IP Spoofing & its Detection Techniques

HINNA HAFEEZ, TAYYABA KHALIL

MPhil Computer Science, Kinnaird College, Lahore.
hinnahafeezsh@gmail.com

1. BRIEF SUMMARY OF PAPER: IP SPOOFING DETECTION FOR PREVENTING DDOS ATTACKS IN CLOUD COMPUTING [1]

Cloud computing uses different available technologies i.e grid computing, cluster etc to provide the user with the pooled resources, the main security issues to be addressed in cloud computing are confidentiality, integrity and availability (CIA). DDoS is the main threat facing by cloud computing, DDoS is used to target the availability of services by flooding and consuming network bandwidth to exhaust resources. The most considerable part of DDoS is IP spoofing where the source address is forged to disallow easy traceback. This paper provides methods for detecting IP spoofing one of the effective ways to detect IP spoofing is Host-based OS fingerprinting , it uses active and passive (idle mode) methods to match OS of incoming packets from its database to filter spoofed IP packets. Figure printing method called ANTID (Anti-Dos) is efficient way used in detecting and filtering spoofed packets used in attacks. It was used to filter flooding traffic during DDoS by using Time to Live TTL value of the source packet header. TCP interactive method is also the good way to detect IP spoofing as it uses acknowledgment messages, it doesn't receive ACK message it detects it as spoof IP source. OS fingerprinting monitors the incoming packets to determine the operating system of the source on which source packets are running, in this approach administration detects outdated OS and loopholes in the network. Vulnerabilities are identified. OS fingerprinting uses two approaches Active and passive .The inactive approach, a special craft packet is sent towards the true source while passive obtains the header features from incoming packets. Nmap and POF are used in this approach Nmap are networking mapping tool, POF analyses TCP/IP packet headers and determine remote host OS.

2. BRIEF SUMMARY OF PAPER: IP SPOOFING & ITS DETECTION TECHNIQUES [2]

This paper is also based on detecting IP spoofing techniques, it explains packet marking, hop by hop tracing, reactive and logging. Packet marking is further in two ways deterministic packet marking (DPM) & Probability packet marking (PPM). Firewalls are also used to prevent the unauthorized user entering in network In packet marking method trace back data is inserted in the packet which has to be traced. In deterministic packet marking, 16 bit of id in the header and 1 bit of flag information are marked of source router, from this market information we can retrieve the traced information. IN hop by hop approach, if hop by hop program detects any unauthorized packet it sends it to the upstream router and it repeats until it reaches to the last spoofed packet. Logging is the most effective method, in this method, the logging information of internet traffic packet throughout the internet is used and then mining operations are performed to detect the spoofed packet.

a) Based on the papers, some scenarios of attack that may be possible to apply to some component of the cloud.

Components of Could:

Cloud provides the pool of services to the user, cloud computing uses some existing technologies i.e. grid computing, utility computing, cluster computing and distributing computing.
Cloud service model is divided into three

- Software as a service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)

Cloud can be the private, public or hybrid cloud.

The core components of cloud computing using its services are

- Bandwidth
- Routers
- Data packets
- IPs of source and target systems

DDoS Attack:

DDoS is the most important threat in cloud computing, DDoS target the availability trade of C-I-A. As cloud computing provides the pool of services to many users, by DDoS attackers the core service of cloud computing by flooding and consuming the network bandwidth to exhaust services. DDoS carries out amplification which can either be a direct or reflection attack.

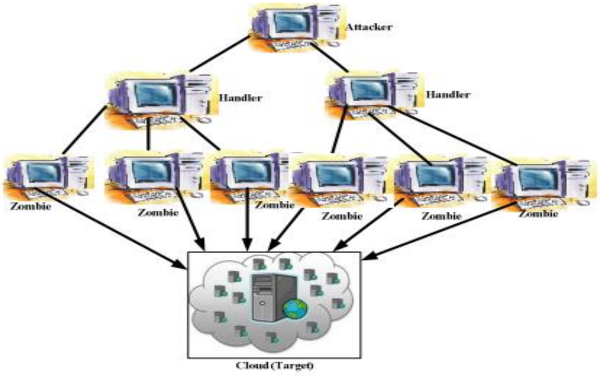


Figure 1: DDoS Attack in Cloud

DDoS attack is often characterized by spoofing of source IP address to disguise its identity to disallow easy traceback or deceive the Cloud Provider to enjoy certain service accrued to a trusted host.

1) One possible Scenario:

The attacker creates a network, which contains many systems, then the attacker finds the targeted network's trusted IPs which are IPs of source systems for spoofing and then starts send data from its source systems, as many systems will start interaction with the targeted network, this heavy traffic of data packets will consume the network bandwidth and server will be down.

With this approach, the **availability**, which is the fundamental of cloud computing can be targeted.

2) Used and targeted components:

The attackers use data packets to consume bandwidth of the network. They use IPs in their attack. Packets travel through network with the help of routers which sort of maps are providing information from where to where data should be sent

3) Other Related services which can be Target:

Availability is the main targeted C-I-A trade other related trades can be

- ➢ Confidentiality
- ➢ Integrity

Once an attacker access IPs of targeted network, the attacker can also access the information from the targeted IPs.
Once information is accessed then not only confidentiality, integrity can also be targeted. An attacker can leak the information and can fabricate the information by sending harmful data which can modify the targeted system's internal database.

