DOI: https://doi.org/10.46632/daai/2/4/25

Data Analytics and Artificial Intelligence
Vol: 2(4), 2022
REST Publisher; ISBN: 978-81-948459-4-2
Website:http://restpublisher.com/book-series/data-analytics-and-artificial-intelligence/

Predictability of ip address Allocations for cloud Computing platforms

***P Selvarani , Dr.J Senthil Murugan, Dhanush S, Gowshin S J, Iyyappan R**
Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College,
Avadi, Chennai,Tamil Nadu, India
*Corresponding author Email: drselvarani@velhightech.com

Abstract: The problem of DoS attack on cloud-based networks can be tackled by using a wide range of unpredictable IP address, thus increasing the work put by the attackers by making these attackers to look up a ton of IP address space to get to the target host. Many target defences use randomization of IP addresses based on the assumption that newly assigned IP addresses will be harder to predict by attackers. Many samples were calculated using frequency computation, and the Markov process sample address prediction was made from a list of time series data of the collected IP addresses.
Keywords:Denial-of-Service, Hypertext Transfer Protocol; Virtual Private Network; Application Programming Interface; EC2 – Elastic Compute Cloud; GCP - Google Cloud Platform;

1. Introduction

DoS attackers deplete a certain set of network services that users demand, resulting in clients being refused access to those services. Specific IP addresses can be targeted when DoS attacks occur at the network, transport, or application layer, and the loopholes can be leveraged at any targeted tier. Target defence systems can use IP address randomization to reduce the impact of DoS attacks on hosts linked to the internet. The server provides a VPN-like service to a huge number of users, and anonymous users are not permitted to use it. Over time, the process of changing IP addresses Randomization of IP addresses is alluded to as IP randomization. The primary purpose of this project is to devise a feasible assault. This is possible because to the tools and APIs provided by cloud computing providers. While establishing and maintaining an IP address database, we consider the attacker. This database is used to anticipate the immigration service's IP address.

2. Background and Related Work

The background for shifting target security is provided in this section. And here's a short rundown of IP address shifting in cloud-based technology. The effort required in evaluating the efficacy of shifting target defences is summarised in Section II-C.

A. Moving Target Defences:A moving target attempts to thwart security breaches. Depending on the attack, certain of the target's assets continue to alter. The idea is to make the necessity for assault more prevalent. Time and resources are expended by the attacker as a result of constant alterations in the network or mechanical structures. When it comes to a fascinating attitude, not to mention the aforementioned labour, Specific attributes and techniques for networks are offered. Virtual networks that are hosted in the cloud.

B. Cloud-based Virtual Networks: Infrastructure as a service is provided by cloud computing providers such as Amazon Web Services. A user is someone who owns or administers a cloud computing Issuer account. The user gets full access to all services. Any service, host, or privacy rule in the profile may be added, edited, or deleted. Users may use this to establish virtual networks. Hosts with routing rules and specialised web portals that provide one or more apps. Cloud computing sites provide virtualized computer services that may be utilised for production right away. Virtual machines made from predefined or personalised machine images, public fixed or ephemeral IP addresses that can be dynamically designated to virtual machines, virtual networks with underlying IP addresses and routing tables, and security rules that encompass one or more virtual machines are all included in these services.

C. Evaluating Moving Target Defences

The following works are thought to be the most closely related. It also seeks to assess the efficiency of moving target security randomization. Because of the vast range of address sorting, earlier work are centered on memory addresses. Operating system randomization prevents the usage of memory corruption issues. Randomization of the process of ambiguity resolution I s similar to switching IP addresses for machines on a network at random, except it utilises accessible memory addresses instead. The purpose of this strategy is the same as it was before: to analyse space performance and streamline the instruction set in practise, with a particular focus on network address randomization and the development of novel prediction algorithms for this area.

