Design of Network-based Real-time Connection Traceback System with Connection Redirection Technology

Yang-Sec Choi*, Hwan-Guk Kim*, Dong-il Seo* and Sang-ho Lee**

* ETRI, Daejeon, Korea
(Tel : +82-42-860-3982; E-mail: {yschoi92, rinyfeel, bluesea}@hankook.ac.kr)
**Department of Computer Science, Chung-Buk University, Cheong-Ju, Korea
(Tel : +82-43-261-2253; E-mail: shlee@cbucc.chungbuk.ac.kr)

Abstract: Recently the number of Internet users has very sharply increased, and the number of intrusions has also increased very much. Consequently, security products are being developed and adapted to prevent systems and networks from being hacked and intruded. Even if security products are adapted, however, hackers can still attack a system and get a special authorization because the security products cannot prevent a system and network from every instance of hacking and intrusion. Therefore, the researchers have focused on an active hacking prevention method, and they have tried to develop a traceback system that can find the real location of an attacker. At present, however, because of the characteristics of Internet - diversity, anonymity - the real-time traceback is very difficult. To over-come this problem the Network-based Real-Time Connection Traceback System (NRCTS) was proposed. But there is a security problem that the victim system can be hacked during the traceback. So, in this paper, we propose modified NRCTS with connection redirection technique. We call this traceback system as Connection Redirected Network-based Real-Time Connection Traceback System (CR-NRCTS).

Keywords: Traceback, Hacking, Security, NRCTS

1. INTRODUCTION

The Internet is already a part of life. It is very convenient and people can do almost everything with the Internet that should be done in real life. As can be seen in Fig. 1, along with the increase of the number of Internet user, various attacks through the Internet have been increased as well.

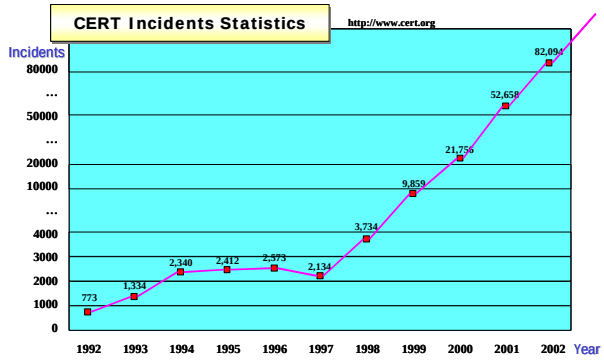

Fig. 1 The number of intrusions [1].

The security companies have developed numerous security reinforcement systems to protect systems and networks from various intrusions. However, there are some problems with the reinforcement systems. Security reinforcement systems that have been developed up to now cannot limit the hacking attempts themselves. They just make the hacking more difficult to do. That is, they cannot cope with a hacker's spontaneous hacking attempts because security products only can defend passively. Furthermore, since the security reinforcement systems that are adapted to the Internet are very varied, mutual cooperation regarding a hacker's hacking is almost impossible. Because of such problems, hacking attempts are increasing, and cannot be protected effectively.

To solve these problems, there has been considerable effort in developing an active hacking prevention system that can limit a hacker's hacking attempts. With that the traceback systems have been proposed. However, because of the variety and anonymity of the Internet, real-time traceback is very difficult in the current Internet environment. But there was a possible solution to traceback a hacker in real-time that called Network-based Real-time Connection Traceback System (NRCTS) that uses packet marking techniques [2]. But it has an critical problem that the target(victim) system could be hacked during traceback. So, in this paper, we propose modified NRCTS that uses Connection Redirection Technique. We call the traceback system as Connection Redirected NRCTS (CR-NRCTS).

This paper is consisted of 4 chapters. In chapter 2, we will see about the related works. It contains the actually related works and the definition of traceback system. In chapter 3, we will propose a new connection traceback system CR-NRCTS. In chapter 4, we will end this paper with conclusion.

