ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 4, April 2012

Overview of Attacks on Cloud Computing

Ajey Singh, Dr. Maneesh Shrivastava

Abstract— Cloud Computing is a new environment in computer oriented services. This system have some similarities of distributed system, according to this similarities cloud computing also uses the features of networking. Therefore the security is the biggest problem of this system, because the services of cloud computing is based on the sharing. In this paper we discussed the different types of attack in cloud computing services and cloud wars also.

*Index Terms— **Cloud computing, Cloud Wars, Attacks, Security.***

I.INTRODUCTION

Cloud computing is currently one the most hyped IT innovations. Most IT companies announce to plan or (suddenly) already have IT products according to the cloud computing paradigm. Though cloud computing itself is still not yet mature enough, it is already evident that it's most critical flaw according to public consent is security. In the nearest future, we can expect to see a lot of new security exploitation events around cloud computing providers and users, which will shape the cloud computing security research directions for the next decade. Hence, we have seen a rapid evolution of a cloud computing security discipline, with ongoing efforts to cope with the idiosyncratic requirements and capabilities regarding privacy and security issues that this new paradigm raises. In line with these developments, the authors closely watch cloud computing security on a very technical level, focusing primarily on attacks and hacking attempts related to cloud computing providers and systems. Here, as Lowis and Accorsi pointed out lately, the specific security threats and vulnerabilities of services and service-oriented architectures require new taxonomies and classification criteria, so do attacks on cloud computing scenarios [1]. In this paper, we try to anticipate the classes of vulnerabilities that will arise from the cloud computing paradigm, and we give preliminary attack taxonomy for these, based on the notion of attack surfaces

II. CLOUD COMPUTING ATTACKS

As more companies move to cloud computing, look for hackers to follow. Some of the potential attack vectors criminals may attempt include:

A. Denial of Service (DoS) attacks

Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging. When the Cloud Computing operating system notices the high workload on the flooded service, it will start to provide more computational power (more virtual machines, more service instances) to cope with the additional workload. Thus, the server hardware boundaries for maximum workload to process do no longer hold. In that sense, the Cloud system is trying to work against the attacker (by providing more computational power), but actually—to some extent—even supports the attacker by enabling him to do most possible damage on a service's availability, starting from a single flooding attack entry point. Thus, the attacker does not have to flood all *n* servers that provide a certain service in target, but merely can flood a single, Cloud-based address in order to perform a full loss of availability on the intended service [2].

B. Cloud Malware Injection Attack

A first considerable attack attempt aims at injecting a malicious service implementation or virtual machine into the Cloud system. Such kind of Cloud malware could serve any particular purpose the adversary is interested in, ranging from eavesdropping via subtle data modifications to full functionality changes or blockings. This attack requires the adversary to create its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and add it to the Cloud system. Then, the adversary has to trick the Cloud system so that it treats the new service implementation instance as one of the valid instances for the particular service attacked by the adversary. If this succeeds, the Cloud system automatically redirects valid user requests to the malicious service implementation, and the adversary's code is executed. A promising countermeasure approach to this threat consists in the Cloud system performing a service instance integrity check prior to using a service instance for incoming requests. This can e.g. be done by storing a hash value on the original service instance's image file and comparing this value with the hash values of all new service instance images. Thus, an attacker would be required to trick that hash value comparison in order to inject his malicious instances into the Cloud system. The main idea of the Cloud Malware Injection attack is that an attacker uploads a manipulated copy of a victim's service instance so that some service requests to the victim service are processed within that malicious instance. In order to achieve this, the attacker has to gain control over the victim's data in the cloud system (e.g. using one of the attacks described above). In terms of classification, this attack is the major representative of exploiting the service-to-cloud attack surface [3]. The attacker controlling the cloud—exploits its privileged access capabilities to the service instances in order to attack that service instance's security domains.

C. Side Channel Attacks

An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack. Side-channel attacks have emerged as a kind of effective security threat targeting system implementation of cryptographic algorithms. Evaluating a cryptographic system's resilience to side-channel attacks is therefore important for secure system design [4].