3. A Model Of Attack And Defense

In cloud computing, this section discusses the issue of shifting target addresses in the context of cloud-based virtual networks. A. Definitions Consider that A is the attacker in charge of the Internet's network of nodes. The attacker is constrained in terms of the number of restrained nodes (which is related to the cost of the assault) and the time of attack. The target network's attack surface, S, is a collection of hosts (indicated by their IP addresses) which are exposed to the Internet from

the outside. These hosts offer a port that accepts requests from any source. The binary relation R ⊂ A × S represents a denial-of-service attack (or just an assault). An attack is when software on a host u ∈ S gets overloaded to the point that it can no longer react to genuine clients.

B. The Attack Model: Consider an attack intended at denying services to a large number of hosts for an extended length of time in the target network's (Limit) resource for a certain amount of time. Remote privilege escalation might potentially be used by the attacker to get remote access to a few of the computers in the target network. From the standpoint of IP address Randomization, the nature of the remote access assault and the Service denial assault differs; both attacks rely on knowledge and need the carrying of target IP addresses for the duration of the attack. As a result, security based on masking and shifting IP addresses is also beneficial.

C. The Defence Model: The Target networks appeal to a certain population by hosting apps that may be accessed over the Internet. While many apps employ the HTTP (or TLS-based HTTPS) protocol, this research makes no assumptions about which network protocol should be used. Ways to prevent undesirable IP addresses from accessing the intended network, which is essentially unknown, are available on cloud computing sites. Based on the security model, we consider:

1) The surface of the intended network has a total of N hosts,
2) A combination of N addresses are sought out from cloud computing website, which transforms N hosts from IP addresses, according to table.
3) The IP addresses are obtained once for each modification and allocated to the N hosts.
4) IP addresses previously assigned to the target network are not remembered by the target network.
5) DoS attacks are ignored by the target network.

D. IP Address Allocation: Cloud service providers build and manage networks that house virtual networks formed by cloud customers. Many cloud users are served by a cloud computing provider. A fraction of cloud customers seek public IP addresses, either by requesting an elastic IP address which could be paired to a virtual machine or through constructing virtual machines that are accessible from the Internet. Until the user delivers the elastic IP addresses or eliminates the virtual machine where an IP address was assigned, the IP address remains reserved for the user. Although no information regarding the underlying logic of Ω is available to the user, we may draw certain

Assumptions regarding its behavior:

1) IP addresses are assigned by cloud computing providers based on the location where the target network gets hosted,
2) Each area has a large number of cloud users,
3) The number of accessible IP addresses and also the variety of IP addresses varies by area,
4) An IP address assigned to a cloud user will only be published if the user explicitly requests it, and
5) The unspecified random function Ω is used to choose IP addresses from a pool of accessible IP addresses in an area.

4. Attack Strategies

The Learning and Prediction model, as well as the General Attack Algorithm, are discussed in this section (Subsection IV-A). The following are the designs for three types analytical quests: random (Subsection IV-B), frequency based (Subsection IV-C), and also a clustering model (Subsection IV-D) for finding freshly allocated IP addresses.

A. Overview: This is the learning stage. Figure 1 depicts the process of studying and anticipating the target network's upcoming IP addresses. The IP address assignment algorithm is used by the cloud computing platform, which generates a function Ω that returns an IP address based on a requesting client's area and other hidden parameters.

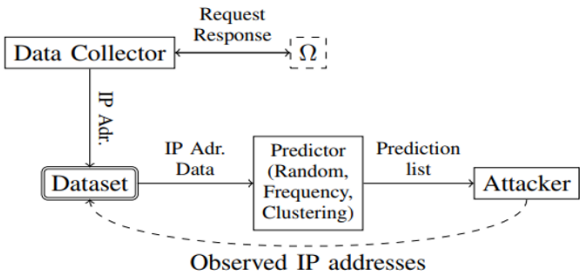

FIGURE 1. The process of predicting IP addresses in the target network.

Ω is a function used by the cloud computing provider to allocate IP addresses. The attacker's aim is to predict its behaviour using either a random, a frequency, or a clustering strategy (Section IV). Observed IP addresses are recorded and used in consequent predictions. Single attack iteration is summarised in Algorithm 1. We'll suppose that each iteration of the assault begins right after the target network assigns N new IP addresses to the intended hosts, and that the attackers' aim is to locate those N IP addresses. The acquired data is used by the prediction model to provide a list of categorized forecasted IP addresses. As a result of the call for action, the priority order is probably to be decreased and omitted.

