A Positive Feedback Mechanism of Adaptive Dynamic System

IOP Conf. Series: Materials Science and Engineering **569** (2019) 042009 doi:10.1088/1757-899X/569/4/042009

A Positive Feedback Mechanism of Adaptive Dynamic System

Pengchao Wang*, Fucai Chen, Guozhen Cheng

National Digital Switching System Engineering and Technological Research Center (NDSC) Zhengzhou, China

*Corresponding author's e-mail: 17616247471@163.com

Abstract. Address dynamic technology can effectively counter reconnaissance of attackers, protect Intranet hosts by hiding their real addresses. This paper combines address dynamics technology with honeypot technology, and provides adaptive strategy guidance for address dynamics by analysing attackers' scanning tendencies. This paper designs and implements an adaptive dynamic system(ADDS) that disguises IP and MAC adaptively based on SDN. The experimental results show that the MAC and IP adaptively dynamic can achieve the optimal balance between benefits and costs, effectively deceive attackers who are sniffing in the internal network, delay the detection speed, reduce the success rate of the attackers in identifying the host, and interrupt the continuity of network attacks.

1. Introduction

As the first stage of most network attacks, reconnaissance is a prerequisite for attackers to determine the target host in the system and launch a series of subsequent attacks [1]. Because the traditional network system is designed to provide efficient and convenient communication services, its consideration of security defense mechanism is very limited, which leads to the basic design vulnerabilities such as static and predictability of traditional network systems being easily exploited by attackers. Initiating an attack, the attacker can use the off-the-shelf scanning tools (such as NAMP, Nessus, etc.) to quickly complete the target reconnaissance, and then initiate the corresponding network attack [2], [3]. This fast and simple target reconnaissance (using off-the-shelf scanning tools) is widely adopted by attackers. In addition, advanced attackers can use the probe to collect as many attributes as possible (including IP/MAC address, service port, operating system, running service, etc.) of the host in the target network system when facing a high-value target network system with certain protection. The attacker analyzes and identifies the fixed host based on the unchanged IP address, MAC address, etc., and initiates an attack such as APT (Advanced Persistent Threat)[4].

Traditional passive network security defense technologies[12], [13] (such as firewalls, intrusion detection systems, etc.) are not effective in responding to various target reconnaissance methods of attackers. For example, studies have demonstrated that scanning worms at a scan rate of once per minute can easily circumvent all major detection techniques [5]. In order to change the asymmetry of attack and defense of cyberspace, various dynamic network defense technologies based on the idea of Moving Target Defense (MTD) have been proposed[11]. But so far, the dynamic network defense technology against the attacker's target reconnaissance stage is mostly the dynamic of single network attributes, such as address hopping [6], [7], port hopping[8], dynamic topology[9], [10], etc. Although the dynamic technology involving multiple network attributes has some research, it lacks the adaptive countermeasure to the complex and changeable attack means[14].

We combine the current dynamic network defense with honeypot technology to realize an adaptive dynamic system(ADDS). The update of dynamic policy is realized through the log of honeypot analysis record. Experiments show that our adaptive defense system has higher security capability, and can counter the sniffer in real time according to the change of the attacker's strategy.

2. Design

Adaptive dynamic system(ADDS) are designed to provide efficient adaptive active defenses while ensuring service availability. ADDS's implementation architecture is shown in Fig.1. ADDS has two key facilities: ADDS controller and Adaptive Strategy Generate Engine(ASGE). ADDS controller follows the dynamic strategy(including the hop cycle and the distribution function of the virtual address) generated by Adaptive Strategy Generate Engine to send the dynamic rules to OF-switches. We divide the internal network into three regions, all connected to OF-Switches. Since the controller has a global view, we can formulate different dynamic strategies for the communication of hosts in different region. The specific workflow of deception based on feedback will be described in next section.

