A Novel Cloud Computing Security Model to Detect and Prevent DoS and DDoS Attack

Masudur Rahman,
Faculty of Business and Services,
Colchester Institute
Colchester,
United Kingdom

Wah Man Cheung
Faculty of Business and Services,
Colchester Institute.
School of Computer Science and Electronic Engineering, University of Essex, Colchester, United Kingdom

Abstract—**Cloud computing has been considered as one of the crucial and emerging networking technology, which has been changed the architecture of computing in last few years. Despite the security concerns of protecting data or providing continuous service over cloud, many organisations are considering different types cloud services as potential solution for their business. We are researching on cloud computing security issues and potential cost effective solution for cloud service providers. In our first paper we have revealed number of security risks for cloud computing environment, which has focused on lack of awareness of cloud service providers. In our second paper, we have investigated on technical security issues involved in cloud service environment, where it's been revealed that DoS or DDoS is one of the common and significant dangers for cloud computing environment. In this paper, we have investigated on different techniques that can be used for DoS or DDoS attack, have recommended hardware based watermarking framework technology to protect the organisation from these threats.**

Keywords—Denial of Service attack; Distributed Denial of Service Attack; mechanism of DoS and DDoS attack; framework to prevent DDoS attack, hardware based watermarking

I. Introduction

Denial of Service (DoS) attack and Distributed Denial of Service Attack (DDoS) are two common types of attacks that do not have a single solution to protect the organisation's IT assets. DoS or DDoS can have severe impact on business and reputation; therefore organisation needs to ensure the security of their IT resources to protect from DDoS attack. By using DoS or DDoS techniques, attacker tries to flood the network or overload the server with traffic so that the legitimate users cannot use the services. Trends to use DoS or DDoS attack have been increased in recent years. These techniques have been used for "cyber warfare" as well. DDoS attack on Visa MasterCard and PayPal by "anonymous" in links to WikiLeaks, DDoS attack on Sony PlayStation, "LulzSec" DDoS attack on CIA and U.K. Serious Organised Crime Agency (SOCA), DDoS attack on WordPress, attack on Hong King Stoke Exchange, CyberBunker DDoS attack are some news, which shows the destructive power of DDoS attack[1].

Successful attacks on these large companies also prove that how vulnerable small organisations are as long as DoS and DDoS are concerned. DDoS attacker may use thousands of different IP addresses to send different types of data packets to the targeted server or network. The process become very complicated for the victim server or network to differentiate between the legitimate traffic and "fake" traffic. Situations become more complicated when the attackers use spoofed IP addresses as source to send the packets, which make it difficult to identify the origins of attacks. The DoS or DDoS attack can cause significant business loss because of less productivity and services, increase downtime; therefore loss in reputation. There are two main reasons that make DoS or DDoS attack very popular among different groups of users. Firstly, there are many tools available to conduct DDoS attack on victim. Most of these tools can be used by attacker without having great deal of technical expertise. Availability of worm maker and ignorance of large number of Internet users make it convenient for attacker to place "bot" into different computers, what can be used for DDoS attack. Secondly, victim organisation will have to spend time and resources to locate attacker, which needs significant involvement of IT security experts[2]. Many organisations are not ready to spend adequate amount of resources to investigate the source of the attack, which encourages the attacker to conduct an attack. Because of the high risk of losing company reputation, number of companies tries not to disclose any security incident in public, which also motivates attacker to use this technique.

In next section we will investigate on different techniques, which can be used in DoS or DDoS attack. After discussing about different DDoS attack, we will propose a framework for cloud computing environment that can use hardware based watermarking technology to detect and prevent DoS or DDoS attack.

II. Techniques of Dos / Ddos Attack:

Aim of Denial of Service attack is to consume the resources of victim computer's processing power or victim's network bandwidth so that the victim network would not be able to serve legitimate users. This attack generally takes place in very distributed ways, which will make the victim network vulnerable within short period of time. Most of the cases, it is difficult to detect the DoS or DDoS attack early enough to adopt appropriate counter measures to protect the resources because of the distinctive nature and source of this attack. Different types of worms can be used for DDoS attack. This type of attack also can take place in a form of flooding or logic attack. In flooding attack, large amount of "real" but unnecessary data will be send to the victim network or the victim network will receive high volume of request from different sources for specific services. Result of this attack will consume the bandwidth, processing power or memory of victim network / server; therefore will cause denial of service to legitimate users[3]. Spam emails, data with errors, large volume of data or simple "GET" request for website can cause DDoS attack. Logic DoS attack will be based on exploitation of vulnerabilities within victim system or network. This type of attack needs expertise or intelligent application to identify or to exploit the vulnerabilities of certain networked service[3]. Example of logic attack can be the situation where attacker injects fake routing information to prevent or redirect legitimate traffic from reaching victim's system by exploiting the missing authentication requirements. Sending traffic to the victim system by using fragmented IP datagram can cause system failure, therefore DoS; if the victim computer's operating system or other application software is not securely configured. DDoS bandwidth attack can take place by using TCP SYN flood, ICMP or UDP flood; which will overload the allocated bandwidth of service provider so that legitimate customers will not be able to access their services because of overloaded network. Smurf attacks, Ping of Death attack, TearDrop or Land attack are some common ways to attacking cloud computing environment, which will consume the resources of victim's network and server[4]. Payload in ICMP or DNS reply also can be used for DDoS attack, which will have high probability to pass through the Firewalls. Public Internet Relay Chat (IRC) has been used as tool for DoS attack in recent years by many different attackers.

