6-7: 인터넷 보안 프로토콜(IPSec)
인증헤더(AH) 프로토콜
캡슐화 보안 페이로드(ESP) 프로토콜

담당교수: 차 영욱

ywcha@andong.ac.kr

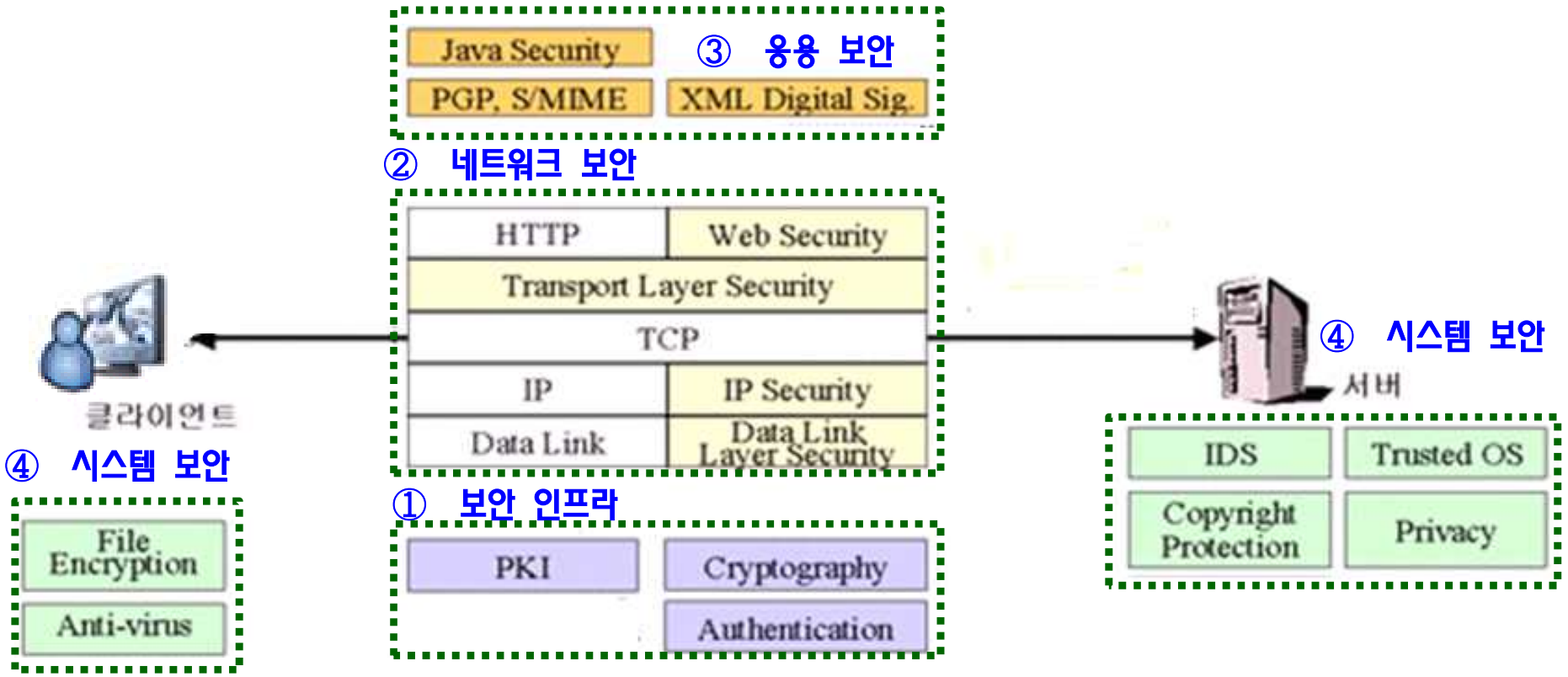
안동대학교
ANDONG NATIONAL UNIVERSITY

IPSec 목차

- 인터넷 보안 프로토콜의 구조
- IP 보안 프로토콜의 서비스
- 보안 연계
- 보안 데이터베이스
  - 보안정책 데이터베이스
  - 보안연계 데이터베이스
- IP 보안 프로토콜의 송신 및 수신 처리

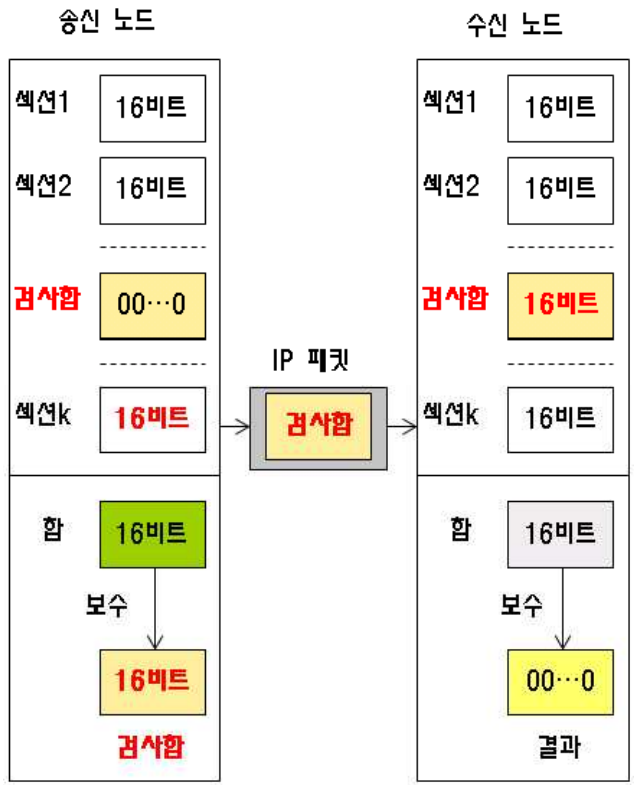
보안기법의 계층 구조

- 응용 보안: S/MIME(Secure/Multipurpose Internet Mail Extensions), PGP, XML 보안, …
- 네트워크 보안: SSL/TLS, IP 보안, 데이터링크 보안, …
- 시스템 보안: 파일 암호화, 앤티 바이러스, IDS(침입탐지시스템), 신뢰성 있는 OS, …
- 보안 인프라: PKI(Public Key Infrastructure), 암호학, 전자서명, …



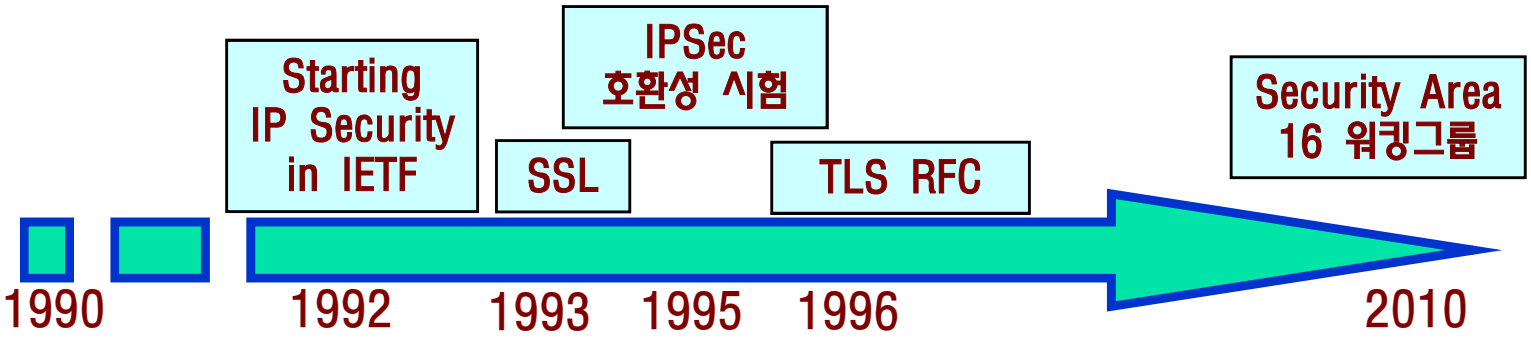
인터넷 프로토콜의 보안 취약성

- 데이터의 신뢰성 있는 전달을 염두에 두고 설계된 인터넷 프로토콜의 보안 취약성
  → 1970년대에는 보안이 중요한 고려 대상이 아니었음
  - IP 주소 및 패킷 내용의 변조, 패킷의 재 전송, 패킷 내용의 훔쳐보기, …
- 헤더 검사합 필드: IP 헤더의 손상 여부를 검사
  - 계산의 용이성에 의한 서비스 거부 공격: 16비트의 덧셈 및 보수 계산
    - 스머프 공격, LAND 공격, UDP 홍수(flood),
    - 과도한 TCP Syn 공격, …

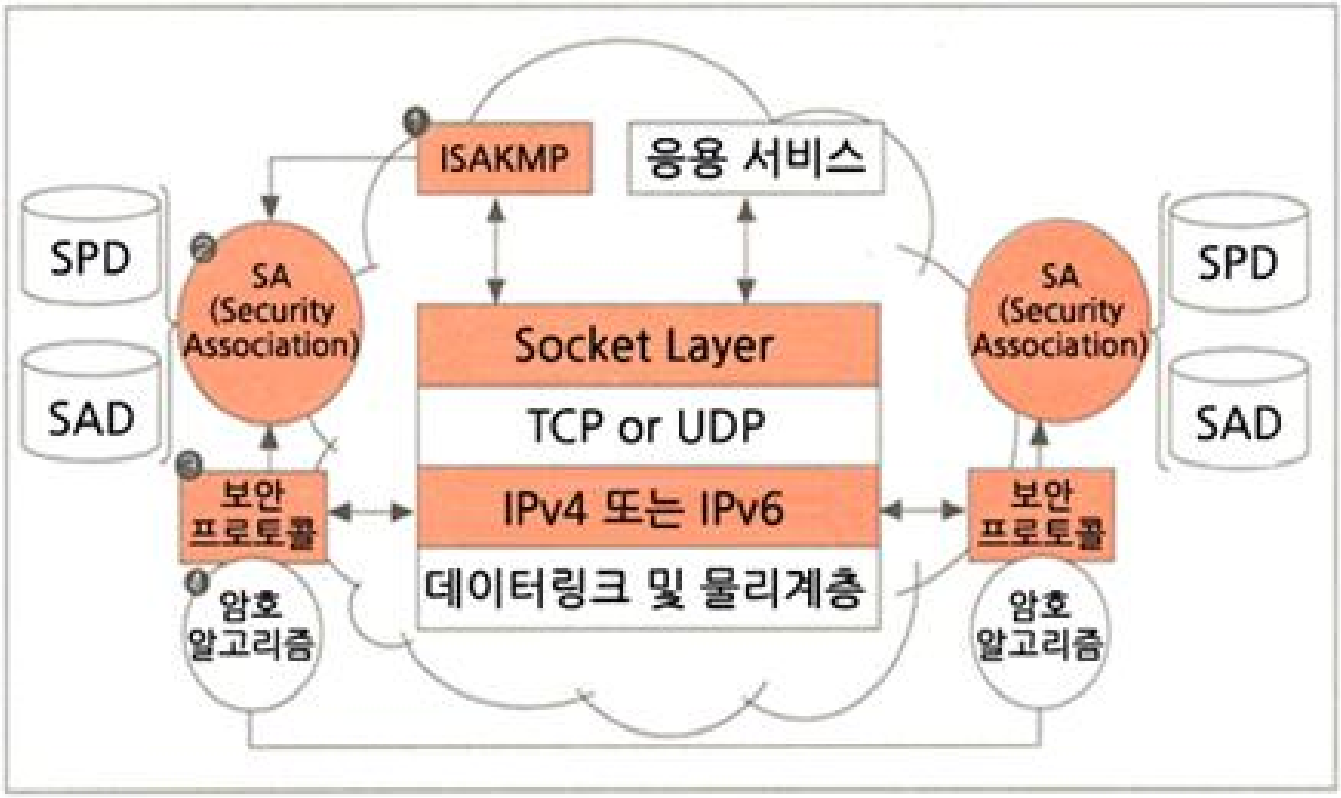


인터넷 보안 프로토콜

- 인터넷 프로토콜의 취약성을 해결하기 위하여 보안 프로토콜 개발
- IP 보안(IPSec)
  - 키관리(ISAKMP), 인증헤더(AH), 캡슐화 보안 페이로드(ESP) 및 압축 프로토콜
- SSL(Secure Socket layer)
  - 1993년 웹 서버와 브라우저 사이의 안전한 통신을 위하여 Netscape 사에서 개발
  - 주요기능: 서버/클라이언트 인증, 기밀성 보장
  - 지원 프로토콜: HTTPS(443), TELNETS(992), POPS(995) 등
- TLS(Transport Layer Security)
  - SSL을 기반으로 1996년 IETF가 TLS 표준화(SSL3.1)



