2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

인터넷 보호 프로토콜에서 IPv4와 IPv6의 예상 평문 공격의 비교 분석

· 소주호° , · 박현민, ··최병석, ∴박재현
· 명지대학교 컴퓨터공학과 ··동국대학교 정보산업과학대학
∴명지대학교 전기전자공학부 정보산업학부
e-mail:jhsoh@wh.myongji.ac.kr

Analysis of Probable Plaintext Attack in IPv4 and IPv6 Under IP Security Protocol

· Soh Ju-Ho° , · Park Hyun-Min, ··Choe Byeong-Seog,
∴Park Jae-Hyun
· Department of Computer Engineering, Myong-Ji University
··College of Information Industry Science, Dong-Guk University
∴Division of Electronics Information and Communication Engineering,
Myong-Ji University

요약

평문과 암호문 쌍에서 일부 예측할 수 있는 평문들을 이용하여 비밀키를 찾는 공격을 예상 평문 공격(Probable Plaintext Attack)[1]이라고 한다. 인터넷 보호 프로토콜은 IP Datagram에 AH(Authentication Header)[2], ESP(Encapsulating Security Payload)[3] 등과 같은 Security Header가 붙여지며, 각 헤더부분에서 예상할 수 있는 영역을 가지고 있으므로 예상 평문 공격의 주요한 대상이 되고, 이러한 취약점은 현재 인터넷 보호 프로토콜에서 사용되고 있는 DES(Data Encryption Standard)[4] 알고리즘에서 두드러지게 나타난다.

본 논문에서는 IPv4와 IPv6를 서로 비교하고 각각의 IP version에서 예측할 수 있는 예상 평문 영역을 조사한 다음, 일어 날 수 있는 예상 평문 공격의 비율을 서로 비교하여 앞으로 상용화될 IPv6의 문제점과 해결방안을 제시한다.

1. 서 론

정보통신의 발달로 분산된 개방시스템들 사이에 다양한 디지털 정보를 공유하거나 교환하는 것이 필수적이 되었다. 점차 확장되어 가는 컴퓨터 네트워크는 유통되는 정보량의 엄청난 증가로 정보를 신속하고 정확하게 전송하는 것이 중요한 과제로 부각되고 있으며, 합법적인 사용자에 대한 안전성과 신뢰성 이외에도 이를 기반으로 한 보다 세분화 된 안전 요구가 대두되고 있다. 이에 따라 보안의 중요성이 더욱 커지고 전자 인증(Authentication) 시장의 확대도 요구되고 있다.

보안 서비스의 주요 요구사항들은 기밀성(Confidentiality), 인증(Authentication), 부인봉쇄(Non-repudiation), 무결성(Integrity) 등이 있는데 이들 요구 사항들을 만족시킬 수 있는 기법은 매우 복잡하다. 분산환경에서 암호화 프로토콜(Cryptographic Protocol)을 효율적으로 실현하려면 합법적인 사용자에 대한 안전한 통신을 확보하는 것과 더불어 적용환경 및 적용업무에 따라서 여러 가지 추가적인 요구 조건이 부가된 다양한 기능을 갖는 암호화 프로토콜에 대한 연구가 필요하다.

본 논문에서는 IPv4와 IPv6를 서로 비교하고, 인터넷 보호 프로토콜에서 예상 평문 공격에 대해서 살펴보며, 예상 평문 공격이 IPv6에서는 어떻게 적용되는지 설명한 다음, IPv6에서의 예상 평문 공격에 대한 해결 방안을 제시한다.

2. IPv4 Vs IPv6

2.1 IPv4

Internet Protocol의 특징은 Unreliable Delivery를 제공한다. 또 ATM(Asynchronous Transfer Mode)

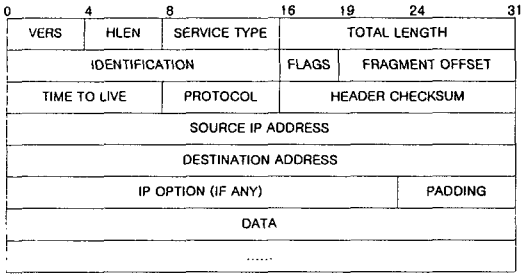

그림 1. IPv4 DATAGRAM FORMAT

방식과 같이 연결설정, 전송, 중단의 Connection 방식을 따르지 않는다.

