새로운 TCP Reset 공격방법

김아영*, 김은기**

*한밭대학교 정보통신전문대학원, **한밭대학교 정보통신공학과

New TCP Reset Attack

Ayoung Kim*, Eungi Kim**

*Graduate School of Information & Communications, Hanbat National University

**Division of Information Communication Engineering, Hanbat National University

E-mail : kima0124@gmail.com*, egkim@hanbat.ac.kr**

요 약

본 논문에서는 새로운 TCP Reset 공격방법에 대해 제시한다. TCP의 3-way Handshake 과정에서 Receiver가 listen 상태일 때, 부정확한 ACK Number를 포함하는 세그먼트를 받게 되면 Sender TCP에게 Reset을 포함한 세그먼트를 전송하여 연결 설정이 이루어 지지 않는다(RFC 792). 본 연구에서는 TCP 초기 연결 설정 과정인 3-way Handshake에서 Sender를 모니터링 하고 있는 Attacker가 Sender보다 먼저 부정확한 ACK Number를 포함하는 세그먼트를 보내고, 이를 수신한 Receiver가 Sender에게 Reset을 포한한 세그먼트를 보내어 연결 설정이 이루어지지 않는 새로운 TCP Reset 공격 방법을 제시한다.

ABSTRACT

In this paper, we propose another TCP Reset Attack. In the process of TCP's 3-way handshake, the receiver in the listen state receives segment including abnormal ACK number, then sends Reset to the sender (RFC 792). In this study, Attacker who monitors sender's packets sent in TCP initial connection sends segment including abnormal ACK number to the receiver before the sender sends normal ACK segment. The receiver received abnormal ACK number sends Reset to the sender. As a result, TCP connection is not established between the sender and the receiver.

키워드

TCP 3-way Handshake, SYN, Reset, Attack

Ⅰ. 서 론

인터넷으로 연결되는 컴퓨터 통신망의 표준 프로토콜인 TCP/IP 프로토콜은 최초 설계 단계에서 보안을 고려하지 않았다. 그런 이유에서 TCP/IP 프로토콜은 근본적으로 보안적인 결함을 가지고 있으며, 이러한 TCP의 보안적인 결함을 악용하는 다양한 해킹 공격이 발생 되고 있다[1].

TCP/IP 프로토콜의 보안적인 취약성을 기반으로 생긴 공격으로는 Sequence Number 추측, IP Spoofing, SYN Flooding, Reset 공격 등이 잘 알려져 있다[2]. 이 중에서 Reset을 이용한 대표적인 공격 방법에는 RFC 5961에 명시되어 있는 Blind Reset 공격이 있다. Blind Reset 공격은 Sender와 Receiver의 TCP 3-way Handshake 초기 연결 설정과정에서 발생한다. Sender의 세그먼트를 모니터링 하고 있는 Attacker가 Sender의 ACK Number를 포함하는 세그먼트보다 먼저 Reset을 포한하는 세그먼트를 Receiver에게 전송한다. 그런 방법으로 Attacker는 Sender의 세션을 가로채서 Sender와 Receiver의 연결을 방해하는 공격 방법이다[3][4][5].

본 논문에서는 Sender와 Receiver의 3-way handshake 초기 연결 설정과정을 모니터링 하고 있는 Attacker가 Reset을 포함하는 세그먼트

(Blind Reset 공격)대신 부정확한 ACK Number를 포함한 세그먼트를 Receiver에게 전송한다. 이러한 부정확한 ACK Number를 포함하는 세그먼트를 받은 Receiver는 Sender에게 Reset을 포함하는 세그먼트를 전송함으로써 Sender와 Receiver간의 연결 설정이 이루어지지 않게 하는 새로운 TCP Reset 공격 방법을 제시한다.

II장에서는 TCP의 정상적인 초기 연결 설정과정을 기술하고 III장에서는 새로운 TCP Reset 공격방법에 대해 제시한다. IV장에서는 결론과 향후 연구 방향에 대하여 기술 한다.

II. TCP(Transmission Control Protocol)

TCP(Transmission Control Protocol)는 IP상에서 수행되는 트랜스포트 계층의 프로토콜이다. 주요 기능은 네트워크를 통한 안정성 있는 데이터의 전송으로 RFC 793에 명시되어 있다[6].

TCP는 새로운 연결을 확립하기 위하여 초기 연결 설정과정에서 3-way handshake를 사용한다. 만일 Sender가 Receiver에 접속을 초기화 하고 데이터 교환이 없다면 정상적인 패킷 교환은 그림 1과 같이 동작한다.

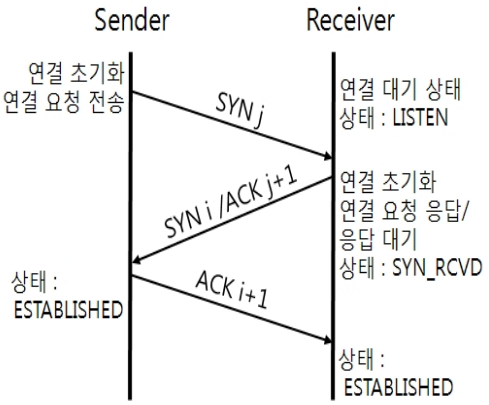

그림 1 . 정상적인 TCP 연결

TCP의 초기 연결 설정과정인 3-way handshake 연결 설정 방법은 다음과 같다.

