A New Worm Exploiting IPv6 and IPv4-IPv6 Dual-Stack Networks: Experiment, Modeling, Simulation, and Defense

Ting Liu, Xiaohong Guan, Qinghua Zheng, and Yu Qu, MOE KLINN Laboratory, Xi’an Jiaotong University

Abstract

It is commonly believed that the IPv6 protocol can provide good protection against network worms that try to find victims through random address scanning due to its huge address space. However, we discover that there is serious vulnerability in terms of worm propagation in IPv6 and IPv4-IPv6 dual-stack networks. It is shown in this article that a new worm can collect the IPv6 addresses of all running hosts in the IPv4-IPv6 dual-stack network for testing. The experiment results show that this worm can infect all hosts in a subnet very quickly, leading to accelerated worm propagation. In fact, one infected host could infect all vulnerable hosts in the same subnet in a short time, while it may take much longer to infect the hosts outside of the subnet in IPv4 networks. Those isolated IPv6 islands would actually become hotbeds for the dual-stack worm, especially in the early phase. As a result, the deployment of IPv6 may not be able to prevent worm propagation as expected.

In recent years, many IPv6 networks have been developed and deployed, such as Internet2 in the United States, National Research and Education Networks (NRENs) in Europe, and China’s Next Generation Internet (CNGI). In fact, China relied on IPv6 technology to transmit real-time footage of all Olympic events to live TV broadcasting systems and video streaming over the Internet. Generally speaking, the evolution from the current IPv4 network toward IPv6 would gradually go from isolated islands to global connection, and the IPv4-IPv6 dual-stack would be a feasible solution in this transition [1, 2]. Much thought and attention have been given to the transition, and a lot of research efforts made to evaluate the security implications during this period. Warfield pointed out that IPv6 offers a number of significant performance and security advantages over earlier versions, which can be wielded by either the defender or the intruder [3]. Since the Internet has been plagued by many worms, the purpose of the present research is to explore worms in IPv4-IPv6 dual-stack networks, and investigate the defense strategies in hybrid networks.

Random address space scanning (referred to as random scanning hereinafter) is one of the most popular mechanisms adopted by most worms to detect vulnerable targets in IPv4 networks. The effectiveness of this mechanism is attributed to the 32-bit IPv4 address, which allows random scanning worms to scan all possible hosts. It is commonly believed that IPv6 is huge and can provide better protection against these worms due to its 128-bit address space, which means that the probability of hitting 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 worms spreading [4].

Researchers have investigated security problems in IPv6 networks and considered several new worms able to spread in IPv6 network with intelligent scanning strategies. Kamra et al. showed that an intelligent worm could exploit the DNS necessary for any network, and modeled the behavior of such a worm in IPv6 Internet [5]. Bellovin and Cheswick outlined a number of scanning techniques that the worms can use in an IPv6 Internet to locate potential targets [6]. Chen and Ji showed that an important-scanning worm may still spread fast in IPv6 networks [7]. We discovered that there is a serious vulnerability in terms of worm propagation in IPv6 and IPv4-IPv6 dual-stack networks. A new worm called the dual-stack worm is developed and released in a contained IPv4-IPv6 dual-stack network for testing. The experiment results show that this worm can collect the IPv6 addresses of all running hosts in a local subnet very quickly, leading to accelerated worm propagation. In fact, one infected host could infect all vulnerable hosts in the same subnet in a short time, while it may take much longer to infect the hosts outside of the subnet in IPv4 networks. Those isolated IPv6 islands would actually become hotbeds for the dual-stack worm, especially in the early phase. As a result, the deployment of IPv6 may not be able to prevent worm propagation as expected.

Since it is dangerous to release a real worm into actual networks, simulation is the common technique for analyzing the characteristics of worm propagation and investigating defense strategies. Stanford et al. used the classical epidemic model to study Code Red right after the Code Red incident on July 19, 2001, assuming the worm spread at a constant rate and the Internet is a homogeneous network [8]. Considering the effects of Internet worms on persistently unpatched hosts and those with refreshed vulnerabilities, Warren proposed a more heterogeneous and realistic worm propagation model [9]. Zou
et al. presented the discrete-time simulator taking the effect of network topology into consideration to study early warning for Internet scanning worms, and to explore propagation and defense of email worms [10, 11].

