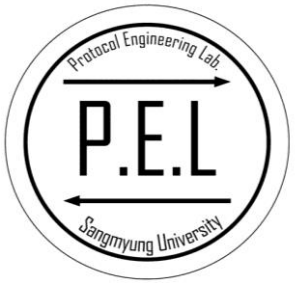


NETWORK SECURITY ESSENTIALS

- IP 보안 (2) -

Boo-Hyung Lee
(boohyung@pel.smuc.ac.kr)
Protocol **E**ngineering **L**ab., **Sangmyung** University

2015. 02. 26

Content

- SA Bundle
- IKE(Internet Key Exchange)
- 암호도구

SA Bundle (1/3)

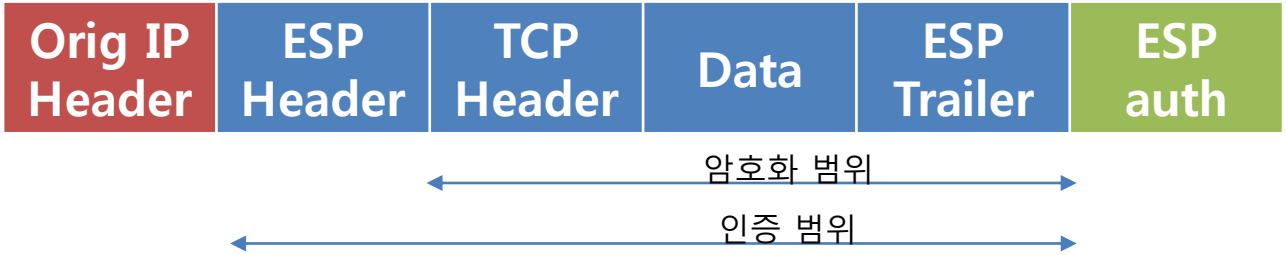
- **SA Bundle의 정의**
  - 단방향일 경우, 하나의 SA는 AH 또는 ESP 프로토콜로 구현되어 있음
  - 실제 통신은 양방향으로 이루어지기 때문에, SA 쌍(bundle)으로 표현할 수 있음
  - 인증과 기밀성을 모두 제공하기 위한 방법

SA Bundle (2/3)