D. Authentication Attacks

Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers. Currently, regarding the architecture of SaaS, IaaS, and Paas, there is only IaaS offering this kind of information protection and data encryption. If the transmitted data is categorized to high confidential for any enterprise, the cloud computing service based on IaaS architecture will be the most suitable solution for secure data communication. In addition, the authorization of data process or management for those data belonged to the enterprises but stored on the service provider's side must be authorized by the user side (enterprises) to instead of the service providers. Most user-facing services today still use simple username and password type of knowledge-based authentication, with the exception of some financial institutions which have deployed various forms of secondary authentication (such as site keys, virtual keyboards, shared secret questions, etc.) to make it a bit more difficult for popular phishing attacks.

E. Man-In-The-Middle Cryptographic Attacks

This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.

III. CLOUD WARS

The promise of cloud computing includes high availability of computational resources for the cloud-hosted services. Nevertheless, flooding attacks that aim at resource exhaustion can still impact the cloud, especially since the attacker may use a cloud for sending his flooding messages as well. Thus, both clouds (the attacker's one and the victim's one) provide more and more resources for sending respectively receiving attack messages until one of both cloud systems eventually reaches its maximum capacities. As a side-effect, if the attacker uses a hijacked cloud service for attack message generation, he can trigger huge usage bills for cloud-provided services that the real user never ordered [1]. This attack involves two cloud systems, hence there are several attack surfaces used. At first, sending attack messages to the victim's service is a typical service-to-user surface attack (as in non-cloud scenarios). As the services on both attacker's and victim's side additionally consume cloud resources, the cloud-to-service interface of both clouds is attacked as well. Further, as other services hosted on the same hardware within a cloud may be affected by the resource exhaustion as well, this implies a cloud to- service surface involvement, and finally the usage bill of the hijacked service misused for attack message generation is a representative of exploiting the user-to cloud surface of the legitimate cloud user that has to pay for the resource usage during the attack [3].

IV. AN ATTACK TAXONOMY FOR CLOUD COMPUTING

A cloud computing scenario can be modeled using three different classes of participants: service users, service instances (or just services), and the cloud provider (Figure 1). Every interaction in a cloud computing scenario can be addressed to two entities of these participant classes. In the same way, every attack attempt in the cloud computing scenario can be detailed into a set of interactions within this 3-class model. For instance, between a user and a service instance one has the very same set of attack vectors that exist outside the cloud computing scenario. Hence, talking about cloud computing security means talking about attacks with the cloud provider among the list of participants [1]. This does not require the cloud provider to be malicious himself; it may also just play an intermediate role in an ongoing combined attack. Figure 1 is shown in Appendix. (a) Service-to-User

(b) User-to-Service

(c) Cloud-to-Service

(d) Service-to-Cloud

(e) Cloud-to-User

(f) User-to-Cloud

V. ATTACK SURFACES

The first and most prominent attack surface is that of a service instance towards a user (a). This is nothing else than the common server-to-client interface, thus enabling (and being vulnerable to) all kinds of attacks that are possible in common client-server-architectures as well. This involves things like buffer overflow attacks, SQL injection, or privilege escalation. In the same way, the attack surface the service user provides towards the service (b) is nothing else than the common environment a client program provides to a server, e.g. browser-based attacks for an HTMLbased service like SSL certificate spoofing, attacks on browser caches, or Phishing attacks on mail clients. The interface between a service instance and a cloud system (c) is a little bit more complex. Here, the separation of service instance and cloud provider can be tricky, but in general the cloud system's attack surface to the service instance covers all attacks that a service instance can run against its hosting cloud system. An example would be resource exhaustion attacks, triggering the cloud provider to provide more resources or end up in a Denial-of-Service, or attacks on the cloud system hyper visor. The other way around, the attack surface of a service instance against the cloud system (d) is a very sensitive one. It incorporates all kinds of attacks a cloud provider can perform against a service running on it.