In this article the species-patch model is presented by exploring a scanning strategy similar to the self-replicating behaviors of biological viruses. A dual-stack worm simulator is developed to validate the worm propagation model and investigate the propagation of the dual-stack worm in various dual-stack networks with different topologies. The simulation results show that the worm may spread in an IPv4-IPv6 dual-stack network much faster than in the pure IPv4 Internet. The structure of IPv6 links may influence worm propagation. Several defense strategies based on network topology, configuration, and management are proposed. The effectiveness of three defense mechanisms is investigated for dual-stack networks with various topologies.

The remainder of this article is organized as follows. We present the IPv4-IPv6 dual-stack worm, and show how it spreads in an actual network. The propagation model and simulator of the dual-stack worm and the simulation results are then presented. Several defense strategies and their effectiveness are shown with experiment and testing results, followed by conclusions.

IPv4-IPv6 Dual-Stack Worm

IPv4-IPv6 Dual-Stack Network

On May 28, 2008, the Commission of the European Communities put forward the target of enabling 25 percent of users to connect to the IPv6 Internet and use important services over IPv6 by 2010 [12]. Today, only a small part of the Internet is running IPv6. CAIDA observed 4,853,991 IPv4 addresses and 5,682,419 IPv4 links during 2–17 January, 2008, but only captured 4752 IPv6 addresses and 17,036 IPv6 links during 1–8 January, 2008 [13]. Therefore, a fast growth of IPv6 networks may be witnessed in the next few years.

The key to successful transition from IPv4 to IPv6 is its compatibility with the IPv4 hosts and routers [2]. Deploying IPv6 while keeping its compatibility with IPv4 will streamline the task of transferring the current Internet structure to IPv6. The dual-stack technology is considered to be the most straightforward mechanism for IPv6 hosts to remain compatible with IPv4 hosts, as both IPv4 and IPv6 protocols stack operate in parallel [1]. Therefore, the IPv4-IPv6 dual-stack network will play a more and more important role in the Internet. At the same time, worms aiming at IPv4-IPv6 dual-stack networks could be a critical threat in the coming years.

It is commonly believed that random-scanning worms can barely detect victims in the IPv6 Internet and IPv6 subnet with 128-bit and 64-bit address spaces. However, we show that IPv6 and IPv4-IPv6 dual-stack networks cannot be immune from worms. A new worm, called the IPv4-IPv6 dual-stack worm, can detect victims in the same IPv6 subnet via multicast-scanning, and scan targets in different IPv6 subnets or pure IPv4 networks via IPv4 address random-scanning, as shown in Fig. 1. When vulnerable hosts are detected, they are infected by exploiting the vulnerability of Windows XP DCOM RPC as W32.Blaster.Worm (first described in “Microsoft Security Bulletin” MS03-026).

FF02::1 is the all-nodes multicast address of link-local scope in IPv6. A packet reaching this address will be transmitted to all hosts in a local subnet. If an IPv6 router sends a router advertisement (RA) message to FF02::1, containing the information required to determine the link prefixes and other configurations, all hosts will send back neighbor solicitation (NS) packets with their addresses in the Target option [14]. The dual-stack worm could collect IPv6 addresses of all active hosts in the same subnet by sending a spurious RA packet and monitoring all NS packets within 0.5 s, as shown in Fig. 2.

The dual-stack worm attacks only running hosts in a subnet. It can hit a vulnerable host with higher probability than those applying unicast/broadcast Address Resolution Protocol (ARP) scanning, Domain Name Service (DNS) scanning, and so on. Although there are some strategies exploiting IPv4 vulnerabilities that could detect all hosts within the same subnet as quickly as multicast-scanning, most of them have been patched. For example, it would be possible to scan an IPv4 subnet by sending an echo request to its broadcast address. This vulnerability was exploited by Smurf (a well-known denial of service [DoS] attack) and has been patched in the current Internet.