Algorithm 1 One iteration of a denial of service attack on N hosts in the target network.

Require: N, M

1: O □ [ ]

2: for A ∈ predict(M) do
3: for A' ∈ complete(A) do
4: attack the server on A'
5: if attack on A' succeeded then
6: append(A', O)
7: if |O| = N then
8: return
9: end if
10: end if
11: end for
12: end for
13: Update (M) with information from this iteration

B. Random Attacker: The model M for Algorithm 1 in this strategy simply delivers a list of all recorded prefixes in random sequence. The random attacker's purpose is to provide a simple and quick attack technique that can be implemented in exercise, and it also relies on the data gathered by the clustering attacker.

C. Frequency Attacker: Based on the frequency of presence in the dataset, the frequency attacker generates estimates from a sorted (in descending order) list of prefixes. According to the frequency attacker, address prefixes with a high frequency are more likely to reoccur.

D. Clustering Attacker: When the surface of the target network changes, the clustering attacker launches an attack. In an ideal world, the attacker knows when new IP addresses are assigned to hosts on the surface. Using the most anticipated transition of the N IP addresses seen in a prior (preferably, the preceding) attack iteration, the assault iteration forecasts the collection Q of IP addresses freshly allocated to the hosts. The attacker combines the dataset and constructs a Markov transition matrix, as explained above, to determine the most likely transitions. The goal is to guess the first 24 bits of the address and leave the final byte to a brute force assault. The suggested approach may be extended to clustering the address's first $x \leq 32$ bits. The notion is that certain IP addresses are assigned first, followed by others in a cyclical pattern. By analysing IP addresses in the time series, a Markov transition matrix is utilised to record the most plausible transition of IP address groups Ak across clusters, forming a prediction set.

5. Evaluation

Subsection V-B examines the IP address data acquired, whereas Subsection V-C discusses the findings of simulated attack trials. Subsection V-D investigates the impact of mixing IP addresses from several regions to expand the address space. Finally, in Subsection V-E, parallelized assaults are discussed.

TABLE 1. Summary of IP addresses collected.

Region	Days	Total IP Addresses	Different IP Addresses	3-byte prefixes
AP-NORTHEAST-1	46	30,689	7,236	235
CA-CENTRAL-1	42	28,578	15,836	439
EU-WEST-1	109	120,142	7,812	550
EU-WEST-3	43	29,309	13,766	203
SA-EAST-1	45	30,187	2,143	88
US-EAST-1	63	44,405	38,744	1666
US-WEST-1	46	30,965	3,907	258
GCP	42	29,025	42	42

Data Collection We utilised an AWS user profile and a GCP user account to assign and record IP addresses at defined time frames using tools available to average users (At the time of the study, a GCP user account was established, and an AWS account that had previously been created was utilised). Amazon Internet Services: AWS only permits customers to establish a total of five elastic IP addresses that may be paired with an EC2 instance (an AWS virtual machine) and then disconnected and reused for another instance.

Google Cloud Platform: GCP has a different policy: you can only generate one universal elastic IP address at a time. As a result, obtaining elastic IP addresses in GCP for the intent of obtaining a varied collection of IP addresses was not feasible at the time of this investigation. Instead, five virtual machines were created to capture IP addresses, then the virtual machines were destroyed and new ones were created.

B. Analysing Collected IP Address: This section provides a statistical summary of the data collected, exposing some details about how AWS and GCP assign IP addresses. The purpose of this subsection is to look at data sequences for three-byte prefixes in particular (IP addresses first 24 bits). The obtained data is then utilised to anticipate three-byte prefixes in Subsection V-C.