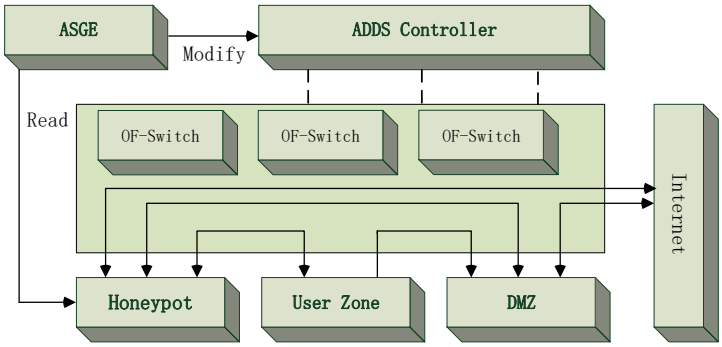

Fig.1 The architecture of ADDS

2.1. ADDS Controller

The implementation of ADDS controller is shown in Fig.2.We developed ADDS controller based on OpenDaylight(ODL). The controller is connected to ASGE through the Northbound Interface. ADDS controller generates flows which modify source rIP(real IP) and source rMAC(real MAC) to vIP(virtual IP) and vMAC(virtual MAC) , and installs them in the OF-Switch connected to the source end-host. The controller is the core component of the whole system, it contains three modules. Each module's function are described below:

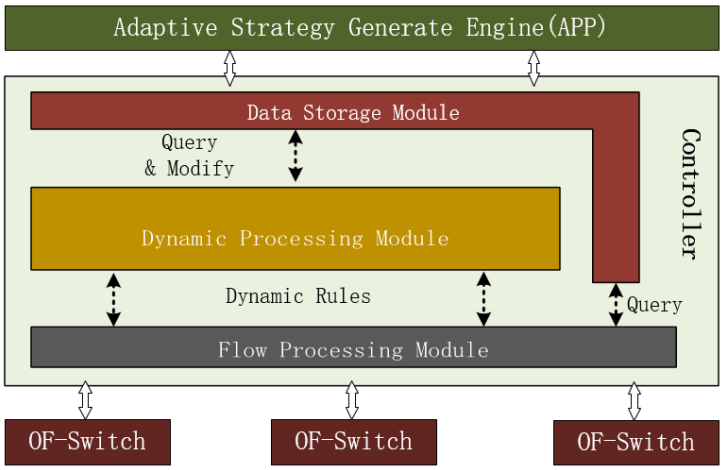

Fig.2 The overview of ADDS Controller

1) Data Storage Module: In ODL controller, we use DataStore to store information.

2) Dynamic Processing Module: Responsible for assigning rIP,vIP,vMAC to host. Handle DHCP ,ARP,DNS messages and reply rIP to host. The dynamic engine modify vMAC and vIP into the Data Storage Module over time.

3) Flow Processing Module: Establish the session path for communication of two hosts, and real-time update and install flows in all OF-switches in the session path.

2.2. DMZ

The DMZ zone places servers providing external services. Servers accessing the DMZ zone on an external network need a firewall to complete the translation from the external address to the server address. Hosts in the DMZ zone are not allowed access to Intranet hosts. If this policy is violated, the DMZ zone can be used as a springboard to attack the entire Intranet when an intruder breaks into the DMZ.

2.3. User Zone

DHCP is used to automatically obtain the real address for hosts in the user area, and the communication between them adopts the method of hiding source address.

2.4. Honeypot

Honeypot records the attack behavior by interacting with the attacker. An attacker may waste time attacking because of multiple services in Honeypot.

2.5. Adaptive Strategy Generate Engine(ASGE)

ASGE reads Honeypot's log file and analyzes the attacker's attack behavior based on it, such as the IP segment attacker tends to scan. ASGE issues real-time hopping strategies to the controller, including hopping frequency and virtual addresses pool and blacklist updates.

