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