Optimization of Blaster worms by Stochastic Modeling

Tatehiro Kaiwa s1080060 Supervised by Hiroshi Toyoizumi

Abstract

The purpose in this paper is to compare the difference between the existing Blaster worms and the optimized ones in local network. In the paper, we investigate activities of the Blaster worms, and optimize the Blaster worms by using stochastic modeling. We use two kinds of Pure Birth Process, Poisson Process and Yule Process.

The work is helpful for preparing the outbreak of the unknown worms similar to the Blaster worm.

1 Introduction

In recent years, many computer worms have attacked many PCs connected to the Internet. Computer worms are kind of computer virus, the worm makes a copy of itself and spreads throughout the Internet through many methods. In this process, the worms attack many PCs connected to the Internet. In a few years, it will be possible for a computer to be infected by a computer worm by just connecting one's PC to the Internet. To avoid problems, a user should know how to defend their PC against worms and viruses.

Computer worms mainly spread to the Internet, capitalizing on some software's security vulnerability that are known. Recently, some new types of worms, including CodeRed [4, 10], Slammer [4, 11] and Blaster, have appeared. One characteristic of these worms is what they are able to infect PCs with security vulnerabilities. The Blaster worm is a worm that exploits recent DCOM (Distributed Component Object Model) RPC (Remote Procedure Call) vulnerability [2]. This worm targets only Windows 2000 and Windows XP machines with vulnerable DCOM RPC Services running. By the consequence of worm penetration if these machines are attacked and their RPC systems become unstable, these operating systems may clash as a result. In addition, the worm does a DoS (Denial of Service) attack to windowsupdate.com. The worm has infected more than 381,000 computers in the world in four days.

The purpose of this research is to analyze the Blaster worm for creating a worm model. Although the worm program is poor in many respects, this worm success to infect many PCs. [2] This paper studies the method used to spread this worm is not optimal, and how bad it could be if the threat of this worm is optimized by using a Pure Birth Process.

2 Blaster

2.1 Target Virus

The target virus in this paper is called "Blaster." The Blaster worm was discovered in August 11, 2003. The virus was categorized Worm type. The worm is also known as W32/Lovsan.a, Win32.Poza.A, Lovsan, WORM_MSBLAST_A, W32/Blaster-A, W32/Blaster, Worm.Win32.Lovsan and W32/Blaster.A.

2.1.1 Virus activities on the PC

When the Blaster worm is executed, the worm first checks to see whether Blaster worm is running. If the PC is already infected has mutex exclude what Blaster worm runs mutually, the worm does not run two or more in the same PC at the same time. Second, the worm creates a value "windows auto update"="msblast.exe" in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Windows\CurrentVersion\Run registry key to run when the Windows PC in which the worm was executed restarts. Then, the worm attempts to create the mutex named 'BILLY.' Third, Blaster worm waits for an active network connection, and starts searching for machines to infect. If there are no active network connections, Blaster worm will not start.

2.1.2 Search targets

Blaster worm is a worm that targets machines running Windows 2000 and Windows XP. The worm creates two kinds of packets to exploit each vulnerability. The probability that the worm creates packets to exploit vulnerability for Windows XP is 0.8, and 0.2 for Windows 2000 (See Figure 1). Only when the worm starts, this is decided. There are two methods to selects IP addresses to decide as an attack target to spread copies of itself. The probability that the worm will select a random IP addresses entirely is 0.6, and the worm will select the same class-B-sized network IP address on the machine to spread the local area network with probability 0.4(See Figure 1). To scan targets, the worm make the target address increase monotonically until it reaches the end of the IP space.

