제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

TCP Hijacking 을 이용한 역추적 Connection 유지 기법 연구

김환국*, 한승완*, 서동일*
*한국전자통신연구원 네트워크보안연구부
e-mail : rinyfeel@etri.re.kr

A Study of Trace-back Connection Maintenance Techniques using TCP Hijacking

Hwan-kuk Kim*, Seung-Wan Han*, Dong-il Seo*
*Dept. of Network Security Research, ETRI

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 Traceback 기술에서 사용되는 기법 중에 하나인 패킷 워터마킹 역추적 기법에서 TCP Hijacking 해킹기술을 이용하여 Reply 패킷의 Connection 유지 어려움을 해결하는 방법을 제시한다.

1. 서론

인터넷은 이미 일상 생활에 깊게 자리 잡았다. 이러한 인터넷을 이용해서 실생활에서 수행하여야만 했던 많은 일들을 인터넷을 통해 수행할 수 있게 되었고, 인터넷의 편리함 때문에 인터넷 사용자 역시 크게 증가하였다. 이러한 인터넷 사용자의 증가와 더불어 인터넷을 통한 각종 침해사고 역시 크게 증가하였다.

이에, 보안 업체들은 각종 침해로부터 시스템 및 네트워크를 보호하기 위해 각종 보안 강화 시스템을 개발하였고 각 시스템 및 네트워크 관리자들은 이 시스템들을 적용하였다. 그러나, 현재까지 개발되어 사용되고 있는 대부분의 보안 강화 시스템들은 해커의 해킹 시도 자체를 제한하는 것이 아니라, 해커가 해킹을 시도하는 경우, 이를 좀더 어렵게 만드는 수준에 지나지 않았다. 즉, 해커의 해킹 시도를 능동적으로 대처하지 못하고, 수동적으로 방어하는 수준인 것이다. 이와 같은 현재의 보안 시스템 환경 때문에 해킹 시도는 날로 증가하고 있고, 이를 효과적으로 방어하지 못하는 것이 현실이다[1].

이와 같은 문제점을 해결하기 위해 능동적인 해킹 방지를 위한 역추적 기술에 대한 관심이 날로 커지고 있고, 비록 아직은 초보적인 수준이나 역추적 기술에 대한 연구가 진행되기 시작하였다.

최근의 침입자 역추적 기술은 분산 서비스 거부 공격(DDoS) 형태의 스푸핑된 IP 를 추적하기 위한 IP Traceback 기술과 stepping stone 형태의 여러 시스템을 경유하는 공격 형태의 실제 TCP Connection 을 추적하기 위한 TCP Connection Traceback 기술로 분류가 된다 [2].

본 논문에서는 TCP Connection 을 유지하면서 Stepping Stone 형태의 공격에 대한 역추적을 수행 하기 위해 사용되는 패킷 워터마킹 역추적 기법에서 워터마크를 삽입 할 경우 TCP 프로토콜의 특성 상 Sequence 번호의 변화에 의해 TCP Connection 유지가 어려운 점이 발생하는데 이를 보완하기위해 TCP Hijacking 해킹기법을 이용하는 방법을 제안하고자 한다.

2. 역추적 기술

2. 1 TCP connection Trace-back

TCP 연결 역추적(TCP Connection Traceback) 기술은

TCP 연결을 기반으로 우회 공격을 시도하는 해커의 실제 위치를 실시간으로 추적하는 기법이다. 또한, 흔히 연결 체인(Connection Chain) 역추적 기술이라고 불리기도 한다.

여기서, 연결 체인이란 그림 1 에서 컴퓨터 H_0 의 한 사용자가 네트워크를 통해 다른 시스템 H_1 으로 로그인하면, 두 시스템 H_0 와 H_1 간에는 TCP 연결(Connection) C_1 이 생성된다. 이때, 같은 사용자가 시스템 H_1 에서 H_2 로, 또 H_3, ..., H_n 으로 로그인하게 되면, 각각의 해당 시스템들 간에는 TCP 연결 C_2, C_3, ..., C_n 이 같은 방식으로 생성되게 된다. 이때 이 일련의 연결들의 집합 $C = (C_1, C_2, \ldots, C_n)$를 연결 체인이라 한다. 즉, 해커가 실제로 위치한 시스템으로부터 여러 시스템을 경유하여 실제 공격을 당하고 있는 시스템까지의 연결(connection)들의 집합을 말하는 것이다[3].

