

A New Kind of Worm in Next Generation Network

Abstract:

It is commonly believed that the IPv6 protocol could provide better protection against network worms due to its huge address space. In our research, a "dual-stack worm" is designed and programmed, which is the first real worm could spread in IPv6 Internet. It is found in present experiments that the dual-stack worm could possibly collect the IPv6 addresses of all running hosts on the link-local quickly and effectively, which may results in accelerated worm spreading on the IPv6 link-locals. The simulation results show that the worm could spread in IPv6 Internet, even faster than in the IPv4 Internet.

Keywords:

Network security, IPv6, dual-stack network, dual-stack worm, worm propagation

1. Introduction

In recent years, many IPv6 networks have been developed and deployed, such as "Internet 2" and "Moonv6" in US, "NRENS" in Europe, "JNG" in Japan, and "CNGI" in China. Generally, the evolution from current IPv4 networks toward IPv6 would go from "isolated islands" to gradual global saturation and the dual-stack would be the principal solution in the transition [1]. Since the Internet has been plagued by many worms, the purpose of the present research is to explore the activities of the worms in dual-stack networks.

One popular mechanism adopted by the worms in IPv4 networks to detect vulnerable targets is random-scanning. The effectiveness of this mechanism attributes to the 32-bit IPv4 address which allows the random-scanning worms to scan all possible hosts. It is commonly believed that the IPv6 protocol could provide better protection against these worms due to its 128-bit address huge space, so that the probability to hit a valid address in the IPv6 address space by random-scanning is very low. Thus, the transition from IPv4 to IPv6 is considered as an effective approach to preventing or reducing worms from spreading [2, 3].

It is found that the dual-stack worm, which is designed in our research, could possibly collect the IPv6 addresses of all running hosts on the link-local quickly and effectively. In fact those "isolated IPv6 islands" would actually become the "hotbeds" of the dual-stack worm especially in the slow starting phase. That is, one infected host could infect all vulnerable hosts on the same link in a short time, while it may take much longer time in IPv4 networks. The other IPv4 hosts can be found by random-scanning. As a result, the deployment of IPv6 would not help prevent the propagation of worm as expected but rather has opposite effect. And the experimental and simulation results show that the worm could spread in dual-stack network much faster than in the IPv4 Internet.

The rest of this paper is organized as follows. The design of dual-stack worm is described in Section 2. Section 3 discusses the experiment of dual-stack worm. And we conclude this paper in Section 4.

2. Design of Dual-stack Worm

In IPv6 network, there are many information sources where the worm could collect the IPv6 address information of hosts, such as neighbor discovery (ND), routing tables, multicast ping and so on [3]. We found that multicast ping is the most straightforward and effective method when scanning a local-area. Since ICMPv6 echo request was sent to the "link-local scope all-nodes multicast address"(FF02::1), lots of ICMPv6 echo reply packets would be sent back immediately, containing the IPv6 addresses of all active computers, as shown in Fig.1. The attackers could directly find the addresses of all running computers, without scanning the huge address space in IPv6 subnet.

The infected hosts spread the program of dual-stack worm to vulnerable hosts by exploiting DCOM RPC of Windows XP as W32.Blaster.Worm (first described in Microsoft security Bulletin MS03-026). And,

in order to spread rapidly in IPv4-IPv6 Internet, the dual-stack worm can detect the vulnerable hosts by a two-level scanning strategy. As shown in Fig.2, when a hosts is infected, multicast-scanning is used to acquire the addresses of all active hosts on IPv6 link-local. When all collected IPv6 addresses have been attacked or the infected hosts run IPv4 only, random-scanning is applied to find the targets in the global IPv4 Internet.

