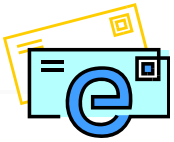
Chap 22.
Internet Security Protocols and Standards

연세대학교

Internet Mail format – RFC 822



- RFC 822 – Internet Text Message Format Standard
  - To, From, Subject를 가진 간단한 heading을 정의
  - **ASCII text format** 가정
  - 일부 헤더는 사용자가 제공
    - To:, Subject:, Cc:
  - 나머지 헤더는 mail delivery system이 제공
    - Date:, Received:, From: …

```
Date:Tue, 16 Jan 1996 10:37:17 (EST)
From: "William Stallings" <ws@host.com>
Subject:The syntax of RFC 822
To: Smith@otherhost.com
Cc: Jones@Yet-another_host.com

This is the main text, delimited from the header by a blank line.
```

연세대학교

MIME

- Multipurpose Internet Mail Extensions (MIME)
  - Old Internet mail format (RFC 822)의 확장
    - RFC 822가 이진파일, 국제문자(â, å, ä, è, é, ê, ë 등, 한글)를 전송할 수 없는 문제점 해결
  - 많은 새로운 header field들을 제공
    - MIME-version
    - Content-Type
    - Content-Transfer-Encoding
    - Content Id
    - Content Description
  - header field는 메시지 body에 대한 정보를 정의
  - 다수의 content format과 전송 인코딩 방법 정의

연세대학교

MIME Content Types and Encoding

- MIME Content types/Subtypes
  - text/plain, text/html …
  - multipart/mixed, multipart/alternative, …
  - image/jpeg, image/gif, image/tiff …
  - video/mpeg, video/avi, …
  - audio/mpeg, audio/mpeg3, …
  - application/octet-stream, application/postscript, application/pdf
  - message/rfc822, message/partial, …
- MIME encoding
  - ASCII
  - base64 encoding
  - UTF8

연세대학교

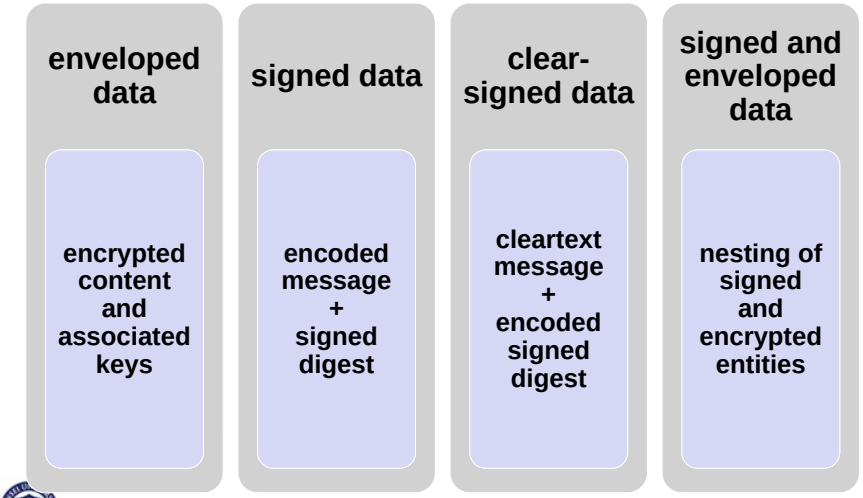
```
From: Steve Zdancewic <stevez@cis.upenn.edu>
MIME-Version: 1.0
To: stevez@cis.upenn.edu
Subject: Example Mail
Content-Type: multipart/mixed; boundary="------------020307000708030506070607"

This is a multi-part message in MIME format.
--------------020307000708030506070607
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit

This is the body.

--------------020307000708030506070607
Content-Type: text/plain; name="example.txt"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline; filename="example.txt"

Hello

--------------020307000708030506070607
Content-Type: image/jpeg; name="doc.jpg"
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="doc.jpg"

/9j/4AAQSkZJRgABAQEASABIAAD//gAXQ3JIYXRIZCB3aXRoIFRoZSBHSU1Q/9sAQwAIBgYH
BgUIBwcHCQkICgwUDQwLCwwZEhMPFB0aHx4dGhwcICQuJyAiLCMcHCg3KSwwMTQ0NB8nOT04
...
```