IPv4의 Datagram Format은 그림1과 같으며 VERS는 현재 사용되고 있는 IP의 Version(4)를 나타내고 HLEN은 Header Length, TOTAL LENGTH는 데이터 그램 전체의 크기, FRAGMENT OFFSET은 MTU(Maximum Transfer Unit)에 따라 Fragment된 Datagram의 Offset을 나타내는 필드이다. TIME to LIVE는 Datagram이 네트워크 상에서 존재할 수 있는 시간을 말해주며 SOURCE IP ADDRESS와 DESTINATION IP ADDRESS는 32bit로서 우리가 현재 사용하고 있는 IP 주소체계를 나타낸다.

2.2 IPv6의 구조

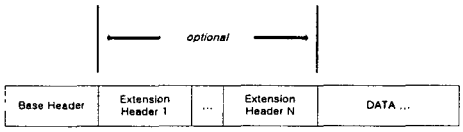

그림 2. IPv6 Datagram Format

IPv6의 Datagram의 두드러진 특징은 Base Header의 크기가 고정적이고 Extension Header가 선택적이라는 점이다. IPv4와는 달리 Header에 쓰이지 않는 기능은 선택적으로 Extension Header를 두어 사용되지 않는 Field의 낭비를 최소화했다.

그림 3은 IPv6의 Base Header Format을 나타내고 있으며 언제나 크기가 고정적이며 Header Length 부분이 생략되었다. IPv4에서의 Datagram Length Field가 Payload Length로 대체되었으며 이것은 패킷에서 헤더를 제외한 나머지 부분의 크기를 의미한다. FLOW LABEL 은 IPv4에서의 SERVICE TYPE이 대체된 것이며, NEXT HEADER는 다음에 쓰여질 Header를 가리키고, HOP LIMIT은 IPv4의

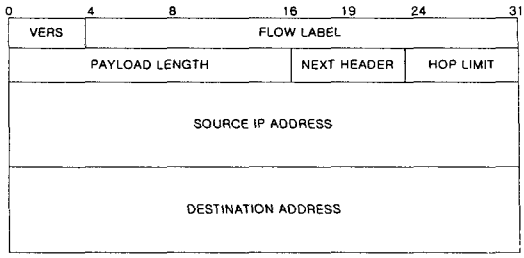

그림 3. IPv6 BASE HEADER FORMAT

TIME TO LIVE가 바뀐 것이다. IPv6의 가장 두드러진 변화중의 하나는 그림에서와 같이 SOURCE IP ADDRESS와 DESTINATION IP ADDRESS 영역이 128bit로 확장된 것이다.

3. 인터넷 보호 프로토콜

IPv4와 IPv6에서 보안서비스를 제공하기 위하여 AH와 ESP를 제공한다. IPSEC[5] 메카니즘의 AH와 ESP는 정보보호 서비스로 인증, 무결성, 그리고 비밀성을 제공한다. 이러한 보호 메카니즘의 구현은 IPv6에서는 필수로 IPv4에서는 옵션으로 되었다.

AH와 ESP는 Security Header이며, 송신자와 수신자간에 키, 인증 알고리즘, 암호 알고리즘, 그리고 이러한 알고리즘에 필요한 부가적인 파라메트 집합들에 대한 합의가 필요하다. 여기서 키, 인증 알고리즘 등 이들 각각을 보호 속성이라 하며 이러한 보호 속성들의 집합을 보호연관이라 한다.

IPSEC의 처리는 보호연관에 의하여 결정되며 각 객체들은 이 연관들을 공유하고 있다고 가정한다. 각 보호연관은 각 종단시스템에서의 속성 집합에 의하여 정의되고 SPI(Security Parameter Index)와 목적지 주소에 의하여 식별된다.

ESP는 IP 패킷의 비밀성과 무결성을 제공한다. 사용자의 요구에 따라 트랜스포트 계층 세그먼트를 암호화하거나 전체 IP 패킷에 대하여 암호화할 수 있다. TCP, UDP, ICMP 등과 같은 트랜스포트 계층 세그먼트를 암호화할 경우 이를 트랜스포트 모드 ESP라하며 전체 IP 패킷에 대하여 암호화할 경우 이를 터널모드 ESP라 한다.