2. RELATED WORKS

2.1 The Traceback System

The traceback system is defined as follows;

Definition 1. Traceback System
A system that searches an attacker's actual position using real-time automated techniques.

And, there are 2 kinds of traceback systems. The first is a connection traceback system and the second is the packet traceback system. Since the IP packet traceback system [3] is not the focus of this study, it will not be mentioned again.

The connection traceback system is a traceback system that chases a hacker's actual position in real time, for cases in which the hacker has attempted to attack in a roundabout way, that is, when the attack is tried via several middle systems. Actually, the connection traceback system tries to find the hosts or connections that are included in a connection chain [4]. The connection traceback system is also can be classified by host-based or network-based. The details are shown in the Table 1.

Table 1 Classification of Connection Traceback System

Classification	Proposed Systems
Host-based	AIAA[5], CIS[6], DIDS[7]

Network-based	Passive	Thumbprint [8], Timing-based [9], SQN Deviation-based [10]?
	Active	IDIP [11], SWT [12], NRCTS [4], CR-NRCTS

The host-based connection traceback system is a traceback system that uses various host-based log records. To accomplish a perfect traceback with the host-based connection traceback system, a traceback module should be installed in every host on the Internet. The fundamental problem with the host-based tracing approach is its trust model. Host-based tracing places its trust upon the monitored hosts themselves. Specifically, it depends on the correlation of connections at every host in the connection chain. If one host is compromised, and is providing misleading co-relational information, the whole tracing system is fooled as well.

The network-based connection traceback system extracts information for traceback from packets that are transmitted on the network. To do this, traceback modules should be installed on network nodes that can identify the network packets.

2.2 Proposed Network-based Traceback Techniques

As we can see in the Table 1, several network-based connection traceback systems are proposed.

2.2.1 Thumbprint Approach

The first is thumbprint method [8]. The thumbprint is a pioneering correlation technique that utilizes a small quantity of information to summarize connections. Ideally, it can uniquely distinguish a connection from unrelated connections, and correlate those related connections in the same connection chain. While thumbprinting can be useful even when only part of the Internet implements it, it depends on clock synchronization to match the thumbprints of corresponding intervals of connections. It is also vulnerable to retransmission variation, which severely limits its usefulness in real-time tracing.

2.2.2 Timing-based Approach

The second is the timing-based scheme [9]. This mechanism is a novel network-based correlation scheme for detecting stepping stones across the connection chain. The correlation is based on the distinctive timing characteristics of interactive traffic, rather than connection contents. It has pioneered new ways of correlating encrypted connections; it requires no clock synchronization; and it is robust against retransmission variation. However, because its timing characteristics are defined over the entire duration of each connection to be correlated, it is difficult to use in real-time correlation.

2.2.3 SQN Deviation-based Approach

The third is the deviation-based approach [10]. It defines the minimum average delay gap between the packet streams of two TCP connections as a deviation. The deviation considers both timing characteristics and the TCP sequence number, and it does not depend on the TCP payload. The deviation-based approach does not require clock synchronization and is robust against retransmission variations. However, it is difficult to use in real-time correlation as the deviation is defined over all the packets of a connection.

2.2.4 Sleepy Watermark Traceback System

The fourth is the Sleepy Watermark Traceback (SWT) system [11]. It uses a watermarked packet to trace the hacker's real location. An actual watermark would be inserted into reply packets created to respond to an attack by tracing the packets. The SWT system, however, should be coordinated with watermark-enabled applications. Watermark-enabled applications are those network service applications that have been modified to inject arbitrary watermarks upon request. Therefore, to use SWT, those applications need to be supplied.

2.2.5 IDIP

The fifth is the Intrusion Identification and Isolation Protocol (IDIP) [12]. In the proposal, boundary controllers collaboratively locate and block the intruder by exchanging intrusion detection information: namely, attack descriptions. While it does not require any boundary controller to record any connections for correlation, its intrusion tracing is closely coupled with intrusion detection. The effectiveness of the IDIP depends on the effectiveness of intrusion identification through the attack description at each boundary controller. Therefore, the IDIP requires each boundary controller to have the same intrusion detection capability as the intrusion detection system (IDS) at the intrusion target host. It is questionable whether the intermediate boundary controller is able to identify an intrusion based on a hard-coded attack description.