IP Spoofing is a very popular technique used with DoS attack, where the IP been forged as the traffic coming from victim's network. Alternatively, fake IP can be used as source of the data packet, which does not exist. Upon receiving the data packet, victim system will try to communicate with the forged source system that does not exist. This whole process will consume large amount of resources to cause successful DoS. However, spoofing the IP address of source is not mandatory for DoS or DDoS attack. Attacker may also use number of compromised hosts or chain of proxies to make "trace back" operation difficult to justify the authenticity of source of the packet. Countries with weak or no information security legislation can play significant role to attackers success, if they take the opportunity of this weakness.

R.K. Chang[5] has divided flooding DDoS attack into two main categories names as: direct attack and reflector attack. He has explained direct attack as attackers have spoofed the source IP address and send the traffic and payload directly to the victim computer or network. This type of attack takes place by using ICMP Echo flooding technique, where victim system will have to handle large amount of ICMP Echo request. UDP data flooding is another popular technique used in direct DDoS attack to connect chargen- and echo- ports between two victims. TCP SYN flooding attacks use large number of data packets with forged IP address as source address in packet header so that victim system tries to connect to the source and because of non-exists source address, there will be many "half-open" connection to consume the resources of victim network. Fragmented IP flooding technique also can be used to consume the resources, specifically the memory of the victim server[7].

Unlike this direct attack, reflector attack takes place when the attacker forges the data packet header's IP address. Victim computer's IP will be used as "source address" to send the data payload to a third party by the attacker. On receiving this data packet, third party system will reply to the victim system as that is given as source address in packet header (Fig 1). This type of attack is complicated to response to protect the organisation while this technique can be used to bring more than one system down at the same time. Many different types of networking protocols can be used for reflector DDoS attack, which can include any application layer protocols to request data from web server or DNS server.

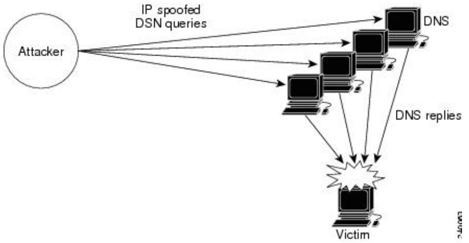

Fig 1: DDoS with Spoofing

This type of attack also can use packet amplification techniques, where third party will reply against a particular request with several packets of data. An example of this type of attack can be, when an ICMP request goes to the broadcast address of a network, therefore each host of that network get the ICMP request. As a result of this request, individual host will reply to the source address to cause DDoS, which has been forged by using victim's IP address. This attack use single ICMP Echo to amplify into many ICMP Echo Reply packets[6].

Flooding attack, both direct and reflector attack can be used against a router to slow down the network or to cause denial of service, which is critical for organisation's network to serve their legitimate users. Using this DDoS attack technique against DNS is a common threats, which cause significant disruption to the organisation's business. Simple tools can be used to perform flooding DDoS attack. This may not requires high volume of resources or bandwidth, which made this type of attack very popular among different attackers. If the flooding attacks take place in a form of distributed attack, attacker must have to have DDoS agents into different systems, which had been compromised before.

In contrast to the nature of flooding attack, logic attack will use different types data packets to exploit the vulnerabilities of victim system. This attack will take place in a form of direct attack, as the attacker will already know the vulnerabilities of the targeted system. Some common methods used in DDoS logic attack include exploitation of syntax or semantic error in victim system. Bugs in the system can be used as vulnerability to attack by attacker (Fig 2).

