The Centralized Containment Strategy and Mathematical Modeling Analysis

Liu Yang*, Wang Bailing, Yuan Xinling, Bai Xuefeng and Zhu Qiang

Department of Computer Science & Technology
Harbin Institute of Technology at Weihai, Shandong, China
** Liuyang322@hit.edu.cn*

Abstract

To solve worm propagate in the network system, the research situations of Internet worm prevention technology by system vulnerability are first discussed; then the concept and the execution mechanism of containment system are given; the Centralized Containment Model based on the active containment scenarios and the worm propagation model under these scenarios are presented afterwards; and finally the research trends in this area are also addressed.

Keywords: *Internet worms; System vulnerability; Centralized containment model; Active containment*

1. Introduction

Worm threats on the Internet security are gradually approaching each ordinary user. Characteristics of the openness of the Internet, the route of transmission of diverse and complex application environments increase the frequency of occurrence of network worms, enhance the latent, augment the coverage and cause a greater loss. Compared to traditional viruses, worms have a stronger ability to reproduce and destroy.

The worm was difficult to control due to the Internet is essentially an open complex system which has a complex structure, lacking of the ability of central control [1], and the open attribute causes a large number of uncontrollable nodes in the presence of network management level. These uncontrollable nodes often lack appropriate security measures or long-term unattended. Once they are infected with worms, the worms will stay here for a long time in the nodes of the infected, and always threats to the Internet as a source of the attack. The most fundamental reason for the existence of the worm is the software loopholes [2]. Worm exploited to attack the system. Although the type of worm has a variety of features, but the use of the vulnerability is limited. Immune the vulnerabilities host is the only effective way to prevent infection worms. Active countermeasure technology designs penetrate and patch technology based on vulnerability and designs killing and immune technology for the vicious worm, and initiative to curb uncontrollable network nodes which are infected by vicious worm to prevent their continued attacks on the Internet [3], or fixes vulnerability of network nodes remotely to prevent them from becoming the target of vicious. The active countermeasure technology has important application prospect in controlling worm outbreaks scope and avoiding worm epidemic repeated. Therefore, the research based on the active countermeasure technology of centralized containment strategy is of great significance.

2. Active countermeasure technology

2.1. Active containment principle

Active containment technical measures to penetrate the target host, and then killing the worm, patching vulnerabilities, making the host has immune ability, and finally be able to self-destruct, exit of the target host safely.

Infiltration of technology: Penetrate the target host is to perform the first step of active containment technical. According to the different network administrative privileges, target host infiltration method includes the target host controlled penetration; the user initiative authorized penetration and forcible penetration.

Immune Technology [4]: Mainly used in worm outbreak early, making the network hosts which have vulnerabilities immune and controlling worm epidemic in the minimum. There are a variety of immunoassay technologies, major technology including memory patch method, resource preemption methods.

The use active containment technical curb vicious worm has the advantage of time, function, mode of transmission:

Time advantage: Making the hosts which have vulnerability immune actively before the outbreak of the vicious worm, so as to control the diffusion range of the vicious worm; Repairing the network hosts which are infected by vicious worms after the vicious worm outbreak, so as to avoid repeated outbreaks of epidemic; Killing virus and repairing loopholes on the hosts which have been infected and repairing loopholes on the hosts which are easy to be infected when various worm outbreaks, so as to control the diffusion range of the vicious worm.

Functional advantages [5]: The Fightable Program are transparent to the user, without hidden module; Fightable Program can enter the host which have vulnerability to complete a number of different restoration tasks by host user authorization, pre-installed client, vicious worm and backdoor.

Advantage of the mode of propagation: Centralized propagation; Make full use of the advantages of centralized control, distributed propagation; Make full use of vulnerability host IP addresses which are offered by third-party for the purpose of propagation.

2.2. The functional structure of the FP

FP (Fightable Program) is a program. When FP into the host that have loopholes, it can take advantage of the transmission function to get tools for killing worms, patching holes, making host immune, and then killing the virus, repairing the host, and finally be able to safely self-destruct, the exit of the host.

