A Study of Connection Maintenance Techniques using TCP Hijacking★

김점구*

요 약

인터넷 사용자의 급증에 따라, 인터넷을 통한 각종 침해사고 역시 크게 증가되고 있다. 이러한 각종 침해사고로부터의 대응 방법으로 해킹을 시도하는 해커의 실제 위치를 실시간으로 추적하는 침입자 역추적 기술에 대한 연구가 활발히 이루어지고 있다. 본 논문에서는 TCP Connection trace-back 시스템에서 사용되는 기법 중에 하나인 패킷 워터마킹 역추적 기법에서 TCP Hijacking 기법을 이용하여 Reply 패킷의 Connection 유지의 어려움을 해결하는 방법을 제시한다.

A Study of Connection Maintenance Techniques using TCP Hijacking

JeomGoo Kim*

ABSTRACT

Internet users drastically increases, also through the Internet to buy various intrusion significantly increased. These various methods of intrusion defense thinking hacker attempting to hack the actual position of the real-time tracking of the intruder backtracking technique for research have been actively carried out. In this paper, a technique used in TCP Connection trace-back System in one packet trace-back technique watermarking technique using TCP Hijacking Connection Reply packets how to solve the difficulties of maintaining presented.

Key words : TCP Hijacking, trace-back, DDoS

접수일(2014년 2월 28일), 수정일(1차: 2014년 3월 17일, 2차: 2014년 3월 18일), 게재확정일(2014년 3월 24일)

★ 본 논문은 남서울대학교 2013년도 교내학술연구조성비 지원에 의하여 연구되었음.

* 남서울대학교 컴퓨터학과

1. Introduction

The Internet has already perched on deeply in everyday life. Use these Internet who must perform in the real world a lot of things can be done through the Internet and the Internet because of the convenience of Internet users also increased substantially. This increase in Internet users through the Internet with various intrusion accidents also increased substantially.

Accordingly, various security vendors to protect systems and networks from intrusion security system was developed for a variety of each system and network administrators are applied to the system. However, currently most developed and used to enhance the security of its own systems to prevent hackers not try to hack, hackers attempt to hack, the more difficult it was only to a level.

In other words, the same way a hacker does not actively cope with hacking attempts, the level of defense will passively. The current security environment, these systems are increasing day by day because of a hacking attempt, and the reality is that it does not effectively defend [1].

In order to solve such problems for preventing hacking actively trace-back increasingly growing interest in the technology and, although still rudimentary and a backtracking technique began to study progresses.

Intruders the latest technology, distributed denial of service attack trace-back (DDoS) type of spoofed IP technology for tracking IP trace-back and form of stepping stone attack via multiple types of systems for tracking the actual TCP Connection TCP Connection trace-back classification technology [2].

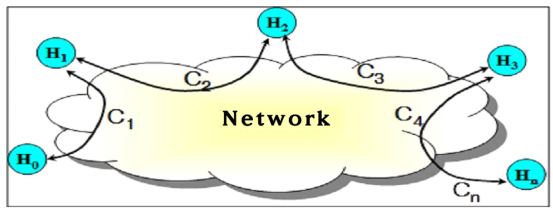
In this paper, to keep the TCP Connection Stepping Stone forms of attack packets used for trace-back watermark detection scheme when the packet is inserted characteristics of the TCP three-way handshaking is encountered which is hard to maintain TCP Connection to compensate TCP Hijacking of a plan to hack how to use trace-back techniques proposed.

2. Trace-back Techniques

2.1 TCP connection Trace-back

trace-back TCP connection technique is based on the TCP connection attempt to circumvent the hacker attacks the physical position of a real-time tracking techniques. In addition, the common connection chain also called backtracking technique.

Here, the connection of the chain is shown in (Figure 1) H0 one computer to another system over the network, the user logged in, the H1, H0 and H1 between the two systems, the TCP connection (Connection) C1 is generated. At this time, the same user, the system H1 to H2, or H3, ..., Hn to the log, each of those systems, the TCP connection between the C2, C3, ..., Cn in the same way generated. At this time, the set of the set of connection C = (C1, C2, ..., Cn) is referred to as a connection chain. In other words, hackers are actually multiple systems from systems located via the physical connection to the system being attacked (connection) to say the set [3].