2.6. Communication Protocol

The communication in the system is executed strictly according to the rules of flow table distributed by ADDS controller. The communication packets are divided into different kind of packets on the basis of partition in enterprise network. In particular, communication between clients in the user area performs address dynamic. If Host A communicates with Host B in User Zone，A send packets <A_rIP,A_rMAC,B_vIP,G_MAC> to B using its real IP(A_rIP) and the real MAC(A_rMAC) and gateway MAC(G_MAC) and the current virtual IP of B(B_vIP), when these packets arrive the first OF-Switch on the path between A and B, packets are modified to <A_vIP,A_vMAC,B_rIP,B_rMAC>. Then, these modified packets will not be modified on other OF-Switches on the path and will be sent to B. As for B, its communication flow is the same as that of A.

ADDS controller imports the traffic whose source IP conforms to the blacklist into the Honeypot, regardless of where the host with the blacklisted source IP is located in any zone. Similarly, if a traffic has a destination IP that conforms to the blacklist, the traffic will also be imported into the honeypot. Specifically, the controller changes the destination address of these flows to the honeypot address. Client hosts in the User Zone are not allowed to access the Internet in principle, but they can access the Internet through an agent in DMZ zone.

3. Mutation Planning based on Feedback

In essence, implementation of adaptive dynamic is a kind of feedback based on honeypot records. In order to ensure that the honeypot can record as much as possible when the system is subject to scanning and attack, SDN controller will adopt a blacklist mechanism to import all possible malicious traffic into the honeypot by issuing flow table. This positive feedback mechanism will continuously update the blacklist and improve system security.

3.1. Problem Definition

Suppose attackers' attack is based on reconnaissance. In time $\left[t_{j-1},t_j\right)$, suppose the set of IP addresses sniffed by attackers is A_j, the set of MAC addresses sniffed by attackers is B_j. If the set of addresses sniffed by ASGE analysis is $A_j^{'}$ and $B_j^{'}$, we want to make $A_j^{'}=A_j$, but it's hard. We expect that $\frac{card(\{x\,|\,x=y,x\in A_j,y\in A_j^{'}\})}{card(A_j)}$ get max by algorithmic optimal design, and determine the frequency of address dynamic, update the virtual IP and MAC pool and blacklist.

3.2. Workflow of deception based on feedback

ADDS's security capability is embodied in two aspects. The ADDS controller import the traffic that conforms to the rules into the honeypot according to the preset blacklist (untrusted IP), and changes the IP and MAC address for the rest traffic by dynamic strategy. If the honeypot does not find the obvious interactive behavior of the attacker, the ADDS will take the initiative to hide the address. According to the information recorded by honeypot, ADDS carries out the rule of address change and updates the blacklist, the detailed workflow as shown in Fig 3:

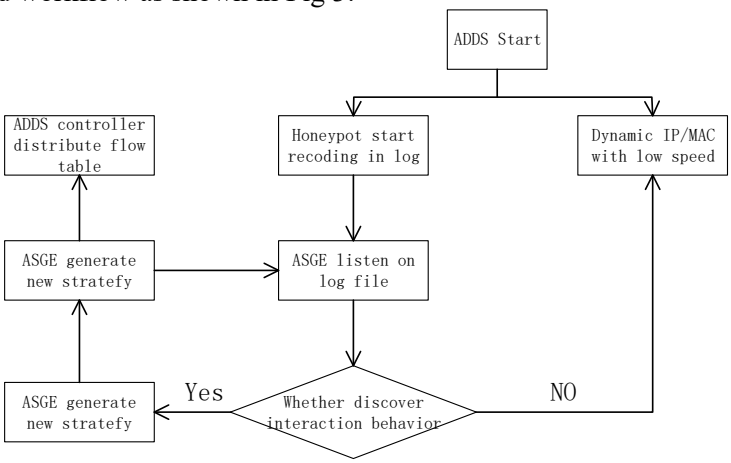

Fig.3 Workflow of deception based on feedback

4. Evaluation

We conduct experiments with little enterprise network(Fig.4) in our laboratory to verify that attacker cannot complete effective attack and ADDS has higher protection performance. We use the host of Kali system to simulate the attacker, ADDS controller and ASGE deployed on two RH2288H V3 servers.