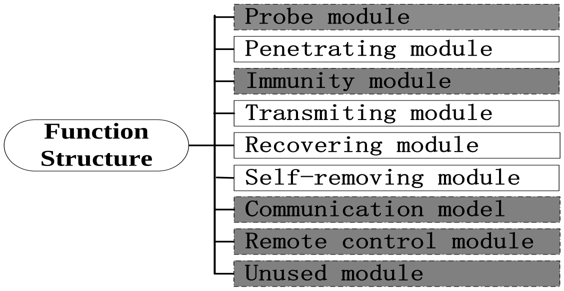


Figure 1. The FP Functional Structure Diagram

FP's main function is constituted by the four essential modules (as solid line without shadow box shown in the Figure 1) and five optional module (as dotted line shadow box shown in the Figure 1).

Detection module: Optional module. Containment strategy determine whether the FP need to include this module. If FP contains this module, its main role is to detect hosts in its scanning space, so as to obtain the target that can be penetrated.

Penetrate module: The function of the module is to find the way to penetrate the host using the vulnerability information collected, and implant the FP into the target host. This module is similar to the attack module of worm.

Immune module: Optional module. It takes temporary immunity technology for some worm after penetrate the susceptible host, and the host will not be attacked or occupied by the worm during the repair. The mechanism of Immune module is simple. For example, in the containment MSBlaster worms, FP can call immune module to occupy the port 444 and creat the same name mutex. That cause the MSBlaster worm transmission and execution fails.

Transmission module: FP using the module gets vulnerability patches and virus removal tools from the original host.

Containment module: When the FP gets vulnerability patches and virus removal tool, the module is responsible for the completion of repair and cleanup task.

Self-destruct module: This module is started after the completion of the patches and anti-virus work, in order to clean up the site and removal of the FP.

Communication module: Optional module. This module not only enables information interaction between the FPs, but alse between the FP and control center. Through the interaction between the FPs share information, the control center can also obtain the conditions of the FP work.

Remote control module: Optional module. The control module function is to adjust the FP behavior and execute instructions from the control center. Such as the control center issued self-destruct instructions in advance, then the FP will give up the current work, immediately to clear itself. The module can make the FP more controllable.

Unused module: Unused module can be used to extend the temporary function of the FP.

2.3. FP working mechanism

Active containment process can be divided into five steps. First, the control host collects information that includes the type of operating system, vulnerability information and IP address information from vulnerability host. The approach taken includes network monitoring, active scanning, user submitting. Next, using the above information, FP penetrates into the vulnerability host internal. The approach taken includes using the host vulnerability or host authorized, etc. After that, the FP from the control host download worm killing and vulnerability patching tool. Then the FP kills virus and patches the vulnerability host internal. Finally, the FP cleans up the site and self-destruct. In practical applications, the control host can be the delivery platform within the control center, and may be a network host has been fixed by the FP.

In the process of containment, according to the strategy of containment, the host has different way of collecting information. Generally, the host A can complete the collection of information, and then to provide information to the FP to create penetration route. However, some active containment strategy allows the FP having the ability of information collection. In this case, the FP transmission mode is similar to worms, and it can discover vulnerability hosts, penetrate, transfer and repair automatically.

3. Centralized Containment Strategy

CCM (Centralized Containment Model) refers to there are one or more worm active containment server in a network. These servers can through active scanning within the management scope to detect in turn, and place the FP on the target host to patch when it detect vulnerability host. FP does not have the initiative to collect information functions under this containment model and does not need to include any optional modules. As shown in Figure 2. The model contains two parts - vulnerability detection part and active containment part.