The dual-stack worm would generate much less abnormal traffic (fail-connection and empty-connection) than most worms when applying its precise scanning strategy. As a result, it is difficult to detect the multicast-scanning traffic as abnormal flows. Most current operating systems (Windows XP, Vista), firewalls, and anti-virus software fail to identify spurious RAs, as shown in Fig. 2. In fact, multicast is the basis of the IPv6 Neighbor Discovery protocol, in place of ARP, Internet Control Message Protocol (ICMP) router discovery, and ICMP redirect used in IPv4 [14]. Thus, multicast-scanning cannot be prevented by filtering the multicast traffic in order to defend broadcast attacks (e.g., DoS Smurf) as in IPv4 networks.
After all the vulnerable hosts in a subnet are infected, the dual-stack worm can migrate across different IPv6 subnets or pure IPv4 networks via many well-known random-scanning schemes (e.g., DNS, email, IPv4 address) [4, 6, 8, 11].

**Dual-Stack Worm Propagation Experiment**

An experimental system is established as shown in Fig. 3. Six victim hosts with Windows XP SP1 and one releasing host are located in three subnets connected by IPv4 Internet. All network packets are captured by our monitoring system. The Releaser starts the dual-stack worm at the beginning of each experiment. The Releaser and Victim A are located in an IPv4 C-class network 219.245.182.0/24. Victims B and C are in Dual-Stack Network I (IPv4: 202.117.4.0/24, IPv6: 2001:DA8:4000:1::/64) with 14 immune dual-stack hosts. Victims D, E, and F are in Dual-Stack Network II (IPv4: 202.117.14.0/24, IPv6: 2001:DA8:4000:2::/64) with 23 dual-stack immune hosts. The IPv4 space the dual-stack worm scans is limited within three C-class subnets to prevent it from spreading outside. The dual-stack worm generates 12 parallel threads to scan and attack victims. This can accelerate worm propagation speed but not crash the vulnerable systems. The timeout limitation of each scan is set as 3 s to fit various network conditions, and the average scanning rate is 4 scans/s. The impact of the scan rate on worm propagation is investigated in the propagation simulation later. Ten experiments are conducted in the actual networks to explore the infection processes of all vulnerable hosts and the nature of the worm spreading. Some very interesting phenomena are observed:

- The propagations of the dual-stack worm are widely divergent and uncertain. The worm takes 17.7–95.1 s to infect the first vulnerable host and 51.2–140 s to infect the last one.
- The infection sequence has a special distribution. The victims in Dual-Stack II would be the first infected on average, and the average time for victims D, E, and F to be infected is 60 s. Victims B and C are infected within 80 s on average. Victim A is always the last to be infected with an average time of more than 100 s.

The dual-stack worm spread remarkably fast due to its hybrid (multicast/random) scanning strategy. The multicast-scanning strategy has probabilities of 1/15 and 2/24 to hit a vulnerable host in Dual-Stack I and II, respectively, which are much higher than that of the IPv4 random-scanning. Once a victim is infected, the entire dual-stack subnet will be infected in a few seconds. Such a short time would be neglected in comparison with the time for the worms to detect a vulnerable host by random-scanning. Thus, to see the outcome of a very large-scale infection experiment impossible to perform physically in actual networks, a dual-stack subnet may be replaced by super nodes with detection probability and scan rate approximately m times higher than one host (assume m victim hosts in a subnet).

**Worm Propagation Modeling and Simulation**

The above experiments in a small network showed that the dual-stack worm can propagate quickly. Since it is foolish to release an actual worm into the Internet, it is desirable to develop a species-patch model and a simulator to study how the dual-stack worm spreads in large-scale networks.

**Species-Patch Model**

It is difficult for a simple model to describe the propagating process of the dual-stack worm in the IPv4-IPv6 Internet, since this worm has different spreading characteristics in different subnets. Therefore, vulnerable hosts were divided into two species: IPv4-only nodes (Species A) and dual-stack nodes (Species B). Considering that the dual-stack nodes run the dual-stack within the subnet and IPv4 outside, we divided Species B into m patches (expressed by $B_1, B_2, ..., B_m$) as the IPv6 subnets in an actual network. This is similar to the method for contagious disease study where the population is classified into different groups by race, gender, and age when epidemiologists analyze how viruses spread in human society.

