정보보호

(5111041)

22장

인터넷 보안 프로토콜
및 표준

MIME 과 S/MIME

MIME

- 전자 우편 형식의 기존 RFC 822 사양 확장
  - RFC 822는 To, From, Subject과 같은 단순한 헤더 정의
  - ASCII 텍스트 포맷
- 메시지 내용에 대한 정보를 명시하는 많은 새로운 헤더 필드 제공

S/MIME

- Secure/Multipurpose Internet Mail Extension의 약어
- MIME 인터넷 e-mail 포맷에 대한 보안 강화
  - RSA 데이터 보안 기술에 기반
- 서명 기능 또는 전자 우편 메시지 암호화 기능제공

전형적인 S/MIME 프로세스

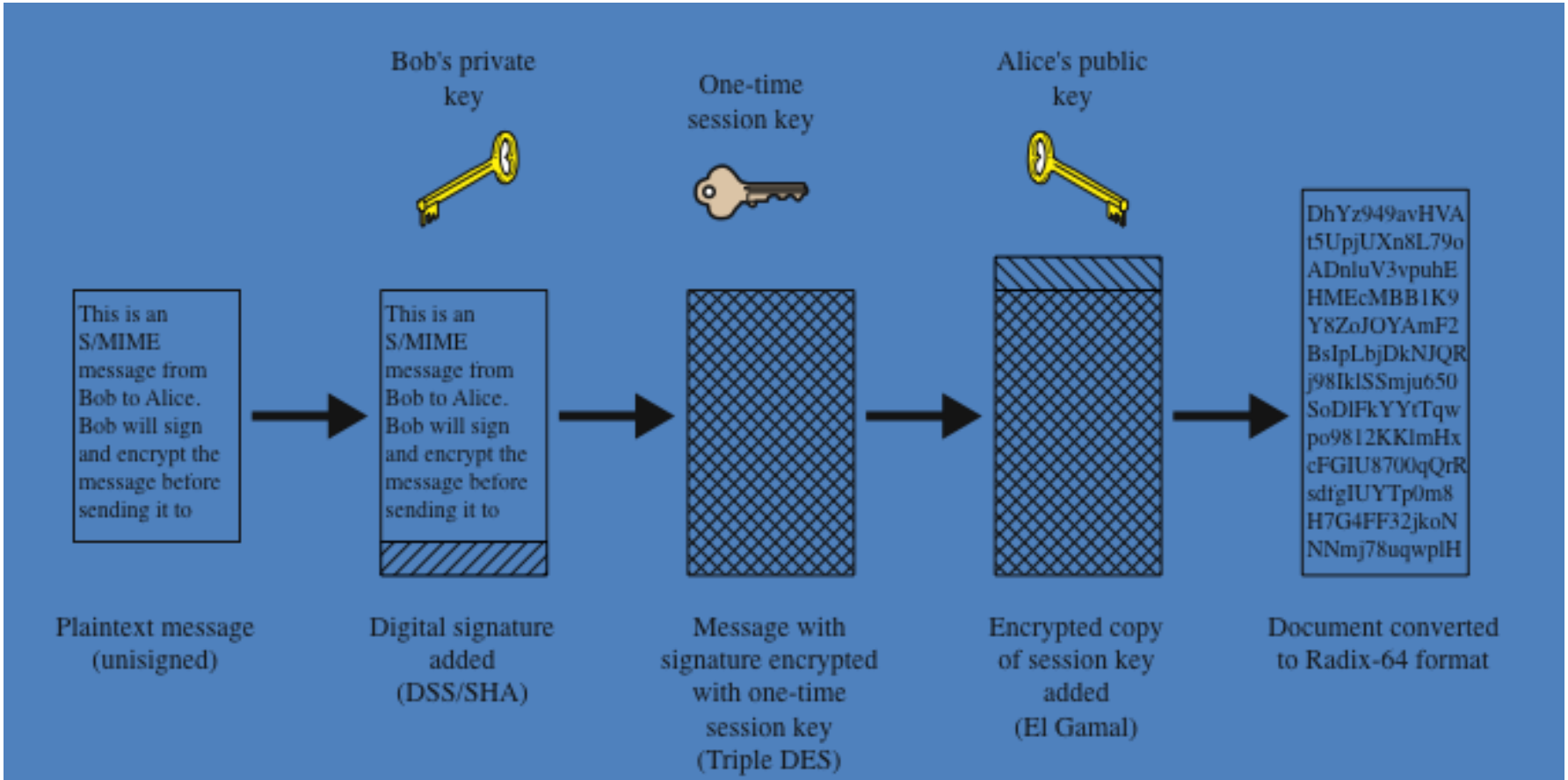


Figure 22.1 Typical S/MIME Process

S/MIME 암호 알고리즘

- 메시지 서명에 사용되는 기본 알고리즘은 DSS와 SHA-1이 있음
- RSA 공개키 암호화 알고리즘은 시그니처를 형성하는 데 SHA-1이나 MD5 메시지 다이제스트 알고리즘이 사용될 수 있음
- radix-64 또는 base64 맵핑은 시그니처와 매시지를 출력가능한 ASCII 문자로 맵핑하는 데 사용됨