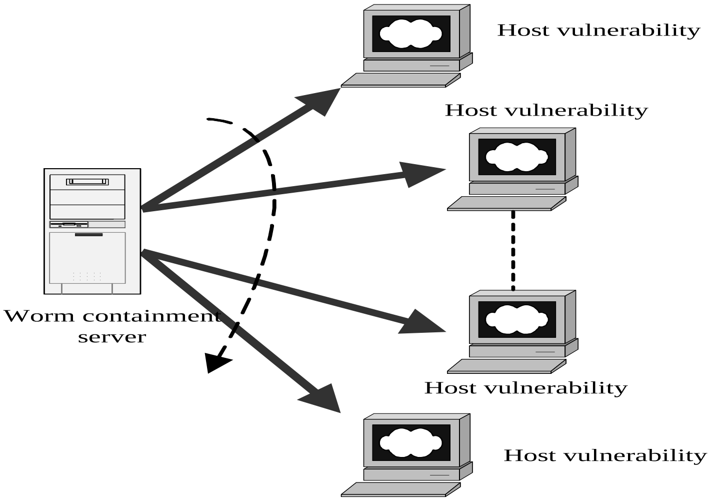


Figure 2. Centralized Containment Model

Detection tools and methods for vulnerability host are given by Yoon-Chan Jhi [6]. Lockwood JW propose two active containment strategy [7]. Active Patching-I is an implementation of centralized active containment that this paper introduces. Active Patching-II assumption that all vulnerability host IP address is known. This generally does not exist, and even if there is only a special case of centralized containment strategy. The centralized containment model has the characteristics of controllability, traceability, flexibility, etc. Each antibody is directly controlled by the control center. Control center know each host that has been repaired by FP. Due to communicate information with the control center directly, we can using a variety of ways to penetrate host and then perform a variety of repair tasks.

4. Mathematical Modeling and Analysis

The worm containment propagation model studied the interaction between the parameters composition included in containment strategy and the parameters in the process of containment, then establish a complete mathematical description and draw worm outbreak curve in the process of containment under different conditions, then compared with the behavioral simulation results and correct each other. By comparing worm epidemic curves before and after containment, the worm spread behavior changes and epidemic trends under the different containment strategy can be analyzed, so as to contrast the effectiveness of the containment strategy and the place need to further improve.

Currently there are three main high efficiency implement, and widely used scanning strategy: uniform random scan, random sequential scan, local priority sequential scan. Reference [8] proved that under the same conditions, the uniform random scanning worm propagation speed is equivalent to a random sequential scan, and both are higher than the local priority sequential scan. This article assumes vicious worms using uniform random scanning strategy.

4.1. Network worm propagation model research

The worm propagation is suitable to describe with infectious disease transmit-ssion model, mainly including Simple Epidemic Model, Kermack-Mckendrick(K-M or SIR) Model, Susceptible→Infectious→Susceptible(SIS) model, two-factor model(Susceptible→Infectious →Removed；Susceptible→Removed).

In Simple Epidemic Model [9], each host remains of two states: susceptible to infection status and infection status, and assume that a host always remains infected state once it is infected. SEM model can reflect the network worm initial propagation behavior, but not suited to the network worm late propagation state. K-M model is different with the SEM model and in this model the host remains three states: susceptible to infection status, infection status and immune status, and assume that the hosts which are infection status change to the immune status in accordance with the fixed recovery rate [10]. KM model on the basis of the SEM consider the immune status of the host which are infection status, more suitable for worm propagation. However, the model is still not considered the condition that infected hosts and susceptible to infected hosts may be patched or contains worm propagation artificially. Further, assume the rate of infection as constants is also not appropriate. Zou's two-factor model [11] makes up for the defects of the K-M model. It not only consider susceptible host and infected host may be removed from the state, but also consider the changes in the infection rate with the network traffic load. Expression of differential equations of the two-factor propagation model expressed as:

$$\begin{cases} dS(t)/dt = -\lambda(t)S(t)I(t) - dQ(t)/dt \\ dR(t)/dt = \gamma I(t) \\ dQ(t)/dt = \mu S(t)J(t) \\ \lambda(t) = \lambda_0[1 - I(t)/N]^{\eta} \\ N = S(t) + I(t) + R(t) + Q(t) \\ I(0) = I_0 << N; S(0) = N - I_0; R(0) = Q(0) = 0; \end{cases} \qquad (1)$$

In the formula (1), R(t) indicates the number of infected hosts which have been immured at time t; I(t) indicates the number of worm infected hosts at time t; Q(t) indicates the number of susceptible hosts which have been immured at time t; S(t) indicates the number of susceptible hosts at time t; J(t) indicates the number of hosts have been infected by worms or FP at time t (Including the host had been infected, but already immune), J(t)=R(t)＋I(t); λ0 is the infection ratio constant of initial moment, λ(t) indicates the infection rate at time t; η is the sensitivity constant that adjust the infection rate λ(t) according to the worm quantity I(t); γ is the percentage constant that infected hosts become immune; μ is the ratio constant that susceptible hosts become immune [12].