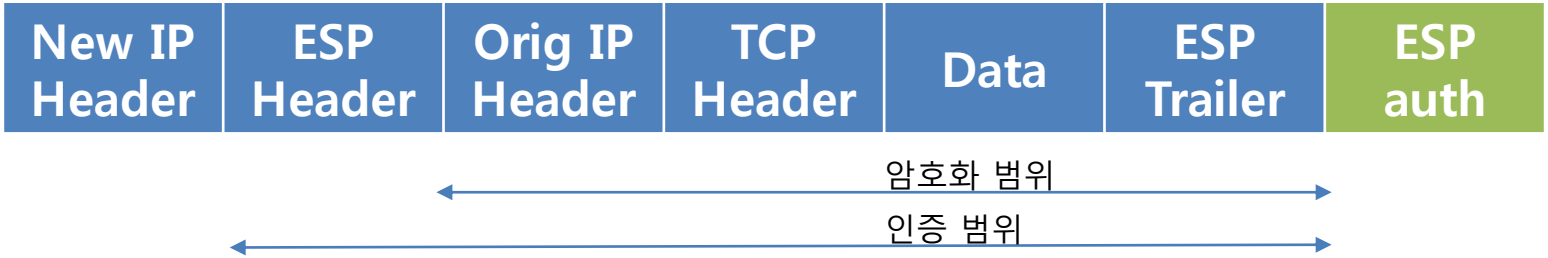
- **기밀성과 인증을 모두 제공하는 방법 (1/2)**

  - 인증 옵션을 갖는 ESP

    1) 전송 모드 ESP : 원래의 IP Header는 보호되지 않음



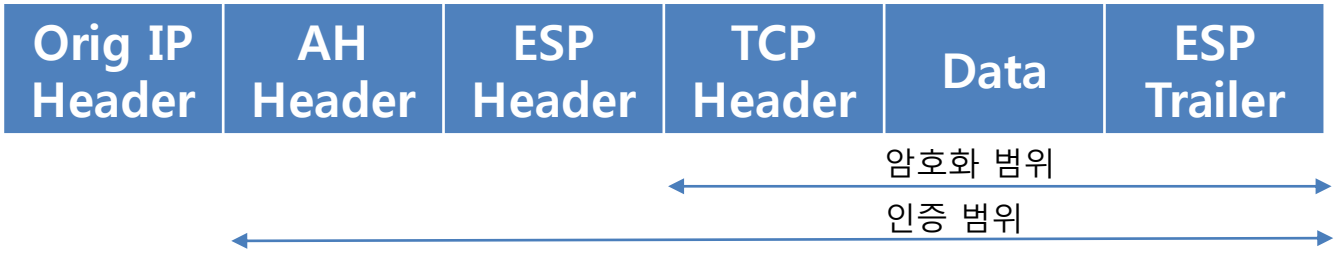
    2) 터널 모드 ESP



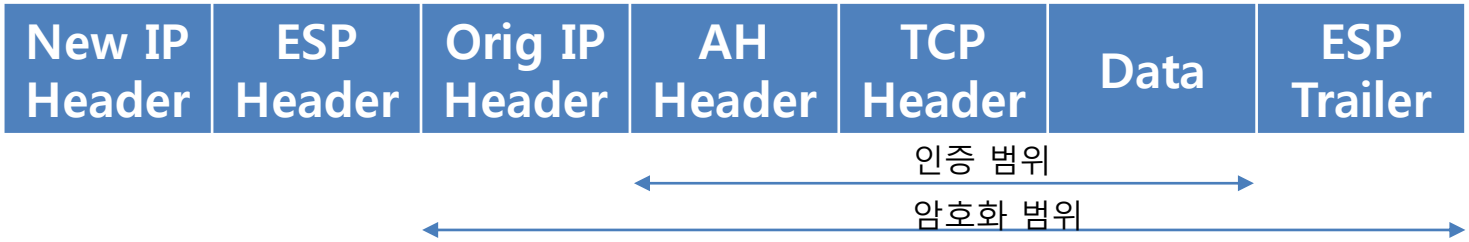
SA Bundle (3/3)

- **기밀성과 인증을 모두 제공하는 방법 (2/2)**

  - 중첩 전송 : 내부에 인증 옵션이 없는 전송모드 ESP를 사용하고, 외부에 전송모드 AH를 사용(암호화 후에 인증)



  - 전송-터널 묶음 : 내부에 전송모드 AH를 사용하고, 외부에서 터널모드 ESP 사용 (암호화하기 전에 인증 : 인증 데이터를 암호화로 보호할 수 있음)



IKE(Internet Key Exchange)

- **IKE의 정의 (IKEv1 : RFC 2409, IKEv2 : RFC 4306)**

  - IKE = ISAKMP + Oakley

  - ISAKMP(Internet Security Association and Key Management Protocol) : SA관리와 key 관리를 위해 IETF에서 제안한 프레임워크

