Poster: SIMD: A SDN-based IP and MAC Dynamic Method against Reconnaissance

Pengchao Wang, Fucai Chen, Guozhen Cheng, Liren Miao
PLA Strategic Support Force Information Engineering University, China
17616247471@163.com

***Abstract*—Network reconnaissance techniques are often used for detecting the vulnerabilities or location of potential targets, and are automatically executed by malware infected hosts. This paper design and implement a SDN-based dynamic method (SIMD) that disguises IP and MAC by virtual addresses at the network level. SIMD effectively cuts off the relevance between L2/L3 address and the real network identity, and maximizes the hidden internal host, and delay the attackers reconnaissance speed.**

I. Introduction

Detecting the vulnerability of target hosts from the inside of the network is the main way to launch a network attack.[1] The basic design vulnerabilities, such as the stasis and predictability of traditional network systems, are easily used by attackers to launch attacks.[2] Attackers can use ready-made scanning tools (such as NMAP and Nessus) to quickly complete target reconnaissance and then launch corresponding network attacks.[3]

Randomization of IP address has been shown to disrupt reconnaissance.[4] But the skilled attacker can identify a host using IP address randomization based on the same MAC, and continue his multi-stage attack. MAC addresses are assigned in the factory, MACs global uniqueness makes it a priority for skilled attackers to use it to identify hosts, except for IP. MAC addresses involve the L2 layer of TCP/IP protocol. The current MAC address randomization is mostly implemented at the operating system level, and is mostly used in wireless networks to prevent attackers from tracking mobile devices based on MAC addresses.[5] There are few studies on how to realize dynamic MAC in enterprise networks.[6] In contrast, dynamic IP in enterprise network has been extensively studied. SDN(Software Defined Network)[7] provides a new possibility to address the synchronous dynamics of IP and MAC in enterprise network to spoof attackers.

In this paper, we propose a SIMD to achieve synchronous mutation of IP and MAC, which is transparent to end-host. SIMD can provide second level dynamic, and end-host configurations dont need to make any modify. Withed SIMD deployed in enterprise network, attackers cant get the real IP and MAC of hosts. When SIMD adopts a high frequency to change virtual addresses, attackers has little probability to sniff the real host, and cannot establish a continuous connection with the victim based on the same IP. In addition, the attacker is unable to identify the host which IP mutation frequently based on the MAC.

II. Design

SIMD runs on SDN controller, its implementation architecture is shown in Fig.1. Considering the cost of flow table, SIMD dynamic changes MAC and IP address synchronously, and in the process of communication, SDN controller generates flows which modify source rIP(real IP) and source rMAC(real MAC) to vIP(virtual IP) and vMAC(virtual MAC) and installs it in the OF-Switch which connected to the source end-host.

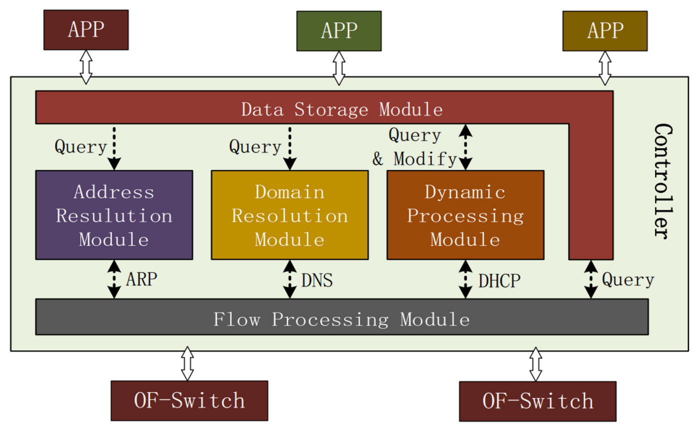


Fig. 1. The overview of SIMD

A. Architecture

We developed SIMD based on Opendaylight controller. The functions of each module in SIMD are described below:

1) Address Resolution Module: Centralized processing of ARP messages, response to the hosts request of gateway MAC.

2) Domain Resolution Module: Realize the translation function of IP and domain name, hosts can only query their own temporary domain name, all hosts can query virtual IP by domain name.

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

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

5) 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.

B. Workflow

The communication packets are divided into intra-domain packets and out-of-domain messages in enterprise network. Intra-domain packets change IP and MAC of source host according to the flow actions, while out-of-domain packets are processed by NAT. The complete communication flow of a packet in intra-domain is as follows:

1) dynamic resource allocation by DHCP: The complete communication process of the system starts from a host accessing the internal network. The DHCP_DISCOVER packet of the host enters the access OF-Switch, and the OF-Switch matches the preset flow rule to send it to the controller. The Dynamic Processing Module in the controller queries the rIP that has been stored in the Data Storage Module, and broadcasts DHCP_OFFER message carrying the rIP. When the DHCP_REQUEST of the host is sent to the controller, the Dynamic Processing Module randomly generates its vIP and Domain, and modifies to the Data Storage Module. Then the controller send DHCP_ACK message to complete the DHCP dynamic resource allocation process.