S/MIME

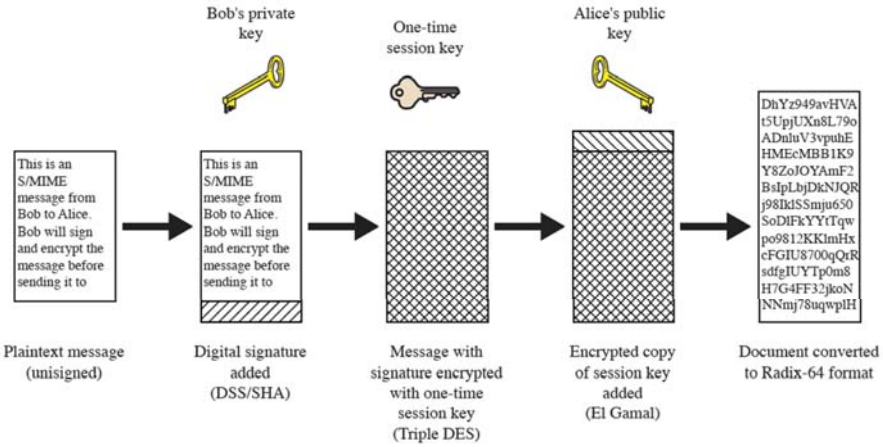
- Secure/Multipurpose Internet Mail Extension(S/MIME)
  - MIME email format에 대한 보안기능을 추가한 개선
    - RSA Data Security 기술에 기반
  - email 메시지를 **서명**하거나 **암호화**하는 기능 제공
- S/MIME Content Types

Type	Subtype	smime Parameter	Description
Multipart	Signed		A clear-signed message in two parts: one is the message and the other is the signature.
Application	pkcs7-mime	signedData	A signed S/MIME entity.
	pkcs7-mime	envelopedData	An encrypted S/MIME entity.
	pkcs7-mime	degenerate signedData	An entity containing only public-key certificates.
	pkcs7-mime	CompressedData	A compressed S/MIME entity.
	pkcs7-signature	signedData	The content type of the signature subpart of a multipart/signed message.

S/MIME Functions



Typical S/MIME Process



S/MIME Cryptographic Algorithms

- 메시지 서명용 알고리즘 :
  - 기본 알고리즘 – Digital Signature Standard (DSS)와 SHA-1
  - 대안 알고리즘 – RSA 공개키 암호화 알고리즘을 SHA-1 또는 MD5 message digest 알고리즘과 함께 사용할 수 있음.
- 서명/메시지 전송에 radix-64(base64) encoding이 사용됨
  - 서명과 메시지를 printable ASCII 문자로 매핑

연세대학교

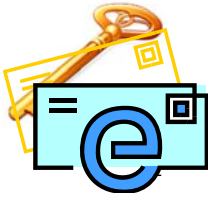
S/MIME Public Key Certificates

- S/MIME 메시지 암호화에 사용되는 기본 알고리즘
  - 3DES와 EI-Gamal
  - **EI-Gamal** : Diffie-Hellman 공개키 교환 알고리즘에 기반
- 암호화가 단독으로 사용되는 경우,
  radix-64가 암호문을 ASCII 형식으로 변환하는 데 사용됨
- 공개키 인증서
  - S/MIME의 광범위한 사용을 가능하게 하는 기본 도구
  - S/MIME은 국제 표준 **X.509v3**을 준수하는 인증서를 사용함