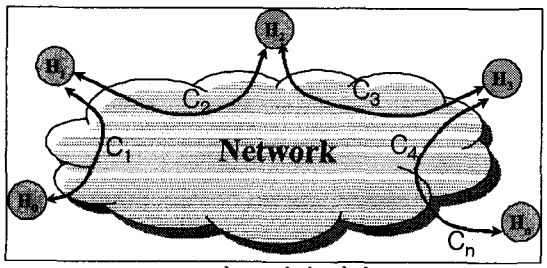

그림 1. 연결 체인

TCP 연결 역추적 기술은 다시, 크게 2 가지로 분류할 수 있다. 이는 호스트 기반 연결 역추적(Host-based connection traceback) 기술과 네트워크 기반 연결 역추적(Network-based connection traceback) 기술로 분류된다[1].

2.2 IP 패킷 역추적(IP Packet Traceback)

IP Packet Traceback 기술은 IP 주소가 변경된 패킷의 실제 송신지를 추적하기 위한 기술을 말한다. 일반적으로 IP 주소가 변경된 패킷은 악의적으로 사용되는 경우가 대부분이다. 특히 서비스 거부(Denial of Service, DoS), 혹은 분산 서비스 거부(Distributed Denial of Service, DDoS) 공격에 주로 사용된다. IP 주소가 변경되는 경우에는 TCP 연결을 유지할 수 없기 때문에, 일방적인 패킷 송신으로 공격이 가능한 DoS 혹은 DDoS 에서 주로 사용되는 것이다. 물론 과거 IP Spoofing 이라 알려져 있는 해킹 기법을 이용하는 경우, IP 주소가 변경된 패킷을 이용하여 공격하고자 하는 대상 시스템에 백도어를 설치하도록 하는 기법이 사용되기도 하였으나, 이를 위해서는 TCP Sequence Number Guessing 과정이 필요하기 때문에 최근에는 거의 사용되지 않고 있다.

또한 IP Packet Traceback 은 현재 특정 시스템으로 IP 주소가 변경된 패킷을 송신하는 시스템을 찾는 기술로서, 여러 중간 경유지를 추적하여 실제 해커의 위치를 찾는 TCP 연결 역추적 기술과는 해결하고자 하는 문제의 대상에 약간의 차이가 있다[1].

3. TCP Session Hijacking

TCP Session Hijacking 은 서버와 클라이언트 사이에서 SEQ, ACK 번호를 비동기화 시키고 세션을 가로채는 기법으로 TCP Stream 을 자신의 머신을 거치게 Redirection 할 수 있는 TCP 프로토콜의 취약성을 이용한 적극적 공격 (Active Attack)이다. Redirection 을 통해 침입자는 SKEY 와 같은 일회용 패스워드나 Kerberos 와 같은 티켓 기반 인증 시스템에 의해 제공되는 보호 메커니즘을 우회할 수 있다. TCP 접속은 누군가 접속로 상에 TCP 패킷 스니퍼나 패킷 생성기를 가지고 있다면 대단히 취약하다.

TCP Session Hijacking 비동기화를 만드는 기법은 그림 2 와 같다.