The term "complete database" refers to a collection of all conceivable three-byte prefixes in a certain cloud Computer operating system area, subject to temporal constraints imposed by Ω (may be such a major hurdle Prefixes are only available to a certain number of users). There are two approaches to the analysis: (1) Counting the number of new data points recorded each day (Fig 2), and (2) Counting the number of potential values in the most recent byte Each three-byte prefix seen (Table III) New 3-byte prefixes seen in each days of data collection for each region

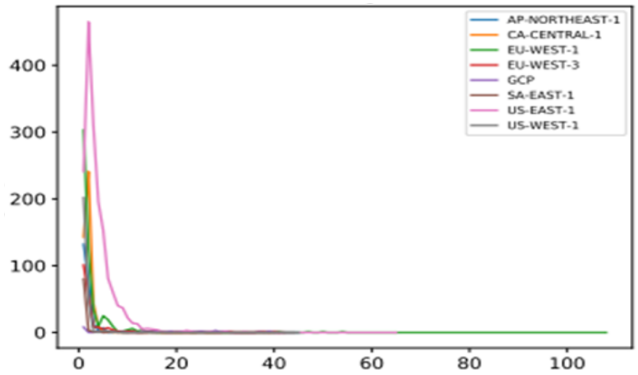

FIGURE 2. Daily new three-byte prefixes in each dataset.

TABLE 2. Days in ascending order

Region	Days	Days to observe all 3-byte prefixes	Days with no new 3-byte prefix
AP-NORTHEAST-1	46	11	38
CA-CENTRAL-1	42	6	35
EU-WEST-1	109	54	88
EU-WEST-3	43	40	23
SA-EAST-1	45	14	37
US-EAST-1	63	34	38
US-WEST-1	46	20	37
GCP	42	39	17

TABLE 3. The number of days until no more new three-byte prefixes are observed in the remainder of the dataset (second column), and the number of days in which no previously-unobserved three-byte prefixes are observed (third column).

Region	Max.	Min.	Mean	Median
AP-NORTHEAST-1	75	1	31	30
CA-CENTRAL-1	66	8	36	36
EU-WEST-1	56	1	14	12
EU-WEST-3	174	1	68	63
SA-EAST-1	139	1	24	14
US-EAST-1	55	1	23	22
US-WEST-1	91	1	15	14
GCP	1	1	1	1

TABLE 4. Statistical summaries for the number of values observed in the last byte for each three-byte prefix.

Region	Max.	Min.	Mean	Median
AP-NORTHEAST-1	0.01	≈ 0	0.00425	0.004
CA-CENTRAL-1	0.005	0.001	0.00229	0.002
EU-WEST-1	0.007	≈ 0	0.00179	0.0015
EU-WEST-3	0.012	≈ 0	0.0049	0.005
SA-EAST-1	0.067	≈ 0	0.01136	0.007
US-EAST-1	0.002	≈ 0	0.00066	0.001
US-WEST-1	0.024	≈ 0	0.00384	0.003
GCP	0.076	≈ 0	0.02379	0.018

TABLE 5. Relative frequencies of three-byte IP prefixes. The value in each cell is computed by dividing the number of occurences of each unique IP prefixes in a region by the total number of recorded IP prefixes. ≈ 0 indicates less than 0.0001.

Region	H1	H2	H3	H	Max.
AP-NORTH-EAST-1	1.106	1.846	4.632	5.342	5.46
CA-CENTRAL-1	0.692	0.699	5.462	6.049	6.084
EU-WEST-1	0.961	2.162	5.06	6.058	6.31
EU-WEST-3	0.565	0.565	5.05	5.06	5.313
SA-EAST-1	0.654	0.661	3.724	3.887	4.477
US-EAST-1	1.495	2.738	5.668	7.577	8.012
US-WEST-1	1.16	1.62	4.993	5.364	5.553
GCP	0.439	1.513	30182	3.364	3.738

TABLE 6. Shannon entropy values provide a measure of diversity in the dataset. Hb is the entropy of byte b, while H is the entropy of the first three address bytes. The last column shows the maximum possible entropy for each region's observations.
The clustering attacker benefits from repetition in the database when selecting their target servers. For distinct three-byte prefixes, the recurrence rate was calculated

Region	Max.	Min.	Mean	Medium
AP-NORTH-EAST-1	13711	1	233	125
CA-CENTRAL-1	7346	1	432	293
EU-WEST-1	40916	1	546	277
EU-WEST-3	26801	1	198	98
SA-EAST-1	8917	1	87	21
US-EAST-1	31383	1	1582	1013
US-WEST-1	14203	1	255	141
GCP	27165	1	25	7

TABLE VI: Gaps between three-byte prefixes' repetitions. Within each region, for each unique three-byte IP prefix, the reported statistic is for the number of three-byte prefixes recorded between every repetition of the three-byte IP prefix.

