A Novel Cloud-based Benign Worm Defense Technology

Xufei Zheng\textsuperscript{a,b}, Tao Li\textsuperscript{a,*}, Hua Yang\textsuperscript{a}, Xin Xiao\textsuperscript{a}

\textsuperscript{a}College of Computer Sciences, Sichuan University, Chengdu 610065, China
\textsuperscript{b}School of Computer and Information, Southwest University, Chongqing 400715, China

Abstract

Due to the proactive defend against the worm propagation and patch the susceptible hosts, benign worms are attracting wide attentions in the field of worm research. In this paper, we point out the errors of worm-anti-worm model (WAW) and present a revised model named Re-WAW based on the law of worm propagation and Two-Factor model. Based on the discussion of the worm propagation factors such as time delay and initial number of benign worms, we put forward a novel cloud-based Re-WAW model to achieve effectively worm containment by quickly delivery of the initial number of benign worms. Simulation results show that the cloud-based Re-WAW model significantly improves the worm propagation containment effect relative to the Re-WAW model and Two-Factor model, cloud computing help achieve the rapid delivery of massive initial benign worms and thus obtain close to valuable 20 hours time delay.

Keywords: Worm; Benign Worm; Cloud-based Re-WAW Model

1 Introduction

Since the Morris worm [1] in 1988, the big years of world-wide internet spreading worms were 2003 and 2004, the years of Blaster and Sasser. About four years later, in November 2008, the Conficker worm spotted and quickly became one of the most notorious worms in the history [2]. The Conficker worm owned the world’s largest cloud network that Conficker controls 6.4 million computer systems in 230 countries at 230 top level domains globally, more than 18 million CPUs and 28 terabits per second of bandwidth [3, 4]. Staniford et al. [5] have predicted that, with better scanning algorithms, it is possible for worms to infect 90 percent of the susceptible hosts in mere minutes. Some fast spreading worms (e.g., Slammer, Blaster) have proven this, and they clearly defeat current defenses such as AV software, IDS and IPS.

*Project supported by the National Natural Science Foundation of China (NO.60873246), the Cultivation Fund of the Key Scientific and Technical Innovation Project by Ministry of Education of China (NO.708075), the Doctoral Fund of Ministry of Education of China (NO. 20070610032), and the Fundamental Research Funds for the Central Universities (XDJK2009C023, XDJK2010C025).

*Corresponding author.

Email address: litaoscut.edu.cn (Tao Li).

1548–7741/ Copyright © 2011 Binary Information Press
December 2011
Due to the strong similarity between worms and biological diseases, epidemiological models have been widely used in modeling the worm propagation. There were vast catalog of mathematical models indicated for epidemiology and they were based on the Kermack-McKendrick model which also referred to as the SIR model for its three states Susceptible, Infected, and Recovered. Some epidemic models representing worm propagations were presented in [6, 7, 8].

Currently, a number of detection and defense technology have been proposed to contain the worm propagation, but they are somewhat to remedy the situation and cannot fundamentally solve the problem [9, 10, 11, 12]. Benign worms, proposed by Frank et al. [13], are beneficial worms that counter the original malicious worms, they can dynamically proactive defend against worm and thus fundamentally solve the worm propagation problem. Frank et al. presents a method that transforms a malicious worm into a benign worm which disinfects its original, and divides benign worm into 4 different categories. In [14, 15, 16, 17, 18] it is discussed these 4 different kind of benign worms with mathematical modeling and simulation.

In this paper, we propose a novel cloud-based proactive benign worm defense architecture which is a kind of strategy of fast and light-load countermeasure technology to contain worm propagation. Based on the WAW model [6], we revise, model and simulate the Re-WAW model, and the cloud-based Re-WAW model. Unlike other models proposed to the date, the cloud-based Re-WAW model which combines cloud computing can attain rapid delivery of massive initial benign worms and to achieve effective containment of the worm propagation. Computer simulations show that the performance of our proposed model is significantly better than other existing models, in terms of decreasing both the number of infectious hosts and the worm propagation speed.