The SIS model [13] did not consider the condition that infected host become immune, so the model is difficult to reflect the worm propagation behavior. Another diffusion model distinguished from the model based on differential equations——discrete mathematical model AAWP model [14] and Markov model [15], *etc.* Due to space limitations, this paper will not discuss in detail, please refer to the relevant literature.

Table 1. Symbols used in Mathematical Propagation Model in this Article following Portion

symbol	meaning
Ω	The number of network hosts.
N	The number of network vulnerability hosts.
I(t)	The number of network worms at time t.
S(t)	The number of susceptible hosts in the network at time t.
R(t)	The number of infected host that have been immune at time t.
Q(t)	The number of susceptible host that have been immune at time t.
J(t)	The number of hosts have been infected by worms or FP at time t . J(t)=I(t)+R(t).
$I_F(t)$	The impact that containment system on network traffic at time t,equivalent to the impact of $I_F(t)$ worms.
α_0	The scan frequency of the centralized containment system at the initial time; or the benign worm scanning frequency at the initial time.
α(t)	The scan frequency of the centralized containment system at time t; or the benign worm scanning frequency at time t. The relationship between α(t) and α_0 the same as the network traffic load impact relationship two-factor model takes.
$\alpha_S(t)$	The centralized containment system scan frequency for susceptible hosts at time t, the benign worm scan frequency for susceptible hosts at time t.
$\alpha_I(t)$	The centralized containment system scan frequency for infected hosts at time t, the benign worm scan frequency for infected hosts at time t.
β_0	The frequency of the worm scans at the initial time.
β(t)	The worm scans frequency at time t. The relationship between β(t) and β_0 is the same as the network traffic load impact relationship that two-factor model takes.
η	The sensitivity constants that scan rate α (t), β (t) changes with the number of worm and the FP.
I_0	The number of the network worms at the initial moment.
IF_0	The number of the network benign worms at the initial moment.

This article will describe the worm propagation model of containment strategy on the basis of the two-factor propagation model [16]. Compared with the two-factor model, the worm propagation model based on the active containment adds the following factors: Consider the change of the number caused by the FP patching infected hosts actively; Consider the change of the number caused by the FP patching susceptible hosts actively; Consider the worm containment model under the circumstance that worm do not close the loophole after infecting the vulnerability host; Consider the worm containment model under the circumstance that worm close the loophole after infecting the vulnerability host; Two-factor model assumes that all of hosts in network have vulnerabilities at the initial time, but only a part of them have in fact.

Assuming the number of network hosts is Ω, make β=λΩ, we call β is the worm scanning frequency. β(t)I(t) indicates the scanning frequency of all worms in the network at time t, and at this moment the susceptible host distribution density is S(t)/Ω, Therefore, from time t to t+Δt, the change in the number of infected host satisfy:

$$dI(t)/dt = \beta(t)S(t)I(t)/\Omega \qquad (2)$$

Suppose at time t, the impact caused by the system in the process of active containment on the network traffic is equivalent to l1(t) a vicious worm; From time t to t + Δt time, the changes in number of susceptible hosts that have been repaired by FP are ΔQ1(t), the changes in number of infected hosts that have been repaired by FP are ΔR1(t); Both the scanning frequency of FP and worm use the flow affecting model in the two-factor model. In the process of actual containment, the number of infected hosts that are immune by FP is far greater than that by killing virus, patching, setting up the firewall, *etc.* So we ignore the number of artificial immune and introduce containment system immune factors; susceptible host immune situation is the same reason; Based on two-factor model (1) and formula (2), the worm containment propagation mathematical model under the active containment strategy satisfy:

$$\begin{cases} dS(t)/dt = -\beta(t)S(t)I(t)/\Omega - dQ(t)/dt \\ dI(t)/dt = \beta(t)S(t)I(t)/\Omega - dR(t)/dt \\ dR(t)/dt = \\ dQ(t)/dt = \\ \alpha(t) = \alpha_0[1-(I(t)+I_F(t))/\Omega]^\eta \\ \beta(t) = \beta_0[1-(I(t)+I_F(t))/\Omega]^\eta \\ I_F(t) = \\ J(t) = I(t) + R(t) \\ N = S(t) + I(t) + R(t) + Q(t) \\ I(0) = I_0 << N; I_F(0) = I_{F0} << N; S(0) = N - I_0; \end{cases} \qquad (3)$$

wherein $dR(t)/dt$ 、 $dQ(t)/dt$ 、 $I_1(t)$ are different with the different containment strategy, the following major discuss $dR(t)/dt$ 、 $dQ(t)/dt$ 、 $I_1(t)$ change models under different strategies.

4.2. Centralized containment propagation model

Analysis from the active containment angle, there are two cases after the worm infect the host successfully: worm turns off the original loopholes and leaves a new backdoor; the worm does not turn off the original loopholes. In the first case, the centralized containment strategy can take two measures: In a complete containment process, the strategy first detects each host whether is a susceptible host (infected host), then carry out active infiltration, containment if it is, and next continue to detect other hosts. On the contrary, the strategy detect each host whether is a infected host (susceptible host), then carry out active infiltration, containment if it is, and next continue to detect other hosts; conduct a complete detection, infiltration, containment to the infected hosts (susceptible hosts) in the network; and then conduct a complete detection, infiltration, containment to the susceptible hosts (infected hosts) in the network. So we divide it into three cases to discuss:

Case1: The worm infects hosts after intrude network, and does not turn off the original loopholes; The FP intrudes the hosts by the same way with the worm. The containment system does not know the vulnerability hosts IP addresses in the network, and detect the network by non-repetitive uniform random scan. At the initial time, the worm scan frequency is β0; the centralized containment system scan frequency is α0.

According to the case, the impact containment system on the network equivalent to α0/β0 worms scanning, therefore:

$$I_F(t)=\alpha_0/\beta_0 \tag{4}$$

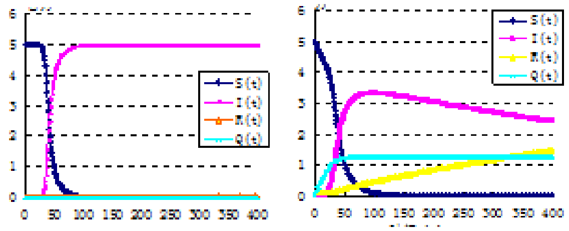
and α(t)=αI(t)=αS(t), so we only use α (t) in formula. The number of hosts that centralized containment system has scanned is $\int_0^t \alpha(t)$ at any time t. According to formula 3 and 4, at any time t, the number of hosts that centralized containment system has scanned is:

$$\int_0^t \alpha(t)=\frac{\alpha_0}{\eta+1}\left[1-\frac{I(t)+\alpha_0/\beta_0}{\Omega}\right]^{\eta+1} \tag{5}$$

The IP number that has not been scanned is $\Omega-\int_0^t \alpha(t)$ at any time t. In the IP space of the unscented, the distribution density of the susceptible hosts is $\delta_S=\frac{S(t)}{\Omega-\int_0^t \alpha(t)}$, the distribution density of the infected hosts is $\delta_I=\frac{I(t)}{\Omega-\int_0^t \alpha(t)}$. The number change of the hosts that have been repaired by the centralized containment system satisfies :

$$\begin{cases}\dfrac{dQ(t)}{dt}=\alpha(t)\times\delta_S=\alpha(t)\times\dfrac{S(t)}{\Omega-\int_0^t \alpha(t)}\\[2ex] \dfrac{dR(t)}{dt}=\alpha(t)\times\delta_I=\alpha(t)\times\dfrac{I(t)}{\Omega-\int_0^t \alpha(t)}\end{cases} \tag{6}$$