(Figure 1) Connected chain

TCP connection backtracking technique again, can be classified into 2. It is connected to a host-based trace-back (Host-based connection

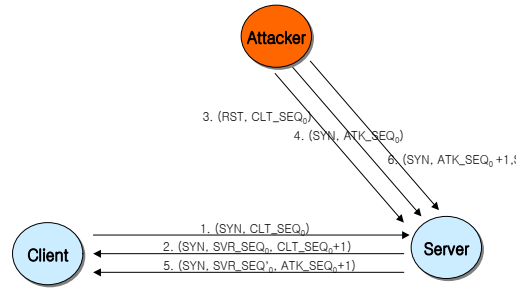
trace-back) trace-back technology and network -based connection is classified as a technology [1].

2.2 IP packet trace-back

IP Packet trace-back technique is the actual IP address is changed, a packet transmission side refers to a technique for tracking. Generally, the IP address is changed, the packet is maliciously used in most cases. In particular, DoS or DDoS attack is mainly used. If the IP address is changed, the TCP connection can not be maintained, the transmission of one-way packet DoS or DDoS attack can be mainly used. Of course, in the past known hacking technique called IP Spoofing is used, IP address is changed, the attack packets, intended to install a backdoor on the target system is a technique often used, but it is necessary in order for TCP Sequence Number Guessing because of recent There are rarely used. In addition to this IP Packet trace-back is the IP address is changed by a particular system to transmit a packet as a technique to find a system, by tracking the number of intermediate destinations hackers to locate the actual TCP connection backtracking techniques and solve the problem that is the subject of some the difference in [1].

3. TCP Session Hijacking

TCP Session Hijacking between the server and the client SEQ, ACK number of Asynchronous techniques to intercept the session on his machine to go through TCP Stream Redirection can active attack using the vulnerability of the TCP protocol. Redirection could allow an attacker, such as a one-time password or SKEY ticket-based authentication such as Kerberos protection mechanisms provided by the system can be bypassed. Someone connected to a TCP connection on a TCP packet sniffer or packet generator if you have very weak. Creating Asynchronous TCP Session Hijacking is shown in (Figure 2).



(Figure 2) Asynchronous TCP hijacking techniques

A. The server and the client to generate the connection and transmits the SYN packet.
B. The attacker goes from the server to the client SYN / ACK packet to Listen to.
C. When it detects packets rst attacker can send packets to the client and the server, the connection is terminated.
D. Attacker packets sent by the client to the same parameters but with a different sequence number and sends the SYN packet to the server. Server has its own different port, such as serial number, have a new connection is opened.
E. Server SYN / ACK packet to the client ship.
F. This packet is detected by the attacker to send out an ACK packet to the server. The server switches to the ESTABLISHED state. The first client from the server, a SYN / ACK packet is received ESTABLISHED state have already been tranced.

Now, through the above process ends in an asynchronous TCP Session hijacking Established state been accomplished [4].

4. TCP Hijacking trace-back scheme using packet marking

4.1 Packet Water-Marking Trace-back

Packet trace-back techniques Stepping stone watermark form multiple systems via the attacker's own IP systems do not want to disclose the purpose of the attack was traced back to elements used in TCP Connection technology.

Conceptually, the packet is a watermark that uniquely identifies the connection that can be used for small information. The watermark is a network packet to the attacker concealed the application should be easy insertion and extraction [5].

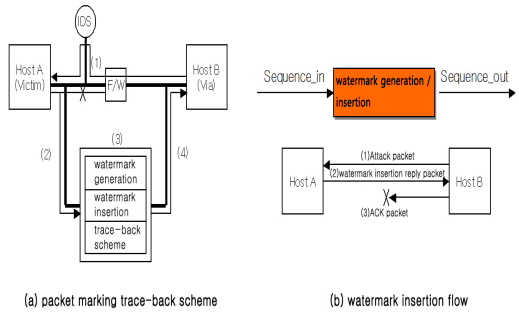
Packet marking technologies to perform a trace back over the following two characteristics are to be considered [6].