2.2.6 NRCTS

The last one is NRCTS [2]. NRCTS is a network based connection traceback system that uses packet marking technique. It is very similar to SWT. But is does not need the watermark-enabled applications. It detects attack with IDS and marks the reply packets from victim that created due to the attack packets and sends the packets to attacker. Then other NRCTSs detect the marked packets and send the marking and connection information to original NRCTS that activates the traceback. With the information the original NRCTS constructs traceback path to attacker. But as we mentioned before, it uses the real connection between attacker and victim system. Therefore, there is a critical vulnerability that the victim could be hacked during the traceback.

3. CONNECTION REDIRECTED NRCTS

In this paper, we propose the design of a modified NRCTS with connection redirection technique that called Connection Redirected NRCTS (CR-NRCTS). The basic concept of CR-NRCTS is same to NRCTS that uses the packet marking technique as the SWT system does. However this approach can remove the vulnerability that we mentioned in the section 2.2.6. The CR-NRCTS has same characteristics as NRCTS. So, it has next potential advantages:

- ? Separates intrusion tracing from intrusion detection
- ? Does not need to record all the concurrent connections
- ? Requires no clock synchronization
- ? Traces only when needed
- ? Accurate and efficient
- ? Can be implemented efficiently

Furthermore, The CR-NRCTS takes away the vulnerability.

There are two assumptions that motivate and constrain the CR-NRCTS design. First, intrusions are interactive and bi-directional; second, there is no encrypted connection. The first assumption represents the assessment made in this study of the nature of the intrusions, where intrusions are those attacks that aim to gain unauthorized access rather than those that deny service attacks. The second assumption represents

the inherent limitation of any tracing based on network contents. Encrypted connections are not considered here.

3.1 Construction

The CR-NRCTS consists of four subsystems: IDS, Connection Redirection System, Path Traceback System and Marked Packet Detection System.

The CR-NRCTS can be installed as can be seen in Fig. 2.

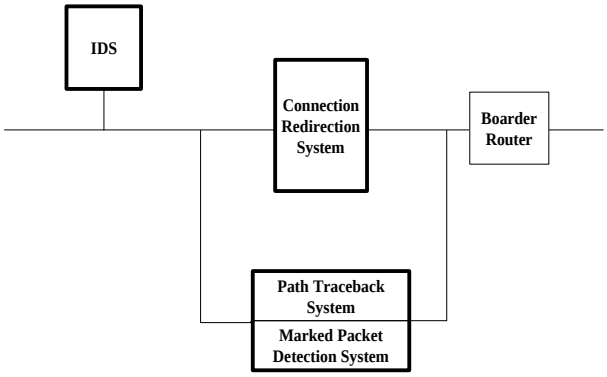

Fig. 2 Construction of the CR-NRCTS

3.1.1 Intrusion Detection System

The purpose of using the IDS is only to check whether hacking has been attempted or not.

3.1.2 Connection Redirection System

The Connection Redirection System redirects the connection between attacker's system and victim system. It redirects the connection to Path Traceback System. And it sends RST signal to victim. With this connection redirection, the victim side connection is closed, however the connection is still maintained with Path Traceback System and the attacker. With this connection the CR-NRCTS traces the attacker.

Connection Redirection System also drops the reply packets from an attacked system. The drop policies are decided by based on the source IP address, destination IP address and port numbers. In a normal situation it does not do anything. This function is activated only when an attack has happened.

3.1.3 Path Traceback System

The Path Traceback System is activated by an intrusion alert from IDS. When this system is activated it waits the redirected connection from Connection Redirection System. When the redirected connection is established then, it waits the attack packets. If the attack packets are received then it creates faked reply packets and marks them. And it sends them to attacker. The marked packet contains some information and back-space characters. Cause of these back-space characters, the attacker can't identify the marks.

