SPREADING OF ACTIVE WORMS USING RANDOM SCANNING

Victor-Valeriu Patriciu, Iustin Priescu, Silviu Petrescu
Department of Computer Engineering, Military Technical Academy,
Department of Computer Engineering, Military Technical Academy,
PfP
vip@mta.ro, iustin@mta.ro, silviu.petrescu@yahoo.com

Abstract Active worms have been a persistent security threat on the Internet since the Morris worm in 1988. Automatically spreaded worms or active worms, like Code Red and Nimda, can flood large part of Internet hosts in a very short amount of time. Modeling the spread of such worms can help understand how they multiply and also help monitoring and defending effectively against the propagation of worms. In this paper, we present a mathematical model which characterizes the propagation of worms that are using random scanning in wide and local area networks. We also present Code Red v2 worm as an example, giving a quantitative analysis for monitoring, detecting and defending against worms of this type.

1. INTRODUCTION

Active worms have been a persistent security threat on the Internet since the Morris worm arose in 1988. The Code Red and Nimda worms infected hundreds of thousands of systems, and cost both the public and private sectors millions of dollars. In this paper, we present a model known as the Analytical Active Worm Propagation (AAWP) model, which characterizes the propagation of worms that employ random scanning. We take advantage of a discrete time model and deterministic approximation to describe the spread of active worms. We also compare AAWP with epidemiological model and Weaver's simulator, then present an extended AAWP model (LAAWP) to characterize the spread of a worm that employs the localized scanning strategy, which is used by the Code Red II and Nimda worms.

2. SPREAD OF ACTIVE WORMS

Briefly, active worm propagation can be described as folowing:
1. attacker releases the worm into Internet;
2. worm starts probing for vulnerable machines;

3. identified vulnerable machines become infected and start spreading the worm as well;

4. as soon as worm outbreak is detected, sysadmins are aplying patches which repairs security holes in order to slow down or stop further spreading.

Worm's authors goal is to perform first three steps as quick as possible and to infect as many machines as possible before step 4. To speed up the spread of active worms, Weaver presented the "hitlist" idea. Long before an attacker releases the worm, he/she gathers a list of potentially vulnerable machines with good network connections. After the worm has been fired onto an initial machine on this list, it begins scanning down the list. Hence, the worm will first start infecting the machines on this list which will become infected very soon, then will start to scan for randomly choosed machines. In this paper we do not consider the amount of time it takes a worm to infect the hitlist since the hitlist can be acquired well before a worm is released and be infected in a very short period of time. Table I shows the parameters involved in the spread of active worms. There are several different scanning mechanisms that active worms employ, such as random, local subnet, permutation and topological scanning.

Parameters	Notation	Description
Number of vulnerable machines	N	The number of vulnerable machines
Size of hitlist	h	The number of infected machines at the beginning of the spread of active worm
Scanning rate	s	The average number of machines scanned by an infected machine per unit time
Death rate	d	The rate at which an infection is detected on a machine and eliminated without patching
Patching rate	p	The rate at which an infected or vulnerable machine becomes invulnerable

Table 1. The parameters for spreading of active worms.

In this paper we focus on two mechanisms, random scanning and local subnet scanning. In random scanning, it is assumed that every computer in the Internet is just as likely to infect or be infected by other computers. Such a network can be pictured as a fully-connected graph in which the nodes represent computers and the arcs represent connections (neighboring-relationships) between pairs of nodes. This topology is called "homogeneous mixing" in the theoretical epidemiology. AAWP model is used to model random scans. In local subnet scanning, computers also connect to each other directly, forming "homogeneous mixing". However, instead of selecting targets randomly, the worms preferentially scan for hosts on the "local" address space. For example, the Nimda worm selects target IP addresses as follows:

- 50% of the time, an address with the same first two octets will be chosen.

- 25% of the time, an address with the same first octet will be chosen.
- 25% of the time, a random address will be chosen.

3. MODELING SPREAD OF WORMS THAT ARE USING RANDOM SCANNING

AAWP is using the discrete time and continuous state deterministic approximation model. In this section, we first describe in detail the AAWP model , then compare it to the epidemiological model and Weaver's simulator, finally use it to simulate the Code Red v2 worm.