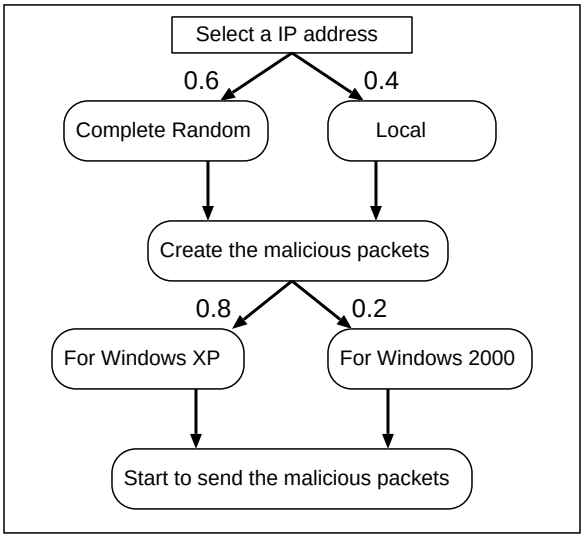

Figure 1: The algorithm of the Blaster worm [7] to select its target machines.

Method	Probability	Name
Select Random	0.6	*Random*
Select Local	0.4	*Local*
Packets for Windows XP	0.8	α
Packets for Windows 2000	0.2	$(1-\alpha)$

Table 1: The table expresses the probability of selecting each method.

2.1.3 Penetration

The infection of a new machine is a three-phase process. First, the worm sends malicious packets port 135/tcp of the target host to exploit the DCOM RPC vulnerability and then causes the remote machine to bind a shell in the SYSTEM context to port 444/tcp.
Second, the worm sends a command to request a download of the worm file from the attacking host to the victim. This transfer uses a tftp protocol (port 69/udp). Finally, once msblast.exe has been downloaded successfully, or after 21 seconds, the worm requests the remote system to execute the downloaded file.

3 The Experimental Network

3.1 Figure of Experimental Network

To confirm and obtain some information about the Blaster worm, we prepare a LAN (Local Area Network) isolated other network for an experiment (See Figure 2). In the experiment, we executed the Blaster worm on one of the Windows XP machines in VLAN1, and then, we investigate the penetration process of the Blaster worm. A way of the data collection of the Blaster worm is written in next section (See Section 3.2).

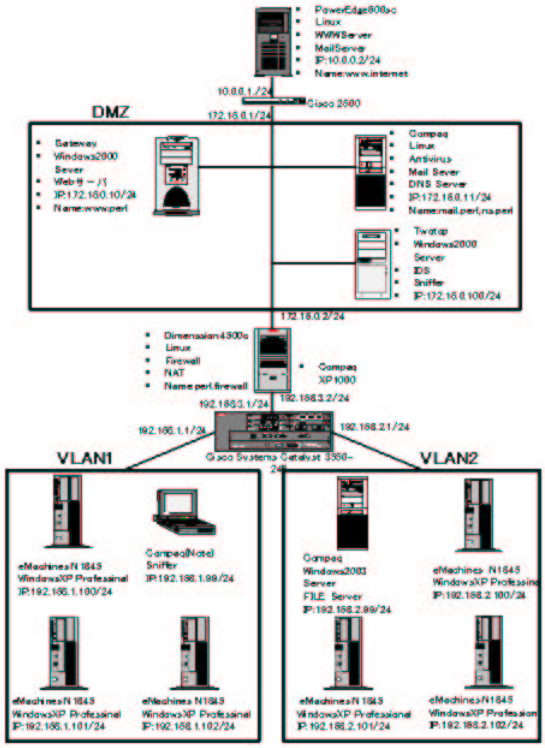

Figure 2: The experimental network figure. We run the Blaster worm in the network to collect some data we need of the Blaster worm.