C. Attack Simulation

Refreshing IP loop addresses are used by moving target defences to distract attackers. A set of My IP Addresses 0 Requested from IP S addresses are changed throughout each refresh cycle. Remember that this is the study's main objective. is to forecast IP Addresses in S 0, on each refreshing cycle, using data gathered from AWS and GCP. The efficiency of each assault technique depends on whether N = 1 or N > 1, measured by one or the quantity of hypotheses needed to forecast More prefixes. The assault repeats on the target network. Attack repetition begins and ends at the start of each refreshing cycle if all N hosts are successfully identified and attacked, or if there are no prefixes to try.

D. Enlarging the Address Space

Three-byte prefixes are often repeated by the function, as the findings of the preceding section reveal. Although fixing this issue is outside the scope of this project and will need in-depth study, there may be a quick fix. Increase the amount of the address space that is available. One way is to alter the IP address of the target server at random. One method is to request addresses from several areas. The experiment was well planned. The purpose is to replicate a self-defense strategy for obtaining IP addresses from several different sites.

E. Parallel attacks

The attack model variation and the process of reducing the IP address prediction time are parallel. The attack can be parallelized to a specific target server; there are three ways to do this:

1) Parallel attacking arsenal for a single attacker,

2) No information shared within multiple independent attackers, and

3) Multiple attackers coordinated attack.

This reduces the time required to predict a parallel attack and execute target IP address but simultaneous attempts many hosts.

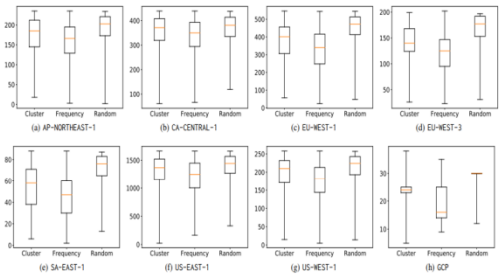

FIGURE 2. Performance of simulated attack iterations.

On each box plot, the x-axis shows the attack strategy, and the y-axis shows the number of guesses from the prediction list to predict the current prefixes used by the target server (not that the scales on the y-axis vary widely across the regions). Each box shows the minimum and the maximum (the whiskers), the median (the horizontal line in the rectangle), and the second and the third quartiles (the rectangle).

F. Study Limitations

In cloud computing pages the used space is seen as limited when scoured through tests and database. Moving target Security system prediction is still affected even if IP address assignment is random and unavailable. Attackers can easily design other methods to collect data given enough resources and time, it can disclose more formats, to collect even larger datasets in the data.

6. Conclusion

Possibility to predict IP addresses assigned by the cloud System operating systems are dangerous for moving target security It considers IP address allocations provided by cloud services very unpredictable. IP address assignments can be reliably predicted by an attacker. Thus, when IP addresses are being allocated while designing moving target security systems with a key mechanism it should be carefully considered to maximize entropy disable accurate predictions on attackers of selected IP addresses.

References

1. A. Yaar, A. Perrig, and D. Song, "Pi: a path identification mechanism to defend against DDoS attacks," in 2003 Symposium on Security and Privacy, 2003., May 2003, pp. 93–107.
2. A. Lakhina, M. Crovella, and C. Diot, "Mining anomalies using traffic feature distributions," SIGCOMM Comput. Commun. Rev., vol. 35, no. 4, pp. 217–228, Aug. 2005. [Online]. Available: http://doi.acm.org/10.1145/1090191.1080118

