IPsec 기반의 WAP 게이트웨이 모델

김동주, 김상욱*, 김건우**

경북대학교, 정보통신학과 *경북대학교, 컴퓨터과학과

**한국전자통신연구원

IPsec-based WAP Gateway Model

Dong-ju Kim, Sang-wook Kim*, Gun-woo Kim**

Department of Information and Communication Kyung-pook National Univ.

*Department of Computer Science Kyung-pook National Univ.

**Electronics & Telecommunications Research Institute (ETRI)

요 약

무선 통신과 인터넷의 결합인 무선 인터넷에서도 유선에서와 마찬가지로 정보의 보안은 중요한 문제이다. 현재 WAP에서는 WTLS라고 하는 전송 계층의 프로토콜로 인증 및 기밀성 문제를 해결하고 있다. WAP 게이트웨이는 유선 구간과 무선 구간의 프로토콜 변환이라는 기능의 특성상 WTLS와 SSL/TLS 보안 메커니즘을 동시에 유지해야 하는 번거로움이 있다. 이러한 문제를 해결하기 위해 본 논문에서는 WAP 게이트웨이에 IP 계층 보안 프로토콜인 IPsec을 적용하여 단일 IPsec 보안 메커니즘으로 유선과 무선의 양 구간에 대해 IP 상위 계층에 투명한 정보보호 서비스를 제공하는 WAP 게이트웨이 모델을 제시한다.

I. 서론

기존의 유선인터넷은 주로 응용 계층에서 제공하는 보안 메커니즘을 사용하고 있다. 응용 계층 보안 메커니즘은 특정한 응용 분야에만 사용이 국한되는 단점이 있는데, 웹에서 사용되는 SSL(Secure Socket Layer)/TLS(Transport Layer Security)가 대표적이다. 응용 프로그램이 SSL/TLS의 보안 서비스를 사용하기 위해서는 SSL/TLS가 제공하는 별도의 API를 사용해야 한다. 현재 무선 인터넷의 큰 축을 이루는 WAP(Wireless Application Protocol) 역시 전송 계층에서 보안을 제공하는 WTLS(Wireless Transport Layer Security) 보안 프로토콜을 사용하고 있는데, WTLS는 SSL/TLS를 기반으로 만들어졌다[1]. 본 논문에서는 SSL/TLS와 달리 IP 계층에서 정보보호 서비스를 제공하는 기술인 IPsec(Internet Protocol Security)을 WAP 게이트웨이에 적용하여 무선 인터넷에 보안을 제공한다. 현재 인터넷의 취약한 보안 문제를 근본적으로 해결할 수 있는 IPsec을 이용함으로써 기존 WAP의 보안 프로토콜인 WTLS보다 한층 진보된 보안 기능을 WAP에 제공할 뿐만 아니라, IPv6가 요구하는 범용성을 갖는 보안 서비스를 제공할 수 있다.

Ⅱ장에서는 IPsec 보안 프로토콜인 AH와 ESP 프로토콜을 설명하고, Ⅲ장에서는 IPsec을 WAP 게이트웨이에 적용했을 때 프로토콜 스택의 변화를 보인다. 그리고, WAP 게이트웨이에 적용되어야 할 두 단계에 걸친 키 교환 과정과 정책 기반의 IPsec 처리 과정을 기술하고 Ⅳ장에서 결론을 맺는다.

II. IPsec 보안 프로토콜

IPsec은 IP 계층뿐만 아니라 그 이상의 계층에 대한 보안을 위해 AH(Authentication Header)와 ESP(Encapsulating Security Payload) 보안 프로토콜을 사용한다. AH와 ESP는 IPv4와 IPv6에서 필요로 하는 보안 서비스를 제공하기 위해 독자적으로 적용되거나 상호 조합되어 적용된다. 각 프

로토콜은 트랜스포트 모드와 터널 모드를 지원하는데 트랜스포트 모드는 주로 상위 계층 프로토콜 보안을 위해 사용되고, 터널 모드는 터널링을 위한 IP 헤더를 패킷 앞에 덧붙임으로써 최종 목적지에 대한 IP 헤더를 은폐하여 트래픽이 어떤 경로로 흐르는지에 대한 비밀성을 제공한다.