3.1. DETERMINISTIC APPROXIMATION MODELING

We assume that worms can simultaneously scan many machines and will not re-infect a machine that is already infected. We also assume that the machines on the hitlist are already infected at the start of the worm's propagation. Suppose that an active worm takes one time tick to complete infection. That is, when one scan hits a machine, regardless of whether this machine is vulnerable, invulnerable, infected or with an unused IP address, the time it takes for the worm to finish communicating with this machine is one time tick. This assumption might not be realistic, but it can simplify the model without significantly affecting the results.

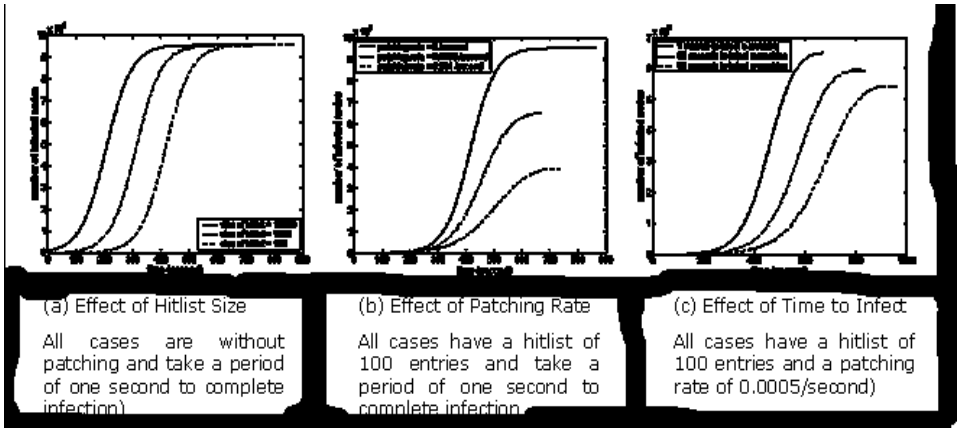

Fig. 1. Modeling the spread of worms that use random scanning (for 1,000,000 vulnerable machines, a scanning rate of 100 scans/second, and a death rate of 0.0001/second).

Although Internet address space is not completely connected, active worms always scan all the 2^{32} addesses. So for random scanning, the probability that any computer is hit by one scan is 2^{-32} .

Let m_i and n_i denote the total number of vulnerable machines (including the infected ones) and the number of infected machines at time tick i ($i \geq 0$) respectively. Before the active worms spread (at $i = 0$), we have $m_0 = N$ and $n_0 = h$.

Theorem 3.1. *If there are m_i vulnerable machines (including the infected ones), and n_i infected computers, then on average, the next time tick will have $(m_i - n_i)[1 - (1 - 2^{-32})^{sn_i}]$ newly infected machines, where s is the scanning rate.*

Proof Let e_i denote the number of newly infected machines at time tick i ($i \geq 0$). Then n_i infected machines can generate sn_i scans in an attempt to infect other machines. So, if we can prove that $E\{e_{i+1}/k\} = (m_i - n_i)[1-(1-2^{-32})^k]$ for any k ($k > 0$) scans, then the equation also holds when $k = sn_i$. We prove the above equation by induction on k. When $k = 1$, since there are $(m_i - n_i)$ vulnerable machines that have not yet been infected, the probability that one scan can add a newly infected machine is $(m_i - n_i)2^{-32}$, which is equivalent to $(m_i - n_i)[1 - (1 - 2^{-32})^1]$. Suppose that the theorem is true for $k = j$, i.e. $E\{e_{i+1}/k = j\} = (m_i - n_i)[1 - (1 - 2^{-32})^j]$. Then, when $k = j + 1$, we divide $j + 1$ scans into two parts: the first j scans and the last scan. There are two possibilities for the last scan: adding a newly infected machine or not. Let $Y = 1$ if the last scan hits a vulnerable machine that has not yet been infected and let $Y = 0$ otherwise. Then,

$$E\{e_{i+1}/k = j+1\} = (E\{e_{i+1}/k = j\}+1)P(Y = 1)+E\{e_{i+1}/k = j\}\cdot P(Y = 0) =$$

$$(E\{e_{i+1}/k = j\} + 1)(m_i - n_i - E\{e_{i+1}/k = j\})2^{-32} + E\{e_{i+1}/k = j\}$$
$$[1 - (m_i - n_i - E\{e_{i+1}/k = j\})2^{-32})] = (m_i - n_i)2^{-32} + (1 - 2^{-32})$$

