TCP/IP패킷의 Port 번호의 생략을 위한 End-to-End 메커니즘

박 상 준　　박 우 출　　이 병 호
한양대학교 전자통신전파공학과
{parksang, wcpark, bhrhee}@hymail.hanyang.ac.kr

Mechanism of End-to-End for Omission about Port Number of TCP/IP Packet

Sang-Jun Park　　Woo-Chool Park　　Byung-Ho Rhee
Division of Electrical and Computer Engineering, Hanyang University.

요 약

오늘날 매우 널리 사용되는 TCP/IP 프로토콜은 많은 보안적 흠을 가지고 있다. 시퀀스 번호를 스푸핑, 소스 번호를 스푸핑, 인증 공격 등 많은 류의 공격이 이런 흠을 통해서 행해지고 있다. 또한 근원적으로 패킷의 TCP헤더 필드의 포트 번호와 IP 헤더 필드의 주소 번호를 분석하여 포트번호와 IP번호를 알아내어 상대방을 공격한다. 이에 상대방으로부터 포트번호나 어드레스 번호를 은닉하거나 생략하여 전송하여 상대방이 패킷을 분석하기 어렵게 만들어 TCP/IP 패킷의 보호하고자 한다. 먼저 본 논문에서는 TCP 헤더의 Port field를 제거하기위한 수정된 TCP 연결설정의 메커니즘을 제시한다.

1. 서 론

인터넷 사용층의 증가와 보안의 요구하는 데이터의 증가에 따라 특정 사이트에 침입하는 일이 빈번해지고 이에 따라 보안에 대한 필요성이 대두되고 있다. 즉 인터넷에 접속하고 어떤 서비스를 제공할 때, 그에 대한 보안에 대한 고려도 이제는 매우 중요한 일이 되었다. 우리나라의 인터넷 관련된 보안 사건을 살펴보면, 93년에 서울대 중앙교육 전산원의 LANd에 침입하여 6대의 워크스테이션의 정보를 지운 침해사건과 당시 HANA망을 운영하던 한국통신 연구센터의 자료를 지운 한국통신연구센터 침해 사건, 94년도의 인천 지역 정보망인 인디텔에 가입한 선배의 아이디를 도용한 홈뱅킹 계좌이체를 시도한 천리안 홈뱅킹 사건, 95년도 2명의 부산지역 해커를 비롯하여 전국 주요 대학의 시스템을 해킹하다 붙잡힌 사건 등 이 한때 간혹 발생하였다. 그러나 오늘날 해킹은 본인이 알게 모르게 하루에 전세계 곳곳에서 빈번히 행해지고 있다.[1,2]

이런 인터넷에서 오늘날 가장 널리 사용되는 TCP/IP 프로토콜은 프로토콜 고유의 여러 가지 흠을 가지고 있다. 이런 결점의 몇몇은 호스트가 TCP의 포트번호나 IP의 어드레스 번호 의지하기 때문에 나타난다. 그래서 본 논문에서는 TCP 단의 사용자끼리 초기에 설정에 의해 Port 번호를 숨기거나 생략하는 방법을 연구하였고, 요즘 인터넷에서 연구중인 망을 통해서 IP 헤더의 주소 필드를 생략하는 방법으로 확장시키고자 한다. 이런 방법을 통해서 인터넷에서 널리 사용하는 TCP/IP의 패킷을 가로채 분석하는 걸 방지하고자 했다.[3]

본 논문의 구성은 다음과 같다. 2절에서는 TCP 헤더의 Port 번호를 은닉하는

방법에 대한 End-to-End 초기 연결 설정에 대한 메카니즘을 설명한다. 마지막으로 3절에서 결론을 내린다.[3,4]

2. TCP/IP 포트 번호을 은닉하기 위해 제안된 방식

본 논문에서 제안된 방식은 TCP 헤더의 Port 번호를 은닉하기 위해 TCP 엔드사용자끼리 End-to-End 초기 연결 설정에 대하여 수정된 메카니즘과 MPLS 라우터를 사용하여 IP 헤더의 주소 필드를 은닉하는 메카니즘을 제안하였다.TCP는 연결을 설정하거나 종료위해서 세 방향 핸드쉐이킹을 사용한다. 가장 간단한 경우, 연결설정 핸드쉐이킹은 그림 1과 같다.