연세대학교

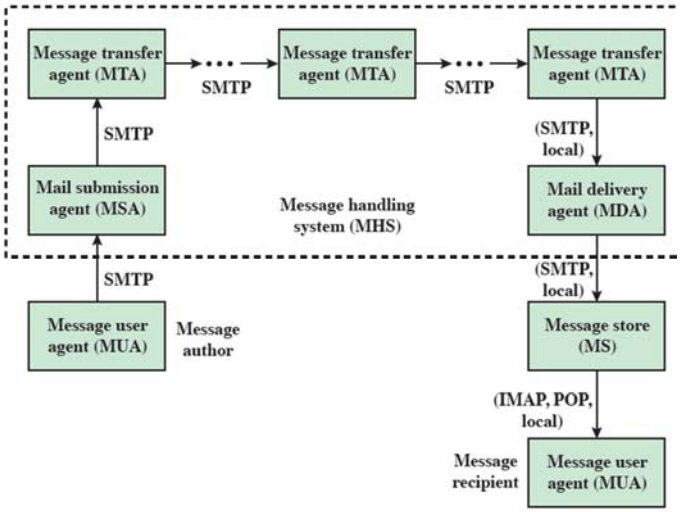
DomainKeys Identified Mail (DKIM)

- 도메인 키 식별 메일(DKIM: Domain Key Identified Mail)
  - 전자메일 메시지의 암호화 서명에 대한 specification
  - 이메일 메시지에 대한 책임을 주장(claim)하기 위한 **서명 도메인**(signing domain)을 허용
  - 이메일 주소에 대한 도용(spoofing) 방지를 할 수 있음
- 제안된 Internet Standard
  - RFC 4871: DomainKeys Identified Mail (DKIM) Signatures
- 다양한 전자메일 공급자가 광범위하게 채택함



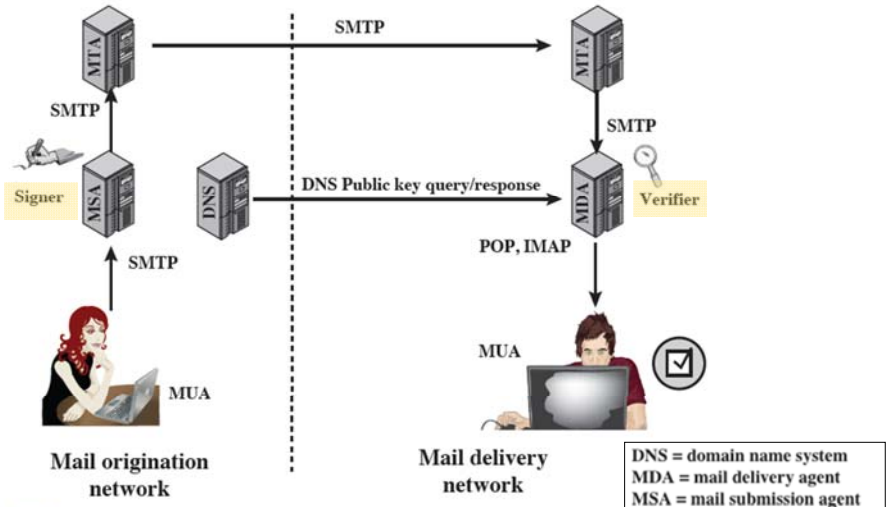
연세대학교

Internet Mail Architecture



연세대학교

Example of DKIM Deployment

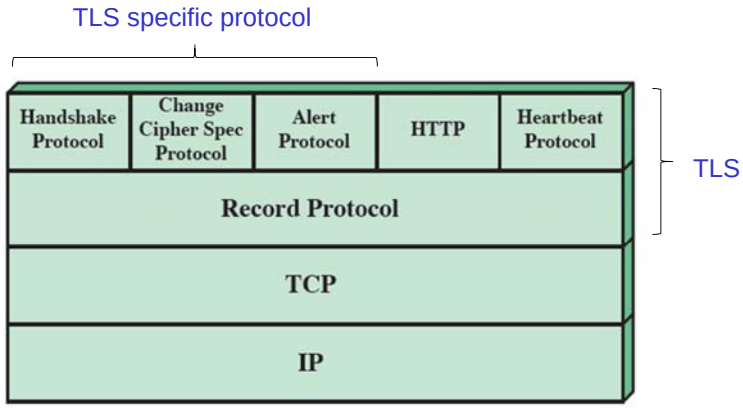


Secure Sockets Layer/Transport Layer Security

- SSL과 TLS
  - 가장 널리 사용되는 security services 중 하나
    - 웹 서버/웹 브라우저 간 통신 등
  - TCP에 기반을 둔 protocol 집합으로 구현되는 범용 서비스
    - reliable end-to-end 서비스 제공
  - SSL이 발전하여 TLS (Internet standard RFC4346)가 됨