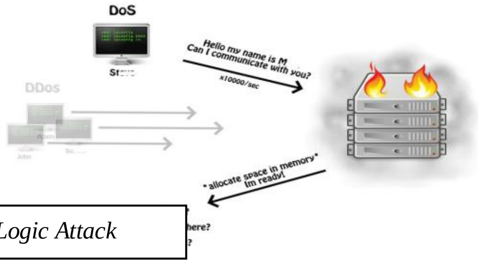

Fig 2: Logic Attack

In next section of this paper, we will be investigating on different mechanisms to detect DoS or DDoS attack.

III. Mechanism To Detect Dos Attack

Different types of techniques and technologies have been used to identify Denial of Service (DoS) or DDoS attach. Incoming traffic can be analysed mainly in two different ways. Manual or automated anomaly detection system can be used to identify DoS attack, where trend of network use can be set against the real network use; therefore any deviation from expected traffic into the network can be identified as sign of DoS or DDoS attack and can be looked into the further details. However, it is a challenge to decide the expected behaviour of the network or users[8]. This type of detection mechanism can detect new or modified attacks including zero days' vulnerabilities. Traffic analysis mechanism to identify DoS or DDoS attack also can work based on signature. Signature based mechanism works in similar principal like antivirus, where the attacks will only be identified if the attack type already given into the detection system. Signature based DoS attack identification mechanism is hugely vulnerable to zero days attack. Attackers also may change or modify the attacks type or tools just to avoid the detection system.

Intrusion Detection System (IDS) are widely been used to identify DoS attack, which normally has three different sections to perform different tasks. Part of IDS will be able to use different sensors to collect data from network or host machine, which will then be analysed to identify abnormal activities and the last function of traditional IDS will be to generate alert for administrator as well as logging the incident for future use. There are two main categories of IDS been used; Network based Intrusion Detection System (NIDS) and Host based Intrusion Detection System (HIDS). NIDS will be able to collect the data from whole network while HIDS will be used to collect the data only from specific host. Having both of these systems in place can provide efficiency in data collection, therefore effective analysis and generating alerts in case of any intrusion attack. Intrusion Detection Systems are necessary part of network now to ensure timely detection of any attacks including DoS or DDoS. Log from IDS is very important to prosecute the attacker. This log also can be used to analyse the attacking method for future attack prevention.

In next section of this paper, we will be investigating on different mechanisms to prevent DoS or DDoS attack.

IV. Mechanism To Prevent Dos And Ddos Attack

There is no single solution against DoS or DDoS attack as the attacker can use many different methods of attack. Organisation will have to adopt different protective mechanisms to have efficient defence against DoS attack. A *defence in depth* approach will help to fight against DoS, where there will be different layers of protection by using different security strategies and technologies. To prevent DoS attack, there needs to be minimum two layers of protective mechanism. First layer will react on *deployment phase* of the attack, when the attacker might try to spread a worm or start the TCP SYN flood to the network. Second layer of defence mechanism will react on time of active attack to prevent the network. In this section, we will be explaining different mechanisms to protect the organisation's IT systems against DoS attack. We also will propose a cost effective potential solution to prevent DDoS attack.

Operating Systems and different applications can raise massive security concerns in terms of being victim of DoS attack, while individual software within a networked system not has been configured efficiently to ensure the optimum security. Unnecessary ports and services can be enabled into a system, which can be used by the attacking tools or attackers. Having updated signature database for antivirus and security patches of OS can contribute significantly in defence mechanism of DoS attack. It is important to ensure that each device within the network does have strong authentication system so that *logic attack* cannot take place by modifying the configuration of router or such other devices. IDS should be used with effective customisation according to the needs of network environment. Both NIDS and HIDS can be used to minimise the false positive and false negative alerts and to detect attacks on early stage. Firewall or similar device should be used for access control to the network. Many resources may needs to be used within the network but not from Internet; therefore access list should be implemented according to the security policy[10]. A support for Quality-of-Service (QoS) features should be configured in router.

If an intrusion has been identified while in *deployment phase of the attack*, there should be an automated mechanism of killing process, restarting application and killing active connections by using TCP RST in case of TCP SYN attack[11]. Propagation of worm typically based on *stack smashing attack*, where attacker managed to access compromised host systems[12]. In terms of propagating worms, a compromised host will establish connection with many different hosts within short period of time; therefore limiting the rate of connections for certain time will be an effective defence mechanism against this type of attack[13]. Vulnerability scanner plays important role for identifying weaknesses within the networked system. Software auditing including checking the vulnerabilities for buffer overflow attack, SQL injection or XSS attack should be conducted regularly to prevent these types of attacks.

In next section of this paper, we will be proposing hardware based watermarking mechanisms to detect and prevent DoS or DDoS attack.

