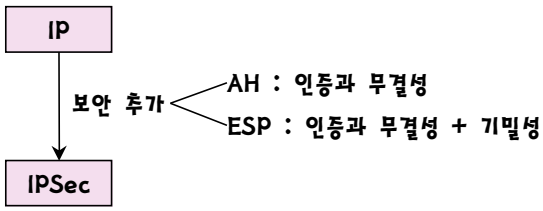
제12장 네트워크 보안

1. IPSec 개요

IPSec은 개방형 IP(internet protocol)에 보안 기능을 첨가한 것이다.



① IPSec(IP Security)은 네트워크층 보안 프로토콜이다.
- IPSec은 보안 기능이 없는 응용프로그램에 대해서도 IP계층에서 보안 방법을 제공한다.
- IP는 도청, 변조, 무인증 등 많은 취약점에 노출되어 있다.
- 취약한 IP에 보안 기능을 첨가한 것이 IPSec이다.
- IPSec는 사용 중인 응용프로그램과는 무관하게 동작한다.
- IPSec는 HTTP, FTP, SMTP 같은 TCP/IP 프로그램에 대해 보안을 제공한다.

② IPSec은 보안을 위해 **"AH와 ESP"**를 사용한다.

③ IPSec은 **"전송모드와 터널모드"**라는 통신 방식이 가능하다.
- 전송모드는 모든 사용자 시스템에 IPSec을 설치하는 방식이다.
- 터널모드는 사용자 시스템에 연결된 라우터에만 IPSec을 설치하는 방식이다.

④ IPSec은 암호화와 인증 서비스를 패킷 단위로 제공한다.

⑤ IPSec은 VPN, VoIP, Mobile IP 등 네트워크 인프라 보호에 널리 사용되고 있다.

1. 인증 헤더(AH, Authentication Header)

AH 포맷은 다음과 같다.

next header (8 bits)	payload length (8 bits)	reserved (16 bits)
security parameters index (32 bits)		
sequence number (32 bits)		
authentication data (multiple of 32 bits) / integrity check value		

① Next header (8bits)
• 다음 페이로드 유형을 식별하기 위한 필드이다. TCP 또는 UDP일 수 있다.

② Payload length (8bits)
• 페이로드 길이를 정의한다. 32비트 단위로 헤아린 값에서 2를 뺀 수이다.

③ Reserved (16bits)
• 미래에 사용하기 위한 필드이다.(0으로 설정함)

④ Security parameters index (32bits)
• IP 데이터그램에 대응되는 보안 연관(SA)을 식별하기 위한 필드이다.

⑤ Sequence number (32bits)
• 되풀이 공격(replay attack, **재전송 공격**)을 방지하기 위한 필드이다.
• 일정하게 증가하는 카운트 값을 가진다. 패킷의 순서를 식별할 수 있다.

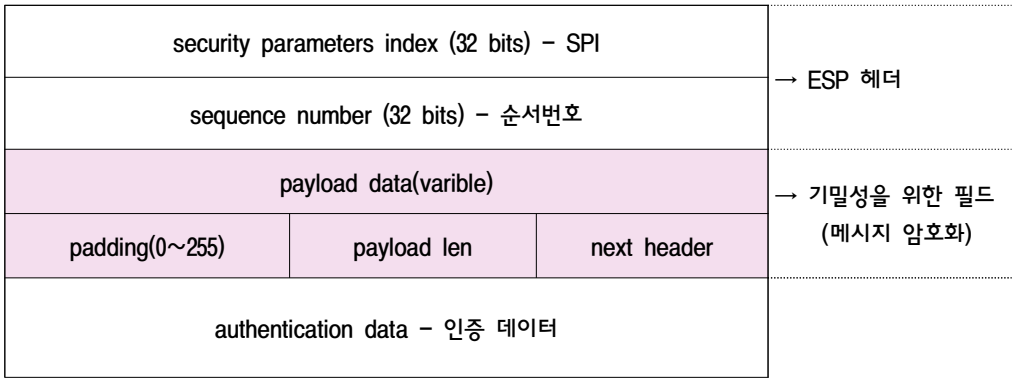
⑥ Authentication data (multiple of 32bits)
• **인증**과 **무결성**을 위한 필드이다. **기밀성은 제공하지 않는다.**
• 패킷 무결성을 위한 검사합 또는 MAC를 가진다.

2. 보안 페이로드 캡슐화(ESP, Encapsulating Security Payload)

① ESP는 IP 데이터그램의 **인증, 무결성, 기밀성(암호화)**을 제공한다.
- ESP는 AH의 기능에 추가로 기밀성을 갖게 한 것이다.**(AH와 차이점)**
- ESP는 옵션에 따라 AH와 동일한 인증 서비스를 할 수 있다.
- ESP는 암호화 알고리즘으로 DES, 3DES, AES 등을 사용할 수 있다.

② 선택적인 되풀이 공격(replay attack, 재전송 공격) 방지 기능이 있다.
③ AH와 ESP를 같이 사용할 수도 있다.(안전성 증가)

④ ESP 포맷은 다음과 같다.