- 두 가지 구현 방법
  - 기본 프로토콜 집합의 일부로 제공 – 범용성, application에 투명
  - 특정 패키지에 포함 – 웹 브라우저

SSL/TLS Protocol Stack



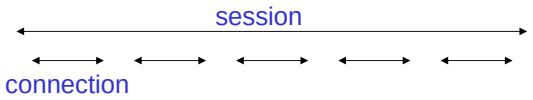
TLS Concepts

TLS Session

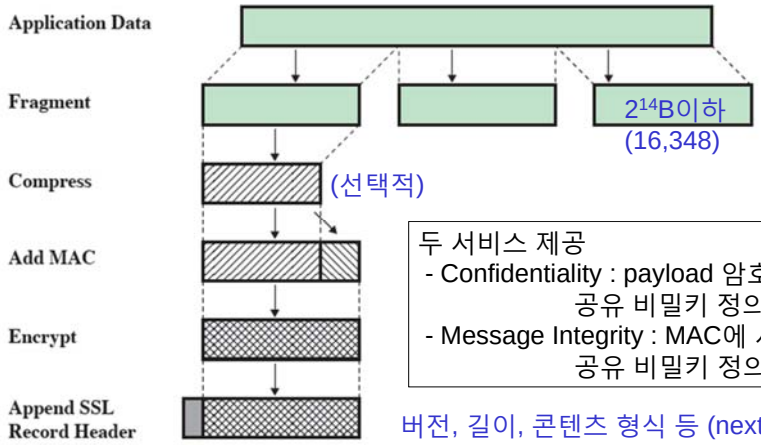
- 클라이언트와 서버 간의 연관
- handshake 프로토콜에 의해 생성
- 다중 연결 간에 공유할 수 있는 암호 보안 매개변수 집합을 정의
- 각 연결 마다 새로운 보안 매개 변수를 협상하는 데 드는 비용을 피하는 데 사용됨

TLS Connection

- (OSI 계층화 모델 정의에서) 적절한 유형의 서비스를 제공하는 전송(transport)
- peer-to-peer 관계
- 일시적(transient)
- 모든 연결은 하나의 세션과 연관됨



TLS Record Protocol Operation



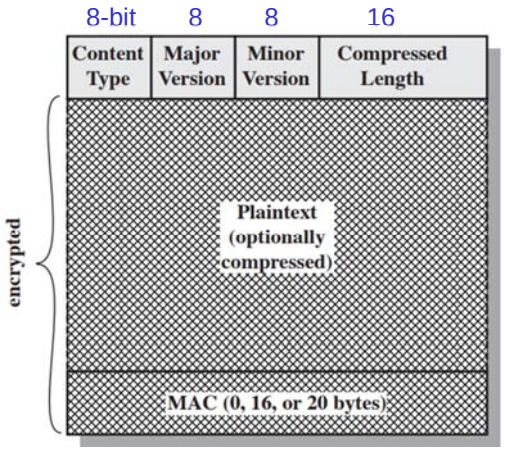
2^{14}B이하 (16,348)

(선택적)

두 서비스 제공
- Confidentiality : payload 암호화 공유 비밀키 정의
- Message Integrity : MAC에 사용할 공유 비밀키 정의

버전, 길이, 콘텐츠 형식 등 (next slide)