  - Oakley : Diffie-Hellman 알고리즘을 기반으로 하여 추가적인 보안을 제공하는 키 교환 프로토콜

  - 자동식 SA 협상, 키 교환

  - 무결성과 기밀성 제공

- **IKE의 기능**

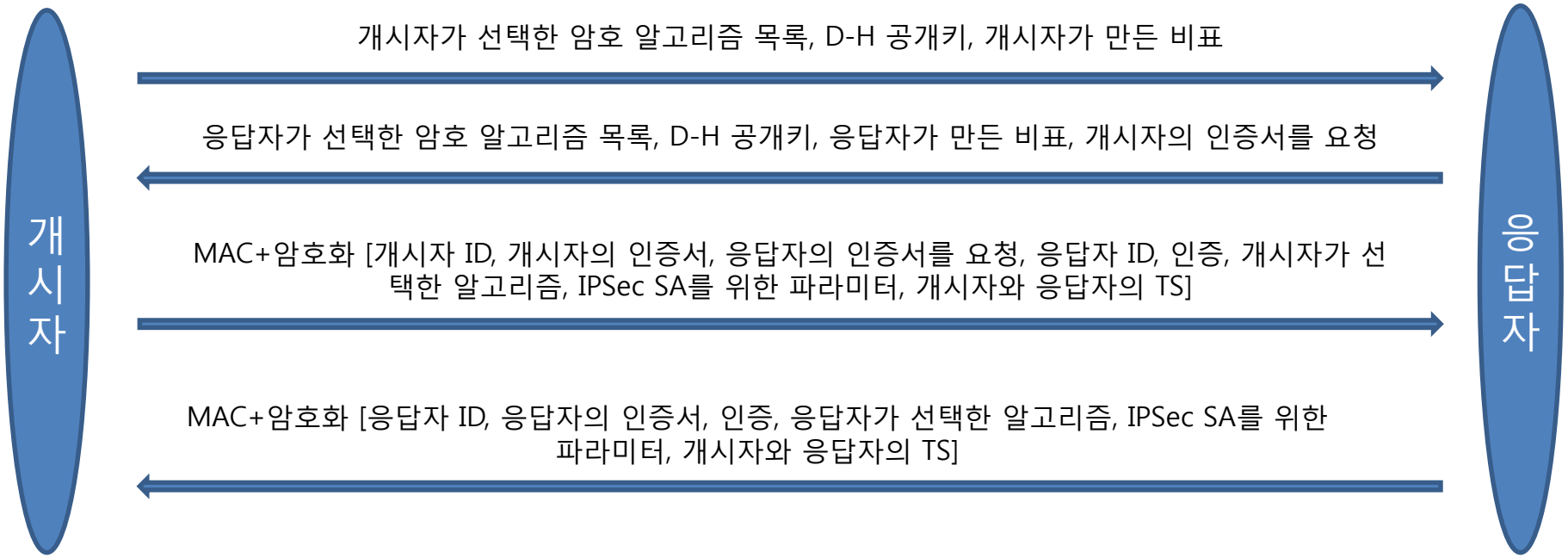
  - 협상 : 사용할 프로토콜과 알고리즘과 키에 동의하고 협상

  - 인증 : 통신하고 있는 상대방이 실제 내가 통신하고 있다고 생각하는 상대방인지 확인

  - 키 관리 : 사용할 키가 합의로 결정된 후 안전하게 교환될 수 있도록 관리

IKE(Internet Key Exchange)

- **IKEv2 키 교환 프로토콜 : 초기 교환**



☞ 인증 : 디지털 서명, 공개키 암호화, 대칭키 암호화

☞ IPSec SA를 위한 파라미터 : SPI, Src/Dest IP addr, Protocol, 암호 알고리즘, 암호화 키, HMAC 알고리즘, HMAC key

☞ TS(Traffic Selector) : 트래픽을 필터링하기 위한 선택자

IKE(Internet Key Exchange)

- **IKEv2 키 교환 프로토콜 : 초기 교환**
  - 첫 번째 교환

    1) IKE SA 설정

    2) 암호 알고리즘과 비표, Diffie-Hellman 알고리즘을 통해 만든 공개키를 교환
  - 두 번째 교환(첫 번째 과정에서 서로 교환한 공개키로 암호화하여 전송)

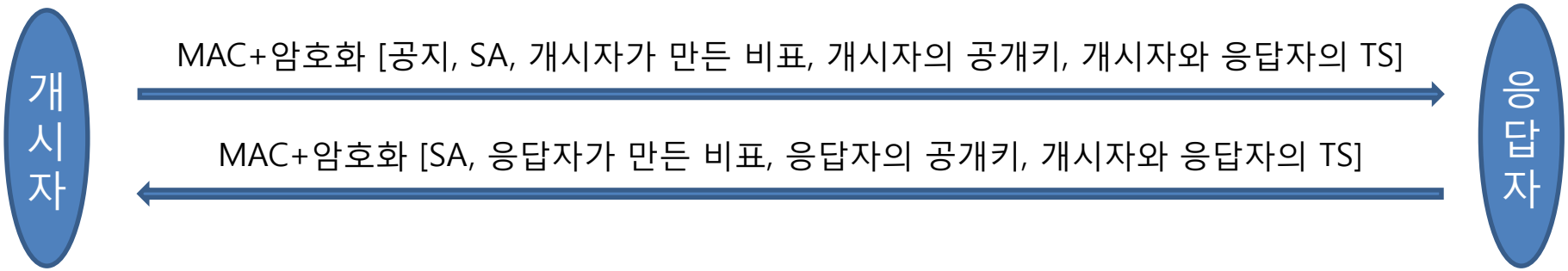
    1) 개시자와 응답자는 상호 인증

    2) IKE에서 IPSec SA를 설정하고 협상

    3) 통신에 필요한 Session Key를 생성

IKE(Internet Key Exchange)