Radix 64 for Email Compatibility

- ASCII format: 01101110 01100101 01110111
- After encryption: 10010001 10011010 10001000
  - 대부문의 메일시스템은 위의 정보를 처리하거나 전송할 수 없음
- Radix-64 Conversion
  - 1. The binary input is split into blocks of 24 bits (3 bytes).
  - 2. Each 24 block is then split into four sets each of 6-bits.
  - 3. Each 6-bit set will then have a value between 0 and 26-1 (=63).
  - 4. This value is encoded into a printable character
- 따라서 Radix-64는 메시지 용량을 33% 증가시킴

6 bit value	Character encoding	6 bit value	Character encoding	6 bit value	Character encoding	6 bit value	Character encoding
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(pad)	=

Radix 64 for Email Compatibility

- The 24-bit block: 10010001 10011010 10001000
- Four 6-bit blocks: 100100 011001 101010 001000
- Integer version: 36 25 38 8
- Printable version: k Z m I


Request
Pretty
Raw
Hex
\n
1 GET /external/mailCount?callback=showMailCount&
svc=gnb HTTP/2
2 Host: mail.naver.com
3 Cookie: N
NID_AUT=
Z38rZSGRbdFL1/IDtHu0C6hwdC
EyQQhpg0OVyOzA/GLeVLvy1hOZ
X09cqQiHwoOGNAAUiaExFaPBYa
QzAQjmQPA01ZrctjDLXuFL31U7Zd4o64I6Nre9+o7nS5OqE4M
CFOaM2ldloBeruKltxHpAl5NyxKcElRhbsEtEQOUlAasZSGcM
nLsob9jRmvLRF90VnwpFfA3E5HY/UP7bfC9EX/ncrAMOHRv9x
PKz9qxcVlegoxHxEtlt5U8vA8b5huMyVaajPNwJxnOSNUdq50
8CBZrIrMiDXWtbCuHxuo1JVMMsKS7+vnOfMJSIiLI4BQPw8A9
4add6TltQU7UNZRmpCma26mxSmI/4cqoWp7NnJQk+kAUMnwuR
38ajz/0ZubzEadBN/GAJ2M/SX5rWi3dQzY5theGzFP1hqT2b3
JbnQlGjGdoG2i/xNduvbfE47YtNyV8QewxxOx2AjV2wIc4qRo
ddOVcfmaJPnyrZ8Gv7fv5hEhnhlw==; NID_JKL=
HWW0uQH3IlIGCfMTObqatp9Exg7KI8gIahd2unFrWRA=
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:91.0) Gecko/20100101 Firefox/91.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:
https://blog.naver.com/PostList.naver?blogId=secu
rity2826&widgetTypeCall=true&topReferer=https%3A%
2F%2Fwww.naver.com%2Fmy.html&directAccess=true
9 Sec-Fetch-Dest: script
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-site
12 Te: trailers
13 Connection: close
1. 시작줄
2. 헤더
3. 빈줄

S/MIME 공개키 인증서

- S/MIME 메시지를 암호화 하는데 사용되는 기본 알고리즘은 3DES와 ELGamal이 있음
  - ELGamal은 Diffie-Hellman의 공개키 교환 알고리즘에 기반을 둠
- 암호만 사용될 경우, radix-64는 암호문을 ASCII 포맷으로 전환하는 데 사용됨
- 공개키 인증서는 S/MIME의 광범위한 사용을 허용하는 기본 툴
- S/MIME은 국제 표준 X.509v3를 따르는 인증서를 사용함

- **S/MIME 이 제공하는 보안 서비스**

보안 서비스	보안 메커니즘	암호 알고리즘
메시지 기밀성	암호화	Triple-DES, RC2/40bit
메시지 무결성	해시함수	SHA-1, MD5
사용자 인증	공개키 인증	x.509 v3인증서
부인방지	전자 서명	DSS, RSA

S/MIME 기능

enveloped data	signed data	clear-signed data	signed and enveloped data
암호화한 내용과 관련 키	인코딩한 메시지 + 서명한 다이제스트	평문메시지+ 인코딩한 서명 다이제스트	서명 및 암호화한 개체들의 네스팅 (nesting)