인터넷 보안 프로토콜의 구조



ISAKMP: Internet Security Association Key Management Protocol
SAD: Security Association Database
SPD: Security Policy Database

IP 보안 프로토콜의 서비스와 구현

- IP 보안 프로토콜(IPSec)이 제공하는 보안 서비스
  - 인증코드를 이용한 IP 패킷의 무결성과 인증 기능 제공 → IP 주소 및 패킷의 위조 방지
  - 암호화를 통한 IP 패킷의 기밀성 제공
  - 재전송되어 수신된 IP 패킷의 감지 및 폐기

- 네트워크 계층에서 제공되므로 전송 계층 및 모든 응용 서비스들이 IP 보안 프로토콜의 보안 서비스를 사용할 수 있음

- IP 보안 프로토콜의 구현
  - IP 버전 4: 기존 IP 계층 아래에 IPSec을 추가적으로 구현하여 보안 기능 제공
  - IP 버전 6: 인터넷의 보안 문제를 근본적으로 해결하기 위하여 IP 계층의 확장 헤더에 보안 기능 구현
    - 인증 헤더: 인터넷 보안 프로토콜의 인증 기능
    - ESP 헤더: 인터넷 보안 프로토콜의 암호화 기능

IP 보안 프로토콜의 개요

- 키 관리 프로토콜(ISAKMP)
  - 인증과 암호화에 필요한 알고리즘 선택 및 키의 생성과 분배
- AH 및 ESP 프로토콜
  - 인증 헤더(AH) 프로토콜: 패킷의 근원에 대한 인증과 전송 중에 변조되지 않았음을 보장하는 무결성 서비스 제공
  - 캡슐화 보안페이로드(ESP) 프로토콜: IP 패킷의 기밀성 제공을 위한 암호화 기능과 무결성 및 인증 기능 제공
  - 보안 알고리즘
    - 인증 및 무결성 서비스: HMAC-MD5, HMAC-SHA-1
    - 기밀성 서비스: 3DES-CBC, AES-CBC
- IP 압축(IPComp) 프로토콜
  - IP 보안 프로토콜의 사용으로 증가되는 IP 패킷의 길이를 감소시켜 대역폭 사용의 효율성을 높임

보안연계

- 보안연계 (SA: Security Association): IP 보안 프로토콜, 프로토콜의 운용 모드, 보안 알고리즘, 보안 키와 키의 수명 등에 대한 통신 쌍방 간의 합의
- 키 관리 프로토콜(ISAKMP)은 보안연계의 설정 및 해제 기능 담당
- 각 호스트는 송신과 수신 트래픽을 위하여 별도의 보안연계 설정
- 보안연계의 종류:
  - 인증헤더(AH) 보안연계
  - 캡슐화 보안 페이로드(ESP) 보안연계
  - 압축(IPComp) 보안연계

보안연계의 운영 모드(1/2)

❑ 트랜스포트 모드

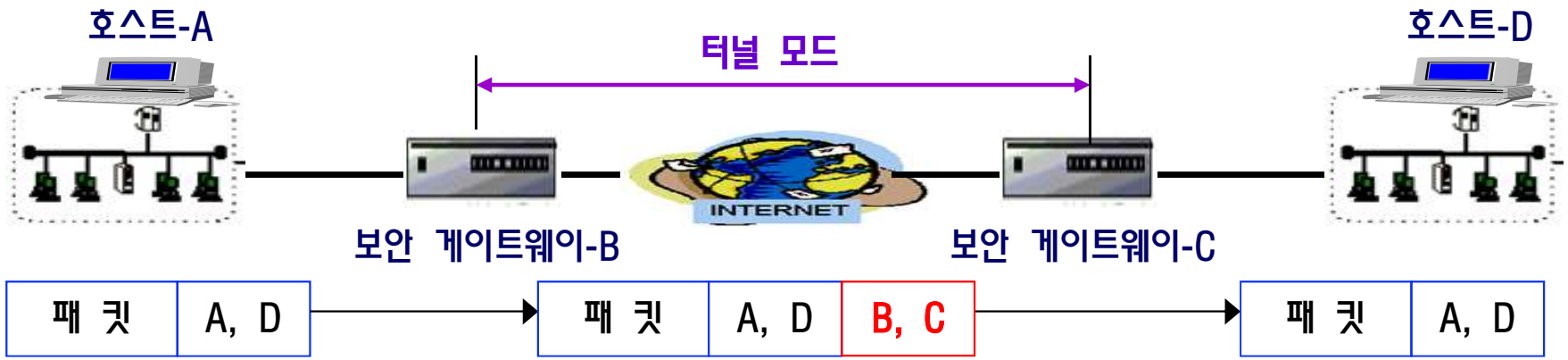
- 호스트와 호스트 간의 보안연계
- 원래 IP 헤더의 발신지 및 목적지 주소를 그대로 유지

❑ 터널 모드

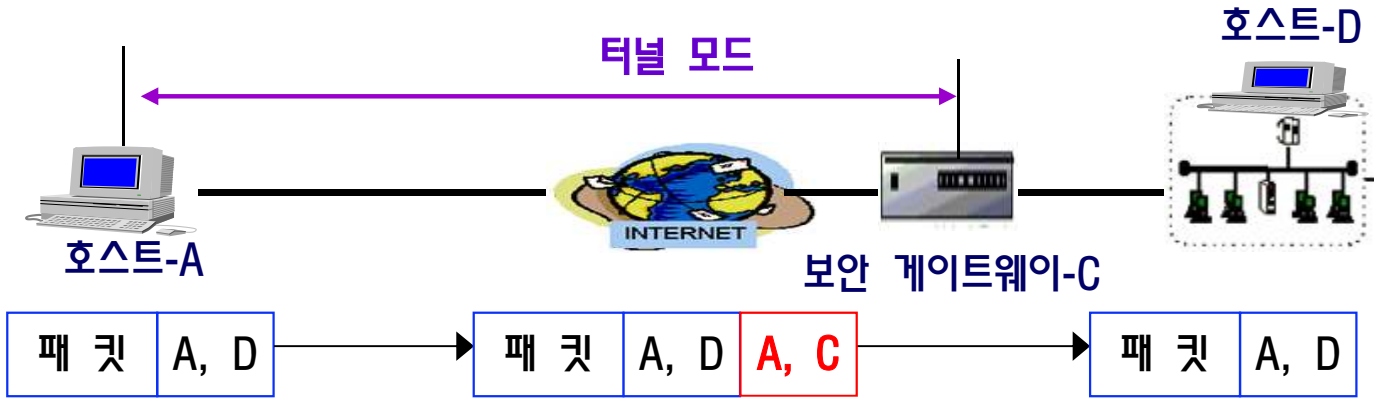
- 적용 구간: 보안 게이트웨이와 보안 게이트웨이 사이 또는 호스트와 보안 게이트웨이 사이
- 로컬 네트워크의 호스트들을 대신하여 보안 게이트웨이에 IPSec 프로토콜 구현
- 새로운 IP 헤더를 만들어 원래의 IP 패킷을 모두 페이로드화 함

보안연계의 운영 모드(2/2)

❑ 보안 게이트웨이와 보안 게이트웨이 사이의 터널



❑ 호스트와 보안 게이트웨이 사이의 터널



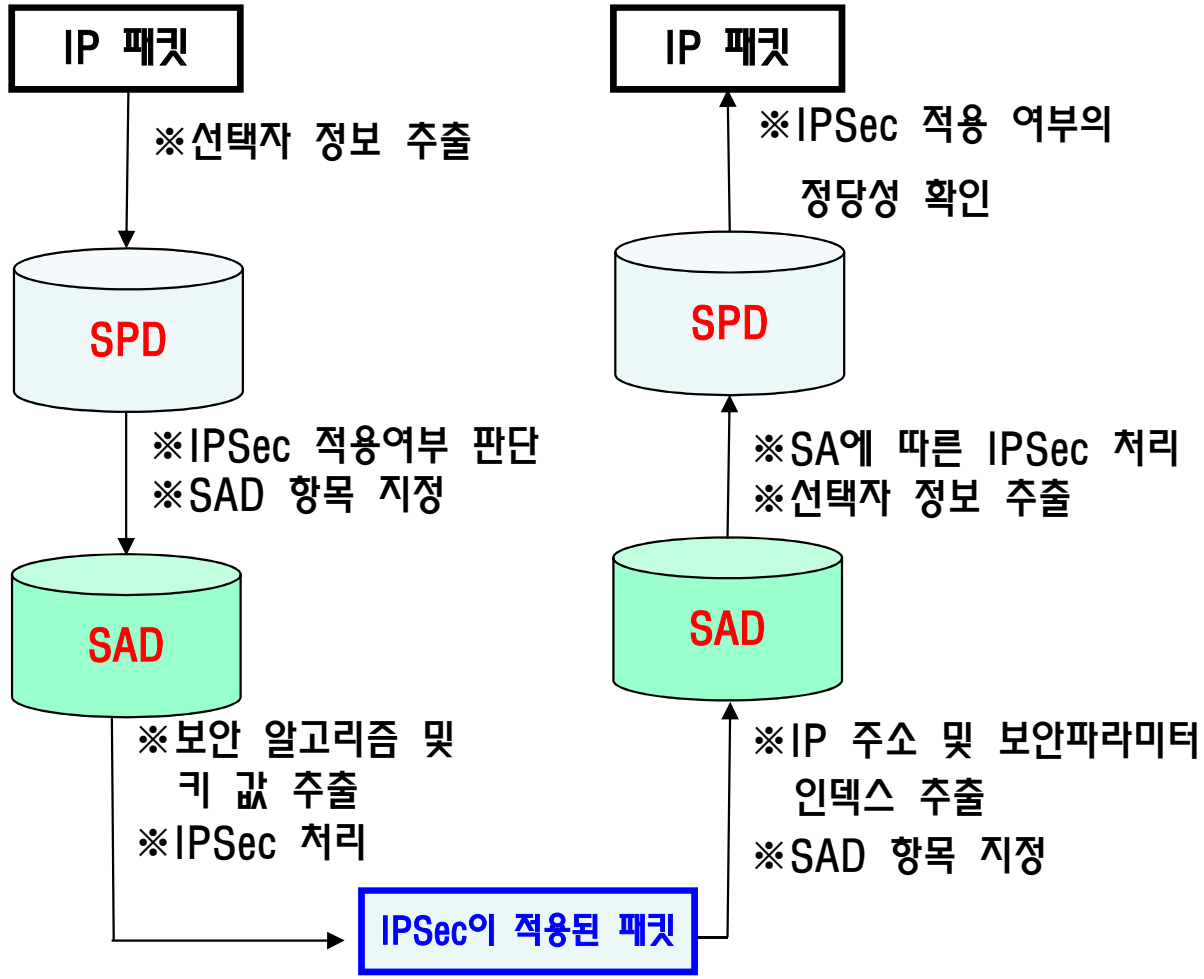
보안 데이터베이스

❑ 보안정책 데이터베이스(SPD)

- IP 패킷의 선택자 정보(IP 주소 또는 포트 번호)를 이용하여 송.수신할 IP 패킷에 IPSec의 적용 여부 판단
- 패킷에 IPSec을 적용하는 경우 보안연계 데이터베이스(SAD)의 관련 항목 지정

❑ 보안연계 데이터베이스(SAD)

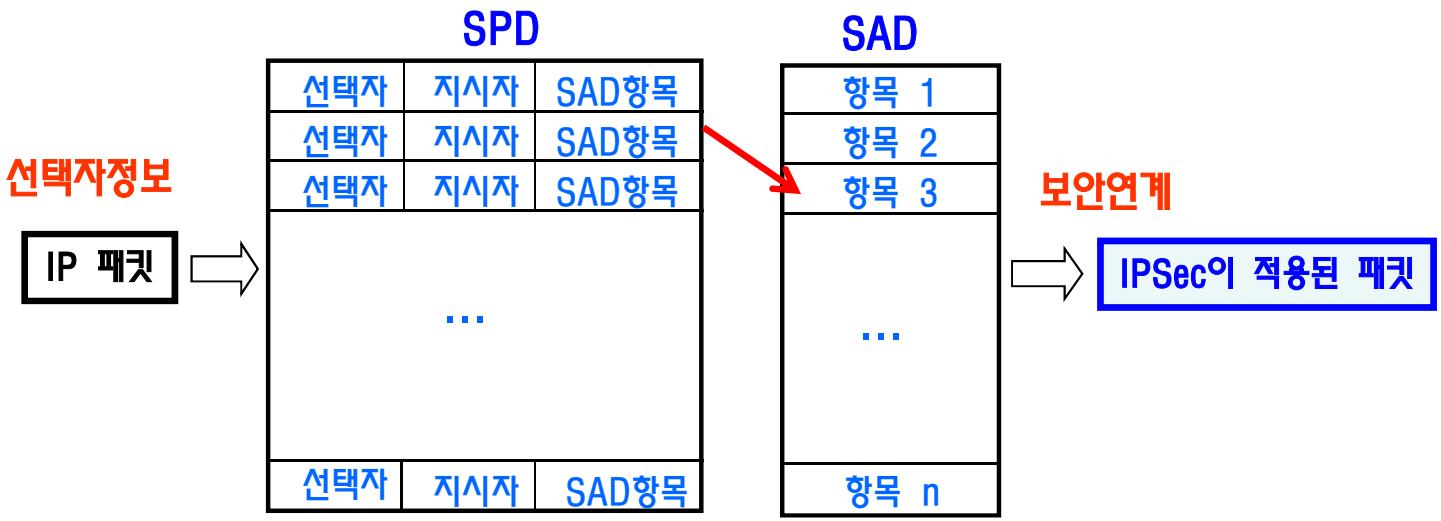
- 보안연계와 관련된 암호 및 인증 알고리즘과 키 값 등의 매개변수 저장