The information that can be modified by the attacker but with the trusted IP may cause confusion hence affecting the integrity of the data.

b) **CIA Objectives addressed by proposed Techniques**:

Availability:
DDoS is the main threat used to target the availability of the services provided by cloud computing, DDoS sends data in bulk to exhaust resources, IP spoofing is the related concept, the attackers try to hide their source IP by spoofing to disallow backtracking. They used forged IPs so that they cannot be traced, for this purpose they used other trusted IPs.
Both papers provide different ways to **trace** the exact source IPs
Paper 1 mentioned above provides following techniques:

1. Packet marking method

a) Deterministic packet marking (DPM)

b) Probabilistic packet marking (PPM)

2. Hop by Hop

3. Logging

Paper 2 provides following technique:

1. OS fingerprinting method

Details are given in summary.
By using these methods source IP can be detected and can be blocked

Confidentiality:
Techniques provided in these two papers help in detection of source system used in unauthorized access. If someone can access the network's system IPs he/she can also get the access to the information. By getting this access the confidentiality of the information can be a break and this information can be leaked.
Integrity:
If someone can access the internal systems of any network they can also fabricate these systems information by using this access.
The provided methods in both papers can identify such harmful accesses and by detecting techniques they can block such accesses to the network and network can be secure.

Comparison of approaches mentioned in two papers:

The paper "**IP spoofing & its detection technique** "provides networking based techniques, the techniques used in that paper are using routers and packets information in detection. In this paper different techniques which have been discussed are mentioned below out of them the Logging is considered to be the most effective technique of tracing the source IP address of the intruder.

Firewall

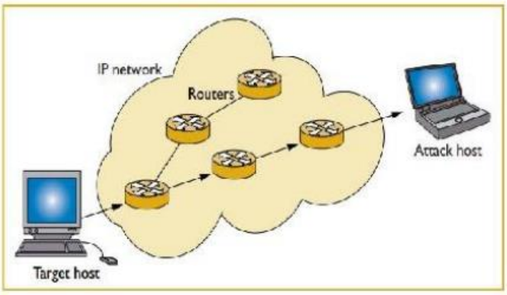
1. Packet filter firewalls
2. Application-level gateway firewalls and
3. Circuit-level gateway firewall

PACKET MARKING METHODS FOR IP TRACING

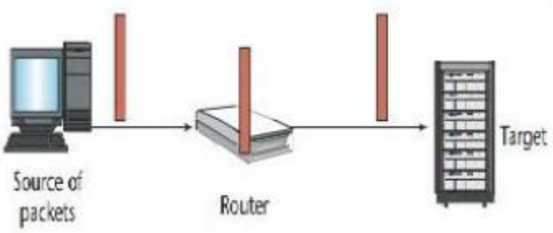
- ➢ Deterministic packet marking

Other Methods of IP tracing

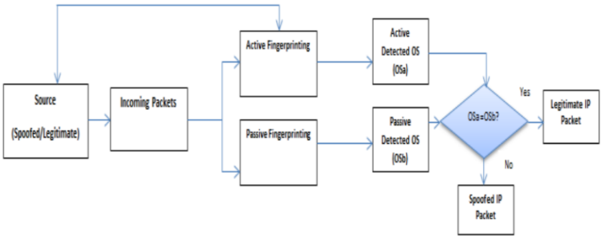
- Hop-By-Hop



- Logging



The paper "**IP Spoofing Detection for preventing DDoS Attacks in Cloud Computing** "provides techniques for detection and prevention which are OS based. This is more effective and authentic way of detection and prevention.
It includes "OS fingerprinting" technique to detect and prevent the DDoS attacks in Cloud Computing. It monitors the incoming packet to determine the OS the source is running on.



It also covers the cases of active and passive i-e when user system is active and the case when it's idle.

Findings:

On the basis of provided comparison, it is observed the approach used in the paper "IP Spoofing Detection for preventing DDoS Attacks in Cloud Computing "is more reliable and comprehensive, it not only provides the way of detection but also covers the methods of prevention. Both active and passive host-based OS fingerprinting that verifies the true source of an incoming packet by identifying its OS in Cloud Computing environment. Two major scenarios which have been implemented has discussed in the paper which verifies the detection and prevention of attacks.

Conclusion

In this report, we have concluded that, if the techniques are implemented properly the attacks can be detected and also help us to prevent out cloud computing network system from intruders. We have seen that "OS Fingerprinting" and "logging" are most effective techniques.

References:

1: Opeyemi.A. Osanaiye, Mqhele Dlodlo, "IP Spoofing Detection for Preventing DDoS Attacks in Cloud Computing ",EUROCON 2015 - International Conference on Computer as a Tool (EUROCON) IEEE, pp. 1-6, 2015

2: 1Maderi Lavanya, 2P.K.Sahoo PG Scholar, Professor, Dept. of CSE, Sreenidhi Institute of Science and Technology (Autonomous), Hyderabad , "IP spoofing and its Detection Technique ", IJACTA, 2016