ESP는 그림4, 5와 같이 Transport Mode와 Tunnel Mode에 따라 IP Datagram에 첨가되는 위치가 다르다. Transport Mode하에서는 실제 IP Header 뒤에 붙여져 Header에는 아무런 영향을 끼치지 못한다. Tunnel Mode하에서는 실제 IP Header 전체를 암호

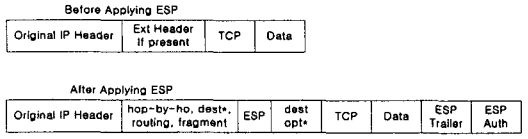

그림 4. Adding an ESP to an IPv6 datagram in Transport mode

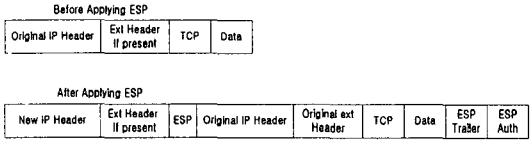

그림5. Adding an ESP to an IPv6 datagram in Tunnel Mode

화한 후 Tunneling 하기 때문에 새로운 IP Header가 생성이 되었고, 네트워크 상에 노출되지 않는다.

4. IPv6에서의 예상 평문 공격

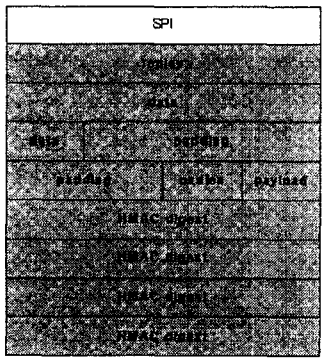

그림 6. ESP 패킷의 구조

그림 6은 ESP에 대한 패킷 구조이며 회색 부분은 DES를 이용하여 CBC(Cipher Block Chaining)모드로 암호화한 영역을 나타낸다. 싱글패킷 공격은 복호화하려는 시도가 한 번에 한 패킷 내에서 이루어지는 공격을 말하며 터널 모드의 사용여부, 그리고 초기벡터를 아느냐에 따라서 예상할 수 있는 평문의 수가 달라진다.

ESP 패킷의 첫 번째 워드는 Replay Counter이다. 이것은 패킷의 시작점을 나타내주며 보호연관이 시작될 때 패킷을 가로챈다면 약 30비트에서 32비트를 얻을 수 있으며, 보호연관이 시작된 후에 패킷을 가로채도 상위 20-24비트의 값이 모두 0이라는 것을 예상할 수 있다.

터널모드를 사용할 경우 IP Header가 나오는데 VERSION NUMBER는 언제나 6_{16} 이고 헤더의 길이가 고정적이기 때문에 HEADER LENGTH 필드가 존재하지 않으며 길이는 항상 40 octet이다. FLOW LABEL은 IPv4에서의 Type-of-Service 필드와 같으며 앞의 4bit인 TCLASS는 값이 0-7, 8-15일 때의 값에 따라 필드의 내용을 감지 할 수 있다. PAYLOAD LENGTH는 헤더를 뺀 나머지 부분의 크기를 의미하며 Extension Header가 선택적이기 때문에 값이 고정적이지 않다. NEXT HEADER는 Base Header 뒤에 오는 Header를 가리키며 값이 43_{16}일 때 Routing Header, 44_{16}일 때 Fragmentation Header, 50_{16}일 때 ESP, 51_{16}일 때 AH를 나타내며, 다음에 올 헤더가 존재하지 않을 때는 값이 59_{16}이다. HOP LIMIT는 IPv4에서의 Time-to-Live가 대치된 것으로서 송신자 호스트의 Protocol Stack에 의존한다. SOURCE와 DESTINATION IP ADDRESS는 각각 128bit 이며 Host-to-Firewall 모드에서는 송신자의 IP Address와 암호화된 복사본을 매칭시키기 때문에 128bit를 예상할 수 있고, Host-to-Host 모드에서는 헤더가 네트워크 상에 노출되기 때문에 256bit 모두를 예상할 수 있다.

투 패킷 공격은 하나의 연결이 이루어진 상태에서 패킷 쌍을 분석하는 공격방법으로서 더 많은 예상 평문을 얻을 수 있는데, 서로 다른 두 패킷에서 어떤 필드가 일정하고, 동시에 같은 방법으로 복호화를 시도한다면 그 패킷에 대한 정보를 얻을 수 있다. 또, IP 헤더내의 Source address와 Destination address를 보다 쉽게 추출할 수 있다는 장점이 있고, 비용이 많이 든다는 단점이 있다. Connection이 이루어지고 같은 방법으로 복호화를 시도한다면 이 두 필드는 서로 매칭될 것이다. TCP나 UDP Port Number가 이러한 방법으로 사용된다. IPv6의 Header에서 이상적인 환경에서 약 272비트의 예상 평문이 존재한다.