3.2 Virus Data Collection

A purpose of observing the worm activity is to obtain the mean time that a Blaster worm spend searching targets per hour. Thus, we needed to capture many Blasters' packets. To capture the packets, we used a hosting-type packet capture software named Sniffer [7]. Hosting type means running on a target client for something. Because the worm may causes the system instability to an infected PC and the targets, it is difficult to collect the accurate data by that PCs installed Sniffer. To avoid such problems, we prepared a PC set up with no infection and collected the worm's packet data used in the PC. In the experiment, we executed a Blaster worm and the Blaster worm infected a PC. Then, many packets the Blaster worm sends to investigate the worm running were captured. The information obtained from the experiment was a Blaster worm that spends 5916.165 second scanning one class-B-sized IP address. As the result, we

obtained the number of packets that one Blaster worm sends on average, 10.905 packets per second. In other words, one Blaster worm sends 39,258 packets per hour. (See Table 2)

Blaster worm sometimes fails to infect a PC because it is defective. When the worm sends malicious packets to local network, the worm regards infected PCs IP address as class C IP address. Then, the worm starts to attack to the network address of the address with the target address increasing monotonically. Since the probability that a Blaster worm outside of the local network and other worms inside of local network will attack the same IP address is very high by the above reasons, the infection rate of all the worms except the first worm in the network is small. For the reasons mentioned above, we need to consider and treat the infection rate of first Blaster worm and other worms.

At the University of Aizu in Dec 2003, a Nachi worm [4, 12] infected a PC in the university network. According to UBIC [5] announcement, the number of infected PCs was 71 in total. A vulnerability the worm exploits is the same as the one a Blaster worm exploits. Thus, we regard the number 71 as the number of PCs the Blaster worm could also potentially infect. In other words, a rate of machines having the vulnerability is about 0.11 %. In addition, we obtain the fact that the Blaster worm can not infect once per five times.

Information		Name
Average packets/h	39258	M
Rate of successful infection	1/5	R_{Suc}
Probability of Vulnerability	0.0011	P_{Vul}

Table 2: The table expresses the information we obtained with some experiments.

In the next section, we will solve a virus model based on the above parameters (See Table 2).

4 The Virus Model

4.1 Pure Birth Model

We consider that one infected machine outside of the local network attacks to machines in the local network(See Figure 3). We suppose that the local network is enough large and the infection activity of each machine infected by Blaster worm is the Pure Birth Process with transition rate λ_n, where n is the the number of PCs infected by Blaster worm in local network(See Figure 4).

Therefore, let the infection rate ν and λ (See figure 3) of Blaster worm be as following,

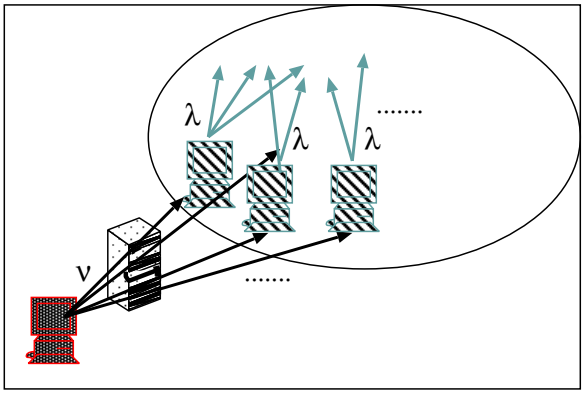

Figure 3: This Figure express Infection Model of the Blaster worms. ν and λ is infection rate.

ν: Infection rate of Blaster worm outside of the local network
λ: Infection rate of Blaster worms inside of the local network

Let $N(t)$ be the number of infected machines in a local network at time t, then $\{N(t), t \geq 0\}$ is a pure birth process with

$$\lambda_n = \nu + n\lambda \qquad (n = 0, 1, 2, \ldots). \tag{1}$$

As each infection activities are independent, (1) is regarded as the mixture of the Poisson Process and Yule Process [3] (See Figure 4). Then, we can use a equation from Performance Evaluation of Defense Strategies against Computer Virus. [9] Now, as our model have no death rate, we make the death rate in the equation 0. Thus, we obtain the following equation:

$$P\{N(t) = n\} = \binom{n + \frac{\nu}{\lambda} - 1}{\frac{\nu}{\lambda} - 1} p^{\frac{\nu}{\lambda}} (1-p)^n, \tag{2}$$

where

$$p = \frac{\lambda}{\lambda e^{\lambda t}} = \frac{1}{e^{\lambda t}}.$$

A equation (2) expresses the probability that the number of PCs infected by Blaster worms is n. If we can obtain the value of ν and λ, we can see some relation between the probabilities and time with the equation (2),