2) address resolution by ARP: We set the virtual IP address space and real IP address space on different network segments. This ensures that the hosts ARP cache table will only cache the gateways MAC, thus bypassing the problem that virtual MAC update in the ARP cache table and the corresponding flow rules generate and install. Specifically, the host sends only the ARP_REQUEST message to query the gateway MAC address.

3) establish the session between communicating parties: SIMD uses a ten element array S to represent a communication session. S is the match of the flow rule delivered by the controller to the OF-Switch. $S = \{sRip, sVip, dRip, dVip, sRmac, dVmac, sPort, dPort, Protocol, TTL\}$.In order to ensure the continuity of the session and the consideration of improving the communication efficiency, even if the virtual IP and the virtual MAC in the Data Storage Module of the controller expire, the virtual IP and the virtual MAC in the established session remain unchanged until the TTL(Time to Live) expires. The specific process for establishing a communication session between communicating parties(Host A and Host B) is as follows:
First, A requests the domain name of B through out-band mode, B get its domain name by DNS and tell A; Secondly, A queries the IP corresponding this domain name by DNS_QUERY message, and get the vIP of B by DNS_RESPONSE which was delivered by controller; Last, 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,AvMAC,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.

III. PRELIMINARY EXPERIMENTS AND DISCUSSIONS

We conduct experiments with little enterprise network in our laboratory to verify that attacker cannot scan real IP and MAC of hosts. Fig.2 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. Further, we simulate a attacker using NMAP to scan and attack the network on a host. We can see that as the frequency of hopping increases, the number of hosts scanned by the attacker decreases. 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 attackers multi-stage persistent attacks and increasing attackers overhead.

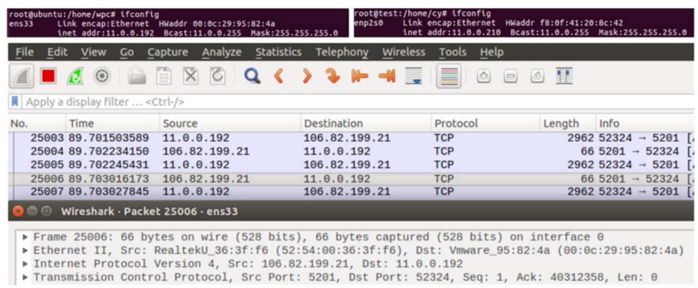


Fig. 2. Real configuration information and Wireshark capture results

The proposed method effectively disrupts the detection process of the attacker. The periodic mutation of L2/L3 layer address makes the attacker unable to accurately locate the victim and destroys the periodic attack attempt of the skilled attacker.

REFERENCES

[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] Zhao, Zheng, et al. "SDN-based Double Hopping Communication against sniffer attack." Mathematical Problems in Engineering 2016 (2016)

[4] Jafarian J H, Niakanlahiji A, Al-Shaer E, et al. Multi-dimensional Host Identity Anonymization for De-feating Skilled Attackers[C]// ACM Workshop on Moving Target Defense. ACM, 2016:47-58.

[5] Vanhoef, Mathy, et al. "Why MAC address randomization is not enough: An analysis of Wi-Fi network discovery mechanisms." Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016.

[6] Clestin Matte, Cunche M, Rousseau F, et al. Defeating MAC Address Randomization Through Timing At-tacks[C]// ACM Conference on Security Privacy in Wireless and Mobile Networks.ACM, 2016:15-20.

[7] Kreutz D, Ramos F M V, Esteves Verissimo P, et al. Software-Defined Networking: A Comprehensive Survey[J]. Proceedings of the IEEE, 2014, 103(1):10-13.