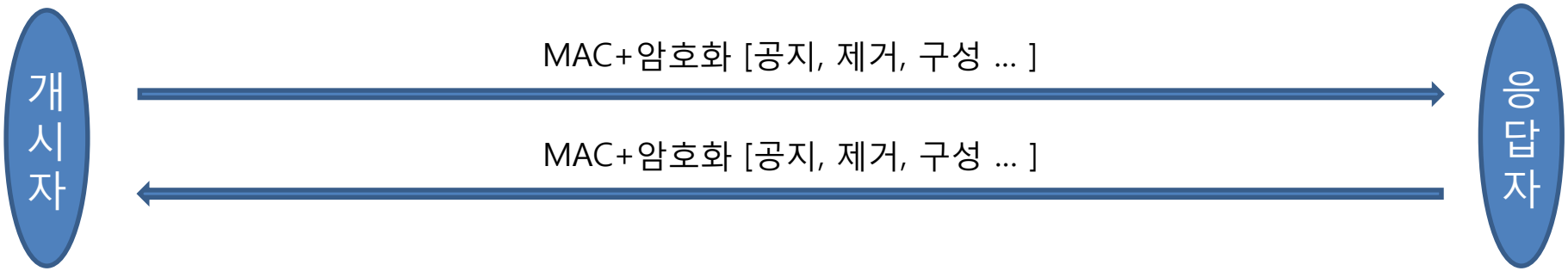
- **IKEv2 키 교환 프로토콜 : CREATE_CHILD_SA 교환**



- 기능 : 트래픽 보호를 위한 추가 SA를 설정하기 위해 사용

IKE(Internet Key Exchange)

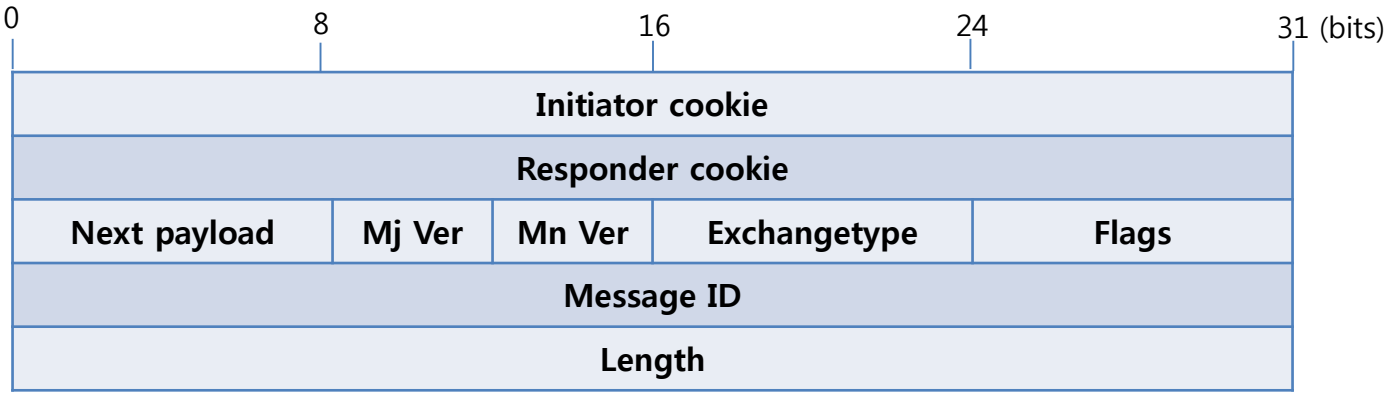
- **IKEv2 키 교환 프로토콜 : 정보 교환**



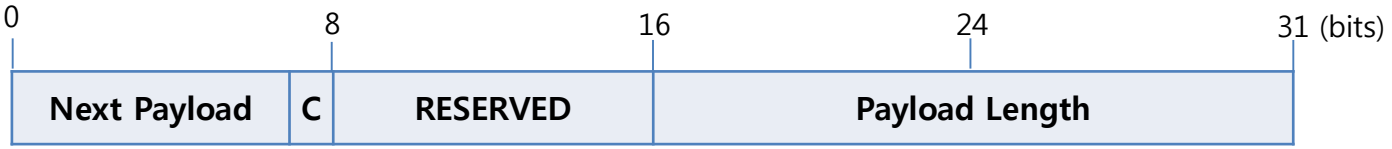
- 기능 : 관리 정보, IKEv2 오류 메시지 등을 교환하기 위해 사용

IKE(Internet Key Exchange)

- 헤더와 페이로드 형식 : IKE 헤더와 기본 페이로드 헤더



[그림] IKE 헤더



[그림] 기본 페이로드 헤더

IKE(Internet Key Exchange)

- **헤더와 페이로드 형식 : 필드 설명**

  - Initiator cookie(64 bits) : IKE SA를 구별하기 위해 개시자가 만든 값
  - Responder cookie(64 bits) : IKE SA를 구별하기 위해 응답자가 만든 값
  - Next Payload(8 bits) : 메시지 안의 페이로드 유형을 나타냄
  - Major Version(4 bits) : 사용 중인 IKE의 주 버전
  - Minor Version(4 bits) : 사용 중인 IKE의 부 버전
  - ExchangeType(8 bits) : 교환 유형
  - Flags(8 bits) : IKE 교환에 대한 특정 옵션 집합; 현재는 3비트만 정의됨

