An Architecture Design of Distributed Internet Worm Detection System for Fast Response

Jung-Muk Lim*, Young-Ju Han*, and Tai-Myoung Chung*
*School of Information Communication Engineering
Sungkyunkwan University, {izeye, yjhan}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

Abstract - As the power of influence of the Internet grows steadily, attacks against the Internet can cause enormous monetary damages nowadays. A worm can not only replicate itself like a virus but also propagate itself across the Internet. So it infects vulnerable hosts in the Internet and then downgrades the overall performance of the Internet or makes the Internet not to work. To response this, worm detection and prevention technologies are developed. The worm detection technologies are classified into two categories, host based detection and network based detection. Host based detection methods are a method which checks the files that worms make, a method which checks the integrity of the file systems and so on. Network based detection methods are a misuse detection method which compares traffic payloads with worm signatures and anomaly detection methods which check inbound/outbound scan rates, ICMP host/port unreachable message rates, and TCP RST packet rates. However, single detection methods like the aforementioned can't response worms' attacks effectively because worms attack the Internet in the distributed fashion. In this paper, we propose a design of distributed worm detection system to overcome the inefficiency. Existing distributed network intrusion detection systems cooperate with each other only with their own information. Unlike this, in our proposed system, a worm detection system on a network in which worms select targets and a worm detection system on a network in which worms propagate themselves cooperate with each other with the direction-aware information in terms of worm's lifecycle. The direction-aware information includes the moving direction of worms and the service port attacked by worms. In this way, we can not only reduce false positive rate of the system but also prevent worms from propagating themselves across the Internet through dispersing the confirmed worm signature.

Keywords: Internet Worm, Intrusion Detection System (IDS), Network-based IDS (NIDS).

1 Introduction

As Internet becomes more popular, Internet becomes major infrastructure of houses and industries. Internet is also utilized for processing and publishing official documents in the government. Therefore, huge damage will occur in every area based on Internet if Internet can't provide services due to attacks.

Among these attacks, an attack by Internet worm can affect widely throughout Internet. Internet worm starts with Morris worm in 1988 and evolves with worms which damage Internet enormously like Code Red worm and Nimda worm recently. Furthermore, novel worms which make Internet destroyed in seconds are predicted in several papers [1], [2], [3]. Therefore, industries and universities study methods to detect Internet worm and to defend from Internet worm attack.

For detecting Internet worms, Host-based Intrusion Detection System (HIDS) and Network-based IDS (NIDS) are utilized. HIDS is monitoring worm's actions like specific file creation, modification, and deletion. NIDS is monitoring excessive scan activities and signatures of vulnerability exploit code.

However, it is hard to detect worms doing nothing in file-system for HIDS. And it is hard to detect worms using slow scan rates for anomaly-based NIDS. It is impossible to detect worms using new signatures due to absence of the signatures in its database for misuse-based NIDS. Furthermore, there is a major problem which previously proposed worm detection mechanisms can't distinguish Internet worm attack from general attacks.

Our proposed system is based on previously proposed mechanisms and additionally focuses on newly proposed mechanism which is based on worm's properties as a mobile agent. In other words, our system can distinguish Internet worm attack from general attacks because only Internet worm has the properties of a mobile agent. Finally, the convinced worm traffic information is propagated to all the distributed worm detection systems. So each distributed worm detection system can block the worm's traffic with firewall.

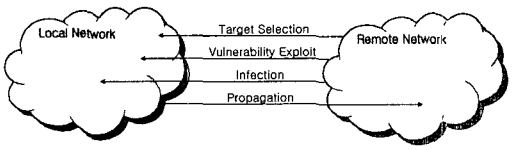
2 Related Works

2.1 Internet Worms

Internet worm is a program which propagates itself without a host file [4]. Internet worm is different from virus in terms of propagating without a host file and it is different from Trojan horse in terms of self-replication capability.

Internet worm resides in memory or file-system and it propagates from one host to another host in the form of packets. It consists of a set of execution code and the code can be divided as follows: target host scan code, vulnerability exploit code, worm body transmission code, and miscellaneous code [5], [6].

Internet worm has four stages as follows: target selection, vulnerability exploit, infection, and propagation [7]. The transitions between these stages are presented in [Figure 1].



[Figure 1] Internet Worm's 4 Stages

In the target selection stage, the infected host searches vulnerable hosts to be infected through scanning. In the vulnerability exploit stage, the infected host exploits the vulnerability of the target host and obtains the right of the host. In the infection stage, miscellaneous code like launching DDoS (Distributed Denial of Service) attack might be executed optionally. In the propagation stage, new infected host searches new vulnerable hosts to be infected through scanning.

In theoretical papers, ideal worms like perfect worm and flash worm can make Internet destroyed in seconds [8], [9]. Therefore, human response against these attacks might be too late. And worm executable platforms become more various from personal computers to mobile phones [10].

