

A Proposal of Internet Worm Detection Using ICMP

Yoshimasa SAJIMA
Course of Electrical
Engineering, Graduate
School of Engineering,
Tokai University

Hiroshi ISHII
Department of Information
Communication, and
Electronics, School of
Information Science and
Engineering, Tokai University

Hiroaki NISHIKAWA
Department of Computer
Science, Graduate School of
Systems and Information
Engineering, University of
Tsukuba

Abstract

With the rapid proliferation of various types of worms that create different types of threats to the network security in recent years, The conventional worms detection techniques are no longer effective in playing their roles. However, it is important for the contemporary society to protect the network, the Internet, as one of the most widely used social infrastructure nowadays. Therefore, we propose and implement that a worm detection method using the characteristics of ICMP traffic be generated during the spread of the worm's infection. From the implementation, we observe that our proposed techniques are not only low-cost and low-overhead, but also capable in detecting unknown worms as compared to the conventional methods.

Key words: Internet worm, security, ICMP, intrusion detection

1. Introduction

In the recent society making the most of the internet, it is incredible to administrate the network environment in continuous and safe manner. Threats, however, such as computer virus, worm, and illegal access originated by malicious users are increasing. Consequently, the network administrators must tackle these threats daily by many means [1]. Damage caused by threats over the internet is increasing year by year. The investigation made by the Japanese government says that the ratio of the enterprises having suffered damage related to information security in year of 2004 is 83.5% and that 47.8% of the damage was caused by virus infection[2]. In case of computer virus and worm infection, loss for restoration from the infection as well as taking measures for it becomes big, and in Japan about 600 million yen is paid for restoration from virus infection every year. Moreover, as the infection penetrates more, a sufferer is likely to be an assailant, which may lose the credibility of the organization.

As the internet becomes larger and internet access lines become permanent and broadband, the damage caused by virus infection is becoming large. This circumstance is making it very difficult to manage the network system perfectly. And a new threat is likely to appear within a shorter interval, conventional measure may not sufficient for them [3]. Table 1 shows the number of days between the program patch distribution and the appearance of the worm
In our study, a "worm" is defined as an illegal self-replicating program. We propose a simple but

effective way of detecting the “possibility” of worm infection and the suspicious location, and alerting the administrator of the possibility and the location of worm infection.

Table 1: Number of days between patch and worm

Name	Patch distribution	Birth of worm	between patch and worm
SASSER	2004/4/13	2004/4/30	17 days
MSBLAST	2003/7/16	2003/8/11	26 days
SQLP1434	2002/7/24	2003/1/25	185 days
NIMDA	2000/10/17	2001/9/18	336 days

2. Worm infection routes

Worm infects systems via versatile routes, as services, OSs and application become much variety. Typical examples on how the systems are infected by the worm are shown below[3].

- (1) mail attached file
- (2) attack to the security hole via network
- (3) web browsing
- (4) file sharing

In the case (1), a system is infected by the worm due to opening a file attached to a mail sent by other worm-infected host. Different from virus in narrow sense virus, a worm is self-contained and does not need to be part of another program to propagate itself. So, the penetration of damage is rather quickly by mails sent without users' intention.

In the case (2), worms try to detect and intrude on hosts with security holes in OS and/or applications. During the time frame from the discovery of security hole to distribution of patch program, hosts are unprotected in very dangerous situation.

In the case (3), worms first infect web servers with weakness in security and then distribute themselves to hosts which visit the servers.

In the case (4), worm is distributed via file sharing system which enables file sharing by several hosts.

The way of infection is categorized into two groups, i.e., (a) user-assisted multiplication requiring users' judgment and action, and (b) self-multiplication without any users' action.

Cases (1), (3) and (4) are categorized into group (a) where infection can be controlled by users' judgment. But the case (4) is self-multiplication type and the infection speed is rather faster than the group (a).

This paper tackles with the case (2), which is self-multiplication type, and proposes a primary detection mechanism.

3. Existing worm detection methods and requirements to worm detection

3.1 Worm detection methods

Typical worm detection methods are as follows:

(a) Pattern matching

This method detects worms utilizing pre-defined worm characteristics and program codes, whose typical examples are Anti-virus software and IDS (Intrusion Detection System). The defect of this method is that it cannot detect worms if pattern definition files are not the newest and which are unknown to the detection system.

(b) Rule-based

This method detects worm by using rules that are established through the analysis of behavior of a specific application and worm activities (signature). Rule-based detection has a merit that it can handle unknown worms. However, the demerits are: (i) load problem caused by collection of all the packets belonging to the traffic to be observed, and (ii) difficulty in deciding a threshold judging normal or abnormal condition that requires expertise and learning time.