1. AH

AH는 IP 패킷의 페이로드, 헤더의 변하지 않는 부분, 변하더라도 예측 가능한 헤더 부분에 대해 인증을 제공한다. 패킷의 내용보다는 헤더의 옵션이나 확장 헤더 부분이 보호되어야 하는 경우에는 AH만으로도 충분한 보안 기능을 제공한다.

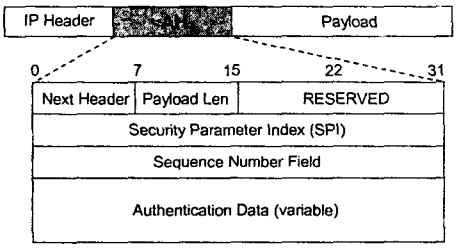

그림 1: AH 헤더 포맷.

AH 헤더 구조는 그림 1과 같다. SPI는 목적지 주소, 보안 프로토콜의 종류(AH)와 더불어 패킷에 IPsec 처리를 하기 위해 필요한 정보인 보안연계를 식별하는데 사용되는 32 비트 값이다. SN 필드는 재연 공격을 방지하기 위하여 동일 패킷이 중복 수신 여부와 일정한 타임 윈도우 내에 도착하였는지를 검사하는데 사용된다. Authentication Data 필드는 IP 페이로드, 헤더의 불변 필드, 가변이지만 예측 가능한 헤더 필드에 대한 무결성 검증을 위해 단방향 해쉬함수를 이용하여 계산한 MAC 값으로서, 수신된 패킷이 중간 경로에서 위조되었는지를 알 수 있다. IP 패킷에 AH 처리를 할 때 동작 모드에 따라 AH의 위치는 다르다. 트랜스포트 모드에서 AH 헤더는 IP 헤더와 상위 계층 프로토콜 패킷의 사이에 위치한다. 터널 모드의 경우, AH 헤더는 패킷의 IP 헤더 앞에 붙고 AH 헤더 앞에는 터널링을 위한 새로운 IP 헤더가 추가된다[2]. 그림 1은 트랜스포트 모드를 나타낸다.

2. ESP

ESP는 IP 패킷에 대한 인증만을 제공하는 AH와는 달리, 패킷의 데이터를 암호화하여 트래픽에 대한 비밀성을 제공한다. 비밀성과 더불어 ESP 보안연계에 인증이 협상되어 있다면 AH보다 좁은 범위의 인증도 제공된다.

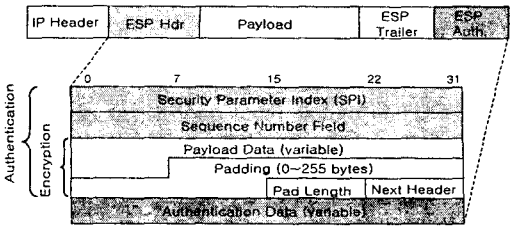

그림 2: ESP 패킷 포맷.

그림 2의 ESP 패킷 포맷에서 SPI는 목적지 주소, 보안 프로토콜의 종류(ESP)와 더불어 패킷에 IPsec 처리를 하기 위해 필요한 정보인 보안연계를 식별하는데 사용되는 32 비트 값이다. SN 필드는 AH 헤더에서와 동일하게 재연 공격 방지를 위해 사용된다. Payload Data 필드는 비밀성 제공을 위해 암호화할 데이터로서 트랜스포트 모드의 경우 IP 상위 계층의 데이터만 Payload Data 필드에 놓이지만 터널 모드일 경우에는 ESP를 적용할 전체 IP 패킷이 Payload Data가 된다. 패킷에 ESP 보안 처리 시 Payload Data 필드부터 Next Header 필드까지를 보안 연계에 따라 암호화한다. Authentication Data 필드는 인증이 선택되었을 때, ESP 헤더와 암호화된 Payload Data 필드에 대한 무결성 검증 값이다. IP 패킷에 ESP 처리를 할 때, 트랜스포트 모드에서 ESP 헤더는 그림 2처럼 IP 헤더와 TCP, UDP, ICMP 등의 상위 계층 데이터 사이에 위치한다. 터널 모드일 경우에는 앞에서 설명한 것처럼 전체 IP 패킷이 암호화를 위해 Payload Data 필드에 놓이므로 ESP 헤더는 원래의 IP 헤더 앞에 놓여 전체 IP 패킷을 보호하고, 터널링을 위한 새로운 IP 헤더가 ESP 헤더 앞에 오게된다[3].