A model for worm infection or spreading is largely based on the susceptible-infected epidemic model for biological disease infection. The basic idea is that the derivative of the number of infected hosts is proportional to it, so linear differential equations can be formulated. We first modeled the propagation of the dual-stack worm in IPv4 networks, $I_4(t)$, and then investigated how the worm spread in each IPv6 subnet, $f_i(t)$ and between different IPv6 subnets, $I_6(t)$. The propagation model of the dual-stack worm in the IPv4-IPv6 Internet is represented by the following differential equations:

**Figure 2. The responses of multicast-scanning.**

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>28.357</td>
<td>fe80::216:ecff:fe20:73c</td>
<td>ff02:1</td>
<td>Router advertisement</td>
</tr>
<tr>
<td>28.383</td>
<td>::</td>
<td>ff02::11f8:1114</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>28.386</td>
<td>fe80::94d:3f4fe:78da:7ce8</td>
<td>ff02:14</td>
<td>Multicast Listener Report Message v2</td>
</tr>
<tr>
<td>28.412</td>
<td>::</td>
<td>ff02::19c78</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>28.452</td>
<td>::</td>
<td>ff02::13571</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>28.470</td>
<td>::</td>
<td>ff02::c3:7be</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>28.474</td>
<td>::</td>
<td>ff02::1a3e0</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>28.484</td>
<td>::</td>
<td>ff02::f33:a02</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>28.491</td>
<td>ff02:1</td>
<td>ff02::20:73c</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>28.564</td>
<td>::</td>
<td>ff02:1fda:7ce8</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>28.586</td>
<td>::</td>
<td>ff02::1fde:463</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>28.600</td>
<td>::</td>
<td>ff02::f1::463</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>28.601</td>
<td>::</td>
<td>ff02::f9b:1699</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>28.603</td>
<td>::</td>
<td>ff02:ff3c:aff</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>28.611</td>
<td>::</td>
<td>ff02:ff35:9133</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>28.707</td>
<td>::</td>
<td>ff02::f3:747b</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>28.712</td>
<td>::</td>
<td>ff02::f3:950</td>
<td>Neighbor solicitation</td>
</tr>
</tbody>
</table>

Victim E

Windows Vista

Victim F
where \( I_A(t) \) and \( I_B(t) \) are the number of the infected hosts in the whole network, Species A and Species B, at time \( t \); \( S_A(t) \) and \( S_B(t) \) are the number of susceptible hosts in Species A and Species B at time \( t \); \( N_B \) is the number of the active hosts in Species B; \( m \) is the number of dual-stack subnets; \( k \) is the average scan rate of infected hosts; \( \Omega \) is the scope of random scanning; \( T_i \) is the time for the first host to be infected in patch \( i \); \( \theta \) is the average time for one infected host to infect an entire local subnet; \( \tau \) is the duration of an IPv6 attack in a dual-stack subnet. The detailed derivations are presented in our research paper [15].

The above species-patch model describes the worm propagation considering scanning strategy and network topology, and provides a systematic way to study how the new intelligent worms spread in hybrid networks.

**Dual-Stack Worm Propagation Simulator**

The worm simulator is developed in C++ based on the following assumptions:

- All events (worm scanning, worm infection, etc.) are assumed to happen right at each discrete time tick \( l \) (1, 2, ...
- Only vulnerable hosts are considered in this simulator, and all of them are in one of three states: healthy, IPv6-attack, or IPv4-attack. Hosts in the IPv6-attack and IPv4-attack states detect vulnerable hosts using multicast-scanning and random-scanning, respectively.
- The infected hosts can further infect any victim if they find one.

A vulnerable host is defined as a node with several attributes: Node-ID, Subnet-ID, Scan-rate, Subnet-protocol, and State. The Subnet-ID shows in which subnet the host is located; the Scan-rate is generated at the beginning of initialization; the Subnet-protocol specifies which protocol the subnet runs (IPv4, IPv6, or dual-stack); and the State identifies the state of the host (0 for Healthy, 1 for IPv6-attack, and 2 for IPv4-attack). The transitions between the states can be expressed by the following equations:

\[
\text{State}(i, l + 1) = \text{State}(i, l) + \text{Attack}(i, l) \quad \text{host } i \in \text{IPv6}
\]
\[
\text{State}(i, l + 1) = \text{State}(i, l) + 2 \cdot \text{Attack}(i, l) \quad \text{host } i \in \text{IPv4}
\]
\[
\text{State}(i, l + 1) = \text{State}(i, l) + \text{Attack}(i, l) + \text{Attack}(i, l - \epsilon) \quad \text{host } i \in \text{Dual-stack}
\]

where \( \text{State}(i, l) \) is the state of host \( i \) at time \( l \), \( \text{Attack}(i, l) \) is the attack event, and \( \epsilon \) is the time of an IPv6-attack host to infect...
the entire subnet. If Healthy host $i$ is attacked at time $l$, $\text{Attack}(i, l) = 1$.

At each discrete time tick, the simulator checks the state of each node to determine the node’s action (staying in the same state or transiting).

If a Healthy host is infected, its state will be changed at the next time tick.

An IPv6-attack host $i$ scans approximately $k_i \cdot \Delta$ targets in the local subnet in one time interval, where $k_i$ is the scan rate of host $i$, and $\Delta$ is length of the interval. Suppose the host $i$ is in the subnet $j$ containing $N_j$ active hosts and $S_j$ vulnerable hosts. Thus, the host $i$ holds the IPv6-attack state for $N_j/k_i \cdot \Delta$ intervals; and $S_j \cdot k_i \cdot \Delta/N_j$ vulnerable hosts would be attacked in an interval on average.

An IPv4-attack host $i$ scans the whole IPv4 address space. It has a probability of $S/\Omega$ to hit a vulnerable host for each scan, where $S$ is the number of all vulnerable hosts, and $\Omega$ is $2^{32}$, much larger than $S$ (the Code Red worm infects about 360,000 hosts). Hence, in the simulation each IPv4-attack host sends one scan per interval with an approximate probability of $S \cdot k_i \cdot \Delta/\Omega$ to hit one vulnerable host.

**Simulation and Testing**

For simulation and testing, the key parameters of the dual-stack worm are set as those of Code Red and Blaster, well-known random and local-pref scan worms. Assume there are 360,000 vulnerable hosts, and the scan rate of infected host follows normal distribution $N(240/\text{min}, (100/\text{min})^2)$, slower than that of Code Red and Blaster $N(358, 100^2)$ [10]. Furthermore, let 20 percent of the victims running dual-stack be evenly located in 2000 dual-stack subnets. The simulation interval is set as 15 s.

We simulate the dual-stack worm propagation for 1000 simulation runs with the above settings. The results are ranked from fast to slow in terms of the time when 10 percent of entire victims are infected. Figure 4a shows the number of infected hosts vs. time for five cases: the 25th (top 2.5 percent), 50th (median), and 75th (bottom 2.5 percent), and the average in comparison with Code Red and Blaster. The propagation of Code Red is simulated by the classical epidemic model used in many Code Red worm models [8], and that of Blaster by the simulator developed by Zou in [10]. It is
observed that the dual-stack worm propagates much faster than Code Red and Blaster, although the scan rate of the dual-stack worm (240/min) is only 67 percent that of the other two. This indicates that the Internet in transition from IPv4 to IPv6 could be vulnerable to dual-stack worms with smart scanning strategies.

It is interesting to see in Fig. 4b that the propagation speed curves for the median, top 2.5 percent, and bottom 2.5 percent are similar but sharply different from the average curve. In fact, due to the filtering effect of averaging, some propagation features would be lost. For example, the first peak of the infection rate, important in analyzing propagation, is lost in the average curve. Therefore, the median curve is more accurate for analyzing propagation rather than the average curve commonly reported in the worm modeling literature [7, 8], and is applied in the following analysis.

The propagation speed of the dual-stack worm in different networks (the IPv4-only, the dual-stack, and the entire network) are shown in Fig. 4c, in comparison with that of Code Red and Blaster. Since dual-stack hosts have a higher probability of being hit, they are infected faster. All dual-stack vulnerable hosts are infected in 184 min, but only 19 percent of IPv4 nodes are infected during the same period. The infection peaks in the dual-stack hosts and the entire network are 3529 and 4192 at 148 min, much higher and earlier than Code Red (2699 at 406 min) and Blaster (2501 at 476 min).