DKIM
(Domain Keys Identified Mail)

- 전자우편 메시지 내용에 대한 책임이 있는 도메인을 서명을 e-mail 메시지를 암호로 서명하게끔 하는 기능
- 제안된 인터넷 표준(RFC 4871: *DomainKeys Identified Mail (DKIM) Signatures)*
- E-mail 제공자의 범주에 따라 다르게 채택됨
  - 기본적인 전력은 E-mail 제공자(관리 도메인)의 개인키에 의해 서명 → 실제로 주어진 영역에서 생성된 메일인지 검증

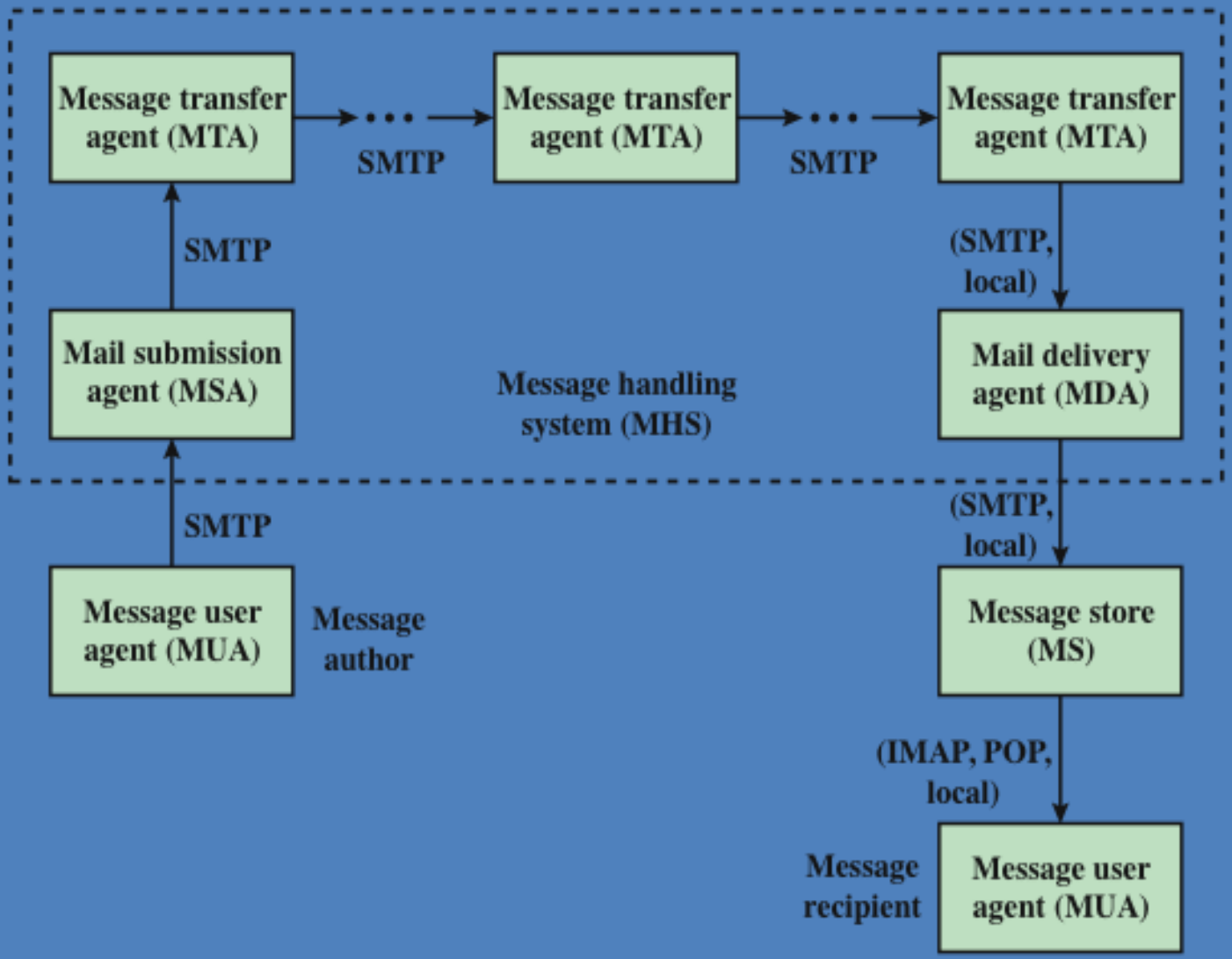
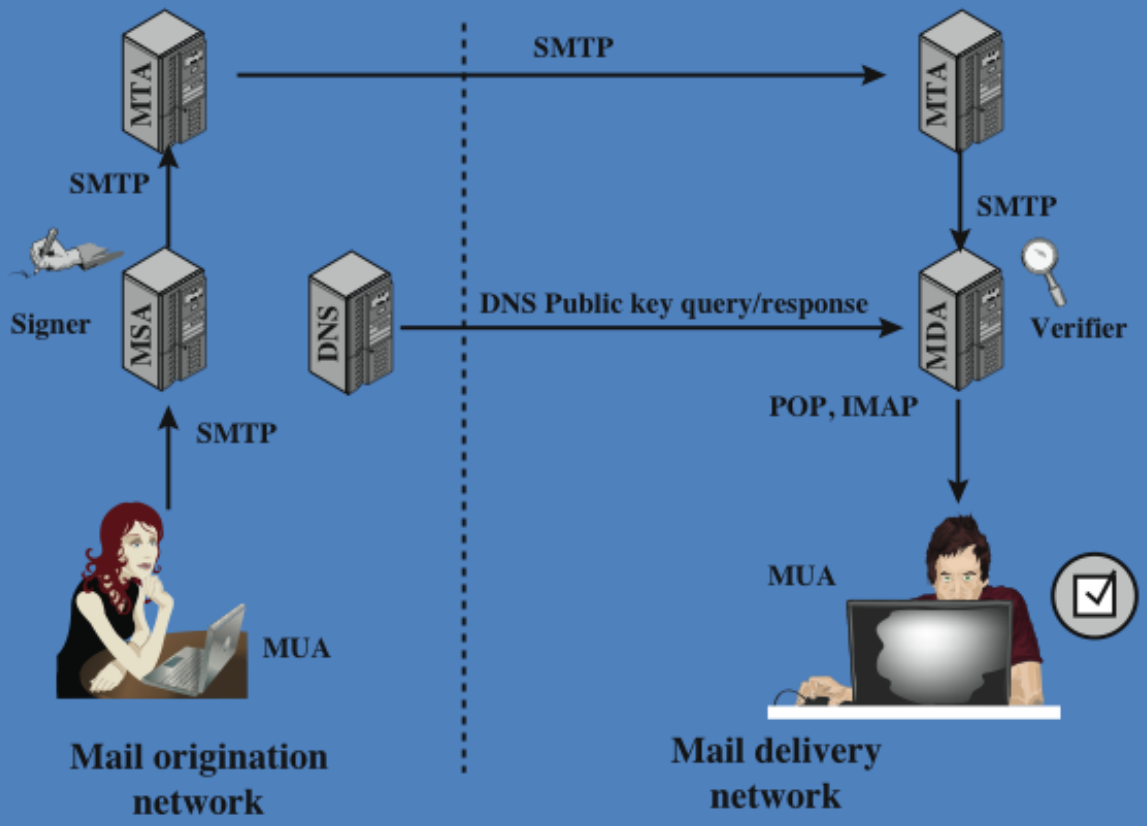