III. IPsec 기반 WAP 게이트웨이

무선 인터넷에서도 유선에서와 마찬가지로 정보의 보안은 중요하다. 현재 WAP에서는 전송 계층 보안 프로토콜인 WTLS를 사용하여 인증 및 기밀성 문제를 해결한다. WAP 게이트웨이는 유선 구간과 무선 구간의 프로토콜 변환이라는 기능의 특성상 WTLS와 SSL/TLS 보안 메커니즘을 동시에 유지해야 하는 번거로움이 있다. 이러한 WAP 게이트웨이에 IP 계층에서 제공되는 보안 프로토콜인 IPsec을 적용하여 단일 보안 메커니즘으로 유선과 무선의 양 구간에 대해 상위 프로토콜에 투명한 정보보호 서비스를 제공한다.

1. 프로토콜 스택

WAP은 무선 구간과 유선 구간을 잇기 위해 게이트웨이 모델을 사용한다. WAP 게이트웨이는 무선 구간의 WAP 프로토콜과 유선 구간의 HTTP/TCP/IP 프로토콜을 적절히 변환하여 이들 사이에 데이터를 전달한다. SSL/TLS와 WTLS의 유선, 무선 보안 프로토콜도 이와 만찬가지로 이동 단말과 웹 서버의 중계 역할을 하는 WAP 게이트웨이에서 변환된다. 결국 WAP 게이트웨이는 이동 단말과 웹 서버간의 보안을 제공하기 위해 WTLS와 SSL/TLS 암호 메커니즘을 동시에 유지해야 한다.

IP 계층에서 보안 서비스를 제공하는 IPsec을 WAP 게이트웨이에 적용하면 WTLS와 SSL/TLS 두 개의 보안 메커니즘을 유지하던 기존의 WAP 게이트웨이와 달리 단지 하나의 IPsec 메커니즘으로 유선, 무선 인터넷 구간 모두에 보안 기능을 제공할 수 있다. 그림 3은 IPsec을 적용했을 때 유선, 무선 구간의 프로토콜을 상호 변환하는 WAP 게이트웨이와 웹 서버, 이동 단말기의 변화된 프로토콜 스택 구조이다.

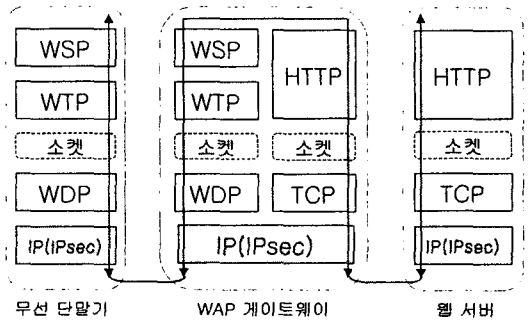

그림 3: IPsec 기반 프로토콜 스택.

무선 데이터 통신이 이루어질 때 초기와 과정의 하나로 이동 단말기와 교환국에 속한 공중망 정합 장치인 IWF는 이동 단말기가 사용할 임시 IP 주소를 협상한다. 협상을 통해 할당된 IP 주소를 사용하여 이동 단말기는 WAP 데이터에 IP 헤더를 덧붙여 무선 구간으로 전송한다. 전송된 무선 데이터를 기지국에서 수신하여 제어국으로 전송하고 제어국은 다시 교환국으로 전송한다. 교환국의 IWF는 디지털 이동통신 패킷 포맷으로 되어 있는 데이터를 공중망에 알맞도록 TCP/IP 포맷으로 변환한 다음, 공중망에 패킷을 띄우고 이 패킷은 라우팅되어 WAP 게이트웨이에 도착한다. WAP 게이트웨이는 수신한 데이터를 HTTP 프로토콜에 적합하도록 변환한 다음 웹 서버로 전송한다. 위에서 설명했듯이 이동 단말기는 WAP 게이트웨이와 IP 통신을 하므로, 이동 단말기에도 WTLS 대신 IP 계층에 IPsec 메커니즘을 적용할 수 있다. 단말기에 적용되는 IPsec은 IP 포워딩과 같은 네트웍 게이트웨이에 필요한 기능을 수행할 필요는 없으므로 WAP 게이트웨이나 웹 서버에 적용되는 IPsec보다는 기능 면에서 간단하다. 이로써 WAP 게이트웨이 뿐만 아니라 웹 서버와 무선 단말기에 IPsec 보안 메커니즘을 적용하여 IP 상위 계층에 투명한 정보보호 서비스를 제공할 수 있다.

