Analysis of IP Address for Cloud Services

Prasad NK[1], Omprakash[2], Varun Kishore[3], Rashmi C[4]

[1,2,3]School of Computing & Information Technology, REVA University, Bangalore, India
[4]Assistant professor, School of Computing & Information Technology, REVA University, Bangalore, India

Abstract—*As the use of internet has increased which also lead to the increased number of cyber-attacks like denial of service attack. The prevention of denial of service attacks on cloud network can be achieved by using randomization of IP addresses that makes it more difficult for attackers to locate the target device by asking them to scan a vast number of IP addresses. IP address randomization is used by many moving target defences under the basis that attackers will struggle to anticipate newly assigned IP addresses. This study examines whether IP addresses used by cloud providers are sufficiently volatile in operation. We examined the behaviour of IP address allocation in two significant cloud computing providers and discovered that the real entropy given by assigned IP addresses is small. A basic frequency-based model as well as a Markov process model that generates an address prediction collection from time series data of collected IP addresses are all evaluated.*

Keywords— IP address randomization, moving target defences, denial of service.

I. INTRODUCTION

There are two definitions for cloud computing. The most popular method is to run workloads remotely in a private provider's data centre over the internet, also known as the public cloud. The most well-known public cloud services are: Salesforce's CRM system, Amazon Web Services (AWS), and Microsoft Azure, all provide similar cloud computing services. Most businesses today use multiple cloud services, this basically means that they make use of many public cloud services. The second concept of cloud computing explains how it functions as a virtualized pool of resources that includes everything from device software to raw processing capacity that is accessible on demand.

Denial of service attacks target individual IP addresses of targeted networks and exploit bugs in those services, making them inoperable. To combat denial of service attacks, researchers have looked at techniques including IP address randomization and shifting target defences. Through analysing the behaviour of IP address randomization in nature, this research focuses on effectiveness of IP address randomization in practice in allocation in major cloud computing platforms.

II. LITERATURE SURVEY

Distributed Denial of Service Prevention Techniques:

The description of the DDoS issue, available DDoS attack tools, security problems and concepts, and a classification of available DDoS protection mechanisms were all covered in this article. This gives a security administrator a clearer view of the situation and allows him to easily arm his arsenal of effective DDoS protection measures. The latest prevention measures examined in this paper are simply insufficient to defend the Internet from DDoS attacks. The big issue is that there are still a lot of vulnerable computers on the internet that could be used to initiate a massive orchestrated DDoS attack.

The increased frequency of DDoS attacks, as well as the intensity of the attacks, has resulted in the development of various countermeasures. Each suggested preventive strategy has its own set of advantages and disadvantages. In this article, we present a classification of usable methods for mitigating DDoS attacks on Internet services that have been suggested in the literature.

Density Estimation for Server-side Prediction of Source IP Addresses:

In computer networks, source IP addresses are often used as a serious feature for user research. The usage of source IP addresses for detecting anomalies is popular in the field of Distributed Denial of Service (DDoS) attack detection and mitigation traffic models. Due to a limited number of measurements, the actual IP address distribution is usually under sampled. By using IP neighbourhood relationships, density calculation overcomes this limitation. As a network-based heuristic, basic models are also used indirectly or intuitively. We study and formalise current models in this article, including a hierarchical clustering approach. We also present a statistically motivated smoothing method using the Nadaraya-Watson kernel-weighted average, as well as an updated k-means clustering algorithm for source IP density estimation. We use a 90-day world dataset of 1.3 million separate source IP addresses to evaluate success and check out to forecast the users for the next 10 days. ROC curves and an example DDoS mitigation scenario reveal that there is no consistently better approach: k-means outperforms statistical smoothing when a high detection rate is needed, while statistical smoothing outperforms k-means when a low alert rate is required, much as in the DDoS mitigation scenario. In terms of efficiency, SBSS or k-means clustering are the best options depending on the programme and desired target variable. Xor, in contrast, seems to have the flaw of producing excessively vast and thus insurmountable distances.