$E\{e_{i+1}/k = j\} = (m_i-n_i)[1-(1-2^{-32})^{j+1}]$, which means it is also true for $k = j+1$. Therefore, when $k = sn_i$, $E\{e_{i+1}/k = sn_i\} = (m_i-n_i)[1-(1-2^{-32})^{sn_i}]$. That is, on the next time tick there will be $(m_i - n_i)[1 - (1 - 2^{-32})^{sn_i}]$ new infected machines. Given the death rate d and the patching rate p, on the next tick there will be $dn_i + pn_i$ infected machines that will change to either vulnerable machines without being infected or invulnerable machines, and the total number of vulnerable machines (including the infected ones) will be reduced to $(1 - p)m_i$. Therefore, on the next time tick the number of total infected machines will be $n_{i+1} = n_i+(m_i-n_i)[1-(1-2^{-32})^{sn_i}]-(d+p)n_i$. At the same time, $mi + 1 = (1-p)m_i$, which means $m_i = (1-p)^i m_0 = (1-p)^i N$. That is

$$n_{i+1} = (1 - d - p)n_i + [(1 - p)^i N - n_i][1 - (1 - 2^{-32})^{sn_i}], \qquad (1)$$

where $i \geq 0$ and $n_0 = h$. The recursion process will stop when there are no more vulnerable machines left or when the worm cannot increase the total number of infected machines. ■

Using equation (1), we can find the characteristics of the active worms' spreading. For example, fig. 1(a) shows the propagation of the active worms with different hitlist sizes. As the size of the hitlist increases, it takes the worms less time to spread. Fig. 1(b) depicts another example. As the patching rate grows, the spread of active worms slows down. It should be noted that because the patching rate $p > 0$, the two slower curves return to zero at the end. At the beginning, we assume that it takes the worms one time tick to infect a machine. To display the effect of the amount of time it takes to infect a machine on the worm propagation, we change the time unit. For example, in fig. 1(c) we first draw the curve with a time interval of one second, which is the amount of time required to complete infection. If the worm needs 30 seconds to infect a machine, we set the time unit to 30 seconds and change the corresponding parameters $s,\ d,\ p$ for this period of time. In this case, the parameters will become $30s,\ 30d,\ 30p$ for a period of 30 seconds. Then, we can use the AAWP model to get the result, but now, n_i $(i \geq 0)$ expresses the number of infected machines at $30i$ seconds $(i \geq 0)$. The figure shows the effect of the time to complete infection on the worm's propagation. The worm's propagation will be slowed down as the time required to infect a machine increases.

3.2. COMPARING AAWP MODEL TO THE EPIDEMIOLOGICAL MODEL AND WEAVER'S SIMULATOR

In the epidemiological model, a nonlinear ordinary differential equation is used to measure the virus population dynamics $\frac{dn}{dt} = \beta n(1-n) - dn$, where $n(t)$ is the fraction of infected nodes, β is the birth rate (the rate at which an infected machine infects other vulnerable machines) and d is the death rate. The solution to the above equation is

$$n(t) = \frac{n_0(1-\rho)}{n_0 + (1-\rho-n_0)e^{-(\beta-d)t}}, \tag{2}$$

where $\rho = d/\beta$ and $n_0 \equiv n(t=0) = size\_of\_hitlist/N = h/N$, where from here we deduce the relationship between the birth rate and the scanning rate $\beta = N_s 2^{-32}$.