The rest of this paper is organized as follows. In section 2 we put forward a novel kind of cloud-based proactive benign worm defense architecture and discuss the advantages and limitations of the proposed approach. In section 3 we point out the errors of WAW model and present a revised WAW model which named Re-WAW model, and discuss the cloud-based Re-WAW model as well as simulation. The conclusions are given in section 4.

2 The Cloud-based Benign Worm Defense Architecture

Currently, the only effective way to prevent a computer infected by the worm is to patch the corresponding vulnerabilities. But it is almost impossible to achieve for these reasons: 1) there are a lot of vulnerabilities in various kinds of software systems; 2) the worm propagate faster and faster, and more and more vulnerabilities to appear; 3) the computer users’ security awareness is very frail, according to statistics, the updating of antivirus software to new version is less than 20%; and 4) there are many hosts of the network is under the state of no management in long-term. Frank et al. presented a method that is to transform a malicious worm into an anti-worm which spread itself using the same mechanism as the original worm and immunizes a host [13]. The anti-worm is a kind of beneficial worm that counter the original worm, it can dynamically proactive defends against the malicious worm and patches the vulnerable hosts, which fundamentally solve the worm propagation problem.

In this paper, we put forward a novel cloud-based proactive benign worm defense architecture which combines cloud computing technology to defend against the malicious worms. The framework is divided into three stages: 1) worm detection and capture, 2) worm analysis, and 3) benign worm generation.
Stage 1: Worm Detection and Capture. At step (1) the worm message enters the system and the network monitors record the message. In (2) the message is received by a Honey Pot instance which compares the message based signatures and determines it is a worm traffic or not. In (3) and (4) the now infected instance retransmits the same worm message. The source and destination port number of the attack message itself is recorded by an active Virtual Machine (VM) image in the cloud and send to the generation module.

Stage 2: Worm Analysis. At step (5) in stage 2, the worm message from active Virtual Machine further confirmed through heuristics analysis of the data is collected from the comparison of the before-infection and after-infection VMs, including what files changed on the system, what registry entries were changed and what processes were started.

Stage 3: Benign Worm Generation. The stage is the main focus of this paper. At step (6) in stage 3, the same attacking method used by the original worm messages is used to produce the corresponding benign worm. After necessary test and deployment, benign worms can proactive defend against original worms and patch the vulnerable hosts through virtual patching node in the cloud or patch upgrade websites in step (8). As we will discuss in section IV, benign worms will lead to network congestion and potential DDoS attacks to patch upgrade website, thus it is necessary to clear off the benign worms when malicious worms have been eliminated.

3 The Cloud-based Worm-Anti-Worm Model

3.1 The Worm-Anti-Worm Model: WAW Model

Qing et al. put forward the WAW model which considers two types of worms: a malicious worm A and an oppositional benign worm B. The propagation process is divided into two stages: when benign worm B is absent, the propagation of worm A is subject to the Two-Factor model; when benign worm B is present, there are four potential cases: 1) B detects and cleans A, and patches the hosts infected by A; 2) B only detects and cleans A; 3) B patches all susceptible hosts; and 4) B patches all susceptible hosts, and detects and cleans A. Based on Two-Factor model [7], Qing et al. discussed the worm A propagation and gave the differential equations of WAW model and propagation trend in case 4 are shown as Eq. (1) and Fig. 1.

\[
\begin{align*}
\frac{dS(t)}{dt} &= -\beta(t)S(t)I(t) - \frac{dQ(t)}{dt} - \frac{dR_B(t)}{dt} \\
\frac{dR(t)}{dt} &= \gamma I(t) + \frac{dR_B(t)}{dt} \\
\frac{dQ(t)}{dt} &= \mu S(t)J(t) \\
\frac{dR_B(t)}{dt} &= \beta_1 R_B(t)[S(t) - R_B(t)] \\
\beta(t) &= \beta_0 \left[1 - \frac{I(t)}{N}\right]^\eta \\
N &= S(t) + I(t) + R(t) + Q(t) \\
0 &\leq S(t), I(t), R(t), Q(t) \leq N
\end{align*}
\]

The WAW model takes the existence of the benign worm into account. However, the WAW model doesn’t consider the relationship between the propagation of the benign worm itself and
the other limiting factors, as well as the states of the benign worm after it enters the susceptible hosts.