TCP/IP for Cyber-Physical Systems: A Time-predictable TCP/IP Stack:

Networks of machines linked to the physical world are known as cyber-physical structures. Time is also of the essence when interacting with the real universe. The calculation and coordination must be done in real time in this situation. A standard network stack architecture, on the other hand, is far from predictable in terms of timing. For a time-predictable network stack, this paper tackles the problem of real-time connectivity for time-critical cyber-physical networks. TCP/IP, a real-time implementation of the TCP/IP stack, is shown. Two properties help one forecast the passage of time: (1) The appliance interface is based on polling functions rather than blocking sockets, which is appropriate for periodic real-time tasks; (2) the architecture is carefully designed to enable static worst-case execution time analysis of all functions.

III. METHODOLOGY

First we make different models of attacks and defences using different strategies then we predict the behaviour of IP address allocation in the cloud services. Given the available resources, the attacker's aim is to deny access to as many hosts in the target network as possible for as long as possible. This is done by using different attack strategies they are

Clustering attack: When the surface of the target network varies, the intruder launches an clustering attack. In an ideal attack, the attacker knows the exact time when new IP addresses are assigned to hosts on the surface. Using the most probable transformation from the N IP addresses observed in a prior (ideally, the previous) attack iteration, the attack iteration estimates the collection Q of IP addresses recently allocated to the hosts. The intruder clusters the dataset and creates a Markov transition matrix to determine the most possible transitions.

Calculating the Transition Matrix. The theory is that certain IP addresses are assigned first, followed by others in a cyclical pattern. By observing IP addresses in the time series, a Markov transition matrix is used to capture the most possible transition of IP address sets Ak among clusters, forming a prediction set. One can estimate the next category of IP addresses using the analytical likelihood in the transition matrix.

Random Attack: The model M for attack algorithm in this technique simply returns a list of all observed prefixes in random order. The random attacker's rationale is to provide a simple and fast attack technique that can be implemented in operation, and it also relies on the data gathered by the clustering attacker.

Frequency attack: The frequency attacker's theory is that address prefixes with a high frequency of occurrence are more likely to reappear, so he makes predictions based on their frequency of occurrence in the dataset using a sorted list of prefixes. In the first iteration of the algorithm, M will return all unique prefixes (first 24-bits of IP addresses) in decreasing order of their frequency in the dataset. The model updates the frequencies for the next attack iteration after each attack iteration.

IV. PROPOSE SYSTE

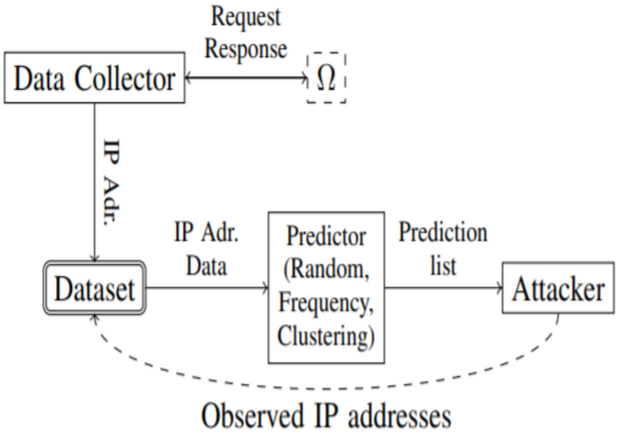

Fig -1: Attack model

1. The cloud computing provider uses a function Ω to allocate IP address.
2. Using a random, frequency, or clustering technique, the intruder attempts to anticipate the behaviour of the IP address.
3. IP addresses that are observed are collected.
4. And it was used to make subsequent predictions.