Figure 4d shows that fast scanning could accelerate the propagation of the dual-stack worm. It is observed that the worm propagation speed almost linearly increases with the scan rate before saturation. The dual-stack worm infects 10 percent of the vulnerable hosts for 71, 141, 278, and 556 min with scan rates of 480, 240, 120, and 60/min.

**Defense Strategy**

Many techniques are widely used to prevent worm propagation (anti-virus software, firewalls, etc.), which could detect and defend against most viruses, Trojans, worms, and other network attacks effectively. However, it is difficult to require all Internet users to install network security tools and update in time. Even if 0.1 percent of the Internet populations (1.4 billion) are vulnerable, there would be 1.5 million possible victims, four times more than the 360,000 hosts infected by Code Red in 2001. Therefore, the defense strategies based on network topology, configuration, and management are necessary and desirable.

The detection and prevention techniques for random-scanning worms reported in the literature [5, 7] cannot be directly applied for IPv6 and dual-stack networks. We focus on the defense strategies for the dual-stack networks and investigate the impact of various topologies on worm propagation. Three defense strategies are proposed, and their impact on the network is studied.

**Enlarge the Number of Dual-Stack Subnets**

The propagation of the dual-stack worm is similar to the propagation of biological viruses in human society. Infected individuals will infect those close to them with higher probability but are less likely to infect others at a distance. Hence, when an epidemic disease breaks out, people are advised to stay at home or in quarantine.

Similarly, when the dual-stack worm breaks out, the hosts in a small network would be less likely to be infected than in a large network. If there is only one vulnerable host in each subnet, the dual-stack worm could not hit any effective target using multicast-scanning. In this case, the dual-stack worm
would propagate slower than Code Red since it wastes time scanning the local subnet.

Four groups of simulations are illustrated in Fig. 5a. Assume that 72,000 dual-stack hosts are divided into 2000, 4000, 9000, and 18,000 subnets, respectively. It is seen that 10 percent of the vulnerable hosts are infected at 141, 185, 267, and 359 min in each group. Clearly the dual-stack worm propagates slower in a smaller network. Therefore, it is advisable to deploy the IPv6 hosts in as many subnets as possible rather than having all IPv4 addresses in one IPv6 subnet (64-bit address space). This defense strategy would affect the topology and configuration of dual-stack networks in transition.

**Uniform Sizes of Dual-Stack Subnets**

Deploying new applications uniformly could slow the propagation of local-prefer scanning worms, such as Blaster and the Importance Scanning Worm [4]. Subnet size distribution has a significant impact on dual-stack worm propagation. Assume that 72,000 vulnerable dual-stack hosts are located in 3600 subnets with normal distribution of subnet size $S_{\text{SUB}}$

$$S_{\text{SUB}} \sim \{N(20, 0); N(20, 5^2); N(20, 10^2); N(20, 50^2)\}$$

Figure 5b shows the propagation of the dual-stack worm with different subnet sizes. It is seen that 2 percent of vulnerable hosts are infected at 171, 163, 148, and 129 min for $S_{\text{SUB}}$ with standard deviation = (0, 5, 10, 50). Clearly the worm propagates much faster in more heterogeneous networks. Allocating dual-stack hosts in subnets evenly is a good method of defending against the dual-stack worm. In fact, a large standard deviation of $S_{\text{SUB}}$ means that it is likely to have more large subnets with higher probability of being infected in the early stage of propagation. Therefore, it is advisable to divide the subnets as evenly as possible. This strategy would also affect network topology and configuration.

**Terminate IPv4 Services in Transition as Soon as Possible**

As analyzed above, the dual-stack worm would exploit IPv4 addresses to detect the victims in a local subnet. Assume all vulnerable hosts are installed with IPv6 and located in 36,000 IPv6 subnets. Consider four cases: 100, 50, 20, and 10 percent of the subnets in the dual-stack networks are IPv6. In the IPv6-only subnets, multicast-scanning is applicable but random-scanning is not. It is shown in Fig. 5c that the infected hosts could not exceed the population of vulnerable hosts in dual-stack networks, and the propagation speed would decrease with the proportion of dual-stack hosts.