The formula 4 and formula 6 into the formula 3, and get the worm containment propagation model under the active containment strategy in the case 1 (Worm Propagation Model I under CCM,WPM-CCM I). We draw respectively corresponding change curve of host number in a case of two kinds: the number of network hosts is 10 million, including 5 million vulnerability hosts; and the number of network hosts is 100 thousand, including 50 thousand vulnerability hosts. Shown as Figure 4(Other parameters: Sensitivity constant η=3, the worm scan frequency at the initial time β0=1, the worm quantity at the initial moment I0=1, a total of 10 high-performance containment host, each host is equivalent to 100 vicious worm scanning frequency, α0=100*10=1000).



a. 5 million vulnerability hosts b. 50 thousand vulnerability hosts

Figure 3. Graph of the Changes in the Host Number under the various States of the WPM-CCMI

By comparing the a and b in Figure 3, we found that in the early stages of worm outbreaks, taking the active containment strategy based on WPM-CCM I containment system has a good effect in a small-scale network(Figure 3 b), but the effect is not obvious in the large-scale network (Figure 4 a). So, we can think the WPM-CCM I fits in the condition that worm does not outbreak; Once the worm outbreak, and there are still a lot of vulnerability hosts in the network, the effect of the WPM-CCM I is not very good. WPM-CCM II also has the same situation.

Case 2: Network infected with a worm, and the worm turn off the existing loopholes after it infect the host, but leaving the backdoor that the FP can use; The FP enters the infected host by the new backdoor and enters the uninfected host by the original vulnerability; The containment system does not know the vulnerability host IP address in network, using non-repeat uniform random scanning strategy probing the network; The worm scan frequency in the initial moment is β0; The centralized containment system scan frequency in the initial moment is α0.

For a target host, FP can first detect whether it is a infected host. If it is, FP use the new backdoor penetrate vulnerability host, repairing the host, then scans the next host. If it is not, FP use the original vulnerability penetrate the host, repairing the host, then scans the nest host. Also can determine whether host is susceptible, and then determine whether is infected. The two are different at different moments of the epidemic, we will model for the former, and the latter is similar.

Same as Case 1, Formula 4 is still established in Case 2, but the difference with the Case 1 is that the containment may scan a host twice--First determine whether it is an infected host, the second to determine whether it is a susceptible host. So we can draw $\int_0^t \alpha_I(t)$ is the number of host that the containment system has scanned, $\int_0^t \alpha_S(t)$ is the number of host that the system scanned twice. α(t), $\alpha_I(t)$, $\alpha_S(t)$ satisfy:

$$\begin{cases} \int_0^t \alpha_I(t) + \int_0^t \alpha_S(t) = \int_0^t \alpha(t) \\ \int_0^t \alpha_I(t) - \int_0^t \alpha_S(t) = R(t) \end{cases} \tag{7}$$

Wherein the first equation is obvious, the left of the second equation indicates the extra number of scan that to determine the infected hosts than to determine the susceptible hosts. According to Case 2(second scan the uninfected hosts), this difference is the amount of the infected hosts that have been repaired at time t, (shown as the right side of the second equation). Therefore, under the two-factor model and traffic impact factor model relationship, Equation 7 solution:

$$\begin{cases} \alpha_I(t) = \frac{1}{2}\left(\alpha(t) + R'(t)\right) \\ \alpha_S(t) = \frac{1}{2}\left(\alpha(t) - R'(t)\right) \end{cases} \tag{8}$$

According to the derivation of Equation 7, we can determine both A and B in formula 8 are integrable.