SAD: Security Association Database
SPD: Security Policy Database

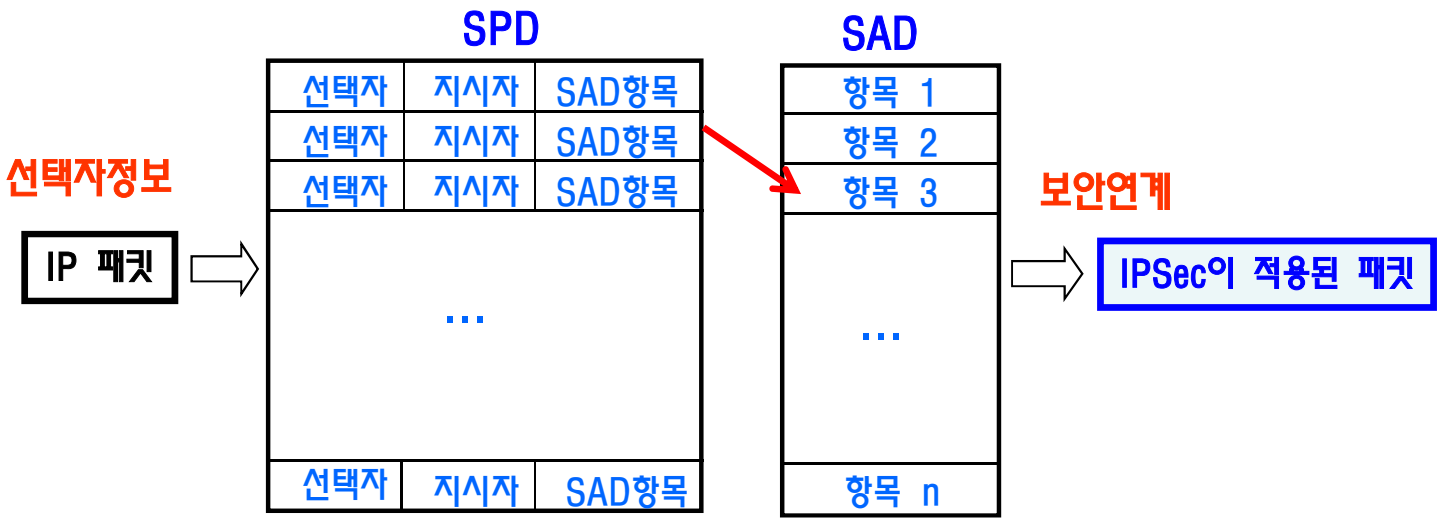
보안정책 데이터베이스(SPD)

- IP 패킷에 IPSec의 적용 여부를 결정하기 위하여 하나 이상의 선택자 정보를 이용
  - 발신지 및 목적지 IP 주소
  - 전송 계층 프로토콜의 종류: TCP 또는 UDP
  - 포트 번호
  - 시스템 이름, 사용자 ID, DNS 이름, 전자우편 주소, X.500 고유명
- 지시자: 선택자들과 일치하는 IP 패킷의 폐기, 통과 또는 IPSec 처리를 지시
- IPSec 처리가 요구되는 경우 보안연계 데이터베이스의 관련 항목을 지정



보안연계 데이터베이스(SAD)

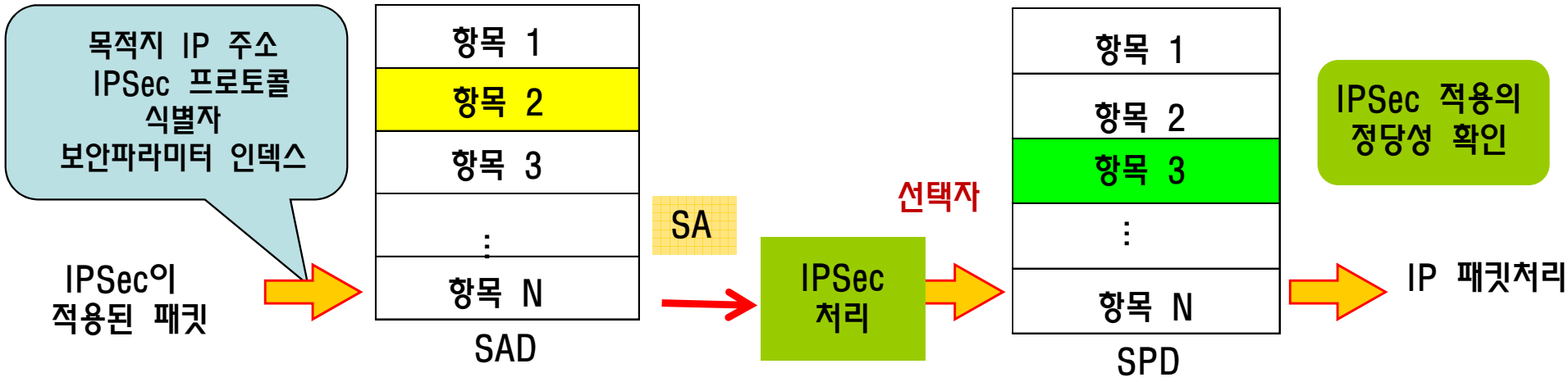
- 각 항목은 IPSec에 적용할 보안연계를 나타냄
  - 인증 알고리즘과 인증 키
  - 암호 알고리즘과 암호 키
  - 보안연계의 수명
  - IPSec 프로토콜의 동작모드(터널 모드, 트랜스포트 모드), …
- 보안연계 데이터베이스 항목의 인덱스: 보안파라미터 인덱스, 목적지 IP주소, IPSec 프로토콜 식별자(AH 또는 ESP)



IP 보안 프로토콜의 송신 및 수신 처리

❑ IP 보안 프로토콜의 송신 처리

❑ IP 보안 프로토콜의 수신 처리



IPSec 요점정리(1/2)

- IP 보안 프로토콜이 제공하는 서비스
  - 인증코드를 이용한 IP 패킷의 무결성과 인증 기능 제공 → IP 주소 및 패킷의 위조 방지
  - 암호화를 통한 IP 패킷의 기밀성 제공
  - 재전송되어 수신된 IP 패킷의 감지 및 폐기

- IP 보안 프로토콜
  - 키 관리 프로토콜(ISAKMP): 인증과 암호화에 필요한 알고리즘 선택 및 키의 생성과 분배
  - 인증 헤더(AH) 프로토콜: 패킷의 근원에 대한 인증과 전송 중에 변조되지 않았음을 보장하는 무결성 서비스 제공
  - 캡슐화 보안 페이로드(ESP) 프로토콜: IP 패킷의 기밀성 제공을 위한 암호화 기능과 무결성 및 인증 기능 제공
  - IP 압축(IPComp) 프로토콜: IP 보안 프로토콜의 사용으로 증가되는 IP 패킷의 길이를 감소시켜 대역폭 사용의 효율성을 높임

- IP 보안 프로토콜의 구현
  - IP 버전 4: 기존 IP 계층 아래에 IPSec을 추가적으로 구현하여 보안 기능 제공
  - IP 버전 6: 인터넷의 보안 문제를 근본적으로 해결하기 위하여 IP 계층의 확장 헤더(AH, ESP)에 보안 기능 구현

IPSec 요점정리(2/2)

- 보안연계(SA: Security Association): IP 보안 프로토콜, 프로토콜의 운용 모드, 보안 알고리즘, 보안 키와 키의 수명 등에 대한 통신 쌍방 간의 합의
  - 트랜스포트 모드
    - 호스트와 호스트 간의 보안연계
    - 원래 IP 헤더의 발신지 및 목적지 주소를 그대로 유지
  - 트랜스포트 모드
    - 호스트와 호스트 간의 보안연계
    - 원래 IP 헤더의 발신지 및 목적지 주소를 그대로 유지

- IP 보안 프로토콜의 처리에 필요한 데이터베이스
  - 보안정책 데이터베이스: IP 패킷의 선택자 정보(IP 주소, 프로토콜, 포트번호)를 이용하여 송.수신할 IP 패킷에 IPSec의 적용 여부 판단
  - 보안연계 데이터베이스: 보안연계와 관련된 암호 및 인증 알고리즘과 키 값 등의 매개변수 저장

인증헤더(AH) 프로토콜

담당교수: 차 영욱

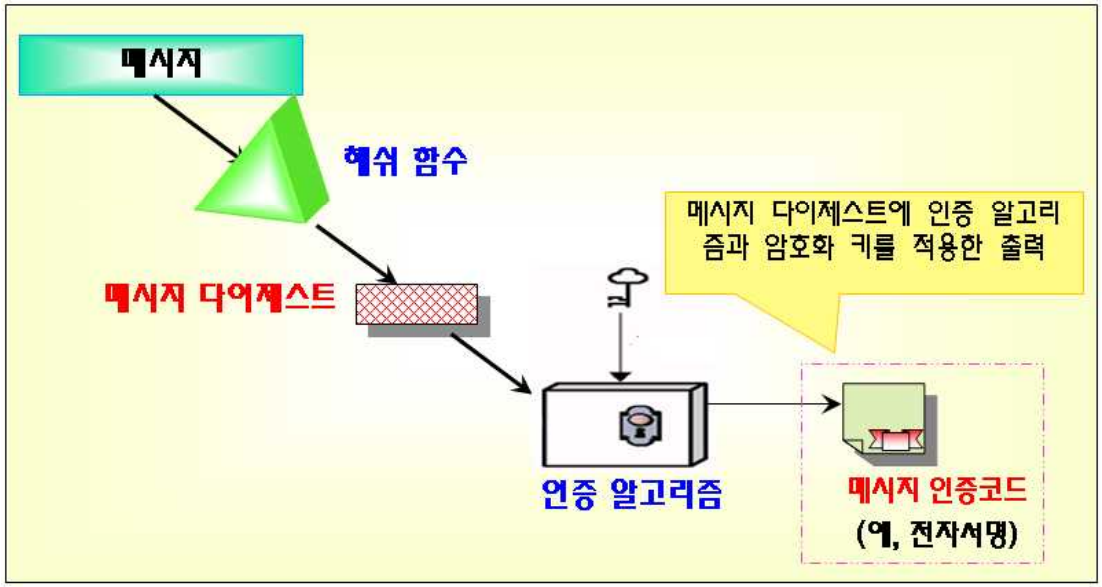
ywcha@andong.ac.kr

AH 목차

- 인증헤더 프로토콜 개요
- 인증헤더 프로토콜의 메시지 형식
- 인증헤더 프로토콜 운영 모드
- IP v4 및 v6에서 인증헤더의 위치
- 무결성 검사값 계산
- 인증헤더 프로토콜의 송신 및 수신 처리