Table 1: Parameters and Initial Values of WAW, Re-WAW and Cloud-based Re-WAW model

<table>
<thead>
<tr>
<th>Notation</th>
<th>Explanation</th>
<th>Initial Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I(t)$</td>
<td>Number of infectious hosts at time $t$</td>
<td>1</td>
</tr>
<tr>
<td>$S(t)$</td>
<td>Number of susceptible hosts at time $t$</td>
<td>1000000-1</td>
</tr>
<tr>
<td>$R(t)$</td>
<td>Number of recovered hosts from the infectious population at time $t$</td>
<td>0</td>
</tr>
<tr>
<td>$R_B(t)$</td>
<td>Number of benignly infectious hosts at time $t$</td>
<td>0</td>
</tr>
<tr>
<td>$J(t)$</td>
<td>Number of infected hosts at time $t$, $J(t) = I(t) + R(t)$</td>
<td>1</td>
</tr>
<tr>
<td>$Q(t)$</td>
<td>Number of recovered host from the susceptible population at time $t$</td>
<td>0</td>
</tr>
<tr>
<td>$\beta_0(t)$</td>
<td>Infectious rate of the worm to susceptible hosts at time $t$</td>
<td>0.8/$N$</td>
</tr>
<tr>
<td>$\beta_1(t)$</td>
<td>Infectious rate of the benign worm to susceptible hosts at time $t$</td>
<td>0.8/$N$</td>
</tr>
<tr>
<td>$\beta_2(t)$</td>
<td>Infectious rate of the benign worm to infectious hosts at time $t$</td>
<td>1/$N$</td>
</tr>
<tr>
<td>$\eta$</td>
<td>A worm’s average scan rate</td>
<td>3</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>Recovered rate of infectious hosts</td>
<td>0.05</td>
</tr>
<tr>
<td>$\mu$</td>
<td>The death rate of infectious population</td>
<td>0.06/$N$</td>
</tr>
<tr>
<td>$N$</td>
<td>Total number of hosts under consideration</td>
<td>1000000</td>
</tr>
<tr>
<td>$T$</td>
<td>Time delay</td>
<td>changing</td>
</tr>
<tr>
<td>$K$</td>
<td>Radio of the benign worm to the worm</td>
<td>changing</td>
</tr>
</tbody>
</table>

3.2 The Revised Worm-Anti-Worm model: Re-WAW

However, there is an error description of WAW model by the differential Eq. (1). Based on the differential equations Eq. (1), we can get the state transition diagram of WAW model in case 4 as shown in the Fig.2, which the benign worm $B$ only patches all susceptible hosts but do nothing to the infectious hosts. It is contradictitious and conflict to the original WAW assumptions in case 4 that $B$ patches all susceptible hosts, and detects and cleans $A$. So, the differential Eq. (1) are not the correct description of WAW model in case 4.

Based on the framework and basic assumptions in [6] and taken the interaction of the benign worm with malicious worm and susceptible hosts into account, we put forward a revised WAW model named Re-WAW. There are four states in the Re-WAW model: they are Susceptible ($S$), Infectious ($I$), Recovered ($R$), and Quarantined ($Q$), the same to the WAW model. The propagation process is divided into two stages: when benign worm $B$ is absent, the propagation of worm $A$ is subject to the Two-Factor model; when benign worm $B$ is present, there are four potential cases which will be discussed in detail below. Different to WAW model, we use $\beta_1(t)$ represents the infectious rate of the benign worm to susceptible hosts at time $t$ instead of the constant beta1 of the WAW model, and use $\beta_2(t)$ represents the infectious rate of the benign worm to infectious hosts at time $t$ in Re-WAW model. Based on the Two-Factor model, the change in the number of susceptible hosts $S(t)$ from time $t$ to time $t + \Delta t$ follows:
The comparison of WAW in case 4 and Two-Factor

\[ I(t) \quad J(t) \quad Q(t) \]
\[ I(t) \quad J(t) \quad Q(t) \]