First, the watermark is invisible to the attacker Packet Data Hiding techniques used. The problem of generating a watermark invisible to the attacker by making the response packet (reply packet) to the attacker's system, a kind of invisible control characters in the data field of the packet and null string is used to maintain the stepping stone type of connection the attack on the station track is used for.

Second, look at the host to middle, middle destinations to middle destinations Intermediate between the host destinations to the attacker TCP Session connection response packet is retained in the well is to be delivered. Correlation of backtracking for Multiple Connection is via the watermark should be kept unchanged.

4.2 TCP Hijacking trace-back scheme using packet marking

In this paper, we propose a system architecture for user authentication is shown in (Figure 2).



(Figure 3) Flowchart packet marking trace-back

Packet marking trace-back techniques to perform the following assumptions. (1) existing intrusion detection systems, intrusion detection is used. (2) Detection Reply packets for packets so as to cut off the existing firewall system used.

(Figure 3) is a packet flow diagram of a marking station with tracking system configuration [7].

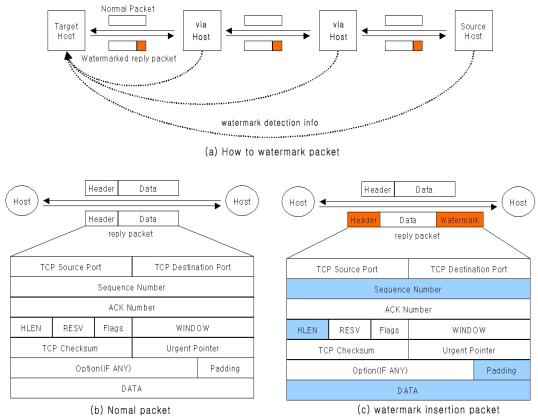
In addition, according to the flowchart trace-back invasion after detecting an attack on the watermark is embedded in the reply packet before and after the Sequence Number is shown in (Figure 4) (b), (c), as due to the size of the inserted watermark changes.

Insert before: Sequence (Host A) = Sequence (Host A) + Data_Len

After insertion: Sequence (Watermark) = Sequence (Host A) + Data_Len + WM_Len

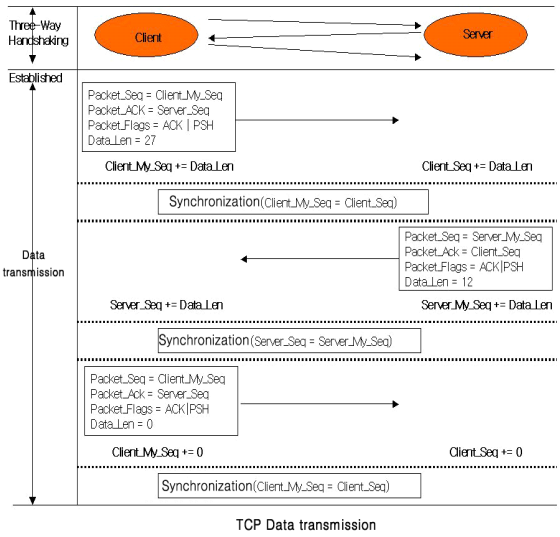
Therefore, you need to keep the attacker Host A will change the Sequence Number of the asynchronous upset occurs.

Asynchronous: Sequence (Host A) ◷ Sequence (Host B)



(Figure 4) Watermarked packet vs normal packet

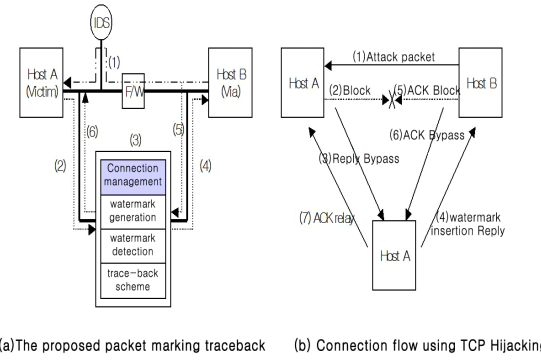
In order to establish a new TCP connection to a server by a client connected to the data exchange, if you try to initialize the normal packet exchange is done, as shown in (Figure 5).