2.2 Internet Worm Detection Mechanisms

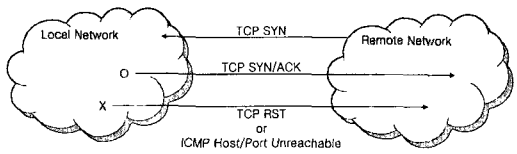
Internet worm detection mechanisms are divided into two categories: HIDS and NIDS.

HIDS detects worm attacks with existing IDS like monitoring buffer overflow, file-system integrity, and open port [11], [12].

NIDS is divided into two categories: anomaly detection and misuse detection.

The anomaly detection can be applied to detect worms in the target selection stage and the propagation stage. This mechanism is based on worm's scan activities. For example, it is monitoring TCP SYN, TCP RST, and ICMP Host/Port Unreachable messages in the case of TCP-based worms.

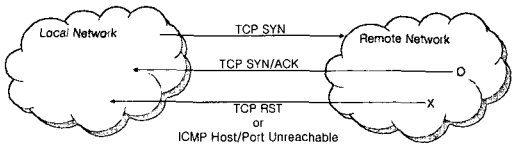
The traffic pattern in the target selection stage is presented in [Figure 2].



[Figure 2] Traffic Pattern in the Target Selection Stage

TCP SYN message is resulted directly by worm scan activities and TCP RST and ICMP Host/Port Unreachable messages are resulted indirectly by worm scan activities.

The traffic pattern in propagation is presented in [Figure 3].



[Figure 3] Traffic Pattern in the Propagation Stage

The detection in the propagation stage is much easier because worms scan in the local network [13].

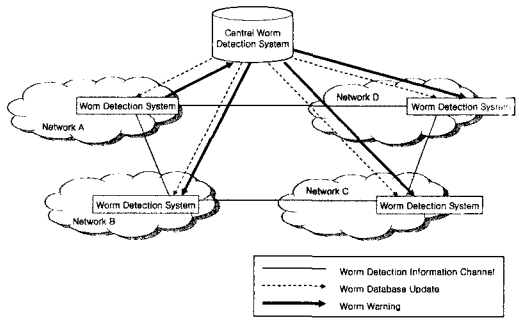
The misuse detection can be applied to detect worms in the vulnerability exploit stage. This mechanism depends on pre-made worm signature database. Therefore, the database must be made in advance. An automatic worm signature generator is proposed because human response is too late [14].

3 System Design

3.1 System Overview

Our system consists of single central worm detection system and multiple distributed worm detection systems. We assume that each network in Internet has its own distributed worm detection system. For detecting worms, each distributed worm detection systems cooperate with each other in terms of worm propagation direction.

The procedure overview of our worm detection system is presented in [Figure 4].



[Figure 4] Procedure Overview of Worm Detection System

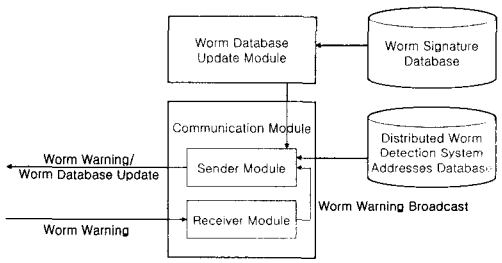
The central worm detection system maintains the central worm database including worm signatures and updates the worm database in each distributed worm detection system periodically for its freshness.

Distributed worm detection systems share the worm detection information with other distributed worm detection systems related to worm propagation direction. The convinced worm detection result can be propagated into all the distributed worm detection systems because our detection system can distinguish Internet worm attack from general attacks.

The convinced worm detection result make worm warning message and the message will be sent to the central worm detection system. And then the central worm detection system will broadcast it to all the distributed worm detection systems. It makes each distributed worm detection system block the worm traffic with its firewall.

3.2 System Specification

The central worm detection system consists of a worm database update module and a communication module. The modules in the central worm detection system are presented in [Figure 5].

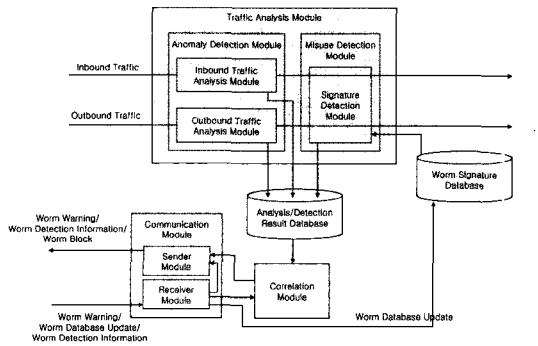


[Figure 5] Modules in the Central Worm Detection System

The worm database update module makes a worm database update message and sends it to all the distributed worm detection systems in the distributed worm detection system addresses database through the sender module when the worm signature database is updated.