    1) Initiator bit : 이 패킷이 SA 개시자가 보낸 것인지 아닌지를 나타냄

    2) Version bit : 현재 나타낸 버전 번호보다 상위 주버전 번호를 사용할 수 있는지 아닌지를 나타냄

    3) Responder bit : 동일한 메시지 ID를 포함하고 있는 메시지에 대한 응답인지 아닌지를 나타냄

IKE(Internet Key Exchange)

- **헤더와 페이로드 형식 : 필드 설명**

  - 페이로드 유형 : Next Payload 필드 정보(마지막 페이로드임을 나타낼 때는 0을 사용)

  1) SA : SA를 설립하기 위한 프로토콜 정보
  2) KeyExchange : 키 교환에 필요한 데이터와 알고리즘
  3) Indetification : 신원정보
  4) Certificate : 자신의 공개키 인증서 유형이나 관련 정보
  5) Certificate Request : 상대방의 인증서를 요청
  6) Authentication : 메시지 인증; 인증에 필요한 데이터를 포함
  7) Nonce : 재전송 공격을 방어하기 위한 난수 데이터
  8) Notify : SA 협상과 관련된 오류나 상태 정보
  9) Delete : 더 이상 유효하지 않은 SA; SAD(Security Association Database)에서 제거한 SA
  10) Vendor ID : 각각의 Vendor가 정의한 상수
  11) Traffic Selector : 패킷 흐름을 식별
  12) Encrypted : 암호화된 형태의 다른 페이로드
  13) Configuration : IKE 구성 정보
  14) Extensible Authentication Protocol(EAP) : IKE SA를 인증할 때 쓰는 프로토콜

IKE(Internet Key Exchange)

- **헤더와 페이로드 형식 : 필드 설명**

  - ExchangeType 필드 정보

    1) Base Exchange : 키 교환 및 인증도구 협상

    2) Identity Protection Exchange : 신원 보호

    3) Authentication Only Exchange : 신원 확인

    4) Aggressive Exchange : SA간의 협상과 키 교환

    5) Information Exchange : 오류, 상태정보 통지, 삭제 등

암호도구

- **RFC 4308**

  - 가설 사설망을 위한 두 가지 암호 도구를 정의

    1) VPN-A : 기업 VPN 보안으로 사용; 3-DES와 HMAC을 사용

    2) VPN-B : VPN-A보다 더 강한 보안을 제공하며, IPSecv3와 IKEv2에 권장; AES를 사용

	VPN-A	VPN-B
ESP encryption	3DES-CBC	AES-CBC(128 bits key)
ESP integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE encryption	3DES-CBC	AES-CBC(128 bits key)
IKE PRF	HMAC-SHA1	AES-XCBC-MAC-96
IKE integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE DH Group	1024 bits MODP	2048 bits MODP

☞ 가설 사설망(VPN) : 인터넷을 경유해서 데이터를 주고 받을 때 사설망과 같은 수준의 보안을 제공하기 위한 기술; 전용선에 비해 훨씬 적은 비용이 들기 때문에 많은 기업이 사용

암호도구

- **RFC 4869**
  - 미국 국가 안보국(NSA)의 suite B 명세와 호환되는 4가지 암호 suite를 정의
  - ESP와 IKE에 대한 선택을 제공
  - AES-GCM, AES-CBC, HMAC-SHA, ECP, ECDSA 알고리즘 사용

	GCM-128	GCM-256	GMAC-128	GMAC-256
ESP encryption/integrity	AES-GCM (128 bits key)	AES-GCM(256 bits key)	Null	Null
ESP integrity	Null	Null	AES-GMAC(128 bits key)	AES-GMAC(256 bits key)
IKE encryption	AES-CBC(128 bits key)	AES-CBC(256 bits key)	AES-CBC(128 bits key)	AES-CBC(256 bits key)
IKE PRF	HMAC-SHA-256	HMAC-SHA-384	HMAC-SHA-256	HMAC-SHA-384
IKE integrity	HMAC-SHA-256-128	HMAC-SHA-384-192	HMAC-SHA-256-128	HMAC-SHA-384-192
IKE DH Group	256 bits random ECP	384 bits random ECP	256 bits random ECP	384 bits random ECP
IKE authentication	ECDSA-256	ECDSA-384	ECDSA-256	ECDSA-384