Fig. 1: The comparison of WAW model and Two-Factor model

\[ Q \xrightarrow{\mu S(t)I(t)} S \xrightarrow{\beta(t)S(t)I(t)} I \xrightarrow{\gamma_{t}I(t)} R \]

Fig. 2: The state transition diagram of WAW in case 4

\[
\frac{dS(t)}{dt} = -\beta_0(t)S(t)I(t) - \mu S(t)[I(t) + R(t)] - \beta_1(t)S(t)R_B(t)
\]  

(2)

For case 4: benign worm B patches all susceptible hosts and cleans worm A. The Fig.3 shows the state transition where the state changes from S to Q with B’s patching of susceptible hosts, and the state changes from I to Q with B’s cleaning of infected ones. The differential equations express the infectious hosts of malicious worm and benign worm as differential equation Eq. (3) and Eq. (4).

\[
\frac{dI(t)}{dt} = \beta_0(t)S(t)I(t) - \gamma I(t) - \beta_2(t)I(t)R_B(t)
\]  

(3)

\[
\frac{dR_B(t)}{dt} = \beta_1(t)S(t)R_B(t) + \beta_2(t)I(t)R_B(t)
\]  

(4)

Fig. 3: The state transition diagram of Re-WAW in case 4

According to the equations Eq. (2)~ Eq. (4), the differential equations of Re-WAW model in case 4 is shown as Eq. (5). Based on the Re-WAW model in case 4, we can easily analyze the
other three cases of Re-WAW and thus we skip this content for the reason of extent length.

\[
\begin{aligned}
\frac{dS(t)}{dt} &= -\beta_0(t)S(t)I(t) - \mu S(t)[I(t) + R(t)] - \beta_1(t)S(t)R_B(t) \\
\frac{dI(t)}{dt} &= \gamma I(t) + \beta_2(t)I(t)R_B(t) \\
\frac{dR(t)}{dt} &= \beta_0(t)S(t)I(t) - \gamma I(t) - \beta_2(t)I(t)R_B(t) \\
\frac{dR_B(t)}{dt} &= \beta_1(t)S(t)R_B(t) + \beta_2(t)I(t)R_B(t) \\
\frac{dQ(t)}{dt} &= \mu S(t)[I(t) + R(t)] + \beta_1(t)S(t)R_B(t) \\
\beta_0(t) &= \beta_0 \left[1 - \frac{N}{I(t) + R_B(t)}\right]^\eta \\
\beta_1(t) &= \beta_1 \left[1 - \frac{N}{I(t) + R_B(t)}\right]^\eta \\
\beta_2(t) &= \beta_2 \left[1 - \frac{R_B(t)}{N}\right]^\eta \\
N &= S(t) + I(t) + R(t) + R_B(t) + Q(t) \\
0 &\leq S(t), I(t), R(t), R_B(t), Q(t) \leq N
\end{aligned}
\]

(5)

The propagation trend of the four different cases in Re-WAW model with and without time delay T is shown in the Fig.4. We can see from the Fig.4 that the worm propagation controlled in almost the same speed in case 1 and case 2, the case 1 has slightly better because of B patches the infected hosts which ensures that the hosts cannot be re-infected. For case 3, benign worm B only patches all susceptible hosts which accelerates the rate of the hosts’ immunization but no direct killing of worm A, so the worm propagation controlled better because of the most of susceptible hosts been immunized before been infected in the case without time delay T and the worm propagation controlled worse because of the most of susceptible hosts been infected before been immunized in the case with time delay T. For case 4, as from the reduction of susceptible hosts and infected hosts to contain the worm propagation, so the worm propagation controlled best. In the rest of this paper, we will only discuss the case 4 if not specified.