(Figure 5) TCP data transfer

Sent from the client to the server an acknowledgment packet after the connection is established on both sides of both ends in the Established state synchronization is Won'T data exchange shall be made. However, watermarking of the Reply Packet Sequence Number, and at both ends to keep the change in the asynchronous state and the Sequence Number Connection maintenance becomes difficult. Accordingly, both ends of the methods for maintaining the Connection state, the asynchronous packet to intercept TCP Hijacking techniques can be used to address this problem.

(Figure 6) is inserted into the response packet is hard to maintain due to Connection system TCP Hijacking trace-back packet marking technique is used to solve this by the proposed system configuration and flowchart. Connection list block and damage the attacker host B to host A Connection between the intercepts in the middle of the management



(Figure 6) Connection using TCP Hijacking Maintenance Scheme

Attack packets from host B to host A, the A host to B host the attacker goes off and backtracking system response packet to be diverted to the response packet and then inserts the watermark is generated by the attacker transmits the host B.

The list of detected attacks Connection ID and Source / Destination address, the watermark information into the packet Size inserted. Connections so that the watermark is inserted into the list of trace-back system manages the

connections between the attacker and the attacked Connection can be maintained without a break. This packet marking trace-back Connection is a successful watermarking should remain unchanged as to satisfy the condition.

Finally, the station detected in the tracking system of the intermediate destinations watermark detection if the path is constructed by gathering information trace-back is completed.

5. Conclusion

Various intrusion using the Internet actively hacking incidents are increasing rapidly as the technology is urgently required to prevent, but to date the various systems used to prevent hacking hacker hack simply a way to lower the success rate, and does not limit itself to a hacking attempt .

Therefor an attacker trace-back of actively response to the growing need for technology grows. The attacker trace-back techniques for distributed denial-of-service attack (DDoS) type of spoofing IP Trace-back for keeping track of the IP technology and the form of stepping stone attack via multiple types of systems for tracking the actual TCP Connection TCP Connection Trace-back technology classification becomes.

This paper presents an asynchronous TCP Hijacking Established state hacking techniques used to intercept the session packet watermarking technique by applying the response packet trace-back technique to insert a watermark on maintenance issues that occur when a Connection. And packet marking trace-back techniques until you find the location of a hacker Multiple Connection requirements that must be maintained by the attacker trace-back will be able to apply to systems development.

Reference

[1] Sei Dong Il, TCP Connection Traceback, KIISE, 2008

[2] Buchholz, Thomas E. Daniels, Benjamin Kuperman, Clay Shields, Packet Tracker Final Report, CERIAS Technical Report 2000-23, Purdue University, 2008

[3] Kunikazu Yoda & Hiroaki Etoh, Finding a Connection Chain for Tracing Intruders, In F. Guppens, Y.Deswarte, D.Gollamann, M.Waidner (ed.): LNCS, Vol.1985, 2008

[4] Jung Hyeon Chul, TCP Connection Hijacking Attack , KISA, 2012

[5] Sei Dong Il, Implement of Internet packets watermark detection system, KISA, 2012

[6] X. Wang, D. Reeves, S. F. Wu, and J. Yuill, Sleepy Watermark Tracing: An Active Network-Based Intrusion Response Framework, Proceedings ofIFIP Conference. on Security, Mar. 2001

[7] Kang dong ho, Sei Dong Il, Packet networks using watermarking technique based connection traceback system design, KIISE, 2012

[8] Sichoon Noh, Kuimam J.Kim, "Improved Structure Management of Gateway Firewall Systems for Effective Networks Security", Springer, 2008.

[9] Sichoon,Noh,"Building of an Integrated Multi-level Virus Protection Infrastructure", IEEE Computer Society, 2005.12.

[10] VeriTest, http://lionbridge.com

[11] ICSA Labs, http://www.icsalabs.com

[12] Tolly Group, http://tolly.com

[13] NSS Labs, http://www.nss.co.uk

[저 자 소 개]

김 점 구 (Jeom Goo Kim)

1990년 2월 광운대학교
전자계산학과 이학사
1997년 8월 광운대학교
전자계산학과 석사
2000년 8월 한남대학교
컴퓨터공학 박사
1999년 3월~ 현재 남서울대학교
컴퓨터학과 교수
IT융합연구소장

email : jgoo@nsu.ac.kr