The Path Traceback System also constructs a path from the attacked system to the real hacker's system. It uses information received from other CR-NRCTSs to construct the whole path.

3.1.4 Marked Packet Detection System

The Marked Packet Detection System is a monitoring system that monitors all the packets transmitted through a network, and it identifies whether a packet is marked or not. If a packet is marked, it gets the information from marked packet and sends the detection information to the original place where the traceback was initiated. The information consists of an IP address and an attack signature. The IP address is owned by the CR-NRCTS that marks the packet. This system, which can be installed individually in the same position as an ISP's backbone router, can detect the marked packets. This mechanism enables the marked packets are detected more efficiently.

3.2 Connection Redirection Technique

The connections can be redirected by connection hijacking technique. Actually it was developed to hack other system. If someone can monitor any connection, it means that he can monitor the sequence number, ACK number and other special bits. With the information, anyone can hijack any connection with ARP spoofing. The HUNT is most famous connection hijacking tool. The CR-NRCTS uses that kind of connection hijacking technique. The Fig. 3 shows the HUNT sniffing and connection hijacking program.

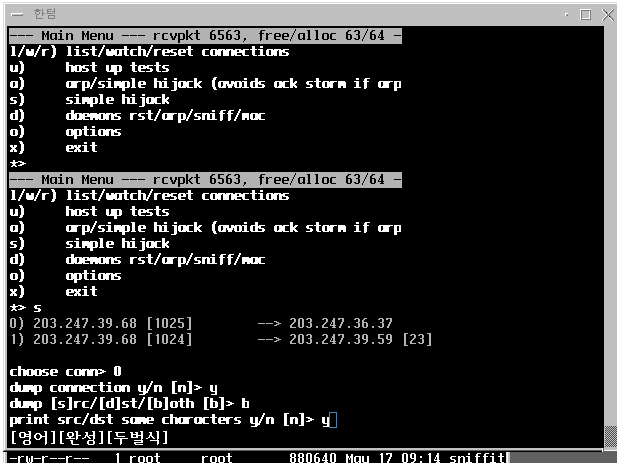

Fig. 3 The HUNT connection hijacking program

This kind of connection redirection technique is also used in the active honeypot system [13].

3.3 Scenarios

First, when the CR-NRCTS is activated, the IDS and the Marked Packet Detection System monitor the network packets.

The next scenarios at the internal network are explained in Fig. 4 as follows:

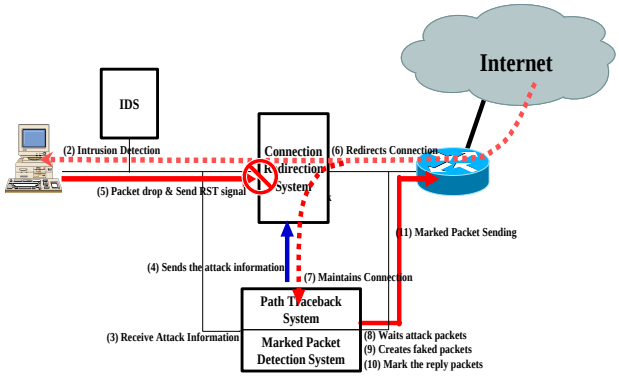

Fig. 4 The CR-NRCTS scenarios for internal network

(1) Intrusion Occurs: An attack is attempted
(2) Intrusion Detection: The attack is detected by IDS
(3) Intrusion Alert Received: The Path Traceback System receives intrusion detection information from IDS and starts the traceback
(4) The Path Traceback System sends the attack information to Connection Redirection system
(5) Connection Redirection System drops the reply packets from victim and sends the RST signal to victim
(6) Redirect the connection to Path Traceback System
(7) Path Traceback System maintains the connection with attacker
(8) Path Traceback System waits until the attack packets are received
(9) When the attack packets are received then the Path Traceback System creates the faked reply packets
(10) Marks the created reply packets
(11) Path Traceback System Sends them to attacker and waits the connection information from other CR-NRCTS's Marked Packet Detection System

Fig. 5 shows how the traceback progresses when the marked packet is sent. Once the marked packet is sent to an external network, the CR-NRCTS that activates the traceback waits for responses from other CR-NRCTSs. With these responses the Path Traceback System constructs the path to the real hacker. All the CR-NRCTSs should respond if they find the marked packet.

