Journal of Network and Computer Applications 34 (2011) 1097–1107

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks

Ashley Chonka, Yang Xiang *, Wanlei Zhou, Alessio Bonti

School of Information Technology, Deakin University, Australia

ARTICLE INFO

Article history:
Received 23 November 2009
Received in revised form
23 April 2010
Accepted 7 June 2010
Available online 23 June 2010

Keywords:
Network security
DDoS
XDoS
HDoS
Cloud computing
Traceback

ABSTRACT

Cloud computing is still in its infancy in regards to its software as services (SAS), web services, utility computing and platform as services (PAS). All of these have remained individualized systems that you still need to plug into, even though these systems are heading towards full integration. One of the most serious threats to cloud computing itself comes from HTTP Denial of Service or XML-Based Denial of Service attacks. These types of attacks are simple and easy to implement by the attacker, but to security experts they are twice as difficult to stop. In this paper, we recreate some of the current attacks that attackers may initiate as HTTP and XML. We also offer a solution to traceback through our Cloud TraceBack (CTB) to find the source of these attacks, and introduce the use of a back propagation neutral network, called Cloud Protector, which was trained to detect and filter such attack traffic. Our results show that we were able to detect and filter most of the attack messages and were able to identify the source of the attack within a short period of time.

1. Introduction

Today, cloud computing systems are providing a wide variety of services and interfaces to enable vendors to rent out spaces on their physical machines at an hourly rate for a tidy profit (Amazon EC2 2009; INetu, 2009; ElasticHosts, 2009). The services that are provided by these vendors can vary from dynamically virtual machines (Enomaly.com, 2009; Keahey et al., 2005; Nurmi et al., 2009; McNett et al., 2007) to flexible hosted software services (Laplante et al., 2008; Hewlett-Packard, 2009; Hibler et al., 2008; Lenk et al., 2009). Each machine and software shares the notion that delivered resources should be allocated and de-allocated on demand, at the same time as providing reasonable performance.

According to the recent e-crime study conducted in 2009 by the E-Crime Congress in partnership with KPMG, it found that online customers are most at risk and that risk increases as time goes by (KPMG, 2009). For example, the study reported that 63% of respondents said their customers were predominately affected by poisoned websites. The survey also reported that 40% of the total respondents said that there had been an increase in technical sophistication of these attacks against their customers.

With any new technology, there will be enthusiastic people who want to learn all about it so they can contribute to the wider community and others who want to exploit it so that they can gain some type of advantage. With the emergence of cloud computing, multi-billion dollar organisations like IBM, Amazon, Google and Ebay have already invested in cloud technology. If extortionists threaten to bring down their Cloud System with a Distributed Denial of Service (DDoS) attack, which is for this paper means many nodes systems attacking one node all at the same time with a flood of messages, it is usually better for a corporation to pay the ransom than see their systems go off line (Fowler, 2009). However, it is not only extortionists that can exploit cloud computing. For example, Amazon or Ebay competitors could also use known vulnerabilities to interrupt the normal operations of their cloud system so their customers move onto the next business that can provide them with the service they require. Renting out its sky-high computer infrastructure from Amazon, this actual example happened to the BitBucket.com cloud, who according to the report, went down for 19 h (Metz, 2009).

The variant forms of DDoS attack tools like Agobot (F-Secure, 2003; Sophos, 2009), Mstream (Dittrich, 2000) and Trinoo (Dittrich, 1999) are still used by attacker today. But most attackers are more inclined to use the less complicated web based attack tools like Extensible Markup Language(XML)-based Denial of Service (X-DoS) and Hypertext Transfer Protocol (HTTP)-based Denial of Service (H-DoS) attack due to their simple implementation and lack of any real defences against them (Chonka et al. (2008a)).

X-DoS and its distributed version, Distributed XML-based DoS (DX-DoS), described by Padmanabhuni et al. (2006) and demonstrated by Jensen et al. (2007), occurs when an XML message is sent to a Web Server or Web Service with malicious content to use

* Corresponding author. Tel.: +61 3 9251 7482; fax: +61 3 9244 6440.
E-mail addresses: ashley.chonka@deakin.edu.au (A. Chonka), yang@deakin.edu.au (Y. Xiang), wanlei@deakin.edu.au (W. Zhou), alessio.bonti@deakin.edu.au (A. Bonti).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.06.004

up all their resources. One example of an X-DoS attack is called a Coercive Parsing attack, which manipulates the Web Service Request when a Simple Object Access Protocol (SOAP) is parsed to it so that it can transform the content to make it accessible to applications. The Coercive Parsing attack uses a continuous sequence of open tags so that the CPU usage on an Axis2 web server becomes exhausted.

H-DoS attacks are discussed and implemented in a web article by Stewart (2007), which describes the attack as a HTTP Flooder that starts up 1500 threads so that it can send randomised HTTP requests to the victim web server to exhaust its communication channels. Stewart (2007), also points out there is no way to distinguish between legitimate and illegitimate HTTP requests and no way to filter such traffic.