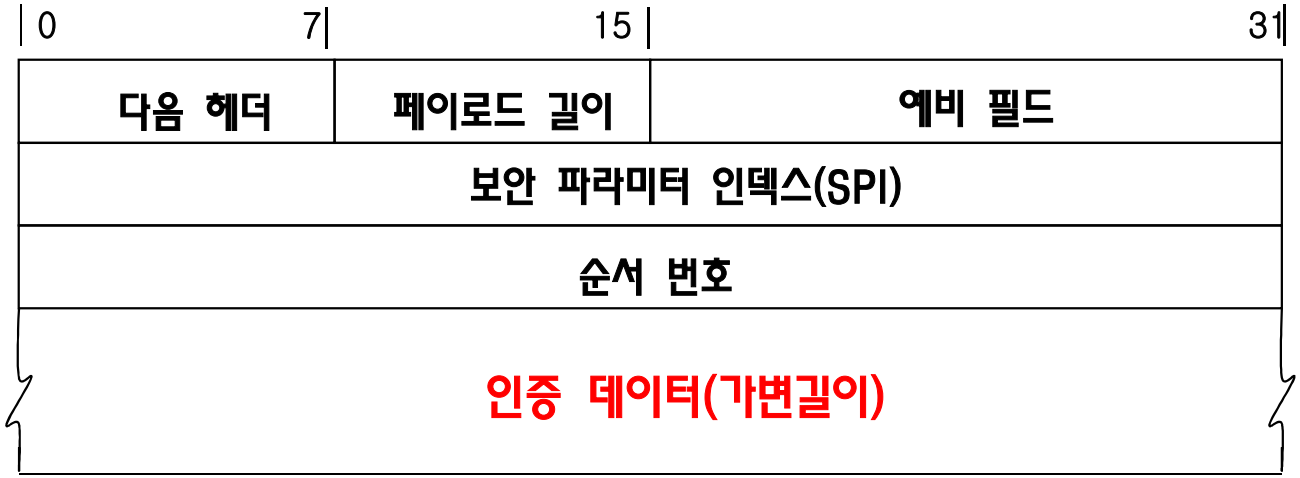
인증헤더 프로토콜 개요

- 인증헤더(AH: Authentication Header) 프로토콜의 보안 서비스
  - IP 헤더 및 패킷 내용의 변조 여부를 확인할 수 있는 무결성 서비스
  - 데이터의 근원지를 식별하는 인증 서비스
  - 공격자에 의한 재전송 패킷의 감지 및 폐기
- 인증헤더 프로토콜은 IP 버전 4의 보안 취약성을 개선하기 위하여 메시지 인증코드 사용
  - IP 버전 4의 보안 취약성: 공격자가 IP 헤더의 필드(예, 송신지 IP 주소)를 변경 후 쉽게 헤더 검사합을 다시 계산하여 수신자에게 전송 가능



인증헤더 프로토콜의 메시지 형식(1/2)

- 다음 헤더: 인증헤더 다음에 오는 페이로드의 유형(예 : ESP, TCP 또는 UDP) 식별
- 페이로드 길이: 인증 프로토콜의 메시지 길이
- 예비 필드: 0으로 설정
- 보안 파라미터 인덱스(SPI: Security Parameter Index)
  - 목적지 IP 주소와 함께 보안연계 데이터베이스의 보안연계를 구분하는 인덱스



인증헤더 프로토콜의 메시지 형식(2/2)

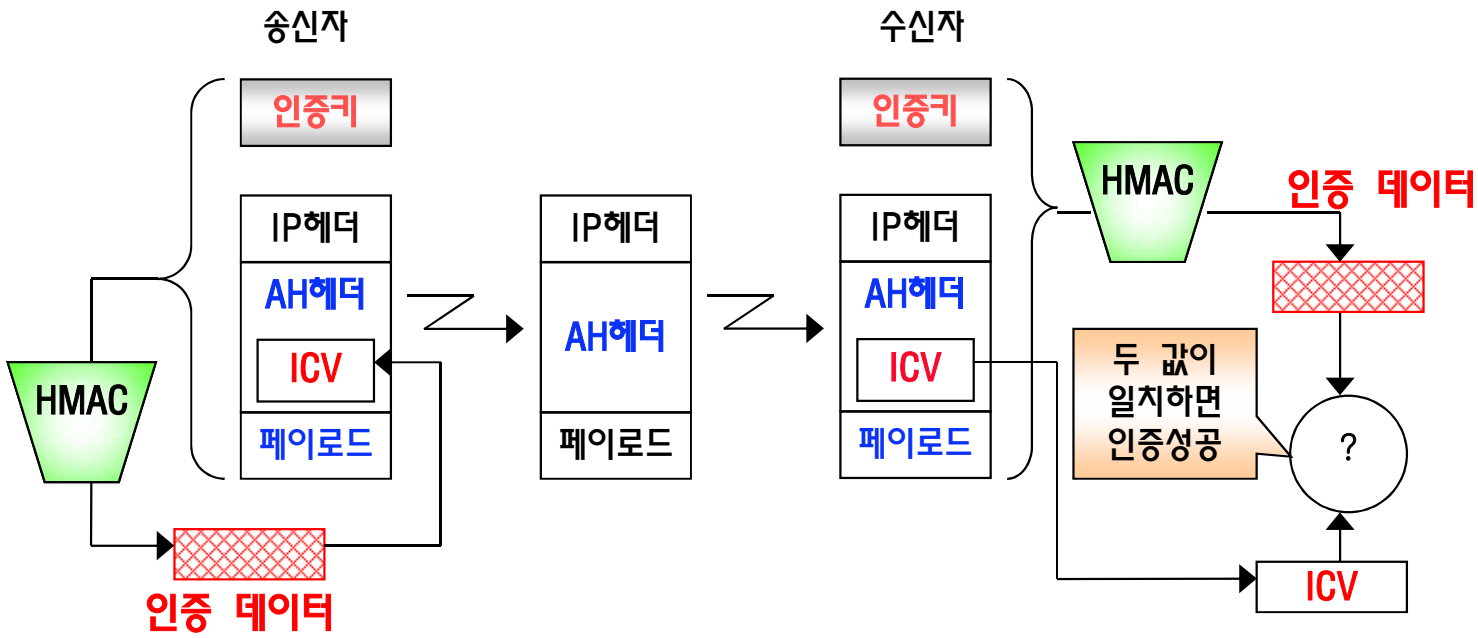
❑ 순서번호

- 송신측과 수신측은 보안연계 설정 시에 순서번호를 0으로 초기화
- 패킷의 송신 시에 순서번호를 1씩 증가
- 수신자는 순서번호를 체크함으로 공격자에 의한 재전송 패킷 감지
- 하나의 보안연계에 대해 순서 번호의 재사용은 허용되지 않음. 즉, 2^{32}개(약 40억개)의 패킷이 전송되기 전에 새로운 보안연계가 협상되어야 함

❑ 인증 데이터

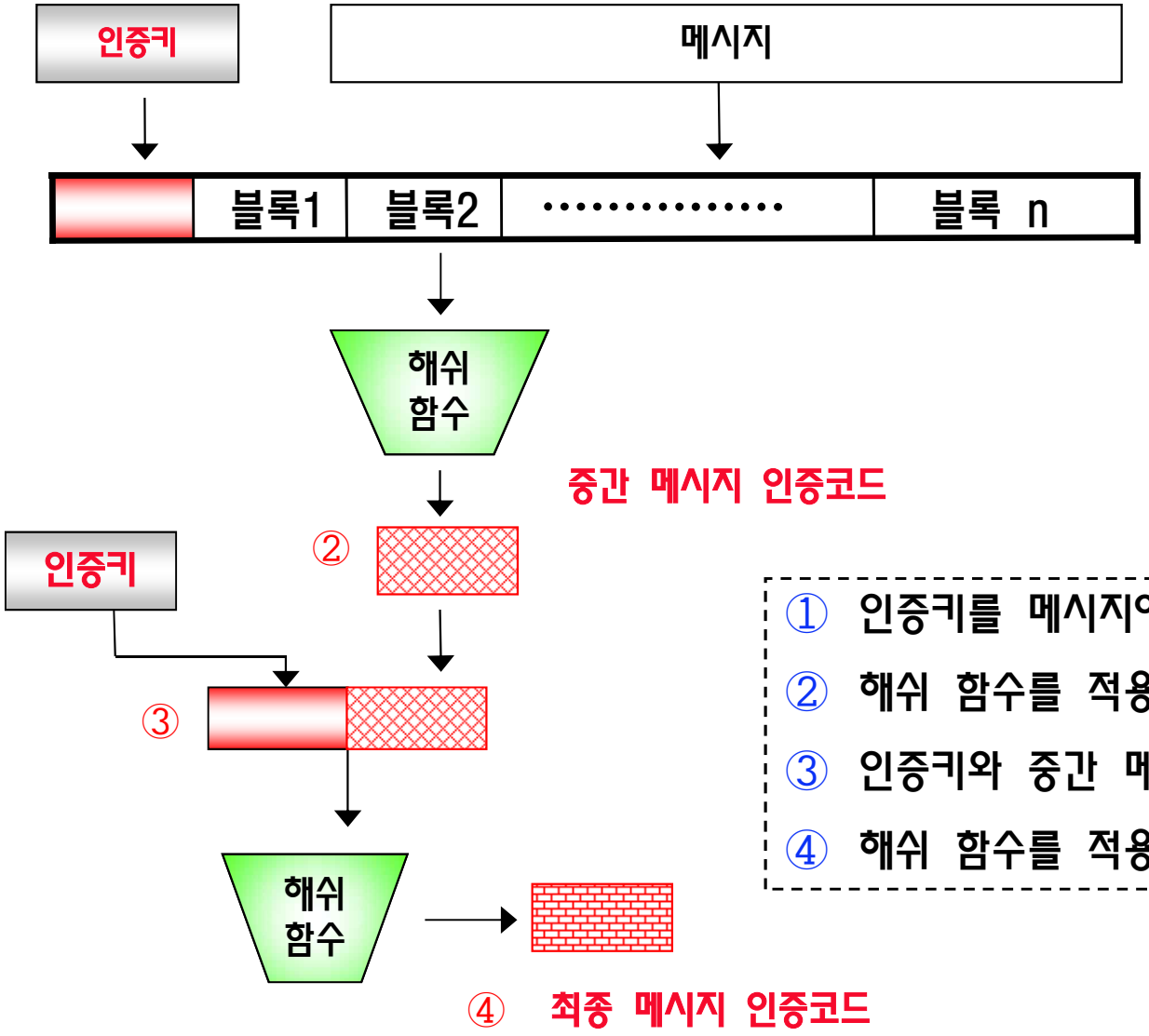
- 무결성 검사 값(ICV: Integrity Check Value)을 포함
- ICV의 생성에 이용되는 알고리즘은 보안연계에 정의되어 있음
- 인증헤더 프로토콜에 필수적인 메시지인증 알고리즘
  - HMAC-MD5와 HMAC-SHA-1, AES-XCBC-MAC

인증 데이터의 생성 및 검증



① 송신자는 인증키를 메시지에 추가하여 HMAC 알고리즘의 수행 결과로 생성된 무결성 검사값을 AH 헤더의 ICV 필드에 세팅
② 생성된 AH를 포함하는 메시지 전송
③ 수신자는 수신된 메시지에 인증키를 추가하여 HMAC 알고리즘 수행
④ 생성된 무결성 검사값과 AH 헤더의 ICV 필드에서 수신한 무결성 검사값이 일치
- 검증된 송신자가 송신한 메시지 임을 인증
- 중간의 공격자에 의하여 메시지가 변조되지 않은 무결성을 보장