V. ALGORITHIM

Algorithm for attacking. One attack cycle is summarised by the algorithm. We'll assume that each iteration of the attack begins right after the target network assigns N new IP addresses to the target hosts, and that the attackers' task is to locate those N IP addresses. The number of cloud servers to target is given to the algorithm, along with a model for predicting the IP address M, which is created using one of the attack strategies. The outer for-loop iterates over M's projections in sequence. Model M makes predictions, and the predict function returns an ordered list of those predictions. Each prediction is an IP address prefix; in our tests, the first three bytes of the IP address were predicted. The bits that aren't mentioned will be searched by brute force. The complete function returns all possible IP addresses, which are achieved by completing the predicted prefix. We think the attacker will determine if the attempted IP address belongs to the target network and that the attacker has no interest in targeting any other network in the same cloud computing platform networks. When the attack is successful, IP addresses are registered in the observation list O. Once N IP addresses have been successfully targeted, or all expected prefixes have been exhausted, then the attack is complete. The model is updated based on information gathered from the different attacks.

Attack Algorithm A denial of service attack on N hosts in the target network in one iteration.

```
Require: N, M
O <-[ ]
for A 2 predict(M) do
    for A0 2 complete(A) do
        attack the server on A0
        if attack on A0 succeeded then
            append (A0, O)
            if [O] = N then
                return
            end if
        end if
    end for
end for
with the information collected from this iteration update(M)
```

VI. CONCLUSION

For moving target defence systems predicting the IP addresses allocated by cloud computing platforms is alarming that assumes that public cloud allocates highly unpredictable IP address. As described in Section IV, the behaviour of IP address allocation in cloud providers can be predicted by an attacker. Unless cloud computing platforms employ limitations on IP address allocation, attackers can conveniently update the database of 12 IP addresses and continue attacking various clients. Policies limiting IP address allocation when serving vast virtual networks, there are usability constraints that are difficult to enforce. As a result, developing moving target security schemes with a central function that relies on newly allocated IP addresses necessitates cautious calculations in order to maximise entropy in the chosen IP addresses, preventing attackers from making accurate predictions.

VII. REFERENCES

1. Q. Jia, H. Wang, D. Fleck, F. Li, A. Stavrou, and W. Powell, “Catch me if you can: A cloud-enabled DDoS defense,” in 44th IEEE/IFIP Conference on Dependable Systems and Networks, 2014.
2. J. Sun and K. Sun, “DESIR: Decoy-enhanced seamless IP randomization,” in IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, April 2016, pp. 1–9.
3. K. M. Carter, J. F. Riordan, and H. Okhravi, “A game theoretic approach to strategy determination for dynamic platform defenses,” in First ACM Workshop on Moving Target Defense, 2014.
4. M. L. Winterrose and K. M. Carter, “Strategic evolution of adversaries against temporal platform diversity active cyber defenses,” in Symposium on Agent Directed Simulation, 2014.
5. S. Achleitner, T. La Porta, P. McDaniel, S. Sugrim, S. V. Krishnamurthy, and R. Chadha, “Cyber deception: Virtual networks to defend insider reconnaissance,” in 8th ACM CCS International Workshop on Managing Insider Security Threats, 2016.
6. H. M. J. Almohri, L. T. Watson, and D. Evans, “Misery digraphs: Delaying intrusion attacks in obscure clouds,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 6, pp. 1361–1375, June 2018.
7. S. Achleitner, T. F. L. Porta, P. McDaniel, S. Sugrim, S. V. Krishnamurthy, and R. Chadha, “Deceiving network reconnaissance using SDNbased virtual topologies,” IEEE Transactions on Network and Service Management, vol. 14, no. 4, pp. 1098–1112, Dec 2017.
8. J. H. Jafarian, E. Al-Shaer, and Q. Duan, “Adversary-aware IP address randomization for proactive agility against sophisticated attackers,” in 2015 IEEE Conference on Computer Communications (INFOCOM), April 2015, pp. 738–746.
9. H. Maleki, S. Valizadeh, W. Koch, A. Bestavros, and M. van Dijk, “Markov modeling of moving target defense games,” in ACM Workshop on Moving Target Defense, 2016.