↓ 설명

SPI	• 데이터그램에 적용할 **보안연관**(SA)을 식별하기 위한 필드이다. • 목적지 주소와 ESP를 조합하여 데이터그램에 대한 SA를 식별
순서번호	• 순서번호는 **재전송 공격을 방어**하기 위한 필드이다. • 송수신자 사이에 SA가 구성될 때, 순서번호는 0으로 초기화된다. • 순서번호는 SA를 사용하여 데이터그램이 전송될 때마다 증가한다.
페이로드 데이터	• 상위층(TCP 또는 UDP)의 **메시지** • 기밀성 서비스가 협상되면 페이로드 데이터는 암호화 된다.
패딩	• **암호** 알고리즘이 블록 단위의 평문을 요구하는 경우에 필요하다. • 페이로드 데이터가 블록 크기의 배수가 되도록 채운다.
패딩 길이	• 패딩 필드의 바이트 수를 나타내는 필드
다음 헤더	• 각 헤더를 다음 헤더와 연결하는데 사용된다. • 다음 헤더의 프로토콜 번호를 기술한다.
인증 데이터	• **무결성 검사값**(ICV, integrity check value) • ESP 메시지에서 인증 데이터 필드를 제외한 부분에 대한 무결성 검사값 • **해시함수** HMAC-MD5 또는 HMAC-SHA를 이용하여 인증 생성

기출문제 분석

1. IPSec 표준은 네트워크 상의 패킷을 보호하기 위하여 AH(Authentication Header)와 ESP(Encapsulating Security Payload)로 구성된다. AH와 ESP 프로토콜에 대한 설명으로 옳지 않은 것은? [2017 경기 추가 9급]

① AH 프로토콜의 페이로드 데이터와 패딩 내용은 기밀성 범위에 속한다.
② AH 프로토콜은 메시지 무결성을 검사하고 재연(replay) 공격 방지 서비스를 제공한다.
③ ESP 프로토콜은 메시지 인증 및 암호화를 제공한다.
④ ESP는 전송 및 터널모드를 지원한다.

♤ IPSec

- AH 프로토콜의 페이로드 데이터와 패딩 내용은 기밀성 범위에 속한다.(×)
  → AH는 IP 데이터그램의 **인증과 무결성**을 제공한다. 기밀성은 제공하지 않는다.
- AH는 인증과 무결성을 위해 **메시지인증코드(MAC)**를 사용한다.

정답 : ①

2. 다음 <보기>에서 설명하는 것은 무엇인가? [2015년 서울 9급]

<보기> IP 데이터그램에서 제공하는 선택적 인증과 무결성, 기밀성 그리고 재전송 공격 방지 기능을 한다. 터널 종단 간에 협상된 키와 암호화 알고리즘으로 데이터그램을 암호화한다.

---

① AH(Authentication Header)
② ESP(Encapsulation Security Payload)
③ MAC(Message Authentication Code)
④ ISAKMP(Internet Security Association & Key Management Protocol)

♤ **보안 페이로드 캡슐화(ESP, Encapsulating Security Payload)**

- AH : 인증, 무결성 제공
- ESP : 인증, 무결성, 기밀성 제공

정답 : ②

3. IPsec의 캡슐화 보안 페이로드(ESP) 헤더에서 암호화되는 필드가 아닌 것은? [2019년 지방 9급]

① SPI(security parameter index)
② payload data
③ padding
④ next header

♤ IPsec : 캡슐화 보안 페이로드(ESP)

- ESP는 IP 데이터그램의 인증, 무결성, 기밀성(암호화)을 제공한다.
- ESP는 AH의 기능에 추가로 기밀성을 갖게 한 것이다.(AH와 차이점)
- ESP는 옵션에 따라 AH와 동일한 인증 서비스를 할 수 있다.
- ESP는 암호화 알고리즘으로 DES, 3DES, AES 등을 사용할 수 있다.
- AH와 ESP를 같이 사용할 수도 있다.(안전성 증가)

- ESP 포맷은 다음과 같다.

<table>
<tr><td colspan="3">security parameters index (32 bits)</td></tr>
<tr><td colspan="3">sequence number (32 bits)</td></tr>
<tr><td colspan="3">iv(varible)</td></tr>
<tr><td colspan="3">payload data(varible)</td></tr>
<tr><td>padding(0~255)</td><td>payload len</td><td>next header</td></tr>
<tr><td colspan="3">authentication data (96 bits)
키를 가진 MD5-HMAC 또는 SHA-1-HMAC</td></tr>
</table>

→ 기밀성을 위한 필드 (메시지 암호화)

- Padding(0~255)
  → 평문에 필요한 만큼의 비트를 채운다.
- IV(initial vector)
  → 초기 벡터값이다.
- 사용되는 알고리즘
  Three key triple DES, RC5, IDEA을 지원
  HMAC-MD5-96, HMAC-SHA-1-96을 지원

정답 : ①