4.2 Infection Rate ν and λ

We suppose that there are some machines having the DCOM RPC vulnerability in local network, and let a ratio of R_{XP} to R_{2k} is Windows XP machines to Windows 2000 machines. Then, let P_{Hit} is the probability

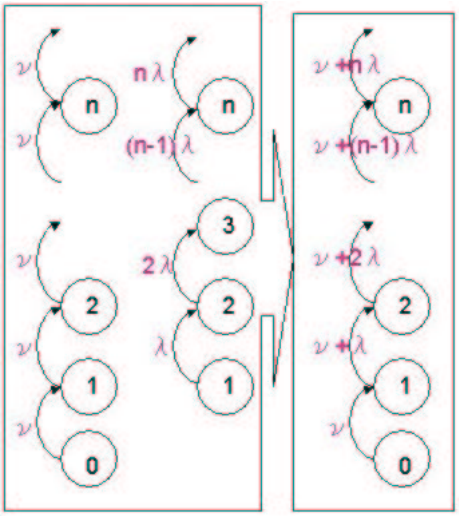

Figure 4: The Stochastic Model of mixture of the Poisson Process and Yule Process.

that a malicious packet for Windows XP arrives at one of the Widows XP machines running the vulnerable DCOM RPC service in the local network or a packet for Windows 2000 arrives at one of the Windows 2000 machines running the vulnerable DCOM RPC service in the local network. Thus P_{Hit} is given by the following equation:

$$P_{Hit} = (\alpha \times \frac{R_{XP}}{R_{XP} + R_{2k}} + (1-\alpha) \times \frac{R_{2k}}{R_{XP} + R_{2k}}) \times P_{Vul}, \quad (3)$$

where α and P_{Vul} are given by Table (1). We consider a infection rate ν. The rate ν is sometimes called immigration rate. Then, the infection rate ν is given by the following equation:

$$\nu = M \times P_{Hit} \times R_{Suc}, \quad (4)$$

where M and R_{Suc} are given by Table (2). Another infection rate λ is the rate of the Blaster worm inside of the local network. Considering the probability that the Blaster worms send the packets to local network, we obtain the infection rate λ is following equation.

$$\lambda = M \times P_{Hit} \times R_{Suc} \times Local, \quad (5)$$

where M, R_{Suc} and $Local$ are given by Table (1) and (2).

By the way, according to CNET Japan [6] article, the ratio of R_{XP} and R_{2k} in the local network in company is following:

$$R_{XP} : R_{2k} = 1 : 8. \quad (6)$$

Thus we suppose that the ratio is general ratio in the local network.

5 Results

5.1 The effect of changing R_{XP} and R_{2k}

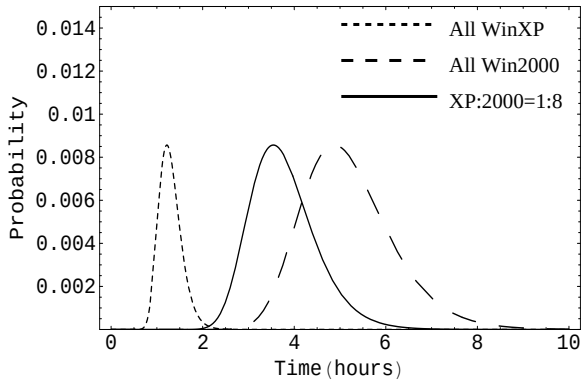

Figure 5: This graphs of $P\{N(t) = n\}$ when the number of infected PCs in the local network is 70(n=70). We can see the difference in a few sets of ratio of each systems in the local network. Each graphs express a case of when the systems are all Windows XP, when the systems are all Windows 2000 and when the ratio by general ratio by (6).