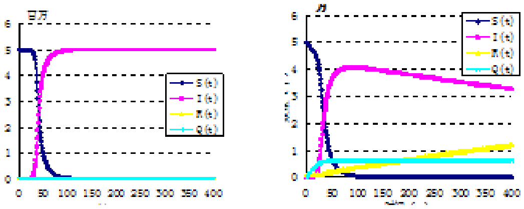
For any time t, the unscanned host number is $\Omega - \int_0^t \alpha_I(t)$. In Unscanned IP space, distribution density of the infected hosts is $\delta_I = \frac{I(t)}{\Omega - \int_0^t \alpha_I(t)}$. The number changes of the infected hosts that have been repaired meets:

$$\frac{dR(t)}{dt} = \alpha_I(t)\delta_I = \frac{\alpha(t)I(t)}{\left(2\Omega - \int_0^t \alpha(t) - R(t) - I(t)\right)} \tag{9}$$

For we do not secondary judge the infected hosts, so the containment system scan space for susceptible hosts is $\Omega - \int_0^t \alpha_I(t)$, distribution density of the susceptible hosts is $\delta_S = \frac{S(t)}{\Omega - \int_0^t \alpha_I(t)}$, the number changes of the infected hosts which are repaired meets :

$$\frac{dQ(t)}{dt} = \alpha_S(t)\delta_S = \frac{(a(t) - dR(t)/dt)S(t)}{2\Omega - \int_0^t a(t) - R(t)} \tag{10}$$

So, we substitute the formula 4, 8 to 10 into Equation 3, and get the worm containment propagation model under the centralized active containment strategy (Worm Propagation Model II under CCM,WPM-CCM II). We draw respectively corresponding change curve of host number in a case of two kinds: the number of network hosts is 10 million, including 5 million vulnerability hosts; and the number of network hosts is 100 thousand, including 50 thousand vulnerability hosts. Shown as Figure 4 (Other parameters: Sensitivity constant η=3, the worm scan frequency at the initial time β0=1, the worm quantity at the initial moment I0=1, a total of 10 high-performance containment host, each host is equivalent to 100 vicious worm scanning frequency, α0=100*10=1000). The same with WPM-CCM I, WPM-CCM II is only suitable for the condition that worm does not outbreak. And for the worm turned off the original vulnerabilities, the FP must second judge the hosts, thus resulting in epidemic slightly heavier(shown as Figure 3b and Figure 4b).



a. 5 million vulnerability hosts **b.** 50 thousand vulnerability hosts

Figure 4. Graph of the Changes in the Host Number under the various States of the WPM-CCM II

Case 3: Network infected with a worm, and the worm turn off the existing loopholes after it infect the host, but leaving the backdoor that the FP can use; The FP enters the infected host by the new backdoor and enters the uninfected host by the original vulnerability; The containment system does not know the vulnerability host IP address in network, using non-repeat uniform random scanning strategy probing the network; Containment system conduct a complete network detection and repair for the original vulnerabilities, then conduct a second complete network detection and repair for the new backdoors. The worm scan frequency in the initial moment is β0; The centralized containment system scan frequency in the initial moment is α0.

Both the first and second complete propagation model can be got according to the model established in Case 1. Due to space limitations, this article is no longer given derivation.

5. Conclusion

From the worm research situation view, the Internet worm containment based on the active containment strategy is an inevitable process and now is maturing stage. This is mainly because the existing software distribution system and vulnerability is inevitable. In addition, network host vulnerabilities have become increasingly frequent and vulnerability associated relationship becomes increasingly complex, worm outbreaks more early (relative to the vulnerability published) and spread faster and faster. Therefore, when we are studying the realizing mechanism of vicious worm, communication strategies as well as preventive measures, we also need to study the active containment technology, in order to narrow the worm outbreak range and eliminate worms stranded in the network

Papers conduct a detailed study from the principle of confrontation technical, functional structure and working mechanism, and analyze the basic premise of containment technical implementation from the technology perspective. Analyzed the containment effect from the containment strategy and corresponding mathematical model. The results showed that we can respectively use different centralized containment strategy for different network size and rights management form. Subsequent key research questions mainly include network worm containment process simulation, the FP automatically generates technology based on a variety of backdoor attack and network host vulnerabilities relationship and the mandatory permission enhance technology.

Acknowledgements

This research was supported by the National Science Nature Foundation of China under Grant No 61170262.