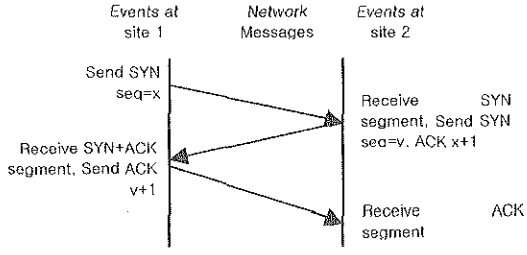

그림1. 기존의 TCP 연결 설정

핸드쉐이킹의 첫 번째 세그멘트는 코드 필드안에 SYN(synchronization) 비트를 설정함으로서 정의된다. 두 번째 메시지는 핸드쉐이킹을 계속하고 있다는 것 뿐만아니라 첫 번째 SYN 세그멘트에 대한 응답이라는 것을 나타내는 SYN 비트와 ACK 비트 집합 모두를 가진다. 첫 번째 핸드쉐이킹 메시지는 두 사이트가 모두 동의했고 연결이 이미 만들어졌다는 것을 알려준다.연결을 종료할 시에는 SYN 비트대신 FIN 비트를 설정하여 응용프로그램과 종료 메시지를 주고 받는다.

TCP 헤더의 Port 번호를 은닉하기 위해 TCP 엔드사용자끼리 End-to-End 초기 연결 설정에 대하여 수정된 메커니즘은 그림 2와 같다.

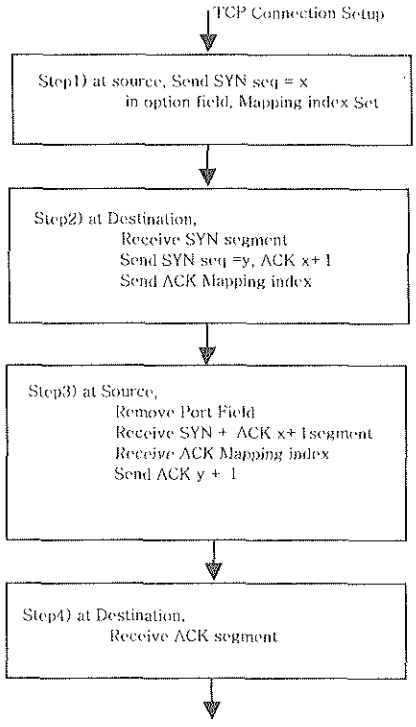

그림2. 제안된 TCP 연결 설정 메커니즘

핸드쉐이킹의 첫 번째 세그멘트는 코드 필드안에 SYN(synchronization) 비트를 설정하고 또한 옵션 필드에서 TCP 연결 설정이 확립된 후에 소스 포트 필드와 목적지 포트 필드를 대체할 Mapping Index(MI)를 임의적으로 설정해 목적지 TCP 단에 보냄으로써 정의된다. 두 번째 메시지는 핸드쉐이킹을 계속하고 있다는 것 뿐만아니라 첫 번째 SYN 세그멘트에 대한 응답이라는 것을 나타내는 SYN 비트와 ACK 비트 집합 모두를 가진다. 또한 제안된 옵션 필드의 Mapping Index(MI)에 대한 ACK를 가진다. 그리고 목적지 TCP 단에서는 Mapping Index Table을 만들어 Mapping Index와 포트 필드와 Mapping 상태를 기록한다. 첫 번째 핸드쉐이킹 메시지는 두 사이트가 모두 동의했고 연결이 이미 만들어졌다는 것을 알려준다. 이제 TCP 패킷이 Segment를 보낼때는 TCP 헤더의 소스 필드와 목적지 필드를 제거하고 임의로 소스에서 정한 Mapping Index를 사용하여 인터넷 망을 통해 목적지까지 도착한다. 그럼으로써 인터넷 망을 통해 전송되는 패킷을 가로채서 TCP 포트정보를 은닉하여 TCP 패킷의 보안을 향상시킬 수 있다. 그림 본 논문에서 제안된 TCP 헤더를 변형된 형태

를 원래의 TCP 헤더와 비교하여본다. 비교의 그림은 그림3 과 그림 4와 같다.