The communication module consists of a sender module and a receiver module. The sender module sends a worm warning message to all the distributed worm detection systems when the receiver module receives a worm warning message.

The distributed worm detection system consists of a traffic analysis module, a communication module, and a correlation module. The modules in distributed worm detection systems are presented in [Figure 6].



[Figure 6] Modules in the Distributed Worm Detection Systems

The traffic analysis module consists of an anomaly detection module and a misuse detection module. The anomaly detection module consists of an inbound traffic analysis module and an outbound traffic analysis module. The misuse detection module consists of a signature detection module.

The inbound traffic and the outbound traffic are analyzed in the inbound traffic analysis module and the outbound traffic analysis module respectively and the results will be written in the analysis/detection result database. And then they are analyzed in the signature detection module based on the worm signature database and the results will be written in the analysis/detection result database.

The communication module consists of a sender module and a receiver module. When the receiver module receives a worm warning message, it sends a worm block message through the sender module. When the receiver module receives a worm database update message, it updates its own worm signature database. When the receiver module receives a worm detection information message, it forwards the message to the correlation module. When the sender module receives a worm

detection information message from the correlation module, it sends the message to the corresponding system. When the sender module receives a worm warning message from the correlation module, it sends the message to the central system.

The correlation module, which is based on the analysis/detection result database and worm detection information messages received from the receiver module, forwards a worm warning message or a worm detection information message to the sender module.

4 Conclusions

To solve the problem which all the previous proposed worm detection mechanisms can't distinguish Internet worm attack from general attacks, we propose and design the worm detection system utilizing worm's properties as a mobile agent.

To solve the problem which worms using slow scan rates can avoid detection systems based on scan rates, our system analyzes worm scan activities in terms of both short period and long period.

In this paper, some undetermined thresholds have to be studied in detail. For this study, we need to utilize a large-scale simulator like SSFNet (Scalable Simulation Framework Network model) and GTNet (Georgia Tech Network simulator).

Acknowledgement

This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment)

References

[1] Darrell M. Kienzle, Matthew C. Elder, "Recent Worms: A Survey and Trends", WORM'03, October 27, 2003.

[2] Stuart Staniford, Vern Paxson, Nicholas Weaver, "How to Own the Internet in Your Spare Time", Proceedings of the 11th USENIX Security Symposium, August 2002.

[3] Stuart E. Schechter, Michael D. Smith, "Access For Sale - A New Class of Worm", WORM'03, October 27.

[4] Symantec, "What is the difference between viruses, worms, and Trojans?", http://service1.symantec.com/SUPPORT/nav.nsf/pfdocs/1999041209131106, March 30, 2005.

[5] Donn Seeley, "A Tour of the Worm", Proceedings of 1989 Winter USENIX Conference, Usenix Association, San Diego, CA, February 1989.

[6] Nicholas Weaver, Vern Paxson, Stuart Staniford, Robert Cunningham, "A Taxonomy of Computer Worms", WORM'03, October 27, 2003.

[7] The CERIAS Intrusion Detection Research Group, "Digging For Worms, Fishing For Answers", Proceedings of the Annual Computer Security Application Conference (ACSAC'02), Las Vegas, USA, December 9 - 13, 2002.

[8] Cliff C. Zou, Don Towsley, Weibo Gong, "On the Performance of Internet Worm Scanning Strategies", Technical Report TR-03-CSE-07, Department of Computer Science Univ. Massachusetts, Amherst, November 2003.

[9] C.C. Zou, D. Towsley, W. Gong, and S. Cai, "Routing Worm: a Fast, Selective Attack Worm based on IP Address Information", Univ. Massachusetts Technical Report TRCSE-03-06, November, 2003.

[10] F-SECURE, "F-Secure Virus Descriptions: Cabir", http://www.f-secure.com/v-descs/cabir.shtml.

[11] Michael Zhivich, Tim Leek, Richard Lippmann, "Dynamic Buffer Overflow Detection", 2005 Workshop on the Evaluation of Software Defect Detection Tools, Chicago, IL, June 12, 2005.

[12] Gene H. Kim, Eugene H. Spafford, "The Design and Implementation of Tripwire: A File System Checker", In ACM Conference on Computer and Communications Security, pages 18-29, 1994.

[13] Shigang Chen, Sanjay Ranka, "An Internet-Worm Early Warning System", Proceedings of the IEEE Globecom 2004 - Security and Network Management, volume 4, pages 2261-2265, November 2004.

[14] Kim, H.-A. and Karp, B., Autograph: Toward Automated, Distributed Worm Signature Detection, Proceedings of the 13th Usenix Security Symposium (Security 2004), San Diego, CA, August, 2004.