Security Profile is in contrast to in-house servers where the implementation of data storage and networking is known. A customer has no guarantee that the security measures promised by a cloud provider are actually in place; there is a level of opacity that is not an issue in alternatives to the cloud.
The below table briefs the level of relevance of existing threats (2013-Q1)

Threat Description	Current Relevance (%)
Data Breaches	91
Data Loss or Leakage	91
AccountorService Hijacking	87
Insecure Interfaces and APIs	90
Denial of Service	81
Malicious Insiders	88
Abuse and wicked Use of Cloud	84
Unknown Security Profile	81
Shared Technology Issues	82

Table. 1

TABLE 1 explores the relevance of threats that has been studied in current quarter. When using software, especially complex software, there is always a risk of an improper implementation or configuration, more so than when using hardware for the same task. Take for example a simple server. The remotely exploitable vulnerabilities are confined to the OS and application software. The same server implemented as a VM is subject to the vulnerabilities of the VMM, OS and applications. It can therefore be assumed that hardware sharing under the management of software is inherently less secure than distinctly separate machines.

C. Malware Detection

Malware detection has been an important issue in computing since the late '80s. Since then the predominant method of malware detection is to scan a computer system for infection by matching malware signatures to files on the computer. Although detection of known samples is extremely reliable, signature based detection only works for malware that has been obtained, analyzed and a suitable signature identified. It has to be understood that signature based detection can be thwarted by analysing the malware instructions and identifying the instructions that comprise the signature. By altering this specific portion of code it is possible to evade detection; in effect the process takes a known sample and converts it into an unknown sample.
Another downside to signature based detection is the maintenance of the signature database. With the constant evolution of malware and the polymorphic nature of many samples it has become necessary to drop old samples from databases. If this practice continues malware samples which have already been identified will become undetectable and will once again become useful to cyber criminals.

Other malware detection techniques are available in order to overcome the problems of obfuscation and polymorphism. Instead of scanning for matching signatures it is possible to analyze the behavior of a malware sample and base detection on observation of running processes. There are a variety of ways this could be achieved. One approach is to monitor the process names themselves. Unfamiliar or uncommon processes can be assumed to be malicious until further information can be obtained. Another approach is to base detection on the behavior of the process itself. If a process begins executing instructions that match the behavior of a known malware sample then that process can be considered harmful. Similar techniques can be applied to the monitoring of network activity. If certain addresses or port numbers, or some other features, are present in the traffic directed towards or away from the computer system it can be assumed that malware is either targeting the system or is already running within the system.

The downside to both signature and behavior-based detection is that they occur within the OS itself. This gives malware the opportunity to alter the information that is provided to the detection software by the OS. If, for example, the security software polls the OS for a list of running processes it is possible that malware can alter this list so that the malware process itself is not present in the list. The detection software will then have no knowledge of the malware process and the malware will have escaped detection. This behavior is usually associated with rootkits, but could be employed by any malware.

To combat, AntiMalware organization offers sandboxing products available in the market. Non-OS processes can be encapsulated in a safe execution environment that monitors for malware using both behaviour-based and signature-based detection. There is, however, no guarantee that malware has not infected the OS prior to installation of the detection software, or that infection could occur due to processes running outside of the sandbox. As long as the detection software exists in the same execution environment as other processes, including malware processes, there is an opportunity for subversion. A better approach would be to perform the detection from outside looking in.

D. Detection in the Cloud

As mentioned in the previous subsection, detection would be best achieved from outside of the OS. This is possible in clouds because they are built on virtualisation which encapsulates each OS in its own VM. Detection is now possible by executing detection software in a privileged domain within the virtualization environment. There needs to be further step in providing libraries to create monitoring softwares through VM introspection.

Detection in the cloud not only enables introspection, it could also improve the reliability of statistics based approaches. Behavioural and anomaly detection techniques are built on statistical analysis and are subject to a level of uncertainty. In an isolated computer system this uncertainty cannot be improved upon because access to additional information is not possible. Detection at the hypervisor level, however, can combine the data from many VMs which has the potential to reduce uncertainty and false positives in any results. Although the solutions for malware detection discussed so far seem promising there is another security risk that is unique to the cloud. The compact network topology of clouds coupled with the likelihood of homogeneous software deployment could allow rapidly propagating malware, such as worms, to propagate even faster and with an increased success rate. This indicates that coordination across the cloud is an important consideration. Not only would a certain level of communication between detection software

CONCLUSION

In this journal we summarized the security issues facing cloud Computing. It was determined that as well as conventional attack vectors, which are present in operating systems, virtualization also introduces new opportunities for malware writers. These are due to the sharing of physical resources through software mechanisms, which if implemented incorrectly would allow malware to access the memory in other VMs. This could lead to new forms of malware that spread in a worm-

like way by writing to memory instead of spreading via the network.

REFERENCES

Journal Papers:

[1] Krešimir Popović, Željko Hocenski, "*Cloud computing security issues and challenges" Proc. MIPRO 2010, May 24-28, 2010*, Opatija, Croatia.

[2] A. Moser, C. Kruegel, and E. Kirda, "*Exploring multiple execution paths for malware analysis," in Security and Privacy, 2007*. SP'07. IEEE Symposium on, *2007, pp. 231–245*

[3] Shivlal Mewada, Umesh Kumar Singh, Pradeep Sharma, "*Security Based Model for Cloud Computing*", IRACST– International Journal of Computer Networks and Wireless Communications (IJCNWC), *Vol. 1, No. 1, pp(13-19),* December 2011

Proceedings Papers:

[4] U. Gurav and R. Shaikh, "Virtualization: a key feature of cloud computing," in *Proceedings of the International Conference and Workshop on Emerging Trends in Technology*, 2010, pp. 227–229

[5] A. Dinaburg, P. Royal, M. Sharif, and W. Lee, "Ether: malware analysis via hardware virtualization extensions," in *Proceedings of the 15th ACM conference on Computer and communications security*, 2008, pp. 51–62W.J. Book, Modelling design and control of flexible manipulator arms: A tutorial review, *Proc. 29th IEEE Conf. on Decision and Control*, San Francisco, CA, 1990, 500-506.

[6] Meiko Jensen, J¨org Schwenk, Nils Gruschka, Luigi Lo Iacono " On Technical Security Issues in Cloud Computing" 2009 IEEE International Conference on Cloud Computing