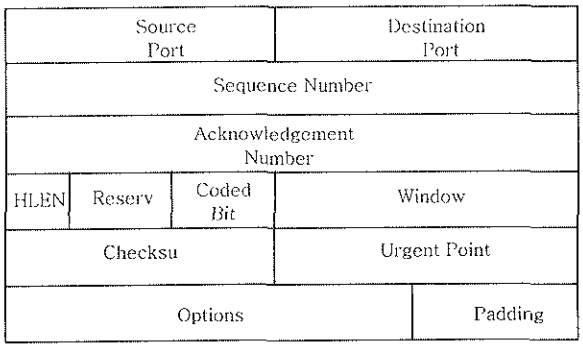

그림3. TCP 헤더

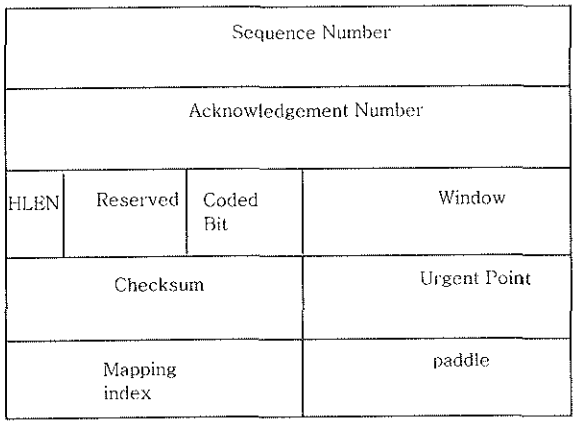

그림 4. TCP Port가 제거된 헤더

본 논문에서 제안된 방식의 TCP Connection 설정방식을 사용한다면 패킷을 가로채였을 때 포트의 보안을 강화할 수 있을 뿐 아니라 그림3과 그림4에서 보는 것처럼 포트 필드가 있을 때보다 제거되었을 때 패킷의 양이 감소되는 것을 알 수 있다.

3 결 론

오늘날 매우 널리 사용되는 TCP/IP 프로토콜은 많은 보안적 홈을 가지고 있다. 시퀀스 번호를 스푸핑, 소스 번호를 스푸핑, 인증 공격 등 많은 류의 공격이 이런 홈을 통해서 행해지고 있다. 또한 근원적으로 패킷의 TCP헤더 필드의 포트 번호와 IP 헤더 필드의 주소 번호를 분석하여 포트번호와 IP번호를 알아내어 상대방을 공격한다. 이에 상대방으로부터 포트번호나 어드레스 번호를 은닉하기나 생략하여 전송하여 상대방이 패킷을 분석하기 어렵게 만들어 TCP/IP 패킷의 보호하고자 한다.먼저 본 논문에서는 TCP 헤더의 Port field를 제거하기위한 수정된 TCP 연결 설정의 메커니즘을 제시한다.

TCP 헤더의 Port field를 제거하여 패킷에 대한 포트의 드러남을 방지하여 보안을 강화할 수 있도록 제안된 TCP 헤더를 사용하여 TCP 연결 설정을 위한 핸드쉐이킹을 한다.

그 과정에서 첫번째로 옵션 필드에서 TCP 연결 설정이 확립된 후에 소스 포트 필드와 목적지 포트 필드를 대체할 Mapping Index(MI)를 임의적으로 설정하고 그리고 목적지 TCP 단에서는 Mapping Index Table을 만들어 Mapping Index와 포트 필드와 Mapping 상태를 기록하여 TCP 포트 필드를 제거할 수 있게 만들어 데이터를 전송할 할 있게 된다. 따라서 그럼으로써 인터넷 망을 통해 전송되는 패킷을 가로채서 TCP 포트정보를 은닉하여 TCP 패킷의 보안을 향상시킬 수 있다. 또한 패킷의 양이 감소되는 것을 알 수 있다.

4. 참고 문헌

1. Comer, D. *Internetworking with TCP/IP : Principles, Protocols, and Architecture.* Prentice Hall, 1988

2. Eichin, M. and Rochlis, J. *With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988.* Massachussetts Institute of Technology, 1988

3. S. Floyd and K. Fall, "Promoting the Use of End-to-End Congestion Control in the Internet", to appear in IEEE/ACM Transactions on Networking, 1999

4. Awduche, D.O., Malcolm, J., O'DELL, M., McManus, J. "Requirements for Traffic Engineering over MPLS", draft-ietf-mpls-traffic-eng-00.txt, OCTOBER 1998