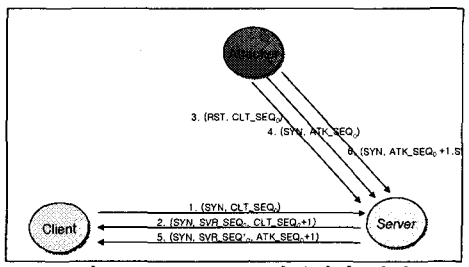

그림 2. TCP hijacking 비동기화 기법

1. 클라이언트는 서버와의 접속을 생성하기 위해 SYN 패킷을 전송한다.
2. 공격자는 서버에서 클라이언트로 가는 SYN/ACK 패킷을 Listen 한다.
3. 패킷을 탐지 했을 때 공격자는 서버에 rst 패킷을 보내 클라이언트와의 접속을 종료한다.
4. 공격자는 클라이언트가 보낸 패킷과 동일한 파라메터들을 가지지만 일련번호가 다른 SYN 패킷을 서버에 보낸다. 서버는 자신의 다른 일련번호를 가지고 같은 포트에 새로운 접속을 개방한다.
5. 서버는 SYN/ACK 패킷을 클라이언트에 발송한다.
6. 이 패킷을 탐지한 공격자는 서버에 ACK 패킷을 발송한다. 서버는 ESTABLISHED 상태로 전환한다. 클라이언트는 서버로부터 최초 SYN/ACK 패킷을 수신했을 때 이미 ESTABLISHED 상태로 전환되어 있다.

위의 과정을 거쳐 이제 양단은 비동기 Established 상태가 되어 TCP Session hijacking 이 이뤄어진다[4].

4. TCP Hijacking 을 이용한 패킷마킹 역추적 기법

4.1 패킷 워터마킹 역추적(Packet Water-Marking Traceback)

패킷 워터마킹 역추적 기술은 공격자가 Stepping stone 형태의 여러 시스템을 중간 경유하여 자신의 시

스템 IP 를 공개하지 않으려는 목적의 공격에 대해 역추적하기 위한 TCP Connection 역추적에 사용되는 요소 기술이다.

개념적으로 패킷 워터마크는 하나의 커넥션을 유일하게 식별하기 위해 사용될 수 있는 작은 정보이다. 패킷 워터마크는 네트워크 어플리케이션 공격자에게 은닉하여 쉽게 삽입하고 추출해야 된다[5].

패킷 마킹 기술을 통해 역추적을 수행하려면 다음의 두 가지 특성을 고려하여야 한다[6].

첫째, 공격자에게 패킷 워터마크가 보이지 않게 Data Hiding 기술을 사용한다. 워터마크를 생성하는 문제로 워터마크가 공격자 에게 보이지 않도록 만드는 것으로 응답 패킷(reply packet) 에 공격자의 시스템에서 보이지 않도록 패킷의 데이터 영역에 일종의 control 문자나 null string 을 사용하여 stepping stone 형태의 connection 을 유지하는 공격에 대한 역추적을 위해서 사용된다.

둘째, 호스트 대 중간 경유지, 중간 경유지 대 중간 경유지, 중간 경유지 대 공격자 호스트 간의 TCP Session 연결이 유지되어 응답 패킷이 잘 전달이 되어야 한다. 역추적의 Correlation 을 위해 워터마크는 Multiple Connection 을 경유하고 변함없이 유지되어야 한다.

4.2 TCP Hijacking 이용한 패킷마킹 역추적 기법

패킷 마킹 역추적 기법을 수행하기 위하여 다음을 가정한다. (1) 침입탐지는 기존의 침입탐지 시스템을 이용한다. (2) 탐지된 패킷에 대한 Reply 패킷을 차단하기 위하여 기존의 침입차단 시스템을 이용한다.

그림 3 은 패킷마킹 역추적 시스템 구성과 흐름도이다[7].

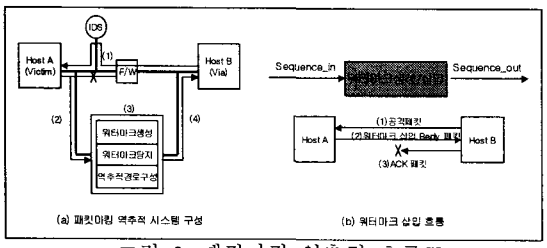

그림 3. 패킷마킹 역추적 흐름도

(1) 공격 패킷 탐지 (2) Reply 패킷 전송 (3) 워터마크 생성 및 삽입 (4) 워터마크 삽입 패킷 전송 (5) 워터마크 패킷 탐지 (6) 역추적 경로구성

또한 역추적 흐름도에 따라 침입에 대한 공격을 탐지한 후 응답 패킷에 워터마크를 삽입 하기 전과 후의 Sequence Number 는 그림 4 의 (b), (c)와 같이 삽입된 워터마크의 크기로 인해 변하게 된다.