In this paper we use our previous work on service-oriented traceback architecture (now called Cloud TraceBack) to defend against X-DoS attacks (Chonka et al., 2008a, 2008b, 2009) the area of cloud computing. We also cover in this paper the implementation of a previously devastating H-DoS attack that affected Iran. This ongoing cyber attack was coordinated by the Iranian opposition party that was successful at disrupting access to the pro-Ahmadinejad websites by using a 3 prong attack (Danchev, 2009a, 2009b). We use this attack as an example of bringing down a cloud system like Amazon EC2, and also use it to train our back propagation neural network called Cloud Protector (formerly known as X-Detector) to detect this form of attack and remove it from the system.

The contribution this paper makes to the field of cloud computing is that it is first to analyse how X-DoS/H-DoS attacks affect cloud computing using real attack traffic that is provided by the StuPot project (StuPot, 2009). The second contribution we make is by updating our previous Service-Oriented Traceback Architectural (SOTA) model to a Cloud model in order to focus on protecting cloud computing from X-DoS/H-DoS attacks.

The rest of the paper is made up of the following: Section 2 covers the related work done in the information technology field on security for cloud computing and the X-DoS/H-DoS attacks that threaten this security. Section 3 covers the Cloud TraceBack model and Chaos Protector. Section 4 covers the experiments and evaluations. Finally, Section 5 covers our conclusions and future work.

2. Related work

In this section we briefly cover some of the attacks that are currently used within cloud computing. We also cover previous research on SOTA, which is based on service-oriented architecture and service-oriented grid architecture. To conclude this section, we briefly cover the research done on X-DoS which is a DDoS attack that could affect cloud computing.

2.1. Cloud computing attacks

In the current research on cloud computing (Laplante et al., 2008; Lenk et al., 2009) most think of cloud computing as the virtualization of on-demand, elastic, scalable, resource that is service. But as Balding pointed out in his Rivest, Shamir, and Adelman (RSA) conference presentation, cloud computing is actually much more, and that it really is the abstraction of services (Balding, 2009).

Since cloud computing security follows the idea of cloud computing, there are two main areas that security experts look at securing in a cloud system: These are VM vulnerabilities and message integrity (Availability, Integrity and Confidentiality) between cloud systems. Some of the attacks that encompass both are: Rafal's Heap Overflow in I/O (CVE-2007-4496), Rafal's against Xen (CVE-2007-5497), Rafal's against Microsoft Virtual Server (CVE-2007-5497) and Greg McManus Shared Folders vulnerability in VMware (CVE-2007-1744).

2.2. Service-oriented traceback architecture

SOTA is a web security service application that is product-neutral (Chonka et al., 2008a, 2008b, 2009). Its main objective is to apply a SOA approach to traceback methodology. This is in order to identify a forged message identity, since one of the main objectives of X-DoS and DX-DoS is to hide the attacker's true identity. The basis of SOTA is founded upon the Deterministic Packet Marking (DPM) algorithm (Belenky and Ansari, 2003).

DPM marks the ID field and reserved flag within the IP header. As each incoming packet enters the edge ingress router it is marked. The marked packets will remain unchanged as they traverse the network. Outgoing packets are ignored. DPM methodology is applied to our SOTA framework, by placing the Service-Oriented Traceback Mark (SOTM) within web service messages. If any other web security services (WS-Security, for example) are already employed, SOTM would replace the 'token' that contains the client identification. Real source message identification is stored within SOTM, and placed inside the SOAP message. SOTM, as in DPM tag, will not change as it traverses through the network. The composition of SOTM is made up of one XML tag, so not to weigh down the message, It is then stored within a SOAP header. Upon discovery of an X-DoS or DX-DoS attack, SOTM can be used to identify the true source of forged messages.

SOTA does not directly eliminate an X-DoS or DX-DoS attack message. This is left for the filter section of a defence system called Cloud Protector. This leaves SOTA with the important task of dealing with the main objectives of X-DoS and DX-DoS, which are:

- Exploit a known vulnerability or to flood the system with useless messages to exhaust the web server's resources to the point of collapse. These vulnerabilities could be found in communication channels (flooding for example) or known exploits within the services provided (for example, an attacker can overload their messages, which will result in the web server crashing).
- Attackers who try to hide their identities. The reasons for this vary, depending on the type of attack, but usually it is to cover their crime or to bypass a known defence that is in place to prevent it. It is with this second objective that SOTA attempts to cover, as other traceback methods do, items like Probability Packet Marking (PPM) (Savage et al., 2001) and DPM.

There are a number of reasons why cloud computing should employ a SOTA type framework:

- Current web security is not up to handling an X-DoS or DX-DoS attack. In fact, Jensen et al. (2007), shows how WS-Security can be used in an X-DoS attack.
- With IPv6 coming into use (van Beignum, 2008), current IP traceback methods will no longer be viable. This is due to the changes IPv6 introduces, such as, IPSec and the packet header format which no longer holds support for the fields that are required for IP traceback.
- SOTA does not violate IP protocols due to storing information in the IP packet.
- Using the SOA model, SOTA can be employed on any ubiquitous grid system.

2.3. XML-based denial of service (X-DoS) attacks

A Denial of Service (DoS) is where an attacker attempts to deprive legitimate users of their resources (Rogers, 2009). An X-DoS