Time	Source	Destination	Info
2.680076	Fe80::20d:87ff:fe61:aa08	ff02::1	Echo request
2.680224	Fe80::20d:87ff:fe61:aa08	Fe80::20d:87ff:fe61:a530	Echo reply
2.680239	Fe80::212:3fff:fe24:9244	Fe80::20d:87ff:fe61:a530	Echo reply
2.680245	Fe80::212:3fff:fe24:8f38	Fe80::20d:87ff:fe61:a530	Echo reply
2.680252	Fe80::20d:87ff:fe61:a536	Fe80::20d:87ff:fe61:a530	Echo reply
2.680258	Fe80::211:43ff:fec2:9906	Fe80::20d:87ff:fe61:a530	Echo reply
2.680265	Fe80::290:27ff:fe5:e4f6	Fe80::20d:87ff:fe61:a530	Echo reply
2.680274	Fe80::200:e2ff:fe52:e0c6	Fe80::20d:87ff:fe61:a530	Echo reply
2.680289	Fe80::200:e2ff:fe96:331c	Fe80::20d:87ff:fe61:a530	Echo reply
2.680295	Fe80::200:e2ff:fe52:c339	Fe80::20d:87ff:fe61:a530	Echo reply
2.680302	Fe80::200:e2ff:fe9a:9ecd	Fe80::20d:87ff:fe61:a530	Echo reply
2.680311	Fe80::201:6cfff:fe35:7a7c	Fe80::20d:87ff:fe61:a530	Echo reply
2.680320	Fe80::20d:87ff:fe2f:aaad	Fe80::20d:87ff:fe61:a530	Echo reply
2.680321	Fe80::211:43ff:fec3:950	Fe80::20d:87ff:fe61:a530	Echo reply
2.680345	Fe80::200:e2ff:fe9a:4b64	Fe80::20d:87ff:fe61:a530	Echo reply
2.680351	Fe80::201:6cfff:fe38:96c4	Fe80::20d:87ff:fe61:a530	Echo reply
2.680358	Fe80::200:e2ff:fe89:61ff	Fe80::20d:87ff:fe61:a530	Echo reply
2.680369	Fe80::20f:1fff:fefa:bb33	Fe80::20d:87ff:fe61:a530	Echo reply
2.680482	Fe80::20d:66ff:fe2e:8ca	Fe80::20d:87ff:fe61:a530	Echo reply

Fig.1 The reply messages for a multicast ping

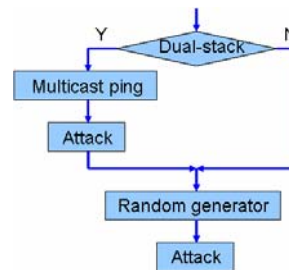


Fig.2 The flow chart of dual-stack worm

3. Experiment

To investigate the worm propagation, a dual-stack worm is released into experimental network developed to demonstrate the propagation characteristics in actual IPv6 networks. As shown in Fig.3, six victim hosts and one Releaser & Console host locate in the experimental network and connected by IPv4 Internet. In the experiment, dual-stack worms infect all victim hosts in several minutes. And all data packets, sent by these hosts are recorded. The sources of all success worm attacks are analyzed from these packets, and the whole propagation in this experiment is shown in Fig.4 as a tree structure.

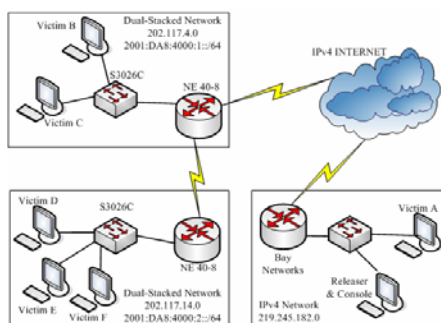


Fig.3 The structure of experimental network

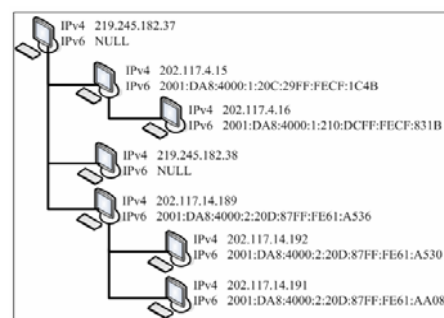


Fig.4 Propagation tree of dual-stack worm

4. Conclusion

A dual-stack worm which could spread in IPv4-IPv6 dual-stack network is investigated in present paper. Detailed analysis on how this worm propagates since the IPv6 address of all hosts on the link-local can be obtained by using multicast-scanning in a few seconds. This can accelerate worm propagation in dual-stack networks. Based on the simulation for an experimental network, it is found and first demonstrated that this worm could spread across links using random IPv4 address-space scanning and can exist and spread in an actual IPv6 network.

Reference:

- [1] D. G. Waddington, F. Chang. Realizing the Transition to IPv6. IEEE Magazine of Communications, June 2002.
- [2] A. Kamra, H. H. Feng, V. Misra, A. D. Keromytis. The effect of DNS delays on worm propagation in an IPv6 Internet. In: Proc. of the IEEE INFOCOM 2005, 2005.
- [3] S. Bellovin, B. Cheswick, A. Keromytis. Worm propagation strategies in an IPv6 Internet. [Online]. <http://www.cs.columbia.edu/~smb/papers/v6worms.pdf>