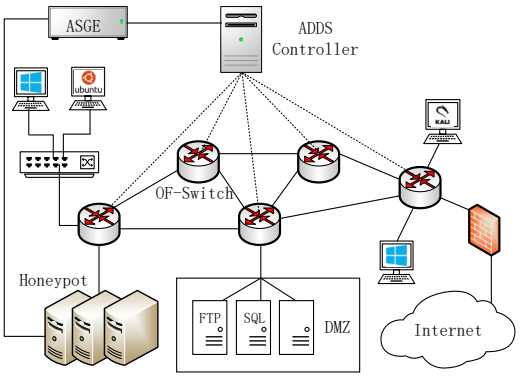

Fig.4 System implementation

We compare ADDS with different frequency OF-RHM and dynamic address technology without adaptability using scanning experiments, and analyse the performance of ADDS. Fig.5 give the real configuration of two hosts at the top, below is the result of Wireshark packet capture, we can see that the source IP and source MAC obtained by the destination host are both virtual and constantly changing with time.

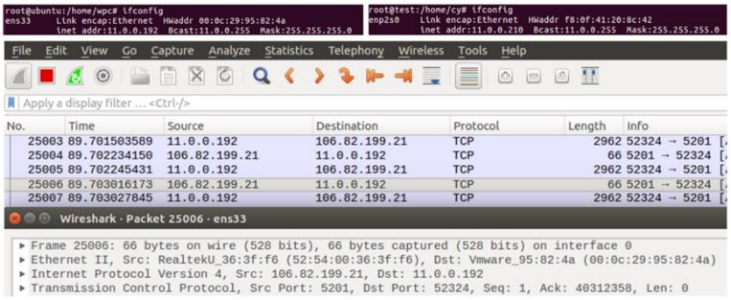

Fig.5 Wireshark packet capture

Further, we simulate an attacker using NMAP to scan and attack the network with 50 hosts. In Fig.6, we can see that as the frequency of OF-RHM hopping increases, the number of hosts scanned by the attacker decreases. But ADDS can decrease the number of sniffed hosts with average low frequency adaptively. And even if the attacker sniffs a certain online host multiple times based on different virtual IP, the attacker does not believe that the host is a previously sniffed host because they observe MAC addresses is different, so that the attack can only be based on different virtual IP. This allows the attack to be deployed only for a limited time(address mutation interval), thus cutting off the attacker's multi-stage persistent attacks and increasing attacker's overhead.

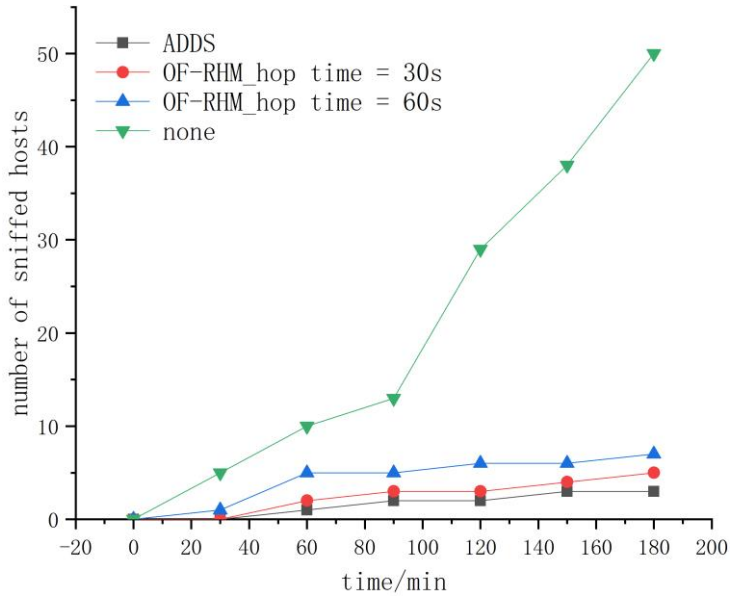

Fig.6 scanning experiments

In addition, because the attacker's malicious traffic is imported into the honeypot, the attacker's attack rate is delayed, and the attacker is tricked into an invalid attack. The attacker acquires the false information in the Intranet, reduces the accuracy of its information acquisition, so as to realize the value of the overall information acquired, and even makes it abandon the entire data due to the difficulty in distinguishing effective data.