1. 처음 Sender는 SYN Flag값을 1로 하고, Sequence Number 필드에 ISN(Initial Sequence Number)이 설정된 세그먼트를 Receiver에게 전송한다.
2. Sender의 SYN을 받은 Receiver가 세션성립을 원하면 SYN Flag를 1로 설정한다. 그리고 Receiver는 Sender가 보낸 Sequence Number+1 값으로 ACK Number를 설정하고 Receiver는 Sender와 마찬가지로 ISN (Initial Sequence Number)를 설정하여 Sender에게 전송한다.
3. 세그먼트를 받은 Sender는 ACK Number를 Receiver가 보낸 Sequence Number+1 값으로 설정하여 Receiver에 전송한다.

이러한 과정을 거쳐서 Receiver와 Sender 측이 ESTABLISHED 상태가 되면 연결 설정이 이루어지게 되고 이 과정을 TCP 초기 연결 설정 과정인 TCP 3-way handshake라고 부른다.

III. TCP reset 공격 방법

본 장에서는 II장에서의 TCP 초기 연결 설정 과정을 기반으로 하여 Attacker의 TCP Reset 공격방법에 대한 구조를 설명하고, Sender를 Host S로 Receiver를 Host R이라 정의 한다.

그림 2는 본 논문에서 제시한 TCP Reset 공격 방법에 대한 기본 구조를 나타낸다.

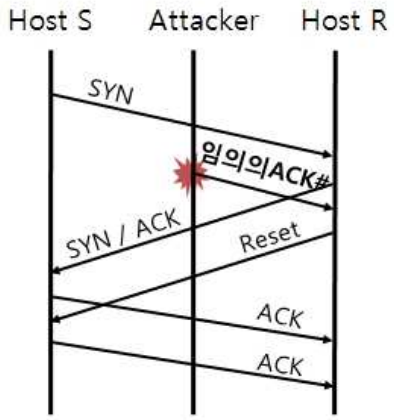

그림 2 . 새로운 TCP Reset 공격 방법

Attacker는 Host S와 동일한 LAN에 위치하여 세그먼트를 모니터링 한다. Host S는 Host R과의 초기 연결 설정 과정을 위해 SYN을 전송한다. Attacker는 Host S가 SYN을 전송한 직후에 Host S가 연결을 시도하려는 Host R에게 Host R이 다음에 받아야 할 ACK Number 대신에 부정확한 ACK Number를 포함하는 세그먼트를 전송한다. RFC792의 내용에 따르면 Host R이 부정확한 ACK Number를 포함한 세그먼트

를 받을 경우, Host R은 Host S에게 Reset을 보내게 되어 초기 연결설정 과정에서 Sender와 Receiver는 연결설정을 할 수 없게 된다.

Ⅳ. 결론

본 논문에서는 TCP의 3-way handshake 과정상의 보안적인 취약점을 이용한 새로운 TCP Reset 공격방법에 대해 제안하였다. TCP의 Flag인 Reset을 이용한 기존의 Blind Reset 공격 방법은 Sender가 Receiver에게 SYN 을 보낼 때 Attacker가 Reset을 포함한 세그먼트를 Receiver에 보내게 되어 Sender의 세션을 빼앗는 방법이다.

본 연구에서 제시한 새로운 Reset공격은 RFC792에 명시된 내용에 따라 Attacker가 Sender의 정상적인 ACK Number를 포함한 세그먼트 보다 먼저 부정확한 ACK Number를 포함한 세그먼트를 보낸다. 이 부정확한 ACK Number를 포함한 세그먼트를 받은 Receiver가 Sender에게 Reset을 포한한 세그먼트를 보내어 Sender와의 연결이 이루어 지지 않게 하는 공격 방식이다. Blind Reset 공격 방법과 다른 점은 Attacker가 Reset을 포함한 세그먼트 대신에 부정확한 ACK Number를 Receiver에게 보내서 Receiver 측에서 Reset을 Sender에게 보내게 되어 연결 설정이 이루어 지지 않는 새로운 형태의 공격 방법이다.

향후의 연구할 방향으로는 본 논문에서 제시한 공격방법에 대해 Libnet과 Libpcap을 이용한 패킷 생성과 모니터링을 수행하여 공격이 성공되는지 확인한다. 또한 공격 성공 여부에 따라 새로운 TCP Reset 공격의 대응방안과 TCP/IP 보안 취약성에 대한 연구가 이루어져야 할 것이다.

본 연구는 2011년 한국산업기술진흥원의 지역산업기술개발사업의 지원으로 수행된 연구로써, 관계부처에 감사드립니다. (과제번호:A001100259)

참고문헌

[1] "A Study on Security System due to structural Vulnerability of TCP/IP protocol", 김선태, 숭실대학교 정보과학 대학원, August 2001

[2] D.H.Kim, S.I.Park, Y.S.Seo, D.E.Choi, K.S.Park, J.Y.Lee, "An Approach for TCP Connection Hijacking Attack", Department of Computer Engineering, Hallym University, May 1999

[3] S.Bellovin, "Defending Against Sequence Number Attacks", RFC 1948, Internet Engineering Task Force, May 1996

[4] J.Touch, "Defending Against Spoofing Attacks", RFC 4953 Internet Engineering Task Force, July 2007

[5] A.Ramaiah, M.Dalal, R.Stewart, "Improving TCP's Robustness to Blind In-Window Attack", RFC 5961, Internet Engineering Task Force, September 1981

[6] J.Postel, "Transmissi Control Protocol. Request for comments(Standard) STD 7", RFC 793, Internet Engineering Task Force, September 1981