2. 보안 정책 시스템

정책은 상이한 네트웍을 적절히 제어하기 위한 일련의 규칙이다. 보안 정책 시스템은 보안 관련 정책 정보를 검색하고 접근, 처리하는데 필요한 메커니즘을 제공하는 시스템이다. 보안 정책 시스템은 크게 정책 서버, 정책 클라이언트, 마스터 파일, 정책 데이터베이스로 구성된다. 정책 서버는 정책 클라이언트로부터의 정책 요구를 처리하거나 다른 도메인의 정책 서버와 정책을 협상한다. 정책 클라이언트는 정책 정보를 요구하는 보안 시스템에 정책을 제공한다. 마스터 파일은 보안 도메인과 정책을 정의하고, 정책 데이터베이스는 협상된 정책을 저장하는 곳이다.

보안 정책 시스템은 기본적으로 WAP 게이트웨이가 패킷에 IPsec 보안 프로토콜을 적용해야 하는지의 여부를 정책 정보로 제공한다[5]. WAP 게이트웨이가 패킷에 AH나 ESP의 보안 처리를 할 때 그 과정 중에 사용되는 암호함수나 해쉬함수는 키를 필요로 한다. 보안 정책 시스템은 이러한 키를 협상하는데 근간이 되는 암호 알고리즘, 해쉬 알고리즘, prf 알고리즘, 인증 방법 등의 정책 정보를 키 교환 시에 제공한다. 안전한 통신을 위해 WAP 게이트웨이는 정책 클라이언트를 두어 자신이 속한 보안 도메인 내의 정책 서버로부터 IPsec 처리 시 필요한 정책 정보를 얻는다.

3. 두 단계에 걸친 키 교환

IKE(Internet Key Exchange) 프로토콜은 IP 패킷에 AH나 ESP 프로토콜 처리를 하기 위해 필요한 키를 교환한다[4]. IKE의 키 교환 과정은 크게 두 단계로 나뉘어진다. 첫 번째 단계에서는 IKE 프로토콜 엔진들이 안전하게 키 협상을 하기 위한 보안연계와 키를 교환하고, 두 번째 단계에서는 IP 패킷에 AH나 ESP 처리 시 사용할 보안연계와 키를 협상한다. 즉, 첫 번째 단계에서 협상된 보안연계와 키는 두 번째 단계에서 이루어지는 협상을 보호하기 위해 사용된다. 단계별로 키 교환 프로

토콜에 의해 생성된 보안연계와 키는 보안연계 데이터베이스에 저장된다. 보안 기능을 위해 저장된 키와 보안연계는 주기적으로 갱신되거나 소멸된다.

4. 정책 기반 IPsec 처리

WAP 게이트웨이는 사전에 협의된 정책에 따라 IP 패킷에 IPsec 보안 처리를 한다. 정책은 패킷에 대한 IPsec 처리 여부와 패킷에 적용할 보안 프로토콜 종류와 IPsec 동작 모드를 지정한다. 정책을 기반으로 패킷에 IPsec 처리를 함으로써 WAP 게이트웨이는 기존의 WTLS나 SSL/TLS와 달리 세분화된 보안 서비스를 제공한다.