삽입전 : Sequence(Host A) =
Sequence(Host A) + Data_Len

삽입후 : Sequence(Watermark) =
Sequence(Host A) + Data_Len + WM_Len

공격자가 유지해야 하는 Host A 의 Sequence 넘버가 변하게 되어 비동기화가 발생한다.

비동기화 : Sequence(Host A) ≠ Sequence(Host B)

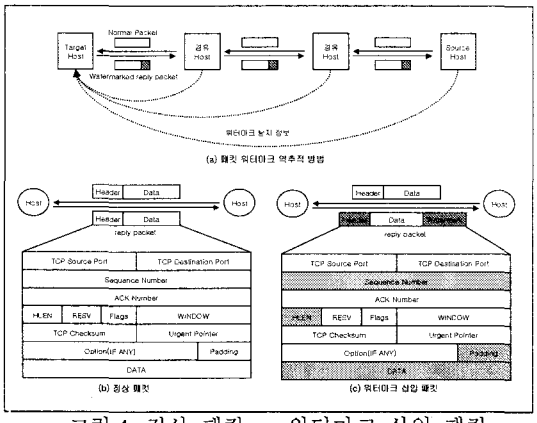

그림 4. 정상 패킷 vs 워터마크 삽입 패킷

TCP 프로토콜은 새로운 연결을 확립하기 위하여 클라이언트가 서버에 접속을 초기화하고 데이터 교환을 시도한다면 정상적인 패킷 교환은 그림 5 와 같이 이루어진다.

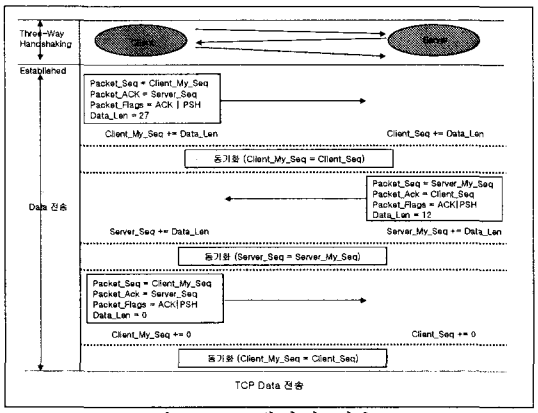

그림 5. TCP 데이터 전송

클라이언트가 서버의 패킷 수신 확인 후 양측의 연결이 확립되는 Established 상태에서 양단의 동기화가 이뤄져 데이터 교환이 이루어져야 한다. 그러나 워터마크 삽입은 Reply 패킷의 Sequence 번호를 변하게 하고 양단에서 유지하고 있는 Sequence 번호가 비동기

상태가 되어 Connection 유지가 어렵게 된다. 따라서, 양단의 Connection 을 유지하기 위한 방법으로 비동기 상태에서 패킷을 가로채는 TCP Hijacking 기법을 이용하면 이러한 문제를 해결할 수 있다.

그림 6 은 응답 패킷(Reply Packet)에 워터마크 삽입으로 인해 Connection 유지가 어려운 패킷마킹 역추적 시스템에서 TCP Hijacking 기법을 이용하여 이를 해결하기 위한 방법이다. 컨넥션 리스트 블록에서는 공격자 호스트 B 와 공격대상호스트 A 간의 Connection 을 중간에 가로채어 Sequence 를 유지하고 관리 한다.

