# EFFECTIVENESS OF MOVING TARGET DEFENSE USING NETWORK ADDRESS SHUFFLING

***Email: meksuvi33@gmail.com**

**[1]Kalaivani, Mekala, Viji, [2]K.S.Giriprasath**

**[2]Associate Professor, Nandha Engineering College**

**ABSTRACT — Moving Target Defense (MTD) has been proposed as a new innovative technology to change the unbalanced condition between attacks and defences. Network address shuffling is an important branch of MTD technology. Adopting moving target defense (MTD) helps to prevent the cyber-attacks by continuously changing the attack outward. Here, we use the transmutation pattern for shuffling the network address. Virtual IP creation and IP address shuffling is the main concept in our project. In this project, we use a server similar to DNS server for mapping the virtual IP to real IP. Then, we summarize and analyze the supporting techniques and related features for each network address shuffling technique mentioned in this paper.**

## I. INTRODUCTION

Cybercrime is a growing issue for global enterprises and individuals. Cyber criminals (i.e., attackers) are focusing more on valuable assets and critical infrastructures in a networked system (e.g., enterprise systems and cyber physical systems). Security mechanisms (e.g., firewalls) may enhance the security, but the overall in-depth security of the networked system cannot be estimated without a security analysis (e.g., cannot identify security flaws and potential threats)[1]. However, cyber-attacks (such as IP prefix hijacking [3], botnet [4], DDoS attack [5]) can be seen everywhere and at any time. Such security disasters are repeatedly showing that the security of the network is always facing severe challenges. Moreover, attackers may explore an attack surface of the networked system to find weaknesses, and exploit them to penetrate through [1]. First, the attackers have the advantage of time, since they can perform susceptibility analysis and penetration testing for specific target repeatedly before they achieve the final goal. Second, the attackers have asymmetric advantage in terms of acquiring the information needed for initiating and launching an attack and the attackers can attack as long as there is a usable susceptibility; while the defenders have to secure all potential susceptibilities and prevent all the attacking means that can be utilized by the attackers. Third, the attackers have the advantage of cost to expand the attack, since the homogeneity in network configurations enables the attackers to carry out large-scale attack easily and at low cost once a small scale attack succeeds. Therefore, in the struggle between cyber network attack and defense, the attackers typically have asymmetric advantages and the defenders are always disadvantaged by being passive. IP address is an important system attribute. Therefore, it is important to reduce and continuously change the attack surface based on a security analysis[1]. Moving target defense (MTD) can continuously change the attack surface of the networked system. Consequently, it is difficult to measure and compare the effectiveness of MTD techniques (e.g., which MTD technique minimizes the system risk?). In this paper, the term effectiveness of the MTD techniques describes the ability to enhance the security of the system by minimizing the efforts of the defender (e.g., to minimize the system risk with a given resources) while maximizing the efforts of the attacker (e.g., to maximize the attack cost). To address this problem, we propose to incorporate MTD techniques into network address shuffling assess the effectiveness of them[5]. For this reason, changing IP address and/or port number is an effective way to increase the work effort for attacking. That is the origin of network address shuffling.

## II. REVIEW TO NETWORK ADDRESS SHUFFLING

Network address shuffling technique aims to change the IP address (and port number) of target periodically or erratically. From the existing research on network address shuffling, we find that there is one pattern called mutation for the changing.

In the transmutation pattern[2], the synchronization of communication is not strict in time, i.e., one side of communication (e.g. the clients) do not need to know the shuffling information of the other side of communication (e.g. the server). The synchronization is usually achieved by routing update and DNS request/respond, or the other supporting third-party mechanism. Next we will take a brief introduction to network address shuffling techniques according to the two patterns.

### Transmutation

SDNA [21] is an architecture that constructively combines hypervisor technology, Common Access Card-based authentication together in a complementary way. In this architecture, the SDNA Entity within each node can rewrite the address of packets entering and exiting the Operating System (OS) to prevent each Guest from knowing the identity of other nodes within the enclave. When a DNS response comes to the guest, the SDNA Entity would replace the real IP with Token IP which is generated by the SDNA Entity. When the guest initiates a connection to a Token IP, the SDNA Entity would rewrite the packets by replacing the Token IP with the real IP. In other words, one side of a communication does not know the other's real address, and the Token IP is obtained from the other's SDNA Entity when it requests a DNS resolution. The SDNA is transparent to the OS and compatible with the existing infrastructure. However, the traffic between the communication endpoints must flow through one or more intermediate nodes to be rewritten for concealing the endpoints' identifies, and it requires multiple key exchanges and authentications in the paths' establishment process, thus the complexity and cost of implementation is high.