Record Format



Handshake Protocol

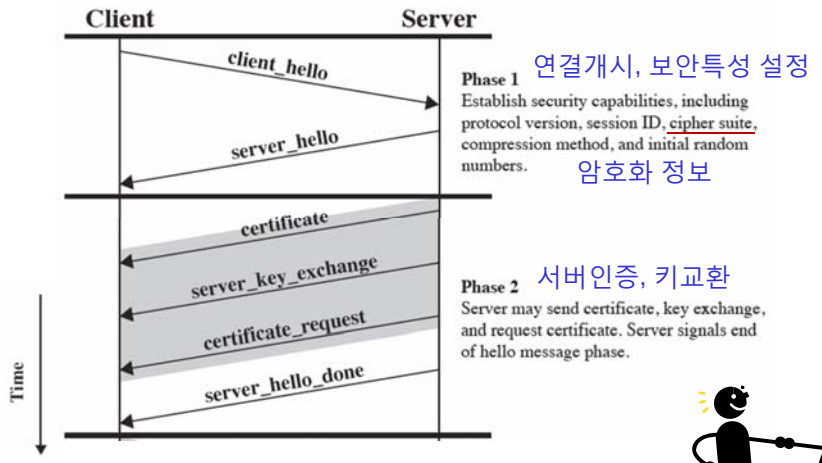
- TLS의 가장 복잡한 부분
- 서버와 클라이언트 간에 다음 동작 허용

Authenticate each other → Negotiate **encryption** and **MAC algorithms** → Negotiate **cryptographic keys** to be used

- application 데이터 전송 이전에 사용
- 클라이언트와 서버 간에 교환되는 일련의 메시지들로 구성됨
- 메시지 교환은 크게 4단계로 구성