Figure 22.2 Function Modules and Standardized Protocols Used Between Them

전자메일 아키텍처



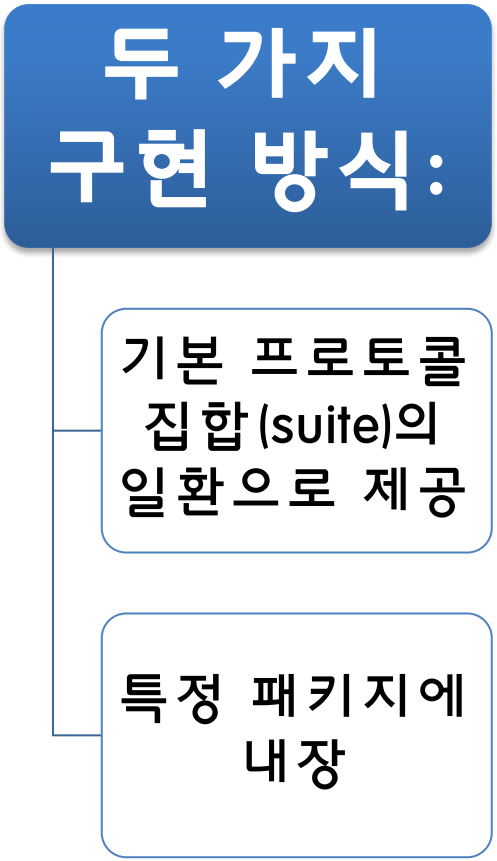
DNS = domain name system
MDA = mail delivery agent
MSA = mail submission agent
MTA = message transfer agent
MUA = message user agent