5. Conclusions

In this paper, we implement adaptive dynamic based on SDN and honeypot to achieve multi-dimensional attribute spoofing against attackers, including IP, Mac, services, etc. We extend the traditional honeypot spoofing and design an adaptive policy update mechanism to guide the dynamic of addresses and the direction of traffic within the system. In the following work, we will focus on the optimization of the hopping algorithm, and probabilize the IP selection of virtual addresses and blacklists, so as to provide a credibility mechanism and increase the adaptability of the system.

Acknowledgments

This work is supported by the Foundation for Innovative Research Groups of the National Natural Science Foundation of China (61521003), the Foundation of the National Natural Science Foundation of China (61602509), and the Key Technologies Research and Development Program of Henan Province of China (172102210615).

Reference

[1] Yadav T, Rao A M. Technical Aspects of Cyber Kill Chain[M]// Security in Computing and Communications. Springer International Publishing, 2015:438-452.
[2] Jajodia S, Ghosh A K, Subrahmanian V S, et al. Moving Target Defense II: Application of Game Theory and Adversarial Modeling[J]. Springer Ebooks, 2013.
[3] Lyon G F. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning[M]. Insecure, 2009.
[4] Jafarian J H, Niakanlahiji A, Al-Shaer E, et al. Multi-dimensional Host Identity Anonymization for Defeating Skilled Attackers[C]// ACM Workshop on Moving Target Defense. ACM, 2016:47-58.
[5] S. Stafford and J. Li, “Behavior-based worm detectors compared,” in RAID, ser. Lecture Notes in Computer Science, vol. 6307. Springer,2010, pp. 38–57.
[6] Antonatos S, Akritidis P, Markatos E P, et al. Defending against hitlist worms using network address space randomization[J]. Computer Networks, 2007, 51(12): 3471-3490.
[7] Jafarian, Jafar Haadi, Ehab Al-Shaer, and Qi Duan. "An effective address mutation approach for disrupting reconnaissance attacks." IEEE Transactions on Information Forensics and Security 10.12 (2015): 2562-2577.
[8] Jafarian J H, Al-Shaer E, Duan Q. Openflow random host mutation:transparent moving target defense using software defined networking[C]// The Workshop on Hot Topics in Software Defined Networks. ACM, 2012:127-132.
[9] Zhao, Zheng, et al. "SDN-based Double Hopping Communication against sniffer attack." Mathematical Problems in Engineering 2016 (2016).
[10] Kai W, Xi C, Zhu Y. Random domain name and address mutation (RDAM) for thwarting reconnaissance attacks[J]. Plos One, 2017, 12(5).
[11] Kewley D, Fink R, Lowry J, et al. Dynamic Approaches to Thwart Adversary Intelligence Gathering[C]// DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings. IEEE, 2001:176-185 vol.1.
[12] Antonatos S, Akritidis P, Markatos E P, et al. Defending against hitlist worms using network address space randomization[J]. Computer Networks the International Journal of Computer & Telecommunications Networking, 2009, 51(12):3471-3490.
[13] Badishi G, Herzberg A, Keidar I. Keeping Denial-of-Service Attackers in the Dark[J]. IEEE Transactions on Dependable & Secure Computing, 2007, 4(3):191-204.
[14] Wang P, Chen F, Cheng G, et al. Poster: SIMD: A SDN-based IP and MAC Dynamic Method against Reconnaissance[J].