V. Proposed Preventive Mechanism Against Ddos Attack:

One of the complicacy to have effective defence against DDoS is identify the attacked traffic separately than legitimate traffics. Attackers normally use many spoofed IP addresses to attack the system, therefore it become resource consuming to check each of the data packets. Edge routers can be used to mark the source of data packet by using reverse checking mechanism. In case of DDoS attack, large volume of data will be coming from certain hosts. If the source IP has been forged, the type of data will be identical for most of the cases. Using TTL or hop counts, data packets can be grouped as trusted or untrusted. To perform this operation, "hardware based watermarking technology" can be used. This section of the network will use *traceback mechanism* by using hop count and TTL to test the authenticity of source of data, anomaly of the type of data and classify the source/data as trusted or untrusted. Hardware watermarking also will maintain a table, which can use certain cache timing, so that traffic from certain host is not blocked permanently. After certain time, hardware watermarking will check the incoming data packets from specific host again as that might be a legitimate host machine, which had been compromised because of attackers worm. Updated table of trusted and untrusted hosts should be passed to the next device of the network such as router to send the traffic to the right destination. This device should have defence mechanism to protect itself from DDoS attack especially for TCP SYN attack. Specific TTL should be assigned *traceback operation* to verify the source of information. Having hardware watermarking and filtering technology can work as efficient and cost effective defence mechanism against DDoS attack for any organisation because of less consumption of resources.

Proposed hardware-based watermarking technology to detect and prevent DoS attack will work on following principles:

1) *Once packet will reach to the network, source of the packet will be identified.*

2) *Traceback mechanism should be used to check the authenticity of source address by using Hop Counts and TTL.*

3) *If the source cannot be verified, packet will be marked as untrusted and will be dropped without sending it to internal network.*

4) *Each packet coming from same untrusted source will be grouped together based on source authenticity (Figure 3)*

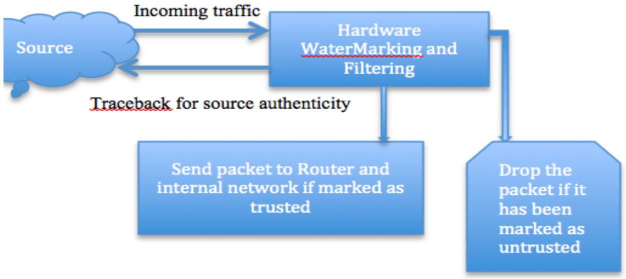
Incoming traffic
Source
Hardware WaterMarking and Filtering
Traceback for source authenticity
Send packet to Router and internal network if marked as trusted
Drop the packet if it has been marked as untrusted

Fig 1: Proposed IDS System

5) *If the source is verified, anomaly of the data packets and connection mechanism should be checked against "knowledge based database". Any suspicious data packets sho* [illegible] *or in depth investigation to reduce the rate of false positive or false negative response.*

6) *Based on known attack type, packet and source should be marked as untrusted and drop the packet on edge of the network.*

7) *Only "trusted" packets should be marked and passed to the internal network.*

VI. Conclusion and Future Research*:*

This paper is very beginning of the research to design a cost effective solution for cloud computing environment to prevent DoS attack. In this early stage of this research, we tried to identify the nature and severity of DoS attack and different techniques used by this attack, so that we can design and build the prototype.

Hardware based watermarking and filtering mechanism can provide additional layer of defence against DDoS attack, which also will consume less resources. We will continue this research to present an algorithm, build and test prototype for Hardware based watermarking and filtering method to prevent the network from DDoS attack.

References

[1] http://www.itbusinessedge.com/slideshows/show.aspx?c=92910&slide=7

[2] CERT Coordination Center, Overview of attack trends, Feb 2002 (online)

[3] Dr. Moore, G.M. Voelker and S. Savage, Inferring Internet Deniel of Service Activity.

[4] M. Rahman, W.M. Cheung, Analysis of Cloud Computing Vulnerabilities.

[5] R.K. Chang, Defending against flooding based distributed denial of service attacks: a tutorial, IEEE Commun. Mag.

[6] S. Northcutt & J. Novak, Network Intrusion Detection, Third Edition

[7] B. Guha & B. Mukherjee, Network security via reverse engineering of TCP code: vulnerability analysis and proposed solution

[8] CERT Coordination Center, Overview of attack trends, Oct 1997 (online)

[9] www.cisco.com

[10] M. Handley, V. Paxson and C. Kreibich, Network intrusion detection: evasion, traffic normalisation and end-to-end traffic semantics

[11] V. Paxon, An analysis of using reflector for distributed denial of service attack.

[12] Cisco Systems, Characterising and tracing packet flood using cisco router.

[13] M.M. Willliamson, Throttling Viruses: restricting propagation to defeat malicious mobile code.