Figure 22.3 Simple Example of DKIM Deployment

DKIM 개발 예제

보안 소켓 계층
(Secure Sockets Layer(SSL))

- 가장 널리 사용되는 보안 서비스 중 하나
- TCP에 따른 프로토콜 셋(set)으로 구현된 범용 서비스
- 차후 인터넷 표준이 RFC2246이 됨: 전송 계층 보안(TLS: Transport Layer Security)



SSL 프로토콜 스택

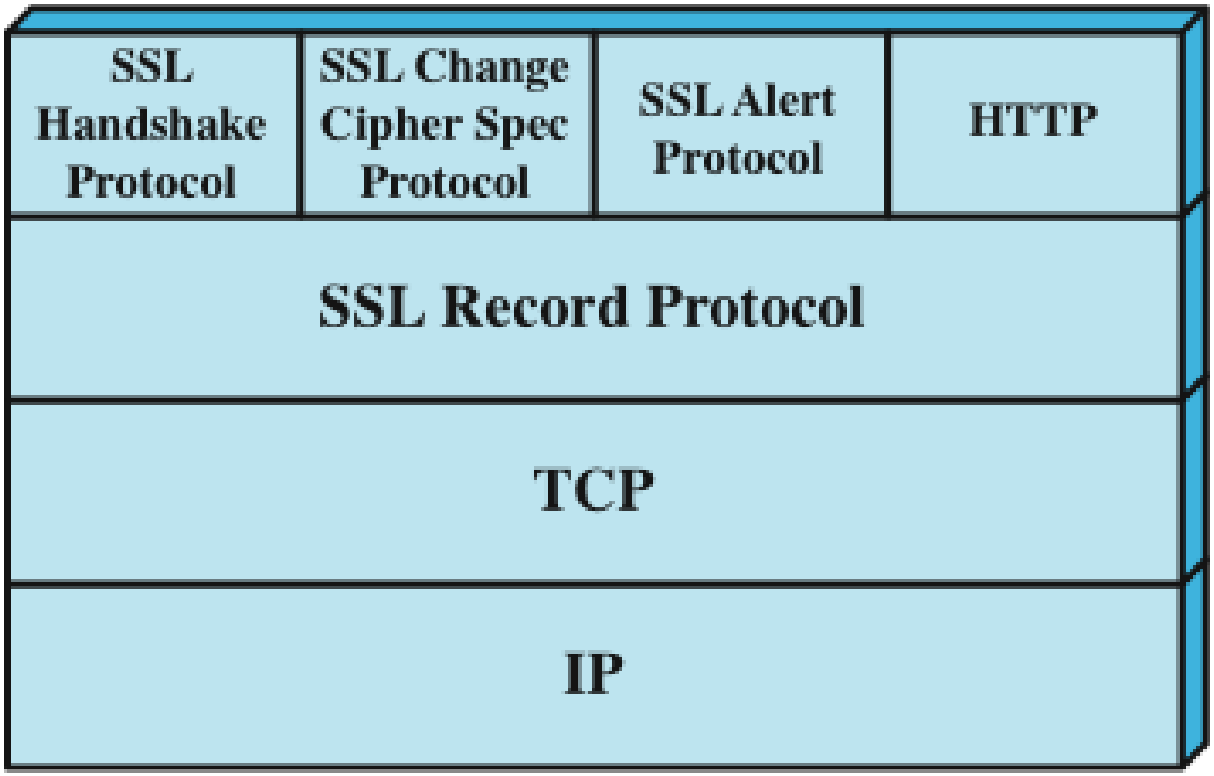


Figure 22.4 SSL Protocol Stack

SSL 레코드 프로토콜 작동

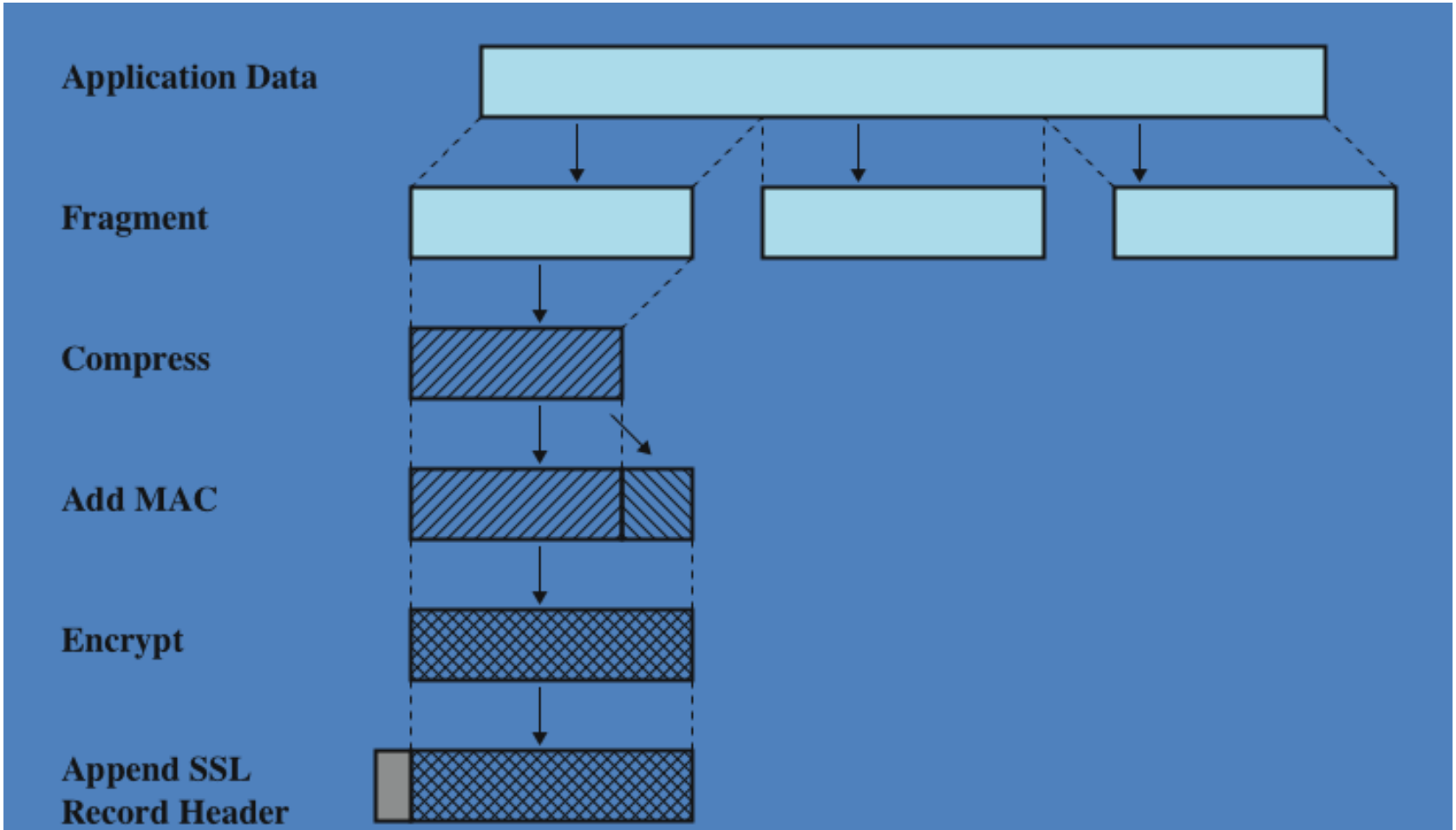
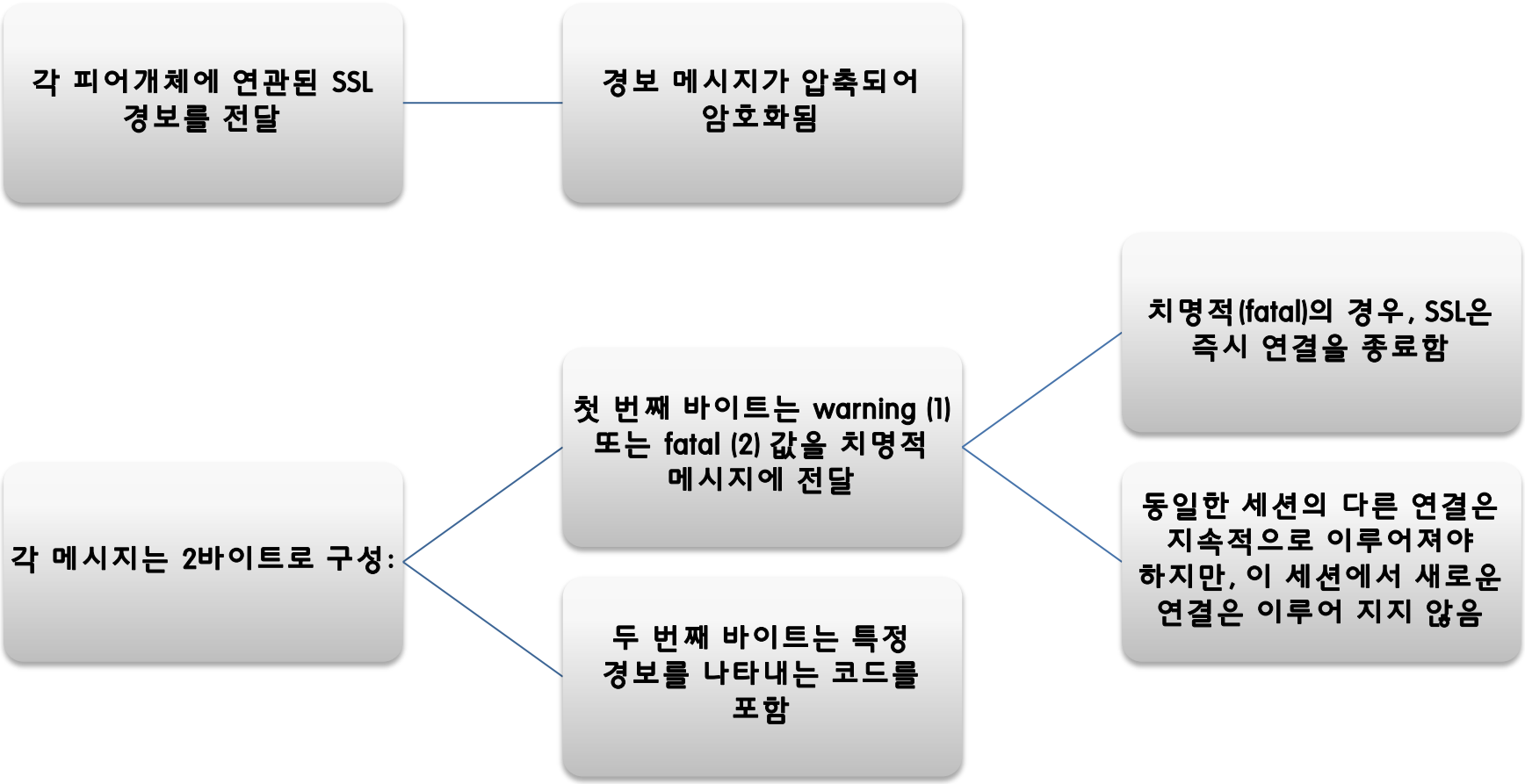