Dual-stack technology is developed for compatibility in transition. However, this compatibility is unnecessary when IPv6 subnets are connected to each other, and would only cause vulnerability to dual-stack worm attacks. Thus, it is advisable to terminate IPv4 services in transition as soon as possible when IPv6 subnets are connected.

The first and second defense strategies are proposed to slow the propagation of the dual-stack worm in subnets and mitigate local-prefer worms such as Blaster and Importance Scanning [4]. The third is for preventing the dual-stack worm infecting victims across IPv6 subnets. This strategy can be combined with other measures such as monitoring Simple Mail Transport Protocol (SMTP) and peer-to-peer (P2P) flow, deploying secured DNS, and defending against other dual-stack worms hitting outside victims by email, P2P, and DNS.

**Conclusion**

An IPv4-IPv6 dual-stack worm with a hybrid scanning strategy is investigated in this article. It is shown how the precise scan strategy can accelerate propagation, and the importance of preventing this kind of scan is discussed. Multicast-scanning is exploited to obtain the addresses of all active IPv6 hosts on the same link to accelerate worm propagation in local subnets. By classifying unpatched hosts into different species and patches, a new worm propagation model is formulated, and a discrete time simulator is developed. Extensive simulations for networks with different topologies show that the dual-stack worm can propagate fast in dual-stack networks. Three defense strategies, focusing on the topological structures, are proposed, and their effectiveness is validated by simulation.

The dual-stack worm discussed in this article is a typical intelligent worm that can automatically change scanning strategies according to network topologies, applications, security measures, and so on. Therefore, we hope that the studies on the model, simulation, and defense strategies of this worm can be extended to research on other intelligent worms.

**Acknowledgment**

The research presented in this article is supported in part by the National Natural Science Foundation (60574087, 60633020), National Science Fund for Distinguished Young Scholars (60525202), Key Projects in the National Science & Technology Pillar Program (2006BAK1B02), and 863 High Tech Development Plan (2007AA01Z475, 2007AA01Z480, 2007AA01Z464, 2008AA01Z415).

**References**


**Biographies**

TING LIU (tilu.china@sei.xjtu.edu.cn) received his B.S degree from the School of Electronic and Information, Xi’an Jiaotong University, Xi’an, China, in 2003. Currently he is a Ph.D. candidate in the Systems Engineering Institute, Xi’an Jiaotong University. His research interests include computer networks and security.
XIAOHONG GUAN [F] (xhguan@sei.xjtu.edu.cn) received his B.S. and M.S. degrees in control engineering from Tsinghua University, Beijing, China, in 1982 and 1985, respectively, and his Ph.D. degree in electrical engineering from the University of Connecticut in 1993. He was a senior consulting engineer with PG&E from 1993 to 1995. He visited the Division of Engineering and Applied Science, Harvard University, from January 1999 to February 2000. Since 1995 he has been with the Systems Engineering Institute, Xi’an Jiaotong University, and was appointed Cheung Kong Professor of Systems Engineering in 1999, and dean of the School of Electronic and Information Engineering in 2008. Since 2001 he has been the director of the Center for Intelligent and Networked Systems, Tsinghua University, and served as head of the Department of Automation, 2003–2008. He is an Editor of IEEE Transactions on Power Systems and an Associate Editor of Automata. His research interests include optimization and security of networked systems, computer network security, and sensor networks.

QINGHUA ZHENG (qhzheng@mail.xjtu.edu.cn) received his B.S. and M.S. degrees in computer science and technology from Xi’an Jiaotong University in 1990 and 1993, respectively, and his Ph.D. degree in systems engineering from the same university in 1997. He was a postdoctoral researcher at Harvard University in 2002. Since 1995 he has been with the Department of Computer Science and Engineering at Xi’an Jiaotong University, and was appointed director of the Department in 2008 and Cheung Kong Professor in 2009. His research interests include network security and intelligent elearning.

YU QU (yqu@sei.xjtu.edu.cn) received his B.S degree from the School of Electronics and Information, Xi’an Jiaotong University, in 2006. Currently he is a Ph.D. candidate at the Systems Engineering Institute, Xi’an Jiaotong University. His research interests focus on trustworthy software systems.