From Figure 5, we can see that the performance of the Blaster worms has a great difference with the ratio of the number of Windows XP machines to the number of Windows 2000 machines. The graphs demonstrate that the performance of the Blaster worms can be improved if the ratio of the Windows XP machines is high in the local network.

5.2 Optimize

We consider what optimizes the spread of the Blaster worm. We suppose that the number of packets the Blaster worms send does not change. Then we the Blaster worms always send the suitable packets to targets. To optimize the Blaster worm, we need to improve both the infection rate α and λ. We optimized the Blaster worm with making R_{Suc} and P_{Hit} maximum value. In Figure 6, we can see the difference in a threat between the optimized Blaster worms and the existing Blaster worms.

6 Conclusion and Future Works

From Figure 6, we can see that the optimized Blaster worms prove great threat, and we can say that the existing Blaster worm also has a potential the same threat, because the Blaster worms can close to the optimized

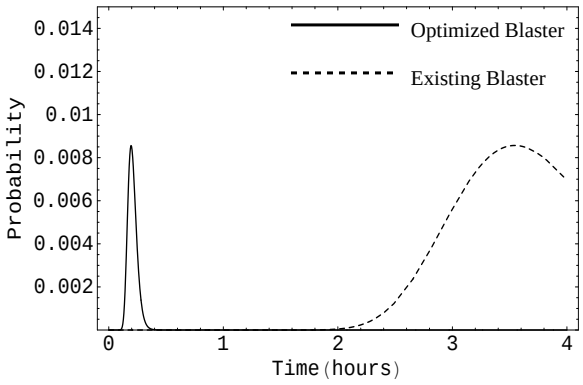

Figure 6: The graphs of the optimized Blaster worm and existing Blaster worm using equation (6), where $P\{N(t) = 70\}$

ones if the poor program are improved. As the penetration of the optimized Blaster worms is very speedy and the worms cause outbreak rapidly, it is clear that we can not treat the worm well after a penetration of the worm. Thus, we may need to be careful a security update individually.

Because some parameters of the optimized Blaster worm in this paper may be different from the ones of the existing Blaster worms, the stochastic model may be not exact one. Thus, we may need to close to the accurate model of the existing Blaster worms in the future.

7 Acknowledgment

I thank Prof. Toyoizumi for his great advise. Moreover, I thank the members of the Performance Evaluation Laboratory for their help in this research.

References

[1] Virus Bulletin,"W32/Blaster", http://www.virusbtn.com/resources/viruses/indepth/blaster.xml *September 2003*

[2] Microsoft Security Bulletin MS03-026 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp *July 2003*

[3] Sheldon M.Ross, Stochastic Processes Second Edition *1996*

[4] Trend Micro, http://www.trendmicro.co.jp/

[5] University-Business Innovation Center http://www.ubic-u-aizu.pref.fukushima.jp/pub/

[6] CNET Japan, http://japan.cnet.com/

[7] Shinsuke Miwa and Hiroyuki Ohno. A report on the analysis of Virus and Worm on the VM Nebula.

[8] Sniffer Technologies, http://www.toyo.co.jp/sniffer/

[9] Hiroshi Toyoizumi, Performance Evaluation of Defense Strategies against Computer Virus, Proceedings Of The Queueing Symposium Stochastic Models And Their Applications,pages 267-274, *January 2004*

[10] Yuuzo Kobayashi, Modeling of Computer Viruses, University of Aizu, Graduation Thesis, *March 2003*

[11] Silicon Defense, The Spread of the Sapphire/Slammer Worm, http://www.silicondefense.com/research/slammer/, 2003

[12] Satoshi Onoda, Optimization of Nachi Spreads, University of Aizu, Graduation Thesis, *March 2004*