HMAC 알고리즘



① 인증키를 메시지에 결합

② 해쉬 함수를 적용하여 중간 메시지 인증코드 생성

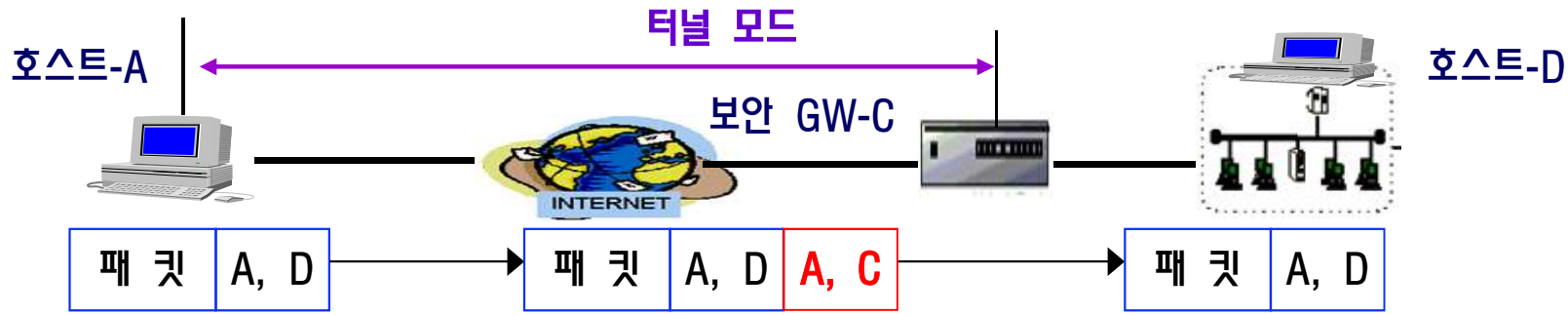
③ 인증키와 중간 메시지 인증코드를 결합

④ 해쉬 함수를 적용하여 최종 메시지 인증코드 생성

AH 운영 모드

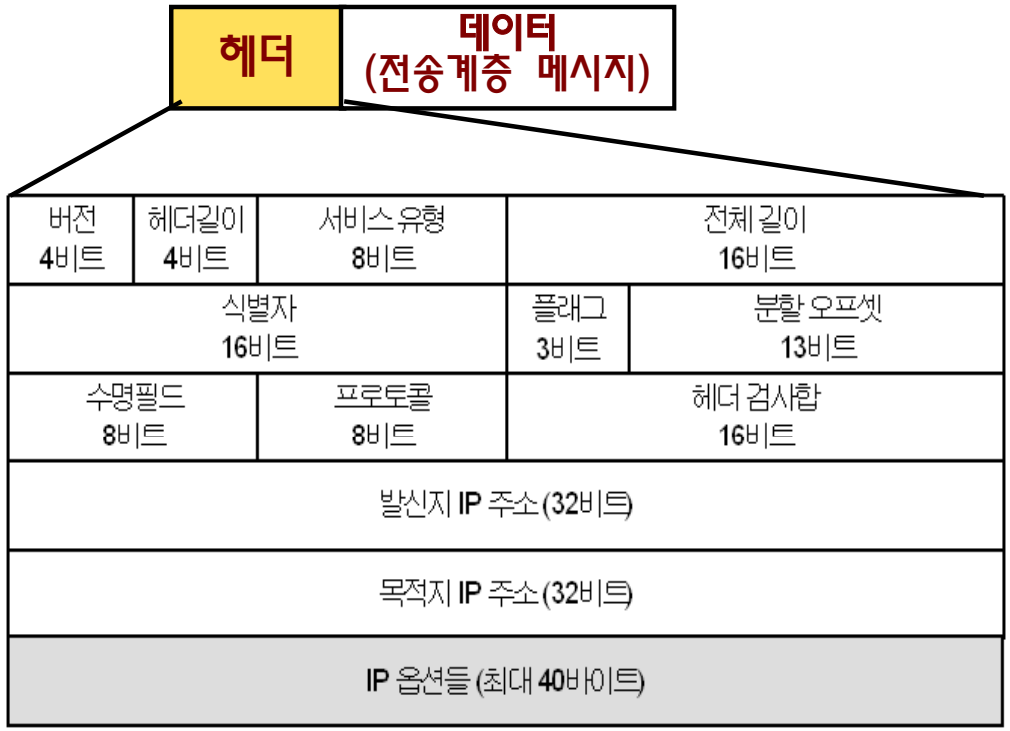
- **트랜스포트 모드:** 원래 IP 헤더의 발신지 및 목적지 주소를 그대로 유지
  - 호스트와 호스트 간의 메시지 인증 및 무결성 제공

- **터널 모드:** 새로운 IP 헤더를 만들어 원래의 IP 패킷을 모두 페이로드화 함
  - 적용 구간: 보안 게이트웨이와 보안 게이트웨이 또는 호스트와 보안 게이트웨이 사이
  - 로컬 네트워크의 호스트들을 대신하여 보안 게이트웨이에 AH 프로토콜 구현



IP v4에서의 인증헤더 위치(1/3)

- IP v4의 패킷 형태
  - 헤더 부분: 20바이트 고정 부분과 가변 길이의 선택사항 부분
  - 데이터 부분: 전송계층(TCP 또는 UDP), ICMP, IGMP, OSPF 메시지



IP v4에서의 인증헤더 위치(2/3)

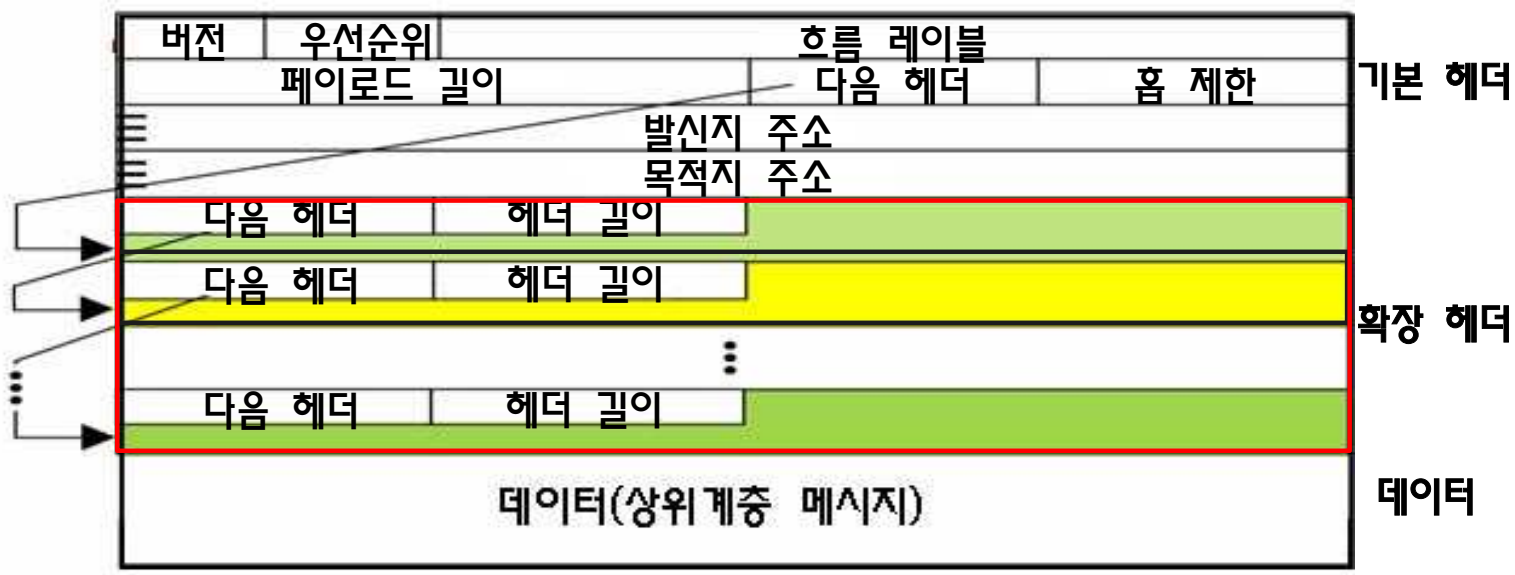
- 트랜스포트 모드에서의 AH 위치
  - IP 헤더의 뒤
  - 다른 IPSec 프로토콜 및 전송 계층 프로토콜의 앞
  - 전체 IP 패킷을 인증

IP v4에서의 인증헤더 위치(3/3)

- 터널 모드에서의 AH 위치
  - AH는 원래 IP 헤더와 새로운 IP 헤더 사이에 위치
  - 새로운 IP 헤더를 포함하여 전체 IP 패킷을 인증

IP v6에서의 인증헤더 위치(1/3)

- IP v6의 패킷 형태: 기본헤더, 선택적인 확장헤더 그리고 데이터로 구성
- 확장헤더
  - AH 확장헤더는 종단에 있는 호스트에서 사용
  - 중간의 라우터들은 경로를 결정하기 위하여 홉대홉 및 발신지 라우팅의 확장헤더 정보를 이용
  - 분할 헤더를 이용하여 분할은 발신지, 결합은 목적지 호스트에서 수행



IP v6에서의 인증헤더 위치(2/3)

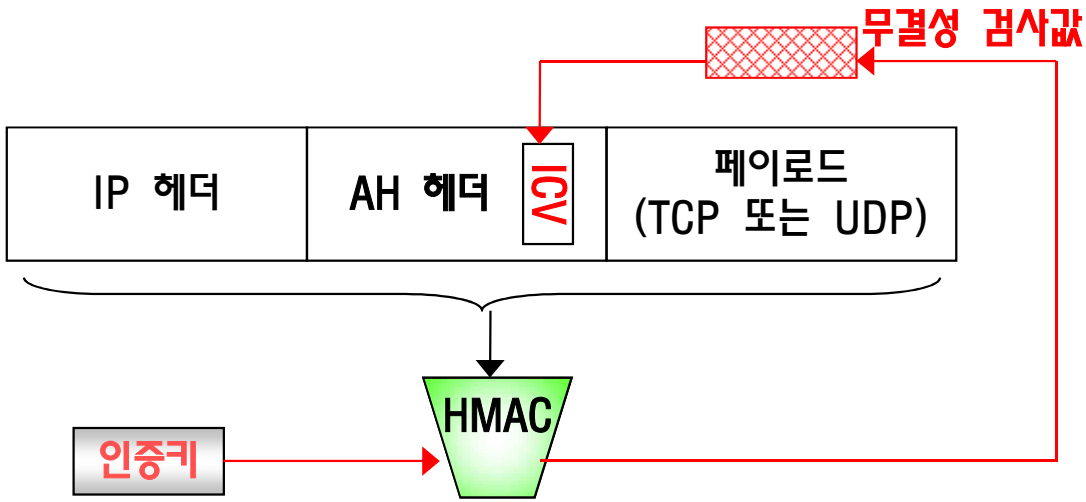
- 트랜스포트 모드에서의 AH 위치
  - 중간 라우터에서 사용되는 확장헤더(홉대홉, 발신지 라우팅 확장헤더) 뒤에 위치
  - 분할 확장헤더 뒤에 위치
    - 발신지에서는 분할 전, 목적지에서는 결합 후의 전체 패킷에 대하여 인증 데이터를 계산하므로 분할된 각각의 패킷에 대한 인증 데이터 계산의 오버헤더 제거

IP v6에서의 인증헤더 위치(3/3)

- 터널 모드에서의 AH 위치
  - 원래 IP 헤더에 있던 확장 헤더들을 AH 앞에 그대로 추가

무결성 검사값 계산

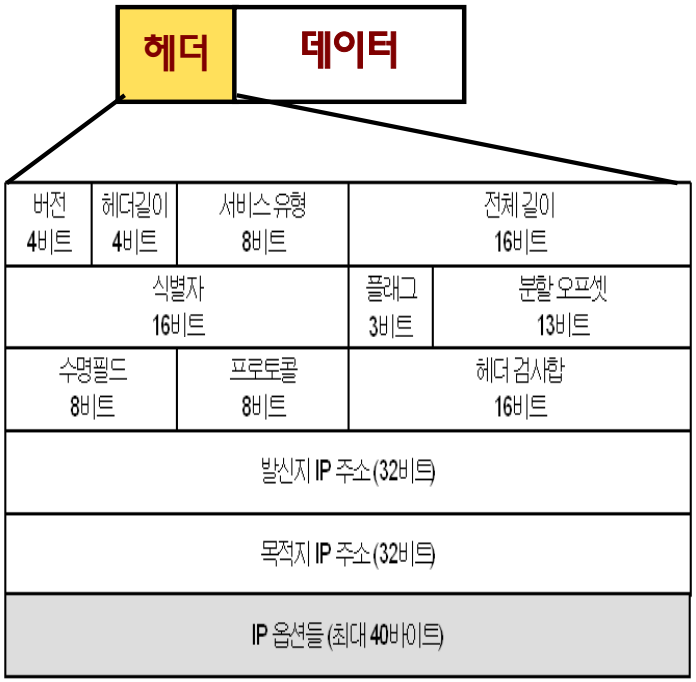
- IP 패킷의 인증 및 무결성 확인을 위해 IP 헤더, AH 헤더 및 페이로드에 대해 ICV 계산
- 목적지로 향하는 중간 라우터에서 변경 가능성이 있는 가변 필드들은 ICV 계산에 앞서 0으로 설정
  - 터널모드의 경우 외부 IP 헤더의 가변 필드들만이 수정되므로, 내부 IP 헤더의 가변 필드들은 0으로 설정되지 않음
- IP 헤더, AH 헤더 및 페이로드들을 인증키와 함께 HMAC 절차에 입력
- 생성된 무결성 검사값을 AH 헤더의 ICV 필드에 세팅



IP v4 헤더의 불변 및 가변 필드

❑ 불변 필드

- 버전, 헤더길이, 전체 길이, 식별자, 프로토콜
- 발신지 IP 주소, 목적지 IP 주소, 데이터(전송 계층 메시지)



