Centralized Containment Model and Mathematics Modeling†

Zhu Qiang, Liu Yang*, Wang Bailing, He Hui, Li Gen

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

Abstract. In order to curb the spread of the worm in the network system, Expand worm containment methods from the point of view of the management system vulnerabilities. First comprehensive exposition Internet worm containment technology research progress ; then dissect initiative to curb the technical principles and given technology based initiative to curb centralized confrontation strategy , and finally to the mathematical modeling analysis for centralized confrontation strategy , to lay the foundation for further study .

Keywords: Worms; System vulnerability; Centralized confrontation strategy

1 Introduction

Worm threats on the Internet security are gradually approaching each ordinary user. 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 [2]. 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 [3]. The active countermeasure technology has important application prospect in controlling worm outbreaks scope and avoiding worm epidemic repeated [4-5]. The research based on the active countermeasure technology of centralized containment strategy is of great significance.

2 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

† Supported by the National Science Nature Foundation of China under Grant No 61170262

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.This article assumes vicious worms using uniform random scanning strategy.

2.1 Network worm propagation model research.

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:

$$dI(t)/dt = \beta(t)S(t)I(t)/\Omega \tag{1}$$

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 $\Delta Q_1(t)$, the changes in number of infected hosts that have been repaired by FP are $\Delta R_1(t)$; 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 formula (1), the worm containment propagation mathematical model under the active containment strategy satisfy:

$$\begin{cases} dS(t)/dt = -\beta(t)S(t)I(t)/\Omega - dQ(t)/dt \\ dI(t)/dt = \beta(t)S(t)I(t)/\Omega - dR(t)/dt \\ dR(t)/dt = \\ dQ(t)/dt = \\ \alpha(t) = \alpha_0[1-(I(t)+I_F(t))/\Omega]^{\eta} \\ \beta(t) = \beta_0[1-(I(t)+I_F(t))/\Omega]^{\eta} \\ I_F(t) = \\ J(t) = I(t)+R(t) \\ N = S(t)+I(t)+R(t)+Q(t) \\ I(0) = I_0 << N; I_F(0) = I_{F0} << N; S(0) = N - I_0; \end{cases} \tag{2}$$

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.

2.2 Centralized containment propagation model

Analysis from the active containment angle, In the 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.

Case: 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 β_0; the centralized containment system scan frequency is α_0.

According to the case, the impact containment system on the network equivalent to α_0/β_0 worms scanning, therefore:

$$I_F(t) = \alpha_0 / \beta_0 \tag{3}$$

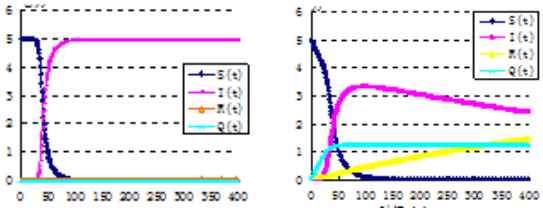
and $\alpha(t)=\alpha_I(t)=\alpha_S(t)$, so we only use α (t) in formula. The number of hosts that centralized containment system has scanned is $\int_0^t \alpha(t)$ at any time t. According to formula2 and 3, at any time t, the number of hosts that centralized containment system has scanned is:

$$\int_0^t \alpha(t) = \frac{\alpha_0}{\eta+1}\left[1-\frac{I(t)+\alpha_0/\beta_0}{\Omega}\right]^{\eta+1} \tag{4}$$

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 :

$$\begin{cases} \frac{dQ(t)}{dt} = \alpha(t)\times\delta_S = \alpha(t)\times\frac{S(t)}{\Omega-\int_0^t\alpha(t)} \\ \frac{dR(t)}{dt} = \alpha(t)\times\delta_I = \alpha(t)\times\frac{I(t)}{\Omega-\int_0^t\alpha(t)} \end{cases} \tag{5}$$

The formula 3 and formula 5 into the formula 2, and get the worm containment propagation model under the active containment strategy in the case (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

Fig. 1. Graph of the changes in the host number under the various states of the WPM-CCMI

By comparing the a and b in Figure 1, 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 1 b), but the effect is not obvious in the large-scale network(Figure 1 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.

3 Conclusion

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.

References

1. Chen Bo, Fang Bin-xing, Yun Xiao-chun: A new approach for early detecting internetworm based on least squaresmethod. J. Journal Of Harbin Institute Of Technology, 431--434 (2007)
2. Symantec security response. EB/OL.: http://www.symantec.com/enterprise/security_response/threatexplorer/azlisting.jsp. 2006
3. Provos N. 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
4. Spitzner L. Honeypots: Tracking Hackers. M. Boston: Addison-Wesley, 277--309 (2006)
5. Zou CC, Gong W, Towsley D.: Code Red worm propagation modeling and analysis. C.In: Proc. of the 9th ACM Symp on Computer and Communication Security.Washington, 138--147 (2002)