This may start with availability reductions (i.e. shut down service instances), but may also cover privacy related attacks or even malicious interference (e.g. tampering data in process, injecting additional operations to service instance executions; everything a root kit can do). To the author's consideration, this is by far the most critical kind of attack surface, as its exploitation is rather easy (once being the cloud provider) and attack Impacts are tremendous. The fifth attack surface of interest is that of the cloud system towards the user (e). This is a little bit hard to define since both usually do not have a real touching point; in common scenarios there always exists a service in between. However, the cloud system has to provide an interface for controlling its services. That interface, which we call cloud control, provides Cloud customers with the ability to add new services, require more service instances, delete service instances etc. As this is not a service instance in the sense of Figure (1), it is discussed here as a separate attack surface, with attack threats being merely similar to the ones a common cloud service has to face from a user. The last attack surface is the one provided by a user towards the cloud provider (f). Considerable attacks may involve phishing-like attempts to trigger a user into manipulating its cloud-provided services, e.g. presenting the user a faked usage bill of the cloud provider [1]. In general, this involves every kind of attack that targets a user and originates at the cloud system.

VI. CONCLUSION

As cloud computing is on the rise, and especially due to its enormous attraction to organized criminals, we can expect to see a lot of security incidents and new kinds of vulnerabilities around it within the decades to come. This paper gives a first step towards classifying them, thus making them more concrete and improving their analysis. Using the notion of attack surfaces, we illustrated the developed classification taxonomy by means of four up-to-date attack incidents of cloud computing scenarios. Being a work-in-progress, we will continue with the collection and classification of cloud-based attacks and vulnerabilities in order to prove or refute our attack taxonomy's applicability and appropriateness.

REFERENCES

[1] Nils Gruschka[1] and Meiko Jensen[2] "Attack Surfaces: A Taxonomy for Attacks on Cloud Computing", 3rd International Conference on Cloud Computing, 2010.

[2] Mohamed H. Sqalli[1], Fahd Al-Haidari[2] and Khaled Salah[3] "EDoS-Shield- A Two- Steps Mitigation Technique against EDoS Attacks in Cloud Computing", 4th IEEE International Conference on Utility and Cloud Computing, 2011.

[3] M. Jensen[1], J. Schwenk[2], N. Gruschka[3], and L. Lo Iacono[4],"On technical security issues in cloud computing," in Proceedings of the IEEE International Conference on Cloud Computing (CLOUD-II), 2009.

[4] Qiasi Luo[1] and Yunsi Fei[2] "Algorithmic Collision Analysis for Evaluating Cryptographic System and Side-Channel Attacks"' International Symposium on H/w- Oriented Security and Trust, 2011.

APPENDIX

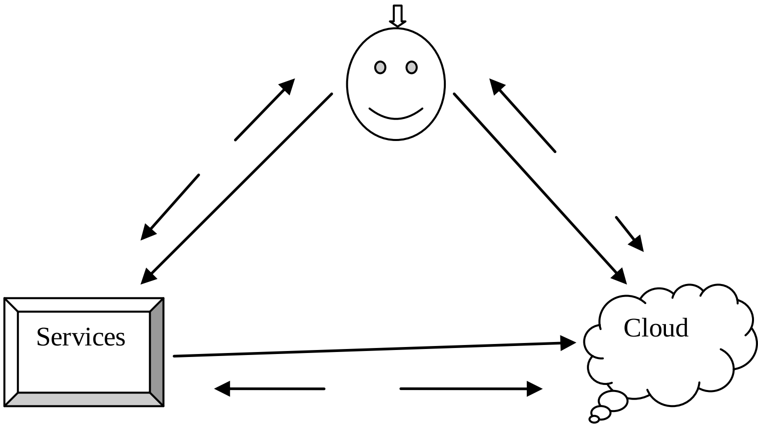

Fig 1. The Cloud Computing Triangle and the Six Attack Surfaces