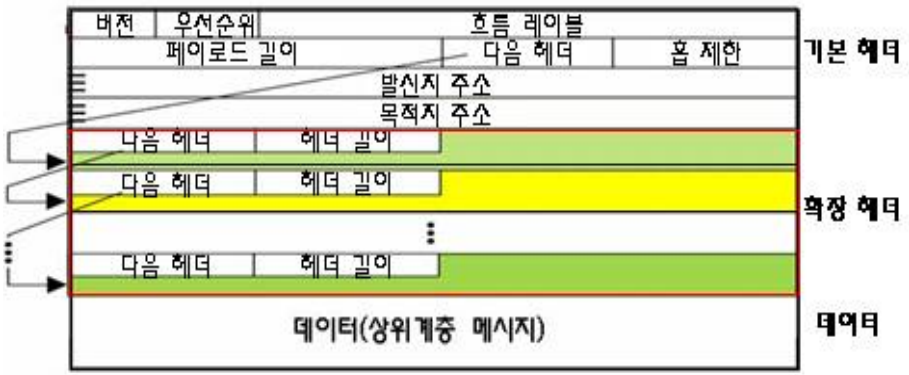
❑ 가변 필드

- **서비스 유형:** 송신자가 네트워크에 요구하는 서비스 유형(지연, 처리율, 신뢰성)
  - IP는 이 필드를 불변 필드로 간주하지만, 일부 제품의 라우터들이 이 필드의 값을 바꾼다고 알려져 있으므로 IPSec에서는 가변 필드로 취급
- **플래그:** 분할 금지 및 마지막으로 분할된 패킷의 여부를 지시하는 플래그
  - 중간 라우터가 분할 금지 플래그를 세팅할 수 있기 때문에 가변 필드로 취급
- **분할 오프셋:** AH는 분할 전의 IP 패킷에 적용되므로 가변 필드로 취급
- **수명:** 라우터를 거칠 때 마다 값이 1씩 감소
- **헤더 검사합:** IP 헤더 부분이 변하면 검사합 값도 변함
- **선택사항 헤더:** 잘 사용되지 않으며, 대부분의 라우터들은 이 필드의 값을 무시
  - IPSec 구현에서는 선택사항 헤더를 가변 필드로 취급

IP v6 헤더의 불변 및 가변 필드

❑ 불변 필드

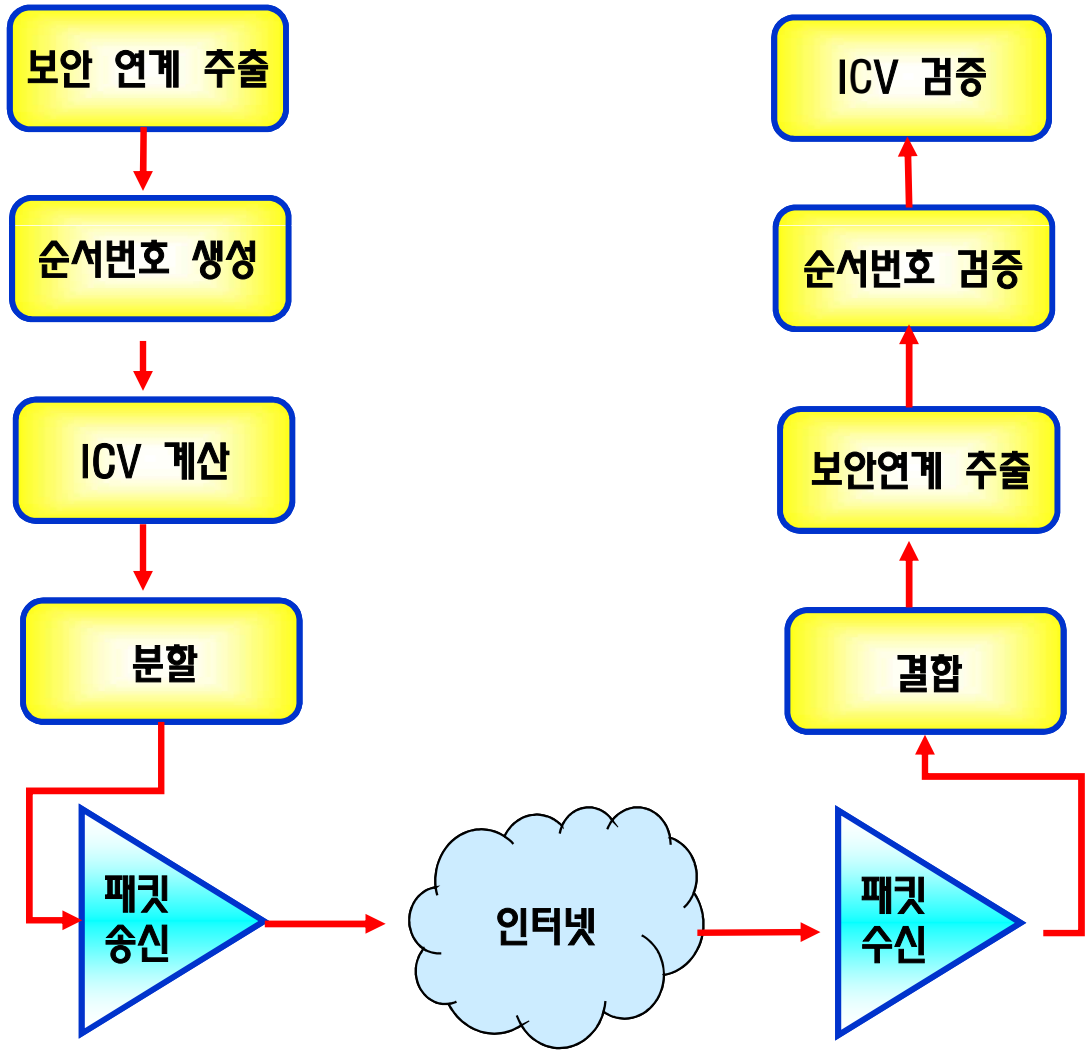
- 버전, 페이로드 길이, 다음 헤더,
- 발신지 주소, 목적지 주소



❑ 가변 필드

- 우선 순위: 중간 라우터들이 변경할 수 있으므로 가변 필드로 취급
- 흐름 레이블: 대부분의 응용에서 현재 이 필드를 무시
  - IPSec에서는 ICV 계산에 앞서 0이 되어야 한다고 규정
- 홉 제한: 라우터를 거칠 때 마다 값이 1씩 감소
- 홉별 확장헤더와 수신지 옵션 확장헤더: 전송 중에 변경될 수 있는지를 참 또는 거짓으로 설정함으로 가변 또는 불변으로 지정
  - 홉별 확장헤더: 패킷의 송신지에서 수신지에 이르는 경로 상의 모든 노드가 검사해야 하는 라우팅 정보를 전달
  - 수신지 선택사항 확장헤더: 수신지 노드에서만 검사될 필요가 있는 선택사항 정보 전달
- 분할 확장헤더: 발신지에서는 분할 전, 목적지에서는 결합 후의 전체 패킷에 대하여 ICV를 계산하므로 ICV 계산 시에 고려 않음

인증헤더 프로토콜의 처리



인증헤더 프로토콜의 송신 처리

- 송신할 IP 패킷의 수신지 IP 주소, 포트, 전송 프로토콜 등의 선택자를 사용하여 보안정책 데이터베이스 검색
- 검색된 보안정책 데이터베이스의 항은 출발용 보안연계 데이터베이스에 있는 보안연계를 지정
- 보안연계가 확립되어 있지 않을 경우, 인터넷 키 교환 프로토콜을 호출하여 보안연계를 협상하고 보안정책 데이터베이스에 연결
- 보안연계를 다음과 같이 인증헤더 프로토콜 처리에 사용
  - ① 순서번호 값을 1만큼 증가
  - ② 무결성 검사값(ICV) 계산
  - ③ 필요하다면 분할하여 패킷을 목적지로 전송

인증헤더 프로토콜의 수신 처리

- 분할된 IP 패킷들의 재조립 후, IP 보안 프로토콜 처리
- 보안파라미터 인덱스, 수신지 IP 주소를 사용하여 보안연계 데이터베이스에서 해당 패킷이 연계된 보안연계 검색
  - 검색에 실패하면 패킷을 폐기하고 이벤트 기록
- 순서번호를 사용하여 패킷의 재전송 여부 확인
  - 재전송된 패킷은 폐기하고 이벤트 기록
- 보안연계에 규정된 메시지 인증 알고리즘을 사용하여 무결성 검사값을 계산하고, 인증 데이터 필드에 저장되어 있는 값과 비교
  - 인증에 실패하면 패킷은 폐기하고 이벤트 기록
- 호스트의 경우는 패킷을 상위 계층으로 전달하며, 보안 게이트웨이인 경우에는 지정된 노드로 전달

AH 요점 정리(1/2)

- 인증헤더 프로토콜의 보안 서비스
  - IP 헤더 및 패킷 내용의 변조 여부를 확인할 수 있는 무결성 서비스
  - 데이터의 근원지를 식별하는 인증 서비스
  - 공격자에 의한 재전송 패킷의 감지 및 폐기
- AH 운영 모드
  - 트랜스포트 모드: 호스트와 호스트 간의 메시지 무결성 제공
    - 새로운 IP 헤더를 포함하여 전체 IP 패킷을 인증
  - 터널 모드: 보안 게이트웨이와 게이트웨이 사이 및 호스트와 보안 게이트웨이 사이에 사용
    - 로컬 네트워크의 각 호스트를 대신하여 보안 게이트웨이에 인증헤더 프로토콜 구현
    - 새로운 IP 헤더를 포함하여 전체 IP 패킷을 인증
- IP v4의 AH 위치
  - 트랜스포트 모드: IP 헤더 뒤, 다른 IPSec 프로토콜 및 전송 계층 프로토콜 앞
  - 터널 모드: 원래 IP 헤더와 새로운 IP 헤더 사이에 위치

AH 요점 정리(2/2)

- 무결성 검사값 계산
  - 목적지로 향하는 중간 라우터에서 변경 가능성이 있는 가변 필드들은 무결성 검사값 계산에 앞서 0으로 설정
  - IP 헤더, AH 헤더 및 페이로드들을 인증키와 함께 HMAC 절차에 입력하여 ICV 계산 → AH 헤더의 ICV 필드에 세팅

- AH 프로토콜의 처리
  - 보안연계 추출 ⇒순서번호 생성 ⇒ 인증 ⇒ 분할 ⇒ 송신
  - 수신 ⇒ 결합 ⇒ 보안연계 추출 ⇒ 순서번호 검증 ⇒ 인증

캡슐화 보안 페이로드(ESP) 프로토콜

담당교수: 차 영욱

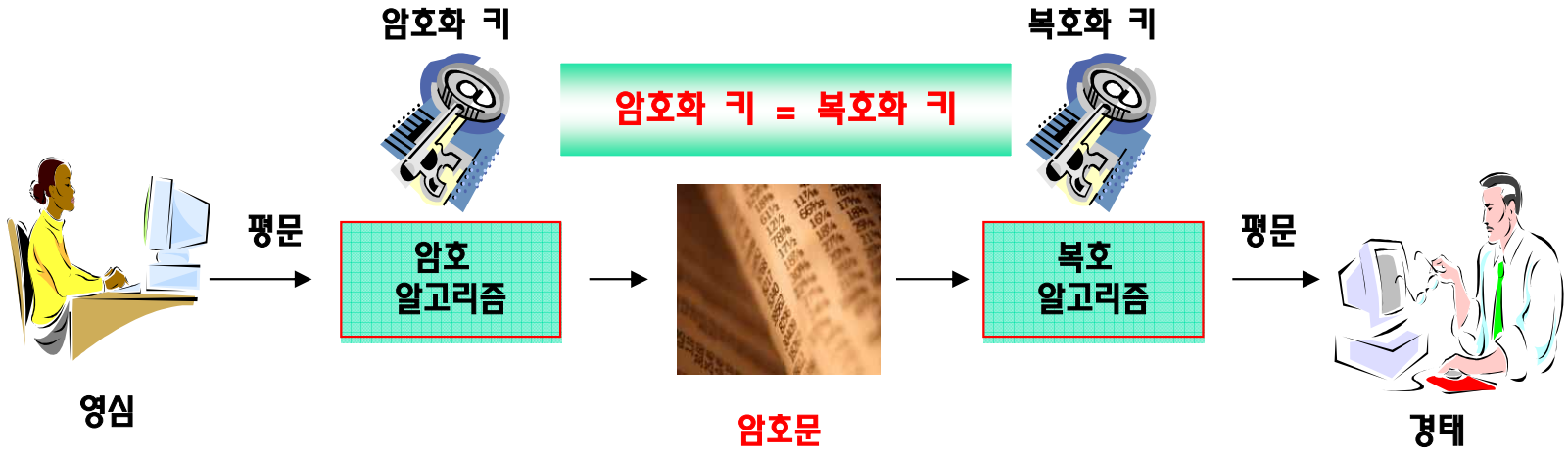
ywcha@andong.ac.kr

ESP 목 차

- 캡슐화 보안페이로드 프로토콜의 개요
- ESP의 보안 알고리즘
- ESP 메시지 형식 및 필드
- ESP 운영모드
- IP v4에서의 ESP 위치
- AH와 ESP의 인증 서비스 비교
- 캡슐화 보안페이로드 프로토콜의 처리