## III. IMPLEMENTATION

In our project, we use the LRU(Least Recently Used) algorithm for shuffle the IP address. It is more efficient for shuffling.

**LFU algorithm in pseudo-code:**

```
LRU (page p)
If p is in the buffer then LAST(p) = current time;
Else
  i) Min = current time + 1;
  ii) For all pages q in the buffer do
    a) If (LAST(q) < min)
      victim = q
      Min = LAST(q)
  iii) If victim is dirty then flush it to disk
  iv) Fetch p into the buffer frame held by victim
  LAST(p) = current time
```

This algorithm is preferred for the timing of the IP shuffling. LRU algorithm is efficient for time consumption, so only we used this algorithm. Triggering process is based on this algorithm. In the triggering table contains a number of virtual IP. Virtual IP mapping the real IP through the DNS server. Here, the DNS server process is mapping the virtual IP to real

IP. Buffering is the one of the concept in the triggering table. In this project, virtual IP's are shuffle based on the triggering.

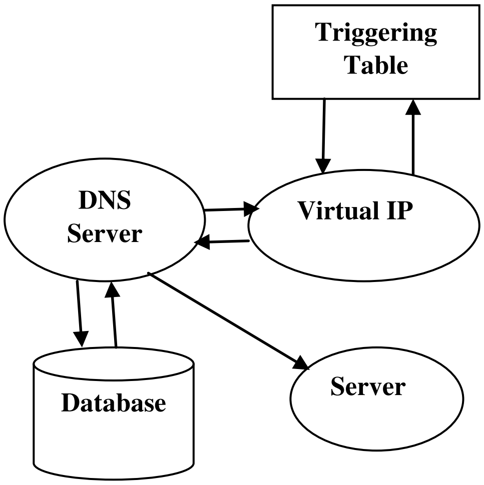

Fig. Network Address Shuffling.

IP TRIGGERING:

In this module through the triggering new virtual IP will be assigned.Here, we using LRU( Least Recently Used) algorithm for efficiently shuffling the IP address.Triggered virtual IP send to the DNS server.

DNS SERVER:

In our project, We use the database for maintain the process of DNS server. The process of DNS server is similar to the IP mapping.

## IV CONCLUSION

Moving target defense is a network defense strategy that continuously changes the attack surface to prevent cyber crimes and thwart attacks. By doing so, we can minimize the potential socio-economic impact on enterprises and individuals, as well as protecting important assets and critical infrastructures. A major problem of adopting the MTD techniques is the inability to guarantee that the security is enhanced by changing the attack surface. Therefore, we must assess the change in security prior to deploying any MTD techniques. However, the effectiveness of deploying the various MTD techniques cannot be compared to one another, because they did not consider using a formal security model to analyze them. Here, we use the transmutation pattern for shuffling the network address. Virtual IP creation and IP address shuffling is the main concept in our project.

In this project, we use a server similar to DNS server for mapping the virtual IP to real IP. What's more, under each category, we gave a detailed description on each mechanism. Thereafter, we analyzed and summarized them. Finally, we discussed some key issues on implementing an effective mechanism in network address shuffling. With this work, we hope to stimulate more follow-up research in this field.

## REFERENCES

[1] Jin B. Hong, Member, IEEE and Dong Seong Kim, Member, IEEE "Assessing the Effectiveness of Moving Target Defenses Using Security Models" VOL. 13, NO. 2, MARCH/APRIL 2016.

[2] Guilin Cai, Baosheng Wang, Xiaofeng Wang, Yulei Yuan, Sudan Li "An Introduction to Network Address Shuffling" Jan. 31 ~ Feb. 3, 2016 ICACT2016.

[3] P. Manadhata and J. Wing, "An attack surface metric," IEEE Trans. Softw. Eng., vol. 37, no. 3, pp. 371–386, May/Jun. 2011.

[4] R. Zhuang, S. Zhang, S. DeLoach, X. Ou, and A. Singhal "Simulation-based approaches to studying effectiveness of moving-target network defense," presented at the Nat. Symp.Moving Target Res., Annapolis, MD, USA, 2012.

[5] R. Zhuang, S. Zhang, A. Bardas, S. DeLoach, X. Ou, and A. Singhal, "Investigating the application of moving target defenses to network security," in Proc. 6th Int. Symp. Resilient Control Syst., 2013, pp. 162–169.