In real network environment, due to the detection of worm A and design of benign worm B will take some necessary time, worm B is always later than A enter into the network. On the basis
of the differential equations Eq. (5), we can also derive the differential equations Eq. (6) which describes the Re-WAW model in case 4 with time delay T.

\[
\begin{align*}
\frac{dS(t)}{dt} &= -\beta_0(t)S(t)I(t) - \mu S(t) \left[ I(t) + R(t) \right] - \beta_1(t)S(t)R_B(t - T) \\
\frac{dI(t)}{dt} &= \gamma I(t) + \beta_2(t)I(t)R_B(t - T) \\
\frac{dR_B(t - T)}{dt} &= \beta_1(t)S(t)R_B(t - T) + \beta_2(t)I(t)R_B(t - T) \\
\frac{dQ(t)}{dt} &= \mu S(t) \left[ I(t) + R(t) \right] + \beta_1(t)S(t)R_B(t) \\
\beta_0(t) &= \beta_0 \left[ 1 - \frac{I(t) + R_B(t)}{N} \right]^\eta \\
\beta_1(t) &= \beta_1 \left[ 1 - \frac{I(t) + R_B(t)}{N} \right]^\eta \\
\beta_2(t) &= \beta_2 \left[ 1 - \frac{R_B(t)}{N} \right]^\eta \\
N &= S(t) + I(t) + R(t) + R_B(t) + Q(t) \\
0 \leq S(t), I(t), R(t), R_B(t), Q(t) \leq N
\end{align*}
\]

(6)

As mentioned above, time delay T is an important factor to the worm propagation. As can be seen from the Fig. 5, the worm propagation contained better when T is shorter. Though reduction of the time delay T is the most direct and effective way in theory, it is impractical in real network environment for the detection of worm A as well as design and delivery of benign worm B will take some necessary time. Furthermore, we hope that the time delay T as long as possible to ensure sufficient time to delivery benign worms before magnitude constructions caused by the malicious worms.

Based on the preceding analysis, we know that the benign worms can effectively contain the propagation of the malicious ones. Therefore, we hope to achieve better containment effect on malicious worm by increasing the delivery of initial benign worms. As can be seen from the Fig. 6, the simulation shows that the malicious worms been better contained with the increase of the initial benign worms.
3.3 The cloud-based Re-WAW model

Zheng et al. [19] put forward a novel cloud-based worm propagation model named MRDC which exploits the parallel processing of cloud computing and achieves much faster propagation than traditional propagation models. The MRDC model can be used to achieve the delivery of a large number of initial benign worms.

The cloud-based MRDC propagation model can infects as many as 65536 susceptible hosts in a very short period of time. The malicious worm propagation will be effectively controlled when these 65536 infected hosts as the initial benign worms of Re-WAW model. As can seen from the Fig.7, the containment of malicious worm with initial benign worm=65536 and time delay T=30h almost the same as with initial benign worm=1 and time delay T=10h. This means that obtaining of valuable 20 hours for the delivery of benign worms by increasing the amount of initial benign worms.

Fig. 7: The comparison of Re-WAW with different of initial benign worm and delay and Two-Factor

4 Conclusion

The fact that Worm Cheese defends against worm Lion and worm Welchia defends against worm MSBlaster reminds us that it is an effective way to curb the worm propagation by use of benign worms. In this paper, we present Re-WAW model that was revised from the WAW model, which can simulate the process of the worm propagation containment by use of benign worms. The cloud-based Re-WAW model can achieve rapid containment of the worm propagation by means of delivery of massive initial benign worms. The mathematical modeling and simulation results show that the cloud-based Re-WAW model can not only effectively contain the worm propagation, but also effectively reduce the overall consumption of network resources.
References