(c) Handshake Protocol

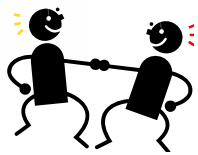
Handshake Protocol Action

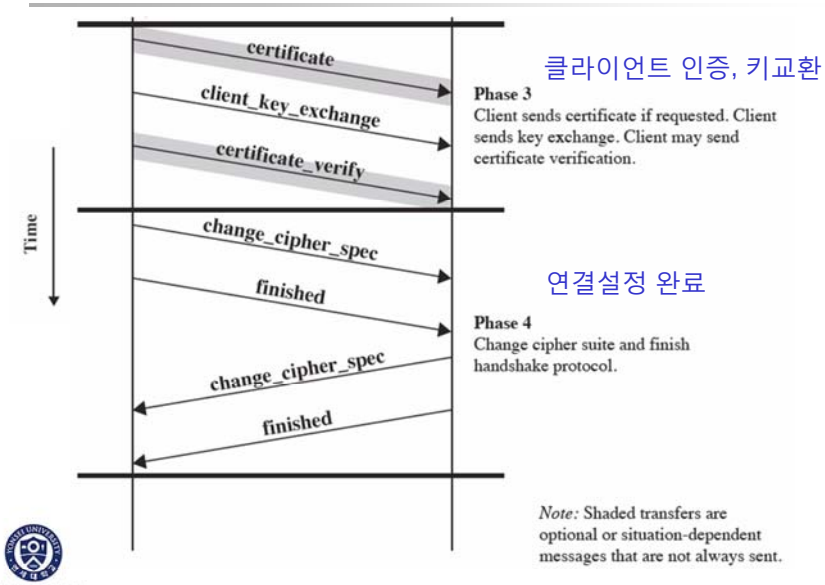


연결개시, 보안특성 설정

암호화 정보

서버인증, 키교환





클라이언트 인증, 키교환

연결설정 완료

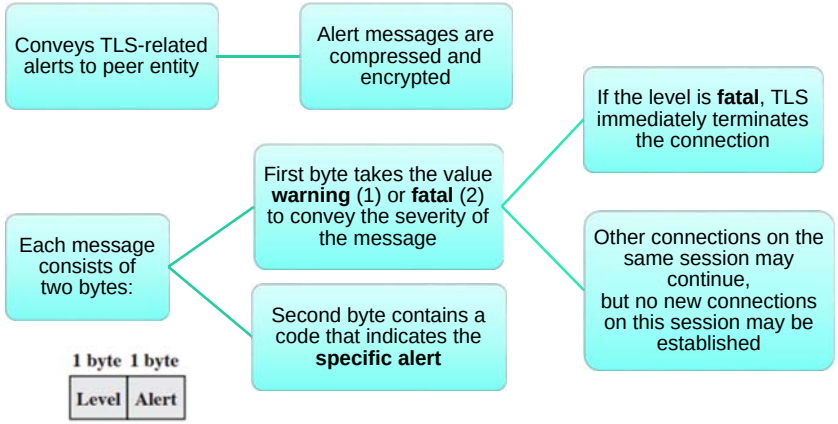
Change Cipher Spec Protocol

- handshake 과정에서 설정된 pending state를 current state로 복사하여 cipherspec을 변경하는 프로토콜
  - 사용 중인 cipher suite(지원되는 인증 및 암호알고리즘의 조합)를 업데이트
- TLS Record Protocol을 사용하는 4개의 TLS specific protocol 중 하나로 가장 간단함
  - 값이 1인 1 바이트 메시지로 구성됨.

(a) Change Cipher Spec Protocol

- Handshake과정에서 사용됨

Alert Protocol

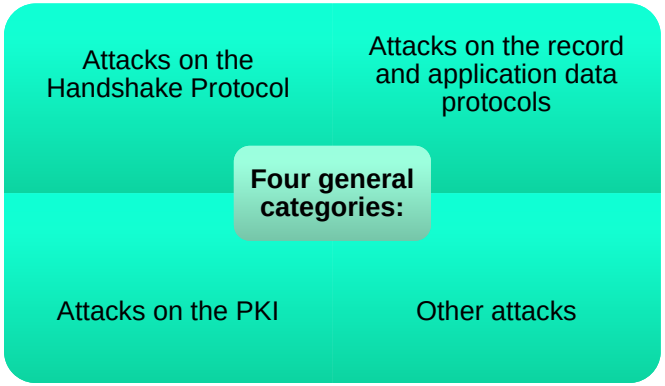


(b) Alert Protocol

Heartbeat Protocol

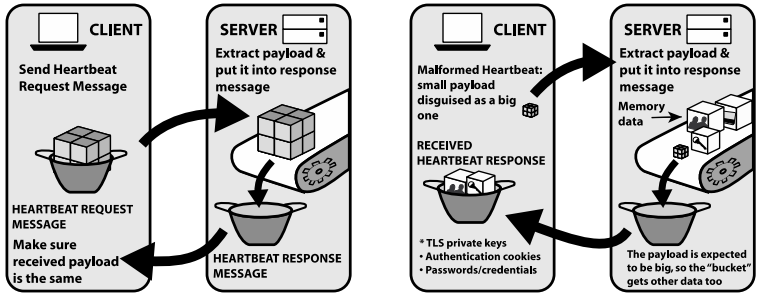
- heartbeat
  - 정상적인 작동을 나타내거나 시스템의 다른 부분을 동기화하기 위해 하드웨어 또는 소프트웨어에 의해 생성되는 주기적인 신호
- heartbeat protocol
  - 프로토콜 entity의 가용성을 모니터링하는 데 일반적으로 사용
  - RFC 6250에서 2012년에 정의됨
  - TLS record protocol 상단에서 실행
  - handshake protocol의 1 단계에서 사용이 설정됨
    - 각 피어는 heartbeat를 지원하는지 여부를 나타냄
- 프로토콜의 사용 목적
  - recipient가 아직 활동 중인지를 sender가 확인하기 위함
  - 휴지 기간 동안 연결이 활성화되게 함 – 휴지 연결을 허용하지 않는 방화벽에 의해 연결이 닫히는 것을 방지

SSL/TLS Attacks



Heartbleed 공격

- OpenSSL 구현의 취약점 이용 – 입력 메시지 길이 조사하지 않음



(a) How TLS Heartbeat Protocol works

(b) How TLS Heartbleed exploit works

Figure 22.7 The Heartbleed Exploit
Source: BAE Systems

HTTPS (HTTP over SSL)