캡슐화 보안페이로드 프로토콜의 개요

- ESP(Encapsulating Security Payload) 프로토콜의 보안 서비스
  - 정당한 사용자 만이 패킷의 내용을 파악하도록 하는 기밀성 서비스
  - 데이터의 근원지를 식별하는 인증 서비스
  - IP 헤더 및 패킷 내용의 변조 여부를 확인할 수 있는 무결성 서비스
  - 공격자에 의한 재전송 패킷의 감지 및 폐기
- 기밀성 서비스를 위하여 암호화에 대칭키 암호 알고리즘 사용
  - 공개키 암호 알고리즘은 계산 시간을 많이 요하는 멱승 연산을 포함
  - 대칭키 암호는 기본 연산인 XOR, AND, 비트 회전 등을 이용하므로 고속처리가 요구되는 IP 보안 프로토콜에 사용



ESP의 보안 알고리즘

- 표준화 문서(RFC 4835): ESP와 AH를 위한 암호 알고리즘의 구현 요구사항, 2007년
- 상호 운용성을 보장하기 위해 규정한 필수구현 암호화 알고리즘
  - NULL 암호화 알고리즘: 암호화를 수행하지 않음을 의미
  - 데이터 암호화 표준(DES)
  - 3 중 DES(3DES-CBC)
  - 128 비트 암호키의 진보된 암호화 표준(AES-CBC)
- 인증 및 무결성 서비스를 위하여 규정한 필수구현 인증 알고리즘
  - NULL 인증 알고리즘: 인증을 수행하지 않음을 의미
  - HMAC-MD5
  - HMAC-SHA-1
  - AES-XCBC-MAC
- NULL 암호화 알고리즘과 NULL 인증 알고리즘은 동시에 이용될 수 없음

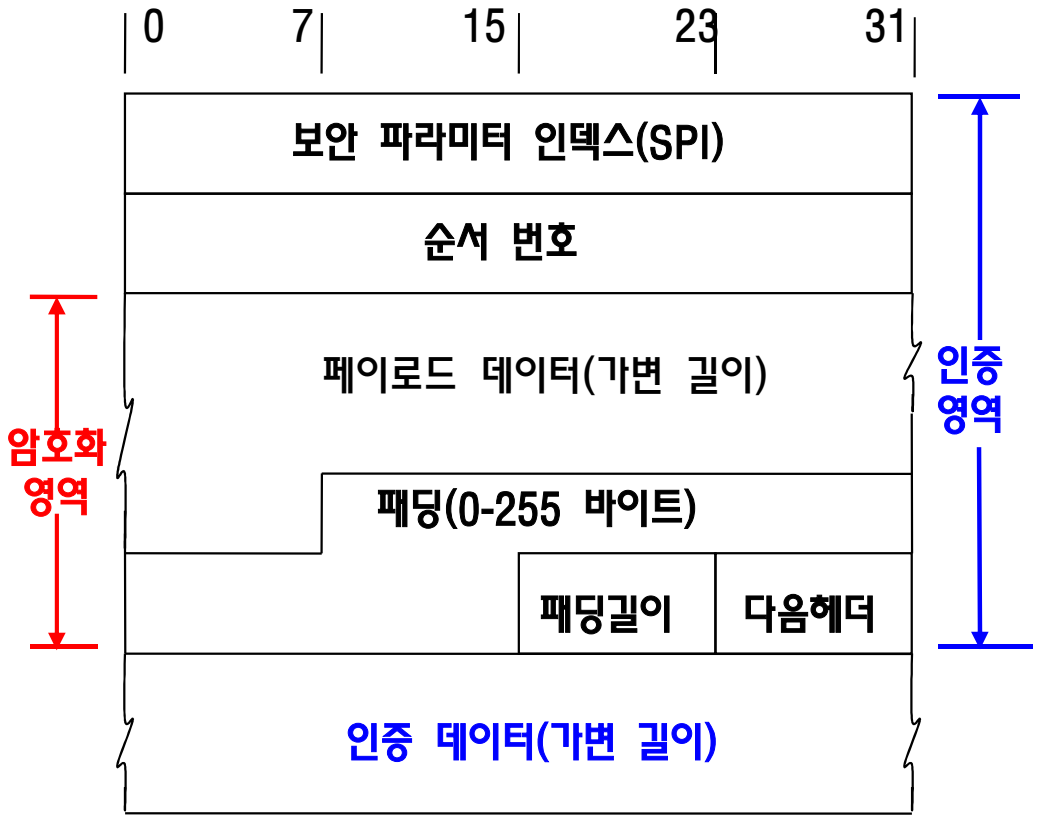
ESP 메시지 형식 및 필드(1/2)

❑ ESP 헤더

- 보안 파라미터 인덱스(SPI): 목적지 IP 주소와 함께 보안연계 데이터베이스의 보안연계를 구분하는 인덱스
- 순서번호
  - 송신측과 수신측은 보안연계 설정 시에 순서번호를 0으로 초기화
  - 패킷의 송신 시에 순서번호를 1씩 증가
  - 수신자는 순서번호를 체크함으로 공격자에 의한 재전송 패킷 감지

❑ 페이로드 데이터

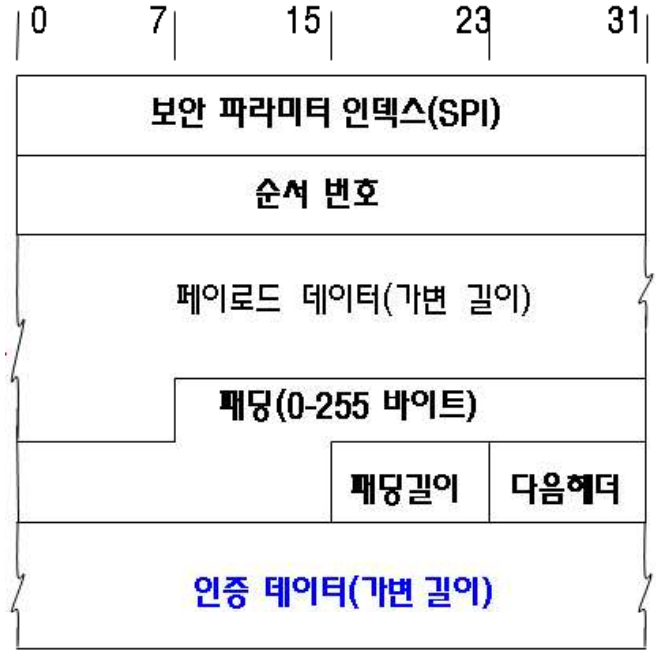
- 상위 계층(TCP 또는 UDP)의 메시지
- 기밀성 서비스가 협상된 경우 페이로드는 암호화 됨



ESP 메시지 형식 및 필드(2/2)

❑ ESP 트레일러:

- 패딩: 암호화 알고리즘이 블록 단위의 평문을 요구하는 경우, 페이로드 데이터를 블록 길이의 배수가 되도록 확장하기 위하여 사용
- 패딩 길이: 패딩 필드의 바이트 길이를 나타내는 필드
- 다음헤더: 페이로드 데이터 필드에 포함되어 있는 데이터의 유형을 식별하는 필드로 전송계층 프로토콜(TCP, UDP) 또는 IPv6 확장헤더를 표시



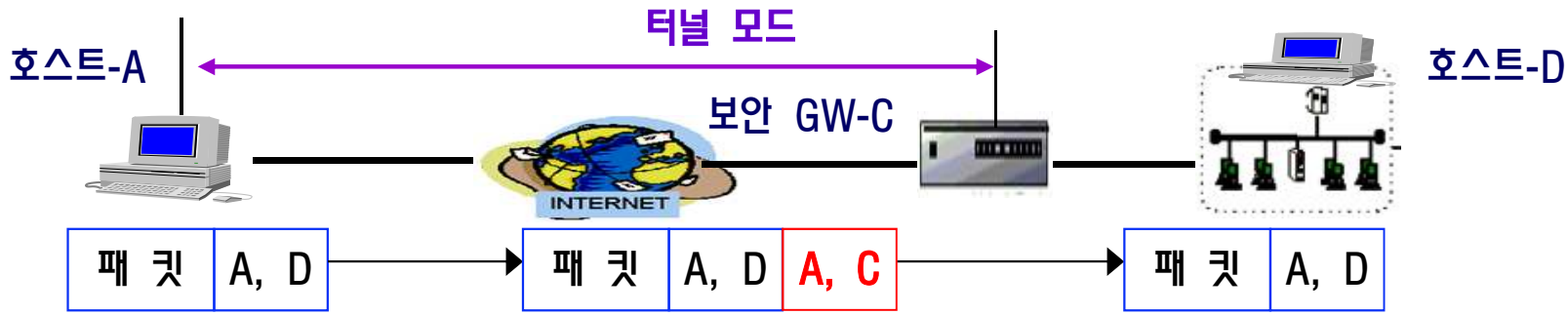
❑ 인증 데이터

- 무결성 검사 값(ICV)을 포함
- ESP 메시지 전체에서 인증 데이터 필드를 제외한 부분에 대해 무결성 검사 값 계산

ESP 운영 모드

- **트랜스포트 모드:** 원래 IP 헤더의 발신지 및 목적지 주소를 그대로 유지
  - 호스트와 호스트 간의 메시지 인증 및 무결성 제공

- **터널 모드:** 새로운 IP 헤더를 만들어 원래의 IP 패킷을 모두 페이로드화 함
  - 적용 구간: 보안 게이트웨이와 보안 게이트웨이 또는 호스트와 보안 게이트웨이 사이
  - 로컬 네트워크의 호스트들을 대신하여 보안 게이트웨이에 ESP 프로토콜 구현

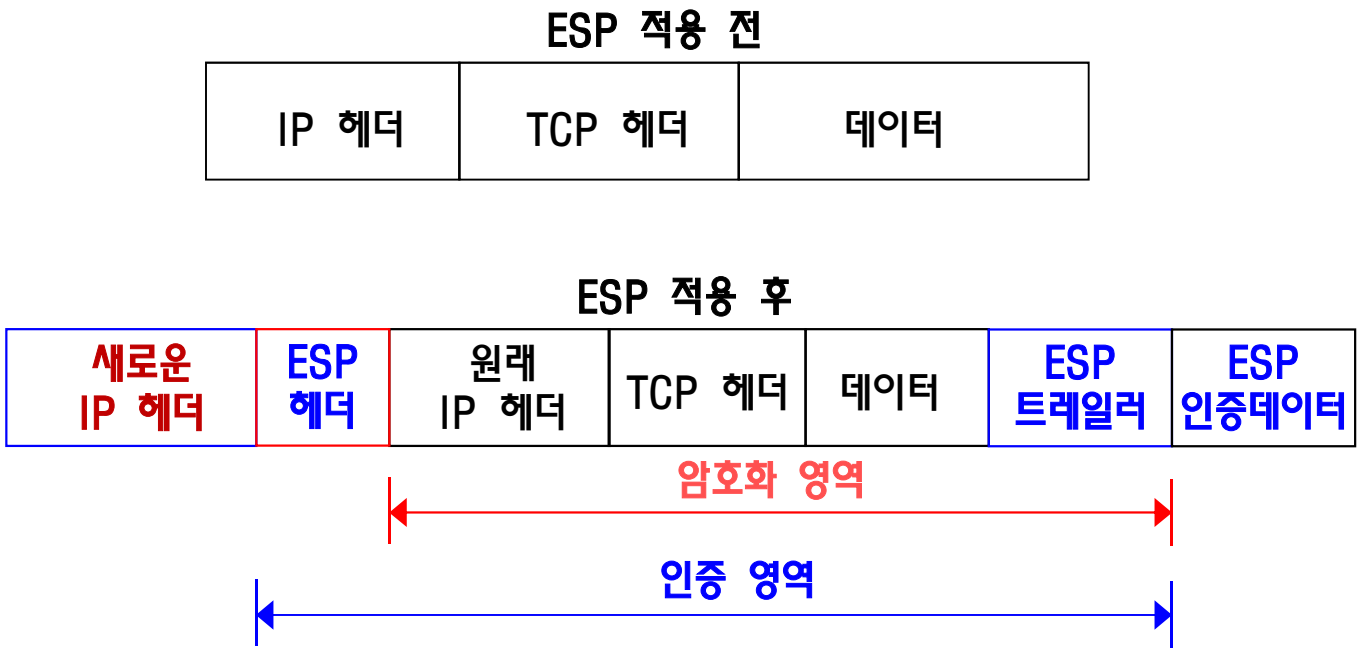


IP v4에서의 ESP 위치(1/2)

- 트랜스포트 모드에서의 ESP 위치
  - ESP 헤더: IP 헤더 뒤
  - ESP 트레일러: 전송계층 프로토콜(TCP, UDP)의 메시지 뒤

IP v4에서의 ESP 위치(2/2)