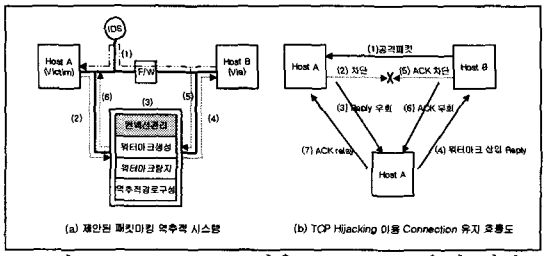

그림 6. TCP Hijacking 이용 Connection 유지 기법

공격 패킷이 공격자 호스트 B 에서 호스트 A 로 탐지가 되면, 호스트 A 에서 공격자 호스트 B 로 가는 응답 패킷을 차단하고 역추적 시스템으로 우회 시킨 후 응답 패킷에 워터마크를 생성/삽입하여 공격자 호스트 B 로 전송한다. 이때 컨넥션 리스트 블록에 탐지된 공격 Connection 아이디, Source/Destination 주소, 워터마크 패킷 Size 정보를 삽입하여 관리한다. 컨넥션 리스트 블록은 워터마크 삽입으로 인해 변하게 된 Sequence 번호의 동기화를 맞추기 위해 공격 탐지된 Connection 의 Sequence 번호를 관리 한다.

그리고 공격자 호스트 B 에서 발생하여 공격 대상 호스트까지 도달하는 ACK 패킷을 역추적 시스템으로 우회하도록 하여 컨넥션 리스트 블록이 유지하고 있는 공격 탐지된 Connection 의 Sequence 번호와 ACK 패킷의 Sequence 번호의 동기화를 맞추어 호스트 A 로 RELAY 한다. 워터마크가 삽입된 컨넥션을 역추적 시스템 내 컨넥션 리스트 블록에서 양단의 Sequence 번호를 유지 관리하여 Sequence 번호를 동기화 시키면 공격자와 공격대상 간의 Connection 연결이 끊기지 않고 유지될 수 있다. 따라서, 공격자의 위치를 찾을 때 까지 Multiple Connection 을 유지할 수 있다.

이러한 과정을 통해 중간 경유지에서 검출된 워터마크 탐지 정보를 수집하여 경로를 구성하면 패킷마킹 역추적 시스템에 적용 가능할 것이다.

5. 결론

인터넷을 이용한 각종 침해 사고가 급증함에 따라 능동적인 해킹방지 기술이 절실히 요구되고 있으나, 현재까지 해킹방지를 위해 사용한 각종 시스템들은 단순히 해커의 해킹 성공률을 낮추기 위한 방법 이엇고, 해킹 시도 자체를 제한하지는 못하고 있다. 그래서 이에 대한 능동적인 대응방법으로 침입자 역추적 기술에 대한 필요성이 점차 커지고 있다. 침입자 역추적 기술은 분산 서비스 거부 공격(DDoS) 형태의 스푸핑된 IP 를 추적하기 위한 IP Traceback 기술과 stepping stone 형태의 여러 시스템을 경유하는 공격 형태의 실제 TCP Connection 을 추적하기 위한 TCP Connection Traceback 기술로 분류가 된다.

본 논문에서는 TCP Hijacking 해킹기법에서 사용되는 비동기 Established 상태에서 세션을 가로채는 기법을 패킷 워터마킹 역추적 기법에 응용함으로써 응답 패킷에 워터마크를 삽입 시에 발생 하는 Connection 유지 문제를 해결하고, 패킷마킹 역추적 기법에서 공격자의 위치를 찾을 때 까지 Multiple Connection 을 유지해야 하는 요구사항을 만족함으로써 침입자 역추적 시스템 개발에 적용 할 수 있을 것이다.

참고문헌

[1] 최양서, 서동일, 손승원, 역추적 기술 동향(TCP Connection Traceback 중심), ETRI 주간기술동향

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

[3] Kunikazu Yoda & Hiroaki Etoh, Finding a Connection Chain for Tracing Intruders, In F. Guppens, Y.Deswarte, D.Gollamann, M.Waidner(ed.): 6th European Symposisum on Research in Computer Security – ESORICS 2000. Lecture Notes in Computer Science, Vol. 1985, 2000

[4] 정현철, TCP Connection Hijacking 공격 및 대책, 한국정보보호진흥원

[5] 최병철, 서동일, 인터넷 패킷 워터마크 검출 시스템 구현, 정보과학회 추계학술대회 2000

[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] 최양서, 강동호, 서동일, 패킷워터마크 기법을 이용한 네트워크 기반 연결 역추적 시스템의 설계, NCS2002