- HTTP와 SSL의 결합
  - 웹 브라우저와 웹 서버간의 보안 통신 구현
- 모든 최근의 웹 브라우저에 내장됨
  - URL 주소는 **https://** 로 시작 (포트 443번)
  - RFC 2818 (HTTP Over TLS)에 문서화
- HTTP 클라이언트로 동작하는 agent가 TLS 클라이언트로도 동작
- HTTPS 연결을 닫으려면 TLS가 원격 피어 TLS entity의 연결을 닫아야 함 → 기반이 되는 TCP 연결 종료를 포함함

IP Security (IPsec)

- 여러 가지 application security mechanisms
  - S/MIME, PGP, Kerberos, SSL/HTTPS
- protocol 계층 간 보안 문제
- 네트워크에 의해서 구현되어 제공되는 보안 기능
  - (보안이 제공되지 않는) 모든 application에 보안을 제공
- 인증 및 암호화 보안 기능은 차세대 IPv6에 포함됨
  - 기존 IPv4에서도 사용 가능

IPsec

- 일반적인 IP security mechanisms
  - LAN, 사설 및 공용 WAN 및 인터넷을 통한 통신에 대한 보안 기능 제공
- IPsec의 기능
  - Authentication:
    - 수신된 패킷이 패킷 헤더에서 소스로 식별된 당사자에 의해 전송되었고 패킷이 전송 중에 변경되지 않았음을 보증함
  - Confidentiality:
    - 통신하는 노드가 메시지를 암호화하여 제3자의 도청을 방지할 수 있게함
  - Key management:
    - 안전한 키 교환
    - Internet Key Exchange standard IKEv2 에 의해 제공됨

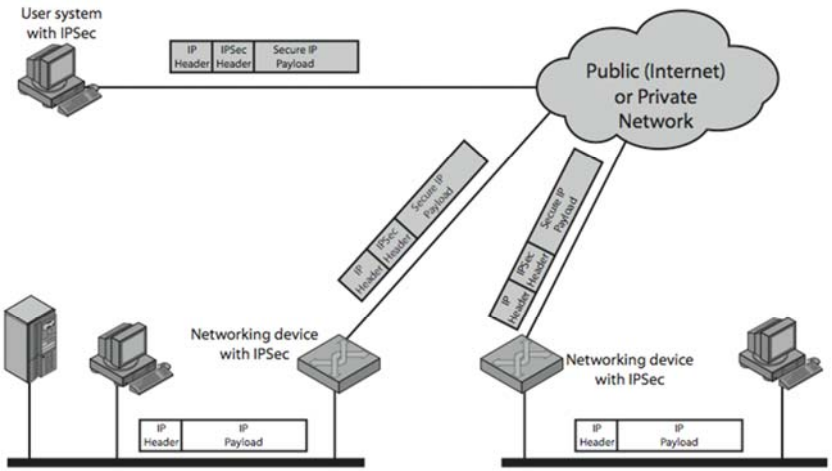
연세대학교

Applications of IPsec

- 인터넷을 통한 지사와의 보안 연결(secure connectivity)
- 인터넷을 통한 보안 원격 접속
- 외부망이나 내부망을 통한 상대방과의 연결 설정
- 전자상거래 보안 강화

연세대학교

IPsec Uses



연세대학교

Benefits of IPsec

- 방화벽 또는 라우터에 구현될 때 주변을 통과하는 모든 트래픽에 강력한 보안을 제공
- 방화벽에서의 IPsec는 우회(bypass)에 강인함(resistant)
- 전송 계층(TCP/UDP) 아래에 있으므로 응용 프로그램에 투명함
- 최종 사용자에게는 투명할 수 있음
- 개별 사용자에게 보안을 제공 가능
- 라우팅 아키텍처를 보호