3. P. Barford, J. Kline, D. Plonka, and A. Ron, "A signal analysis of network traffic anomalies," in Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment. ACM, 2002, pp. 71–82.
4. J. Moore, J. Chase, P. Ranganathan, and R. Sharma, "Making scheduling "cool": Temperature-aware workload placement in data centers," in Proceedings of the USENIX Annual Technical Conference, ser. ATEC '05. Berkeley, CA, USA: USENIX Association, 2005, pp. 5–5. [Online]. Available: http://dl.acm.org/citation.cfm?id=1247360.1247365
5. R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, "Controlling high bandwidth aggregates in the network," SIGCOMM Comput. Commun. Rev., vol. 32, no. 3, pp. 62–73, Jul. 2002. [Online]. Available: http://doi.acm.org/10.1145/571697.571724
6. D. L. Cook, W. G. Morein, A. D. Keromytis, V. Misra, and D. Rubenstein, "WebSOS: protecting web servers from DDoS attacks," in 11th IEEE International Conference on Networks, Sept 2003, pp. 461–466.
7. A. D. Keromytis, V. Misra, and D. Rubenstein, "SOS: an architecture for mitigating DDoS attacks," IEEE Journal on Selected Areas in Communications, vol. 22, no. 1, pp. 176–188, Jan 2004.
8. Q. Jia, K. Sun, and A. Stavrou, "MOTAG: Moving target defense against internet denial of service attacks," in 22nd International Conference on Computer Communication and Networks, 2013.
9. S. Venkatesan, M. Albanese, K. Amin, S. Jajodia, and M. Wright, "A moving target defense approach to mitigate DDoS attacks against proxy-based architectures," in IEEE Conference on Communications and Network Security, 2016.
10. 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.
11. E. Al-Shaer, Q. Duan, and J. H. Jafarian, "Random host mutation for moving target defense," in Security and Privacy in Communication Networks, A. D. Keromytis and R. Di Pietro, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 310–327.
12. 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.
13. J. Ullrich, K. Krombholz, H. Hobel, A. Dabrowski, and E. Weippl, "IPv6 security: Attacks and countermeasures in a nutshell," in 8th USENIX Workshop on Offensive Technologies (WOOT 14). San Diego, CA: USENIX Association, 2014. [Online]. Available: https://www. usenix.org/conference/woot14/workshop-program/presentation/ullrich
14. J. Ullrich, P. Kieseberg, K. Krombholz, and E. Weippl, "On reconnaissance with IPv6: A pattern-based scanning approach," in 2015 10th International Conference on Availability, Reliability and Security, Aug 2015, pp. 186–192.
15. P. Foremski, D. Plonka, and A. Berger, "Entropy/IP: Uncovering structure in IPv6 addresses," in Proceedings of the 2016 Internet Measurement Conference, ser. IMC '16. New York, NY, USA: ACM, 2016, pp. 167–181. [Online]. Available: http://doi.acm.org/10.1145/ 2987443.2987445
16. M. Wright, S. Venkatesan, M. Albanese, and M. P. Wellman, "Moving target defense against DDoS attacks: An empirical game-theoretic analysis," in ACM Workshop on Moving Target Defense, 2016.
17. E. Miehling, M. Rasouli, and D. Teneketzis, "Optimal defense policies for partially observable spreading processes on bayesian attack graphs," in Second ACM Workshop on Moving Target Defense, 2015.
18. R. Zhuang, A. G. Bardas, S. A. DeLoach, and X. Ou, "A theory of cyber attacks: A step towards analyzing MTD systems," in Second ACM Workshop on Moving Target Defense, 2015.
19. R. Zhuang, S. A. DeLoach, and X. Ou, "Towards a theory of moving target defense," in First ACM Workshop on Moving Target Defense, 2014.
20. 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.
21. D. Evans, A. Nguyen-Tuong, and J. Knight, Effectiveness of Moving Target Defenses. Springer, 2011.
22. 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.
23. 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.
24. 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.
25. S. Achleitner, T. La Porta, P. McDaniel, S. Sugrim, S. V. Krishnamurthy, and R. Chadha, "Cyber deception: Virtual networks to defend insider reconnaissance," in 8 th ACM CCS International Workshop on Managing Insider Security Threats, 2016.