[6] P. Manadhata, "Game theoretic approaches to attack surface shifting," in Moving Target Defense II, vol. 100, series Advances in Information Security, S. Jajodia, A. K. Ghosh, V. Subrahmanian, V. Swarup, C. Wang, and X. S. Wang, Eds. New York, NY, USA:Springer, 2013, pp. 1–13.

[7] M. Crouse and E. Fulp, "A moving target environment for computer configurations

using genetic algorithms," in Proc. 4th Symp. Configuration Anal. Autom., 2011.

[8] D. Evans, A. Nguyen-Tuong, and J. Knight, "Effectiveness of moving target defenses," in Moving Target Defense, vol. 54, series Advances in Information Security, S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, Eds. New York, NY, USA:Springer, 2011, pp. 29–48.

[9] J. Yackoski, J. Li, S. DeLoach, and X. Ou, "Mission-oriented moving target defense based on cryptographically strong network dynamics," in Proc. 8th Annu. Cyber Security Inf. Intell. Res. Workshop, 2013, pp. 57:1–57:4.

[10] V. Casola, A. De Benedictis, and M. Albanese, "A moving target defense approach for protecting resource-constrained distributed devices," in Proc. IEEE 14th Int. Conf. Inf. Reuse Integr., 2013, pp. 22–29.

[11] A. Paulos, P. Pal, R. Schantz, and B. Benyo, "Moving target defense (MTD) in an adaptive execution environment," in Proc. 8th Annu. Cyber Security Inf. Intell. Res. Workshop, 2013, pp. 62:1–62:4.

[12] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. Wing, "Automated generation and analysis of attack graphs," in Proc. IEEE Symp. Security Privacy, 2002, pp. 273–284.

[13] B. Schneier, Secrets and Lies: Digital Security in a Networked World. New York, NY, USA: Wiley, 2000.

[14] J. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: Transparent moving target defense using software defined networking," in Proc. Hot Topics Softw. Defined Netw., 2012, pp. 127–132.

[15] S. Antonatos, P. Akritidis, E. Markatos, and K. Anagnostakis, "Defending against hitlist worms using network address space randomization," in Proc.ACMWorkshop Rapid Malcode, 2005, pp. 30–40.

[16] B. Danev, R. Masti, G. Karame, and S. Capkun, "Enabling secure VM-vTPM migration in private clouds," in Proc. 27th Annu. Computer. Security Appl. Conf., 2011, pp. 187–196.

[17] Y. Zhang, M. Li, K. Bai, M. Yu, and W. Zang, "Incentive compatible moving target defense against VM-colocation attacks in clouds," in Information Security and Privacy Research, vol. 376, series IFIP Advances in Information and Communication Technology, D. Gritzalis, S. Furnell, and M. Theoharidou, Eds. New York, NY, USA: Springer, 2012, pp. 388–399.

[18] H. Okhravi, A. Comella, E. Robinson, S. Yannalfo, P. Michaleas, and J. Haines, "Creating a cyber moving target for critical infrastructure applications," in Critical Infrastructure Protection V, vol. 367, series IFIP Advances in Information and Communication Technology, J. Butts and S. Shenoi, Eds. New York, NY, USA: Springer, 2011, pp. 107–123.

[19] S. Vikram, C. Yang, and G. Gu, "NOMAD: Towards non-intrusive moving-target defense against web bots," in Proc. 1st IEEE Conf. Commun. Netw. Security, 2013, pp. 55–63.

[20] Q. Jia, K. Sun, and A. Stavrou, "MOTAG: Moving target defense against internet denial of service attacks," in Proc. Int. Conf. Comput. Commun. Netw., Jul. 2013, pp. 1–9.

[21] J. Rohrer, A. Jabbar, and J. Sterbenz, "Path diversification for future internet end-to-end resilience and survivability," Telecommun. Syst., vol. 56, pp. 49–67, 2014.

[22] A. Newell, D. Obenshain, T. Tantillo, C. Nita-Rotaru, and Y. Amir, "Increasing network resiliency by optimally assigning diverse variants to routing nodes," in Proc. 43rd Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw., 2013, pp. 1–12.

[23] D. Glynis, H. Salim, A. Youssif, and R. Gabriel, "Resilient dynamic data driven application systems (rDDDAS)," Procedia Comput. Sci., vol. 18, pp. 1929–1938, 2013.

[24] T. Jackson, B. Salamat, A. Homescu, K. Manivannan, G. Wagner, A. Gal, S. Brunthaler, C. Wimmer, and M. Franz, "Compiler- Generated software diversity," in Moving Target Defense, vol. 54, series Advances in Information Security, S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, Eds. New York, NY, USA: Springer, 2011, pp. 77–98.