연세대학교

The Scope of IPsec

- 두 가지 주요 기능 제공
  - 결합된 인증/암호화 기능 → ESP
  - 키 교환(key exchange) 기능
- Encapsulating Security Payload (ESP)
  - IP packet에 대한 결합된 인증/암호화 기능 제공
- Authentication Header (**AH**)
  - IP packet에 대한 인증 전용 기능 제공
  - AH 기능은 backward 호환성을 위해 IPsec v3에 포함
  - 새로운 application에서는 사용하지 않아야 함
- VPNs은 인증과 암호화 모두 필요로 함

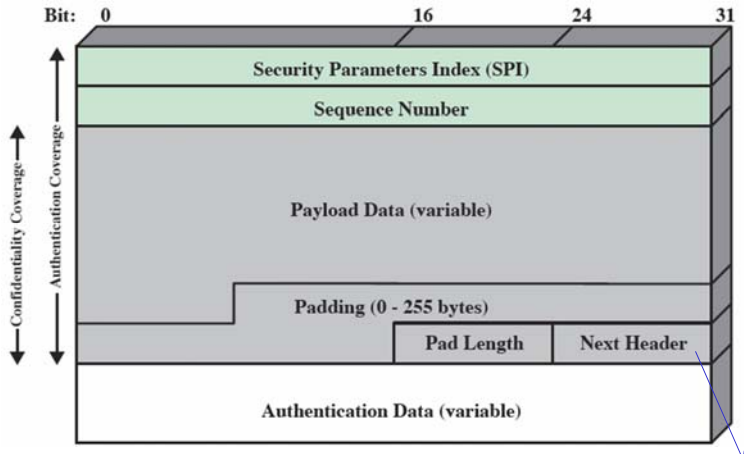
Security Associations

- 보안연관(SA: Security Association)
  - traffic 흐름에 대한 보안을 제공하는 sender와 receiver간의 단방향 관계
  - 양방향 보완 교환을 위해 대등 관계가 필요하면 2개의 SA가 요구됨
- IPv4 또는 IPv6 헤더의 **목적지 주소**와 동봉된 확장 헤더(**AH 또는 ESP**)의 **SPI**(보안 매개변수 지수)로 유일하게 식별됩니다.

Defined by 3 parameters:

Security Parameter Index (SPI)	SA 정보를 찾기 위한 index
IP Destination Address	종단시스템 또는 라우터, 방화벽의 IP 주소
Protocol Identifier	IP 헤더의 protocol field에서 지정 50: ESP, 51: AH

Encapsulating Security Payload (ESP)

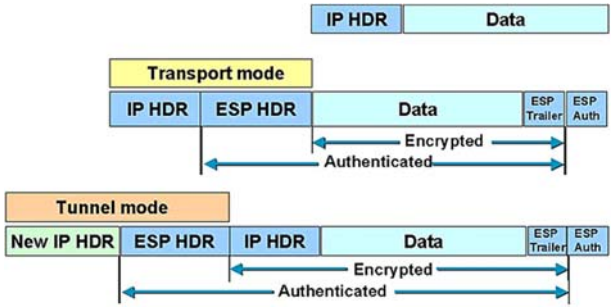


상위프로토콜
6: TCP, 17: UDP

Transport and Tunnel Modes

- 전송모드(Transport Mode)
  - 보호가 IP 패킷의 페이로드까지 확장
  - 두 호스트 간의 종단간 통신에 사용됨
  - ESP는 IP 페이로드를 암호화하고 선택적으로 인증하지만 IP 헤더는 제외됨
- 터널모드(Tunnel mode)
  - 전체 IP 패킷에 대한 보호를 제공
  - original 패킷 전체는 터널을 통하여 IP 네트워크의 한 지점에서 다른 지점으로 이동함
  - SA(security association)의 한쪽 또는 양쪽 끝이 IPsec를 구현하는 보안 게이트웨이일 때에 사용됨.
  - 방화벽 뒤의 네트워크에 있는 많은 호스트가 IPsec를 구현하지 않고 보안 통신을 할 수 있음.

Transport and Tunnel Modes



연세대학교