- 터널 모드에서의 ESP 위치
  - ESP 헤더: 원래 IP 헤더와 새로운 IP 헤더 사이에 위치
  - ESP 트레일러: 전송계층 프로토콜(TCP, UDP)의 메시지 뒤



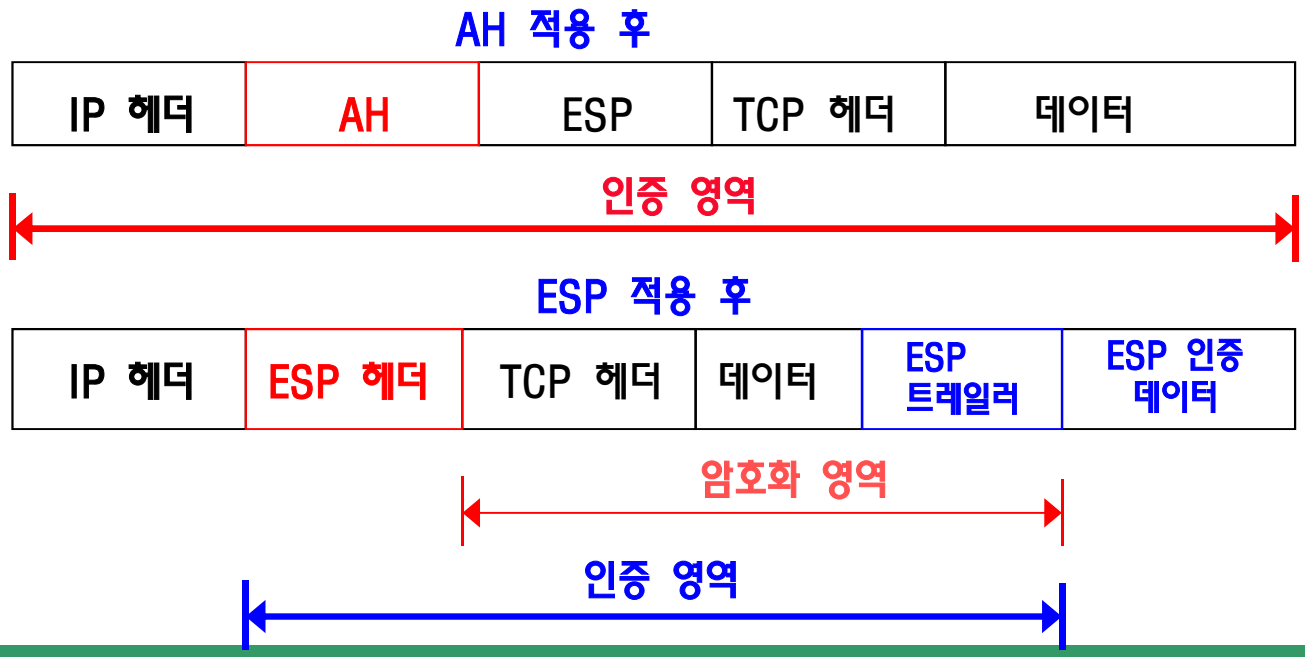
ESP 트랜스포트 모드와 터널 모드 비교

- 터널 모드의 보안 서비스는 트랜스포트 모드에 비하여 높은 보안성을 제공
  - 터널 모드는 새로운 IP 헤더를 제외한 원래의 IP 패킷 전체에 대하여 인증 및 암호화
  - 새로운 IP 헤더가 삽입되므로 터널모드는 트랜스포트 모드에 비해 더 많은 대역폭을 사용

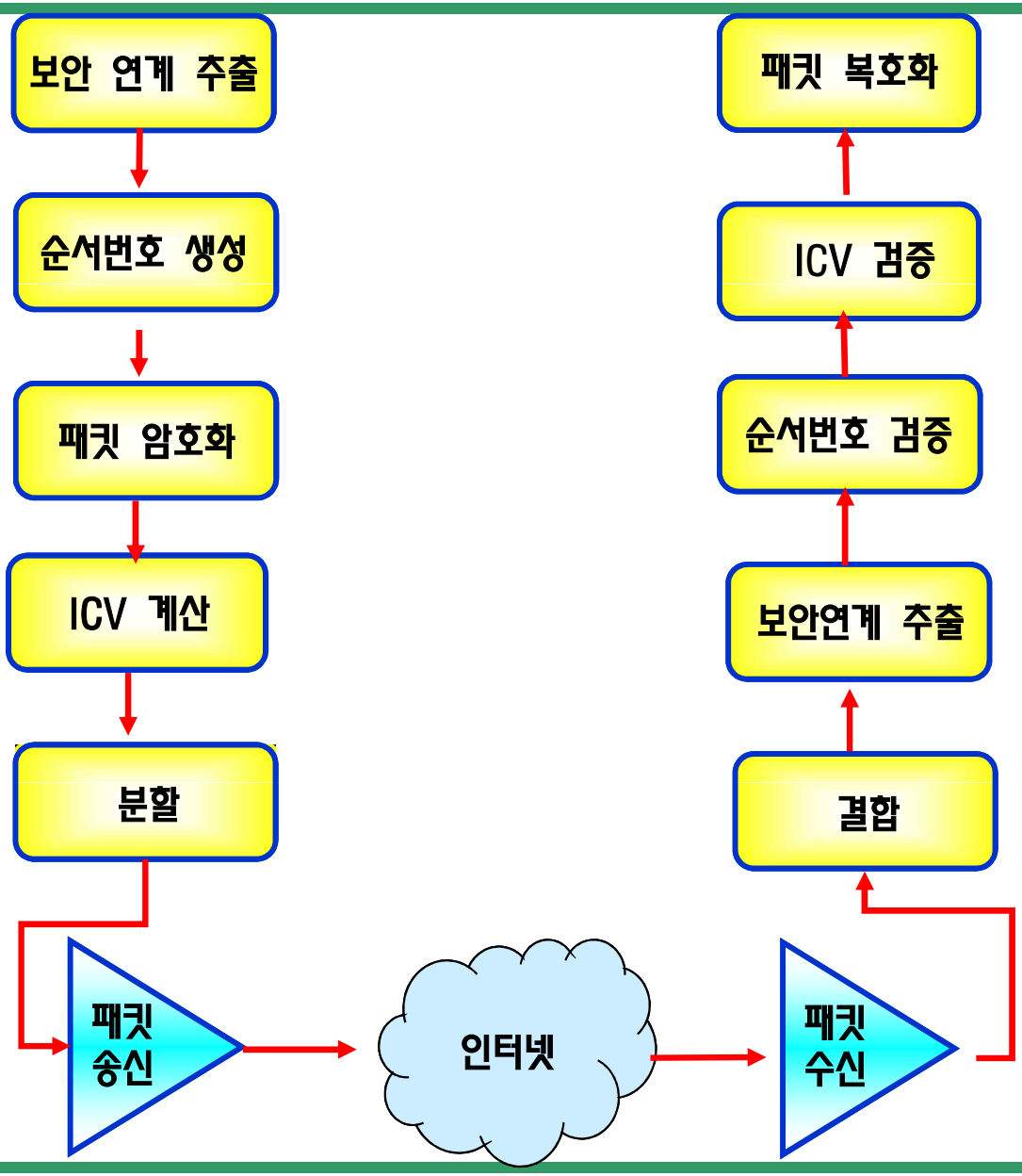
- 보안 게이트웨이에 터널 모드의 기밀성 서비스가 구현될 경우
  - 패킷의 원래 발신지 및 목적지 IP 주소가 있는 원래의 IP 헤더가 암호화되므로 트래픽 흐름의 기밀성 서비스 제공

AH와 ESP의 인증 서비스 비교

- 인증헤더(AH)는 IP 헤더를 포함한 전체 패킷에 대하여 인증 데이터 계산
- ESP는 IP 헤더를 제외한 전체 패킷에 대하여 인증 데이터 계산
  - IP 헤더 필드가 중간에서 변조된 후, 헤더 검사합이 새로 계산된 경우 수신지 노드는 변경을 탐지하지 못함
- 높은 수준의 인증에 대한 보안성이 필요한 경우 IP 헤더를 포함한 전체 패킷을 인증하는 AH 인증 서비스 이용



ESP 프로토콜의 처리


보안 연계 추출
순서번호 생성
패킷 암호화
ICV 계산
분할
패킷 송신
인터넷
패킷 수신
결합
보안연계 추출
순서번호 검증
ICV 검증
패킷 복호화

캡슐화 보안페이로드 프로토콜의 송신 처리

- 송신할 IP 패킷의 수신지 IP 주소, 포트, 전송계층 프로토콜 등의 선택자를 사용하여 SPD 검색
- 검색된 보안정책 데이터베이스 항은 출발용 SAD의 보안연계 지정
- 보안연계가 확립되어 있지 않을 경우, 인터넷 키교환 프로토콜을 호출하여 보안연계를 생성하고 SPD에 연결
- 추출된 보안연계를 이용하여 ESP 처리

① 순서번호 값을 1만큼 증가

② 보안연계가 기밀성 서비스를 요구하는 경우 암호화
- ICV는 암호화 이후 계산하므로 ICV는 암호화하지 않음
- 수신측 노드는 보안연계의 추출에 SPI, 재전송 패킷의 식별에 순서번호를 이용하므로 이들 필드는 암호화하지 않음

③ SA가 무결성 서비스를 요구하는 경우에 ICV 계산

④ 필요하다면 패킷을 분할하여 수신지로 전송

캡슐화 보안페이로드 프로토콜의 수신 처리

- 분할된 IP 패킷들을 재조립한 후, IP 보안 프로토콜 처리
- 다음 각 단계의 처리에 실패할 경우 패킷을 폐기하고 해당 이벤트 기록
- SPI, 수신지 IP 주소를 사용하여 SAD에서 해당 패킷의 보안연계 추출
- 순서번호를 사용하여 패킷의 재전송 여부 확인
- SA가 인증 서비스를 요구하는 경우: 규정된 인증 알고리즘과 키를 사용하여 ICV를 계산하고, 인증 데이터 필드에 저장되어 있는 ICV 값과 비교하여 검증
- SA가 기밀성 서비스를 요구하는 경우: 규정된 알고리즘과 키를 사용하여 복호화. 일반적으로 복호화는 CPU 시간과 메모리를 많이 사용하므로 인증 후에 적용
- 호스트의 경우는 패킷을 상위 계층으로 전달하며, 보안 게이트웨이인 경우에는 지정된 노드로 전달

ESP 요약 정리(1/2)

- 캡슐화 보안페이로드 프로토콜의 보안 서비스
  - 정당한 사용자 만이 패킷의 내용을 파악하도록 하는 기밀성 서비스
  - 데이터의 근원지를 식별하는 인증 서비스
  - IP 헤더 및 패킷 내용의 변조 여부를 확인할 수 있는 무결성 서비스
  - 공격자에 의한 재전송 패킷의 감지 및 폐기

- ESP의 보안 알고리즘
  - 기밀성 서비스를 위하여 암호화에 대칭키 암호 알고리즘 사용
    - NULL 암호화 알고리즘, DES, 3 중 DES, 128 비트 암호키의 진보된 암호화 표준(AES)
  - 인증 및 무결성 서비스를 위하여 메시지인증코드 사용
    - NULL 인증 알고리즘, HMAC-MD5, HMAC-SHA-1, AES-XCBC-MAC
  - NULL 암호화 알고리즘과 NULL 인증 알고리즘은 동시에 이용될 수 없음

- ESP 터널모드는 ESP 트랜스포트 모드보다 높은 보안성을 제공
  - 터널모드 기밀성 서비스의 경우 새로운 IP 헤더를 제외한 원래의 IP 패킷 전체에 대하여 인증 및 암호화
  - 새로운 IP 헤더가 삽입되므로 터널모드는 더 많은 대역폭을 사용

ESP 요약 정리(2/2)

- AH와 ESP의 인증 서비스 비교
  - 인증헤더(AH)는 IP 헤더를 포함한 전체 패킷에 대하여 인증 데이터 계산
  - ESP는 IP 헤더를 제외한 전체 패킷에 대하여 인증 데이터 계산
    - IP 헤더 필드가 중간에서 변조된 후, 헤더 검사합이 새로 계산된 경우 수신지 노드는 변경을 탐지하지 못함
  - 높은 수준의 인증에 대한 보안성이 필요한 경우 IP 헤더를 포함한 전체 패킷을 인증하는 AH 인증 서비스 이용

- ESP 프로토콜의 처리
  - 보안연계 추출 ⇒순서번호 생성 ⇒암호화 ⇒ 인증 ⇒ 분할 ⇒ 송신
  - 수신 ⇒ 결합 ⇒ 보안연계 추출 ⇒ 순서번호 검증 ⇒ 인증 ⇒ 복호화