(c) ARP use

This method utilizes ARP (Address Resolution Protocol) issued by a worm infected host to search possible victims [5]. The ARP use detection is independent of definition file and signature and overcomes the defects of (a) and (b). However, this can only be applied for detection within the same subnet as the worm infected host and cannot be used for the worm intending infection for the outside of the subnetwork.

3.2 Functional requirements to worm detection

Worm infection may occur when the hosts are connected to the internet. Since the internet environment varies, the worm detection system must be applicable for a variety of network environments. The following functional conditions are required for the detection systems to be widely applied [5].

- (I) Low cost
- (II) Independence of pattern files
- (III) Automatic detection
- (IV) Precise detection
- (V) Real-time detection

We propose a worm detecting system trying to satisfy all the requirements above.

4. Proposed system

Aiming to avoid secondary worm infection from inside the LAN to outside, we propose the system that can detect the worm infection to the hosts within the LAN by the use of ICMP, which has a different worm detection mechanism from the existing ones.

4.1 Principle of the proposed system

Generally, worm infected host sends ICMP echo request to search the possible victim hosts. Our system observes ICMP echo request and its reply packets, and presumes the possible infected host from the traffic characteristics of those echo requests and replies. In normal situation, since ICMP echo request is sent by a user to the host that is anticipated to send back an echo reply, the

number of requests and replies are almost the same. Worms generally generate IP addresses randomly to spread infection [6]. The existing number of hosts is reported as 353,284,187 [7] in July 2005, and this number is only 8.23% of total theoretical IPv4 addresses, i.e., 4294,967,296. Hence, if worm infected host generates many random IP addresses and sends ICMP echo requests to those addresses outside of the LAN, the probability becomes high that many ICMP Destination Unreachable packets are sent back. So, observation of ICMP will notify us of the possible existence of worm infected host. This is the main idea of our proposal.

4.2 Effectiveness of the proposed system

The proposed worm detection method utilizing ICMP traffic characteristics can be said effective from the following reasons.

First, it does not need any pattern files required to the conventional methods and is effective to the unknown worm.

Second, since our method also requires observation of only specific traffic types among whole traffic within the network, traffic observation can last for a long period without giving any heavy load to the observation system nor requiring much memory capacity.

4.3 Implementation of the proposal

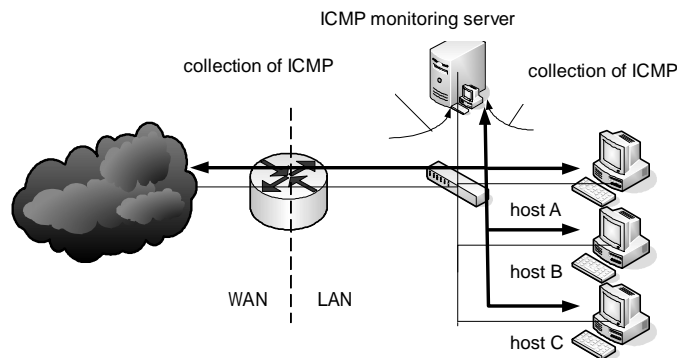


Fig. 1 Overview of implementation

We have implemented the proposed system into a LAN and evaluated the effectiveness of the system. Fig. 1 shows overview of the implementation. The LAN is a Class C network. We setup the ICMP monitoring server with the proposed mechanism at the location where the whole traffic exchange between inside and outside of the LAN can be observed and collected. Fedora Core 1 was installed in the ICMP monitoring server PC with 256MB memory and 733MHz clocked CPU. Observation was executed three times (from 1 to 7 October, November, and December 2005). And each observation has one week length. Within the ICMP monitoring server, Perl script automatically identified and collected data only necessary for worm detection, and calculated "ICMP success rate" by counting the numbers of ICMP echo request from LAN to WAN, ICMP echo reply, and ICMP Destination Unreachable. Here, the ICMP success rate is the percentage of number of successful echo reply packet to number of echo request packets sent from inside the LAN to WAN.

The calculated results are periodically updated so that the evaluated results have a real time

nature

5. Evaluation

Here, we compare our system with existing detection methods and evaluate it from the viewpoint of the requirements described in section 3.2.

5.1 Observed results

Table 2 shows the results for each observed period.