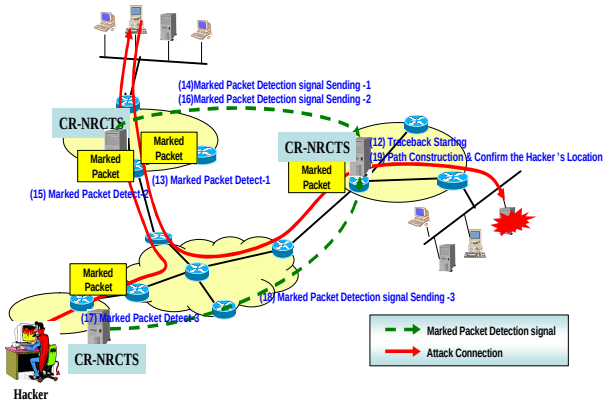

Fig. 5 Traceback scenarios in the external networks

The next scenarios are as follows:
(12) Traceback Starting
(13) Marked Packet Detect – 1
(14) Marked Packet Detection Signal Sending – 1
(15) Marked Packet Detect – 2
(16) Marked Packet Detection Signal Sending – 2
(17) Marked Packet Detect – 3
(18) Marked Packet Detection Signal Sending – 3
(19) Path Construction and Traceback Complete

As can be seen in Fig. 5, the marked packet follows the attack connection in a reverse direction, and because the mark is inserted into the data field, it must go to the hacker's system. The marked packet would be detected twice in each network that includes middle systems and once in a network in which the hacker is included. This can be used to construct the tracing path.

3.3 Characteristics of the CR-NRCTS

Minimize the damage of victim system

The normal NRCTS uses the real connection between victim and attacker to traceback the attacker. So, NRCTS has the critical vulnerability that the victim can be hacked during the traceback. But, the proposed CR-NRCTS has removed the vulnerability with connection redirection technique. With this technique the attack packets do not arrive to victim so the victim is safe. So, the proposed system minimizes the damage of victim system.

Low System Overhead than Others

The NRCTS is not activated until an intrusion has occurred. It just monitors packets to determine whether they are marked or not. Consequently, until the real traceback has started it uses a very small amount of system resources. Actually other proposed traceback systems treat every connection and record all the information about every connection. So, the NRCTS is more efficient than others.

High possibility of traceback success

As mentioned before, the CR-NRCTS has the same characteristic as NRCTS. So, it can trace back even if some middle systems are compromised. Even though there are no CR-NRCTSs in some networks, the traceback can be successful if there is an CR-NRCTS included on the hacker's system. Consequently, the possibility of a successful traceback is higher than in other traceback techniques, though it is impossible to construct the whole path and to find all the middle systems if there are no CR-NRCTSs in some networks.

Have possibility to traceback the encrypted connection

If every connection is encrypted, the traceback is impossible. However, if the last connection that connected between the hacker's system and the next host is not encrypted, and there is a CR-NRCTS, then the hacker's real position can be found. Basically, this is the same property that was mentioned in the previous paragraph.

Should be installed in many networks

CR-NRCTS could not be used alone. It needs other CR-NRCTS systems to success the traceback.

Should monitors the network constantly

To detects an attack and marked packets, the CR-NRCTS should monitors network constantly. But it is same weakness as other traceback systems.