The differences between the AAWP model and the epidemiological model are:

1 the epidemiological model uses a continuous time differential equation, while the AAWP model is based on a discrete time model. AAWP may be considered more accurate because in this model, a computer cannot infect other machines before it is infected completely - compared with the epidemiological model, where a computer begins infecting other

machines even though only a "small part" of it is infected. Therefore, the speed that the worm can achieve and the number of machines that can be infected are totally different;

2 the epidemiological model considers neither the patching rate nor the time that it takes the worm to infect a machine, while the AAWP model does. During the propagation of the worm, it is possible nowadays to promptly patch the vulnerability on computers, assuming a reasonable patching rate. Moreover, different worms have different infection abilities which are reflected by the scanning rate (or the birth rate) and the time taken to infect a machine. The time required to infect a machine always depends on the size of the worm' copy, the degree of network congestion, the distance between source and destination, and the vulnerability that the worm exploit. From fig. 1(c), it can be seen that the time to infect a machine is an important factor for the spread of active worms;

3 AAWP model considers the case that the worm can infect the same destination at the same time, while the epidemiological model ignores this case. In fact, it is not uncommon for a vulnerable machine to be hit by two (or more) scans at the same time. Both models, however, try to get the expected number of infected machines, given the size of the hitlist, total number of vulnerable machines, scanning rate/birth rate and death rate.

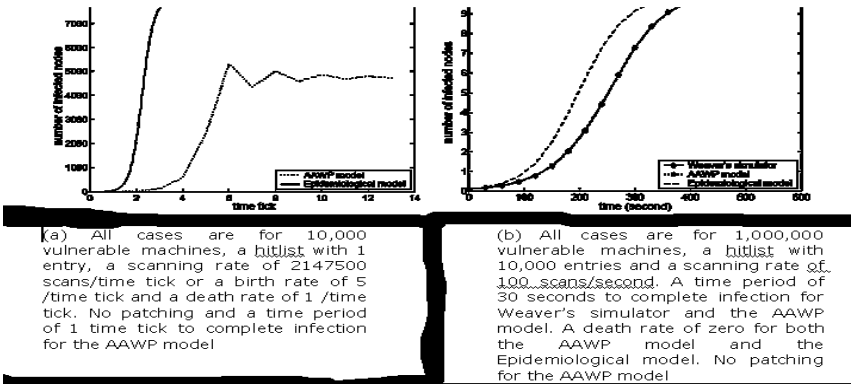

Fig. 2. Comparing the AAWP model to the epidemiological model and weaver simulator.

Fig. 2(a) shows the comparison between these two models with 10,000 vulnerable machines, a hitlist with 1 entry, a birth rate of 5 /time tick and a death rate of 1 /time tick. It takes the epidemiological model about 4 time ticks to enter an equilibrium stage, while the AAWP model needs about 10

time ticks. Moreover, after entering the equilibrium stage, the epidemiological model totally infects 8,000 vulnerable machines (occupying 80% of all vulnerable machines), while the AAWP model infects about 4,750 vulnerable machines (occupying 47.5% of all vulnerable machines). This difference may explain the low level of worm prevalence in attacks analized so far.

Weaver wrote a small, abstract simulator of a Warhol worm's spread. This simulator uses a 32-bit, 6-round variant of RC5 to generate all permutations and random numbers. For the assumption presented above, only one condition of the simulator was modified: all "newly" infected machines on a previous time tick will be activated at the same time on the current time tick, other than based on different clocks.

Fig. 2(b) shows the growing of infected nodes with time for the two models and Weaver's simulator, which have the following parameters: a total of 1,000,000 vulnerable machines, a hitlist of size 10,000, a scanning rate of 100 scans/second, a death rate of zero, no patching, and a time period of 30 seconds to infect one machine. This figure shows that the AAWP model and Weaver's simulator results overlap. While AAAWP model and Weaver's simulator take about 6 minutes to infect 90% of the vulnerable machines, the epidemiological model only takes about 5 minutes.

4. MODELING THE SPREAD OF ACTIVE WORMS THAT USE LOCAL SUBNET SCANNING

Instead of simply selecting destinations at random, the Code Red II and the Nimda worms preferentially search for targets on the "local" address space. Local AAWP (LAAWP) model extends AAWP to understand the characteristics of the spread of active worms that employ local subnet scanning.