1) 출력 패킷 처리

전송 계층에서 내려온 패킷을 페이로드로 하여 IP 계층에서는 IP 헤더를 생성하여 IP 패킷을 만든다[6]. IP 헤더의 <source address, destination address, source port, destination port, protocol> 정보를 키로 하여 보안 정책 데이터베이스를 검색해서 <action, x_protocol, ipsec_mode, SPI> 정책 데이터를 얻는다. 패킷에 대한 IPsec 처리 방법을 나타내는 action은 Discard, Bypass, IPsec의 세 가지 방법을 제공하며 각각은 패킷 폐기, IPsec을 적용하지 않은 보통 패킷으로 전송, IPsec을 적용한 패킷으로 전송함을 의미한다. IPsec 처리가 선택되었다면 x_protocol이 나타내는 적용할 보안 프로토콜(AH/ESP)과 ipsec_mode가 가리키는 동작 모드(트랜스포트모드/터널모드)에 따라 패킷에 IPsec을 적용하여 데이터링크 계층으로 전송한다.

2) 입력 패킷 처리

하위 계층으로부터 IP 계층에 패킷이 도착하면 패킷의 목적지 주소를 보고 포워딩 여부를 결정한다. 최종 목적지 주소이면 패킷 헤더정보 내에 있는 <destination address, protocol, SPI> 값을 키로 하여 보안연계 데이터베이스로부터 보안연계 데이터를 구한다. 얻어진 보안 연계를 이용하여 패킷에 보안 프로토콜 종류와 동작 모드에 따라 복호화나 메시지 인증 등의 IPsec 처리 과정을 거친 다음, 보안 정책 데이터베이스를 검색해서 적용된 보안 연계와 보안 정책이 제대로 일치하는지 확인한 후 패킷을 전송 계층으로 보낸다.

그림 4는 패킷에 IPsec 처리를 하는 IPsec 엔진과 키 교환을 하는 IKE 엔진, 정책을 제공하는 보안 정책 클라이언트 그리고 정책 데이터베이스와 보안연계 데이터베이스로 구성되는 WAP 게이트웨이의 연동 구조이다.

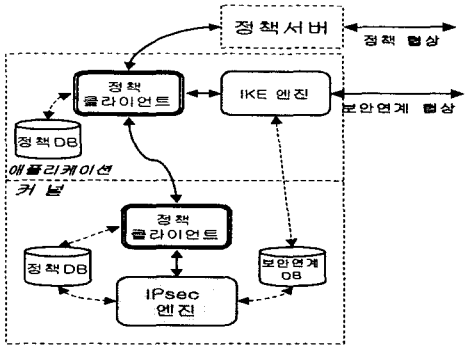

그림 4: WAP 게이트웨이 연동 구조.

IV. 결론

본 논문에서 IPsec을 이용하는 WAP 게이트웨이 보안 모델을 제시하였다. IPsec은 기존 WAP 보안 프로토콜인 WTLS보다 한층 더 진보된 보안 기능을 제공할 뿐만 아니라, WTLS와 SSL/TLS의 두 가지 암호 메커니즘을 유지해야 하는 WAP 게이트웨이의 부담을 줄여준다. 그러나, WAP 게이트웨이에서 WTLS로 통신하는 무선구간과 SSL로 통신하는 유선구간 사이의 프로토콜 변환 시에 메시지의 원문이 그대로 노출되었던 문제는 IPsec을 적용해도 WAP 게이트웨이의 특성상 여전히 남아있게 된다. 이러한 문제점을 해결하기 위해 향후에는 IPsec을 이용하여 단말기와 웹 서버 종단간 보안을 제공할 수 있는 방향으로 시스템을 구성해야 한다.

참고문헌

[1] "Wireless Transport Layer Security Specification," WAP Forum, 18-Feb-2000.

[2] S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402, November 1998.

[3] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406, November 1998.

[4] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, November 1998.

[5] 김건우, 이종태, 손승원, "분산 네트웨크 기반 보안 정책 제어 기법", Proceedings of JCCI 2001, pp. 73-76, 2001년 4월.

[6] 정지훈, 이종태, "C-ISCAP: 제어 기반 인터넷 정보보호 플랫폼", Proceedings of JCCI 2001, pp. 197-200, 2001년 4월.