Table 2 Number of ICMP packets observed

Period (year 2005)	10/1-10/7	11/1-11/7	12/1-12/7
Number of active hosts *1	33	34	53
ICMP echo request	120960	54	13
ICMP echo reply	10	54	12
ICMP Destination unreachable	120950	0	1
ICMP success rate (%)	0.008	100	92.3

(*1 The number of active host is calculated by collecting and analyzing ARP in the LAN)

Table 2 shows that ICMP success rate is extremely low in the period of October than in other two periods. Investigation found that a specific host within the LAN was periodically sending ICMP echo requests. Detailed investigation proved the host was not infected by a worm but some special software was running in it. As a result, the action taken by the host did not come from worm injection but was undesirable. After removing this software from the host, ICMP success rate became about 100%. Any other ICMP echo requests was issued by user itself to check network connectivity and the number of echo response for them are very similar to those of echo requests independent of the number of hosts.

From this observation, our system can be said to be able to detect abnormal traffic independent of change of number of hosts.

Table 3 ICMP traffic volume

Observation period	2005/12/1-12/7
Total traffic	658MB
Total ICMP packets	13.02MB
ICMP packets to be collected	12.58KB

Table 3 shows total traffic, number of total ICMP packets and collected ICMP packets.

The number of packets to be handled in our system, i.e., ICMP echo request and reply, is extremely smaller than the total traffic volume and total ICMP packets, which means our system will give very little influence to processing power and memory.

5.2 Consideration on the requirements

Let us consider our system from the viewpoint of the requirements given to the worm detection system shown in 3.2.

(I) Low cost

As shown in Table 3, it is confirmed that memory size required for our system is extremely small because it only collects specific traffic. Since ICMP can be handled by almost all the network equipments, there is no need for hosts and network equipments except the monitoring server to prepare new functions to implement our method.

These prove that our system can be driven at low cost.

(II) Independent of pattern files

Our system uses ICMP to detect possible existence of worm without any pattern files. Hence, there is no need to prepare pattern definition files a priori and to update the pattern files to be up-to-date. Our system is effective to the unknown worms independent of the pattern files.

(III) Automatically detectable

In our system, as shown in Fig.2, ICMP monitoring server automatically collects specific ICMPs and calculates ICMP success rate. Hence, the network administrator does not need to manually make a primary judgment of possible infection.

(IV) Precisely detectable

The length of time frame and the threshold number of packets to judge whether traffic is abnormal has not yet been well investigated. This point needs further study.

(V) Detectable in real time manner

In our system, ICMP traffic is continuously monitored and ICMP success rate is calculated in real time manner so that real time detection of worm infection is possible.

5.3 Application of the proposed system

The proposed implementation tackles with avoidance of secondary infection caused by worm diffusion from inside the LAN to outside. Intrusion from outside the network can also be detected if our system is applied to reverse direction and observes ICMP echo request from outside to unassigned IP addresses in the network.

6. Summary

We have proposed the internet worm detection method using ICMP observation whose specific behavior may be caused by the worm infection. Through the implementation of proposal, we have shown the effectiveness of our proposal and its possible application. Our system has aimed to satisfy functional requirements shown in 3.2 and has fulfilled them except preciseness. Further study items left is satisfaction of preciseness, which is decision of appropriate observation time length as described in IV of section 5.2.

References

- [1] Information-Technology Promotion Agency, Japan, “Investigation on damage of computer virus in domestic and international area”, http://www.ipa.go.jp/security/fy16/reports/virus-survey/documents/2004_virus_domestic.pdf (in Japanese)
- [2] Ministry of Internal Affairs & Communications, “WHITE PAPER Information and Communications in Japan”, <http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2005/2005-index.html>
- [3] <http://itpro.nikkeibp.co.jp/security/index.html>
- [4] Trend Micro, “Virus Detection Technologies” <http://www.trendmicro.com/jp/security/general/tech/overview.htm/> (in Japanese)
- [5] K. Hato, “Proposal of Worm Sonar”, IEICE Technical Report, IN2004-31, pp.25-30, July, 2004 (in Japanese)
- [6] Internet System Consortium “Internet Domain Survey”, <http://www.isc.org/index.pl?/ops/ds/>
- [7] http://itpro.nikkeibp.co.jp/free/ITPro/NEWS/20030820/1/?ST=itpro_print/
- [8] S. Fujii, et. al., “Detection Method for Anomaly Traffic Based on Alternations of Destination Hosts”, Transaction of IEICE, Vol. J88-B, No.10, pp.1922-1933, Oct. 2005 (in Japanese)
- [9] RFC792 “Internet Control Message Protocol”