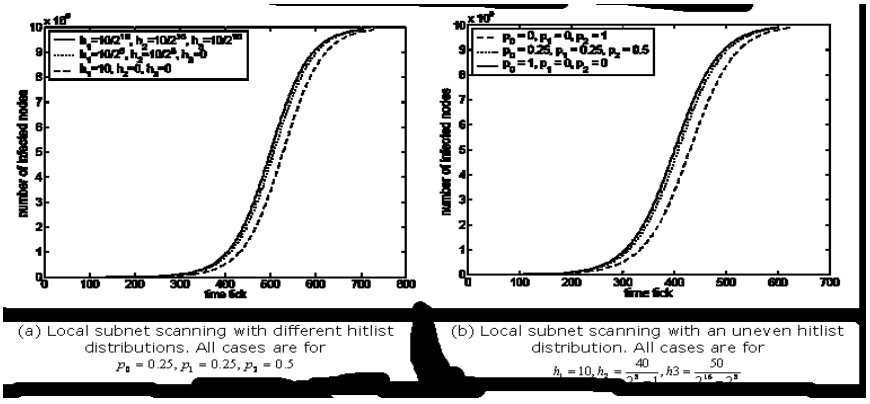

Fig. 3. Modeling the spread of active worms that employ local subnet scanning (All cases are for 1,000,000 vulnerable machines which are evenly

distributed to every subnet, a scanning rate of 100 scans/time tick and a time period of 1 time tick to complete infection).

As the AAWP model, the LAAWP model uses deterministic approximation. We focus on the active worms' scanning policy and ignore both the death rate and the patching rate to simplify the model. The function of firewalls is not considered, either. Suppose that a worm scans the Internet as follows:

- p_0 of the time, a random address will be chosen;
- p_1 of the time, an address with the same first octet will be chosen;
- p_2 of the time, an address with the same first two octets will be chosen, where $p_0 + p_1 + p_2 = 1$. We can regard random scanning as one special case of local subnet scanning, when $p_0 = 1,\ p_1 = 0,$ and $p_2 = 0$.

Assume that the vulnerable machines are evenly distributed in every subnet which is identified by the first two octets. The subnets can be classified into three different kinds of networks:

- a „special" subnet (denoted by Subnet type 1), which always has a larger hitlist size;
- 2^8-1 subnets having the same first octet as the "special" subnet (denoted by Subnet type 2);
- other $2^{16} - 2^8$ subnets (denoted by Subnet type 3).

Different kinds of networks have hitlists of different sizes. In the same type of subnet, all networks have the same hitlist size. Let $h_1,\ h_2,\ h_3$ denote the size of the hitlist in Subnet type 1, 2, and 3, respectively, then let $b_1,\ b_2,\ b_3$ denote the average number of infected machines in Subnet type 1, 2, and 3, respectively and let $k_1,\ k_2,\ k_3$ denote the average number of scans hitting Subnet type 1, 2, and 3, respectively. Then at some time tick, the relationship between the average number of scans hitting Subnet type and the average number of infected machines in different Subnets is:

$$k_1 = p_2 s b_1 + p_1 s[b_1 + (2^8 - 1)b_2]/2^8 + p_0 s[b_1 + (2^8 - 1)b_2 + (2^{16} - 2^8)b_3]/2^{16};$$

$$k_1 = p_2 s b_2 + p_1 s[b_1 + (2^8 - 1)b_2]/2^8 + p_0 s[b_1 + (2^8 - 1)b_2 + (2^{16} - 2^8)b_3]/2^{16};$$

$$k_1 = p_2 s b_3 + p_1 s b_3 + p_0 s[b_1 + (2^8 - 1)b_2 + (2^{16} - 2^8)b_3]/2^{16}.$$

For $k_i,\ (i = 1,\ 2,\ 3)$, the first item is the average number of scans coming from the local subnet (with the same first two octets). The second item is the average number of scans coming from neighboring subnets (with the same first octet). And the last item is the average number of scans coming from

global subnets. In every subnet the scans will randomly hit targets, which can be modeled by the AAWP model. The total number of machines will be 2^{16} instead of 2^{32} and the total number of scans will be k_i. Thus, equation (1) becomes

$$b'_i = b_i + (N2^{-16} - b_i)[1 - (1 - 2^{-16})^{k_i}], \tag{3}$$

where ($i = 1,\ 2,\ 3$) and b'_i is the number of infected machines on the next time tick. The recursion process will stop when there are no more vulnerable machines left. At some time tick, the total number of infected machines will be $b_1 + (2^8 - 1)b_2 + (2^{16} - 2^8)b_3$. Based on the above formulae, we can understand the characteristics of local subnet scanning and the effect of the hitlist's distribution. Different $p_1,\ p_2,\ p_3$ and $h_1,\ h_2,\ h_3$ can generate different patterns for the spread of worms.