SIMD: A SDN-based IP and MAC Dynamic Method against Reconnaissance

Pengchao Wang, Fucai Chen, Guozhen Cheng, Liren Miao
PLA Strategic Support Force Information Engineering University, China

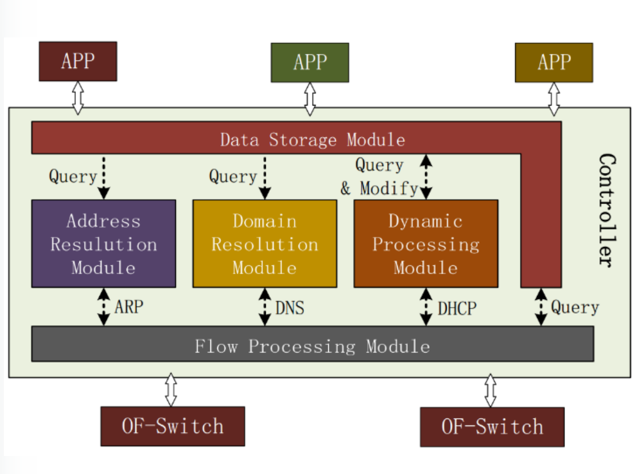
Background

◆Reconnaissance is a prerequisite for most attacks.
◆Randomization of IP address has been shown to disrupt reconnaissance.
◆Skilled attacker can identify a host using IP address randomization based on the same MAC, and continue his multi-stage attack.

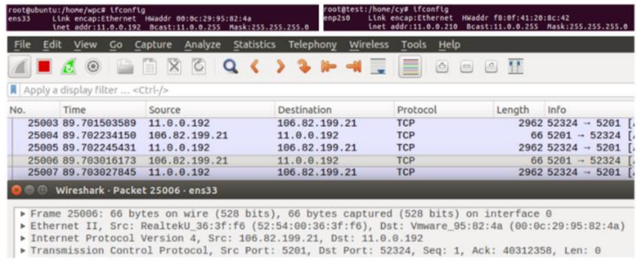
What is SIMD ?

◆ SIMD achieves IP and MAC dynamic over time.
◆ Virtual MAC changes synchronously with the virtual IP.
◆ Based on Opendaylight controller.
◆ SIMD is transparent to end-host.
◆ SIMD is transparent to end-host.

Architecture



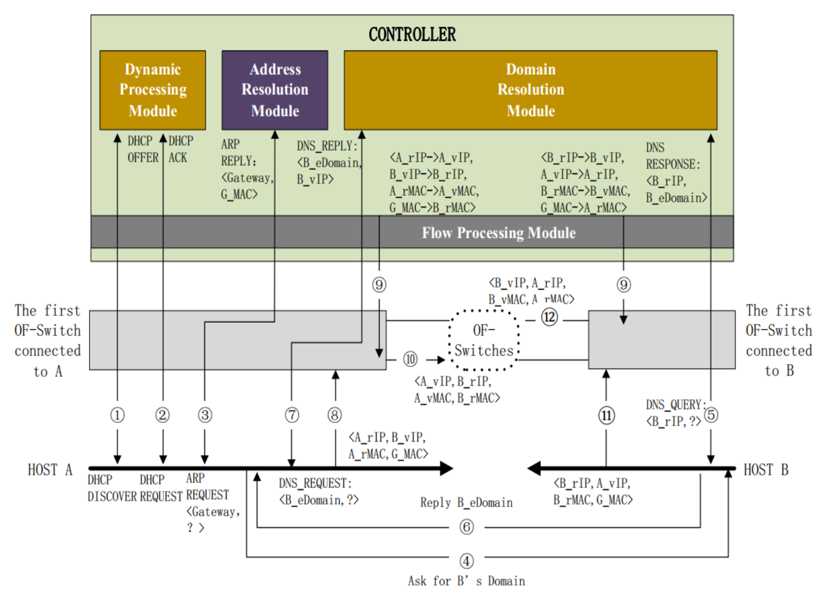
Experiments



Real configuration information and Wireshark capture results

● The source IP and source MAC obtained by the destination host are both virtual and constantly changing with time.
● As the frequency of hopping increases, the number of hosts scanned by the attacker decreases.

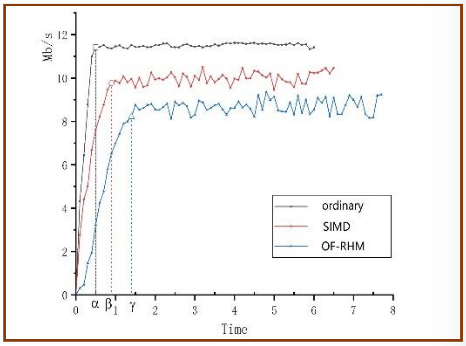
Workflow



Scan Results

	T=3600s, scan 2h		T=3600s, scan 6h		T=1800, scan 6h	
MAC dynamic	√	×	√	×	√	×
Sniffed hosts	151	127	502	541	354	338
Real hosts（rIP）	83	46	147	110	121	78
Number of different MAC addresses（diff_MAC）	151	46	502	110	354	78
$\frac{rIP}{diff\_MAC} * 100\%$	54.97%	100%	29.28%	100%	34.18%	100%

Transmission Rate



For more information, please contact 17616247471@163.com