References

[1] Z. Lina, S. Chaoyi and F. Li, "Early warning of the propagation direction of network worms", J. J. Huazhong Univ. of Sci. & Tech. (Natural Science Edition), **(2009)**, pp. 13-16.

[2] Y. -C. Jhi, P. Liu and L. Li, "PWC: A proactive worm containment solution for enterprise network", C. Third International Conference on Security and Privacy in Communications Networks and the Workshops, **(2007)**, pp. 433-442.

[3] J. W. Lockwood and J. Moscola, "Internet worm and virus protection in dynamically reconfigurable hardware", C. In: Proc. of the ACM CCS Workshop on Rapid Malcode (WORM 2008), Washington, Military and Aerospace Programmable Logic Device (MAPLD), **(2008)**, pp. 356-367.

[4] C. Bo, F. Binxing and Y. Xiaochun, "A new approach for early detecting internetworm based on least squaresmethod", J. Journal of Harbin Institute of Technology, **(2007)**, pp. 431-434.

[5] S. Sellke, N. B. Shroff and S. Bagchi, "Modeling and auto-mated containment of worms", C. Proceedings of the 2005 International Conference on Dependable Systemsand Networks, Washington, IEEE Press, **(2005)**,

pp. 528-537.

[6] Z. Hanxun, Z. Hong and W. Yingyou, “Modeling and Analysis of Divide-and-Rule-Hybrid-Benign Worms”, J. Journal of Computer Research and Development, **(2009)**, pp. 1110-1116.

[7] J. Liu, X. Wang, H. Ren, J. Wang and J. -U. Kim, “An Analytical Model for Hypercube Network-On-Chip Systems with Wormhole Switching and Fully Adaptive Routing”, International Journal of Grid and Distributed Computing, vol. 5, no. 4, **(2012)**, pp. 33-42.

[8] Y.-C. Jhi, P. Liu and L. Li, “PWC: A proactive worm containment solution for enterprise network”, C. Third International Conference on Security and Privacy in Communications Networks and the Workshops, **(2007)**, pp. 433-442**.**

[9] C. Jin, Q. -H. Deng and J. Liu, “Computer Virus Propagation Model Based on Variable Propagation Rate”, International Journal of Advanced Science and Technology, **(2008)**, pp. 29-34.

[10] T. Jun-feng, Z. Chi and L. Tao, “Approach to worm early warning based on local victim behavior”, J. Journal on Communications. **(2007)**, pp. 89-89.

[11] Symantec security response. EB/OL.: http://www.symantec.com/enterprise/security_response/threatexplorer/azlisting.jsp, **(2006)**.

[12] N. Provos, “A virtual honeypot framework”, R. Technical Report, 03-1.Center of Information Technology Integration, University of Michigan, **(2009)**, http://www.citi.umich.edu/techreports/reports/citi-tr-03-1.pdf.

[13] L. Spitzner, “Honeypots: Tracking Hackers”, M. Boston: Addison-Wesley, **(2006)**, pp. 277-309.

[14] C. C. Zou, W. Gong and D. Towsley, “Code Red worm propagation modeling and analysis”, C. In: Proc. of the 9th ACM Symp on Computer and Communication Security, Washington, **(2002)**, pp. 138-147.

[15] Y. Wang and C. X. Wang, “Modeling the effects of timing parameters on virus propagation”, C. In: Staniford S, ed. Proc. of the ACM CCS Workshop on Rapid Malcode (WORM 2007). Washington, **(2007)**, pp. 235-239.

[16] M. Marchetti, M. Colajanni and F. Manganiello, “Framework and Models for Multistep Attack Detection”, International Journal of Security and Its Applications, vol. 5, no. 4, **(2011)** October, pp. 73-90.

Authors

Liu Yang, Associate Professor, his research fields include Network information Security Technology, Internet of Things Security Technology, *etc*. He has participated in many projects of Ministry of Information Industry and National Science, and he has published over 20 academic papers in journals and conferences both home and abroad.

Wang Bailing is working for Harbin Institute of Technology (abstract as HIT) as an associate professor. He got the Ph.D. degree from HIT in 2006. His research is mainly on information security, network security, parallel computing.