IPv4에서의 예상 평문 공격은 이미 다른 논문에서 알려진 바 있으며 결과적으로 표 1에서와 같이 싱글 패킷 공격일 때는 약 16비트, 투 패킷 공격일 때는 약 272bit의 예상 평문이 존재한다. IPv6 에서는 쓰여지지 않는 헤더는 선택적으로 두었기 때문에 상대적으로 IPv4에 비해 Default Value가 적다. 따라서 싱글 패킷 공격일 때 유출되는 예상 평문이 IPv4에 비해 훨씬 적으나 투 패킷 공격일 때 유출되는 예상

	Single	Double
IPv4	54-58	127
IPv6	16	272

표1. IPv4와 IPv6의 예상 평문

평문은 IPv4에 비해 많으나 이것은 IP address의 영역이 크기 때문이다.

TCP 헤더의 경우는 Transport 모드를 사용할 경우 Replay Counter 뒤에 나온다. 이상적인 상황에서 약 88비트의 예상 평문을 가지며 UDP는 28비트의 예상 평문을 가진다.

인터넷 보호 프로토콜에서 예상 평문 공격을 예방하기 위한 이미 알려진 기본적인 보호책으로서는 헤더 필드에서 예측할 수 있는 부분을 줄이는 방법이 있다. 초기 벡터의 누출을 피하는 방법과 재생 카운터의 정의를 바꾸어 1부터 시작하는 대신에 키 정보로부터의 난수로 시작하는 방법, 그리고 호스트간(Host-to-Host)터널 모드의 사용을 피하고 호스트와 방화벽(Host-to-Firewall)터널 모드에서 임시 IP 주소부에 대한 복사 부분을 난수로 대처하는 방법이 있다. 그러나 이러한 방법으로는 근본적인 문제를 해결하지 못하며 투 패킷 공격일 때는 더욱 심각하다.

5. 결론

실험 결과에 의해 싱글 패킷 공격일 때는 IPv4는 약 54-58비트, IPv6는 약 16비트로서 IPv6가 예상평문이 적었고, 투 패킷 공격일 때는 IPv4는 약 127비트, IPv6는 약 272비트로서 IPv4가 예상 평문이 적었다. 그러나 IPv6의 Base 헤더는 크기가 고정적이며 추가적인 기능은 Extension Header를 두었기 때문에 Base Header의 내용이 유출되었을 경우에도 Datagram 전체의 판독이 매우 어렵다. 인터넷 보호 프로토콜은 지금까지 설명한 바와 같이 IP 헤더에 Security 헤더가 붙여지는 것이며 IP 버전은 바뀌었지만 Security 헤더에 대한 사양은 바뀌지 않았으므로 헤더를 암호화하는 알고리즘과 암호화하는 비용은 큰 차이가 없다. 투 패킷 공격일 때는 IPv6가 유출되는 영역이 많았고 그 중에는 Source와 Destination IP Address가 차지하는 영역이 256비트로서 대부분을 차지하므로 Address 영역의 보완이 시급하다.

인터넷 보호 프로토콜에서 차세대 IP의 근본적인 예상 평문 공격을 예방하기 위해서는 난수 생성기를 이용한 보호 메커니즘[9] 이나 그 밖의 새로운 암호화 알고리즘의 향후 연구가 필요하다.

6. 참고문헌

[1] S. Bellovin, "Probable Plaintext Cryptanalysis of the IP Security Protocol", in Proceedings of the Symposium on network
and Distributed System Security, pp. 155-160, Feb. 1997.

[2] IP Authentication Header (RFC 2402)
http://www.ietf.org/html.charters/ipsec-charter.html

[3] IP Encapsulating Security Payload (ESP) (RFC 2406)
http://www.ietf.org/html.charters/ipsec-charter.html

[4] NBS. Data encryption standard, January 1977. Federal Information Processing Standards Publication 46.

[5] Security Architecture for the Internet Protocol (RFC 2401)
http://www.ietf.org/html.charters/ipsec-charter.html

[6] Douglas E. Comer, "Internetworking With TCP/IP", Prentice Hall, 1995.

[7] S. M. Bellovin. Security problems in the TCP/IP protocol suite. Computer Communications Review, 19(2):32-48, April 1989

[8] Advanced Socket API for IPv6 (RFC 2292)
http://www.ietf.org/internet-drafts/draft-ietf-ipngwg-rfc2292bis-01.txt

[9] 최은수, "인터넷 보호 프로토콜에서 예상 평문 공격에 대응한 보호 캡슐 메커니즘", 정보과학회, pp. 339-341, 10. 1999.

[10] Pedro Roque, Ian P. Morris, "Linux INET6 implementation"