Four cases are considered:

1) random scanning $p_1 = 1,\ p_2 = 0,\ p_3 = 0$. In this case $k_1 = k_2 = k_3 =$ (total number of infected machines)$/2^{16}$ which means the distribution of the hitlist cannot effect the spread of active worms;

2) a hitlist with an even distribution $h_1 = h_2 = h_3 = 0$. This gives $k_1 = k_2 = k_3 = sb_1 = sb_2 = sb_3$. Local subnet scanning, therefore, cannot change the spread of active worms in this case;

3) similar to the Nimda worm ($p_1 = 0.25,\ p_2 = 0.25,\ p_3 = 0.5$). In this case, we select different distributions of the hitlist, just as in fig. 3(a). Evenly distributed hitlists give the best performance, while putting all hitlists together in one „special" subnet ($h_1 = 10,\ h_2 = h_3 = 0$) gives the worst performance. This figure shows that the hitlist's distribution can affect the spread of active worms;

4) local subnet scanning with a hitlist of uneven distribution (fix $h_1,\ h_2,\ h_3$ and $h_1 > h_2 > h_3$): This stands for a hitlist of uneven distribution and a centralization of more hitlist machines in the „special" subnet. However, fig. 3(b) shows that in this case local subnet scanning slows down the propagation of active worms. From the four cases above, we see that for local subnet scanning the hitlist's distribution can influence the spread of active worms, while the even distribution gives us the best performance. In addition when the hitlist is more concentrated in the „special" subnet, local subnet scanning slows down the spread of active worms. The LAAWP model implies that local subnet scanning may slow down the spread of active worms. There are two main reasons for this:

1) firewalls can protect vulnerable machines behind it. But local subnet scanning allows a single copy of a worm running behind the firewall to rapidly infect all the other local vulnerable machines;

2) one subnet always belongs to a company or organization and has a lot of similar machines. Therefore, it can be expected that if a machine has a

security hole, then there is a high probability that many other machines in the same network have the same security hole.

5. CONCLUSIONS

In this paper we present the AAWP model to analyze the characteristics of the spread of active worms. Even though the AAWP model also used deterministic approximation, it gives more realistic results when compared to the epidemiological model. AAWP model was extended to the LAAWP model to understand the spread of active worms using local subnet scanning. The distribution of the hitlist can affect the local subnet scanning policy. In particular, a worm using an evenly distributed hitlist spreads at the fastest rate. When the hitlist is concentrated in some subnet, the spread of active worms is slowed down. In the LAAWP model, the vulnerable machines are assumed to be evenly distributed in every subnet.

References

[1] R. Russell, A. Machie, *Code Red II Worm*, Incident Analysis, SecurityFocus, Tech. Rep., Aug. 2001.

[2] A. Machie, J. Roculan, R. Russell, and M. V. Velzen, *Nimda Worm Analysis*, Incident Analysis, SecurityFocus, Tech. Rep., Sept. 2001.

[3] CERT/CC, CERT Advisory CA-2001-26 Nimda Worm, http://www.cert.org/advisories/CA-2001-26.html, Sept. 2001.

[4] D. Song, R. Malan, and R. Stone, *A Snapshot of Global Internet Worm Activity*, http://research.arbornetworks.com/up media/up files/snapshot worm activity.pdf, Arbor Networks, Tech. Rep., Nov. 2001.

[5] S. Staniford, V. Paxson, and N. Weaver, *How to own the Internet in your spare time*, in Proc. of the 11th USENIX Security Symposium (Security '02), 2002.

[6] J. O. Kephart, *How topology affects population dynamics*, in C. Langton, ed., Artificial Life III. Studies in the Sciences of Complexity, 1994, pp. 447-463.

[7] J. O. Kephart, S. R. White, *Directed-graph epidemiological models of computer viruses*, in Proc. of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy, May 1991, pp. 343-359.