4. CONCLUSION

Because the general security products cannot limit or prevent the hacking, active hacking protection techniques are urgently required. To develop active hacking protection techniques, researchers have explored active security products. They have found that the traceback system is the most required system. Consequently, their research has been focused on the traceback system. Until now, however, the proposed traceback systems cannot be adapted to the current Internet environment because of the diversity and anonymity of the Internet. Only the NRCTS had some possibility about adaptation. But, the NRCTS has a critical vulnerability that cause the victim could be hacked and the attacker can have the information what he wants. So, we have proposed a modified Network-based Real-time Connection Traceback System that called Connection Redirected NRCTS (CR-NRCTS).

The proposed traceback system that called as a CR-NRCTS detects an attack and drops the reply packets from victim. And it uses the connection redirection technique that was used in the active honeypot system [13]. With this technique, the attack connection is maintained even though the victim side connection is closed. With this connection, CR-NRCTS creates faked reply packets and marks it. And, it sends the faked packets to attacker. The marked packets are detected by other CR-NRCTSs. And the connection information that collected by other CR-NRCTS is sent to original CR-NRCTS. Then the original NRCTS constructs the traceback path from victim to attacker.

This mechanism is easy and clear, and it does not have to do anything before the traceback activated except monitoring. It is very efficient than other traceback mechanism. And it removes the critical vulnerability of NRCTS that could be hacked during traceback.

There are several advantages. They are same as NRCTS. First, the CR-NRCTS have more possibility to be adapted to the current Internet environment; second, the CR-NRCTS can find the real hacker's location even if some middle systems are compromised, because it does not use the system log files to trace back; and third, if the last connection between the hacker's system and the next system is not encrypted, there is a possibility that the traceback will succeed. We hope this CR-NRCTS can be helpful to the computer security fields.

REFERENCES

[1] CERT, http://www.cert.org

[2] Y.-S. Choi, D.-i. Seo, S.-W. Sohn, S.-H Lee, "Network-Based Real-Time Traceback System (NRCTS) with Packet Marking Technology", Computational Science and Its Applications - ICCSA 2003, Montreal, Canada, 2003. 5.

[3] Dawn X. Song and Adrian Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback", Proceedings of InfoCom 2001

[4] Buchholz, Thomas E. Daniels, Benjamin Kuperman, Clay Shields, "Packet Tracker Final Report", CERIAS Technical Report 2000-23, Purdue University, 2000

[5] Chaeho Lim, "Semi-Auto Intruder Retracing Using Autonomous Intrusion Analysis Agent", FIRST Conference on Computer Security Incident Handling & Response 1999, 1999

[6] H. T. Jung et al. "Caller Identification System in the Internet Environment.", In Proceedings of the 4th Usenix Security Symposium, 1993.

[7] S. Snapp et al. "DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and An Early Prototype." In Proceedings of the 14th National Computer Security Conference, 1991.

[8] S. Staniford-Chen and L. T. Heberlein. "Holding Intruders Accountable on the Internet." In Proceedings of the 1995 IEEE Symposium on Security and Privacy, 1995.

[9] Y. Zhang and V. Paxson, "Detecting Stepping Stones", Proceedings of 9th USENIX Security Symposium, August 2000.

[10] K. Yoda and H. Etoh, "Finding a Connection Chain for Tracing Intruders", In F. Guppens, Y. Deswarte, D. Gollamann, and M. Waidner, editors, 6th European Symposium on Research in Computer Security - ESORICS 2000 LNCS -1985, Toulouse, France, Oct 2000.

[11] D. Schnackenberg, K., Djahandari, and D. Sterne, "Infrastructure for Intrusion Detection and Response," Proc. DARPA Information Survivability Conference and Exposition,

[12] X. Wang, D. Reeves, S. F. Wu, and J. Yuill, "Sleepy Watermark Tracing: An active Network-Based Intrusion Response Framework", Proceedings of IFIP Conference on Security, Mar. 2001

[13] M.Kim, M.Kim, H.K. Lee, Y. Mun, "Design of Active Honeypot System", ICCSA 2003, Montreal, Canada, May. 2003.

[14] Heejin Jang and Sangwook Kim, "A Self Extension Monitoring for Security Management", 16th Annual Computer Security Applications Conference Dec. 2000.