Figure 22.5 SSL Record Protocol Operation

SSL 암호 규격 프로토콜 변경
(SSL Change Cipher Spec Protocol)

- SSL 레코드 프로토콜을 사용하는 SSL 세가지 특정 프로토콜 중 하나
- 가장 간단함
- 값이 1인 싱글 바이트의 단일 메시지로 구성
- 이 메시지의 목적은 보류상태를 현재 상태로 복사(copy) 시키는 것
- 그러므로 사용하는 암호 조합을 업데이트 함

SSL 경보 프로토콜
(SSL Alert Protocol)



SSL 핸드쉐이크 프로토콜
(SSL Handshake Protocol)

- SSL의 가장 복잡한 부분
- 어플리케이션 데이터가 전송되기 전에 사용됨
- 서버와 클라이언트가 다음을 허가:

- 클라이언트와 서버가 교환하는 일련의 메시지 포함
- 교환은 4단계를 거침

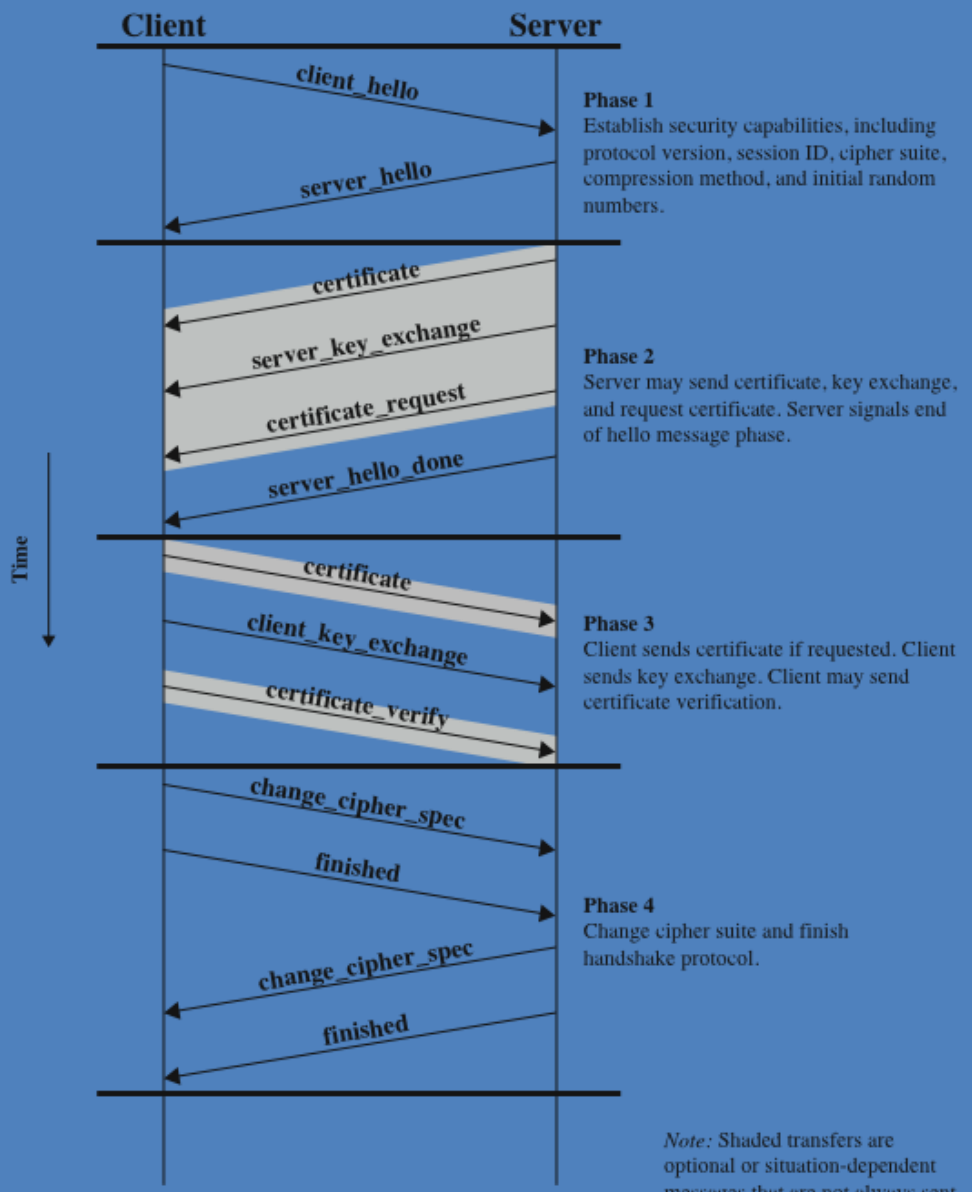
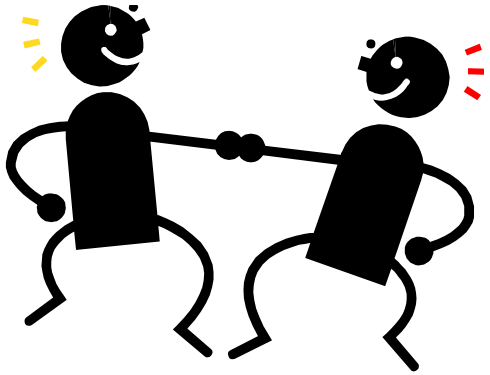


Figure 22.6 Handshake Protocol Action

SSL 핸드쉐이크 프로토콜



HTTPS
(HTTP over SSL)

- 웹 브라우저와 웹 서버간에 안전한 통신을 구현하기 위한 HTTP와 SSL의 조합
- 모든 현대 웹 브라우저에 구축됨
  - 일반 HTTP 포트 번호 : 80번
  - HTTPS 포트번호 : 443 → SSL호출
  - URL 주소가 https://로 시작

- RFC 2818에 정의됨, *HTTP Over TLS*
- HTTP의 역할을 하는 에이전트는 또한 TLS 클라이언트의 역할 또한 수행
- HTTPS 연결 중단은 TLS가 원격의 대등한 TLS 개체와의 연결을 끊도록 요청하며, 기본 TCP 연결도 중단하게 될 것

IP 보안 (IPsec)

- 다양한 어플리케이션 보안 메커니즘
  - S/MIME, PGP, Kerberos, SSL/HTTPS
- 프로토콜 계층간의 보안 문제
- 모든 어플리케이션용 네트워크에 의해 구현된 보안
- 차세대 IPv6를 포함한 인증 및 암호화 보안 기능
- 기존의 IPv4에서도 사용가능

IPsec

- 일반 IP 보안 메커니즘
- LAN, 사설 또는 공용 Wan, 인터넷 LAN을 통한 안전한 통신 기능 제공

제공사항:

인증

- 수신된 패킷이 실제 패킷 헤더의 식별된 인자에 의해 전송되었음을 보장하고 패킷의 전송이 알려지지 않도록 보장

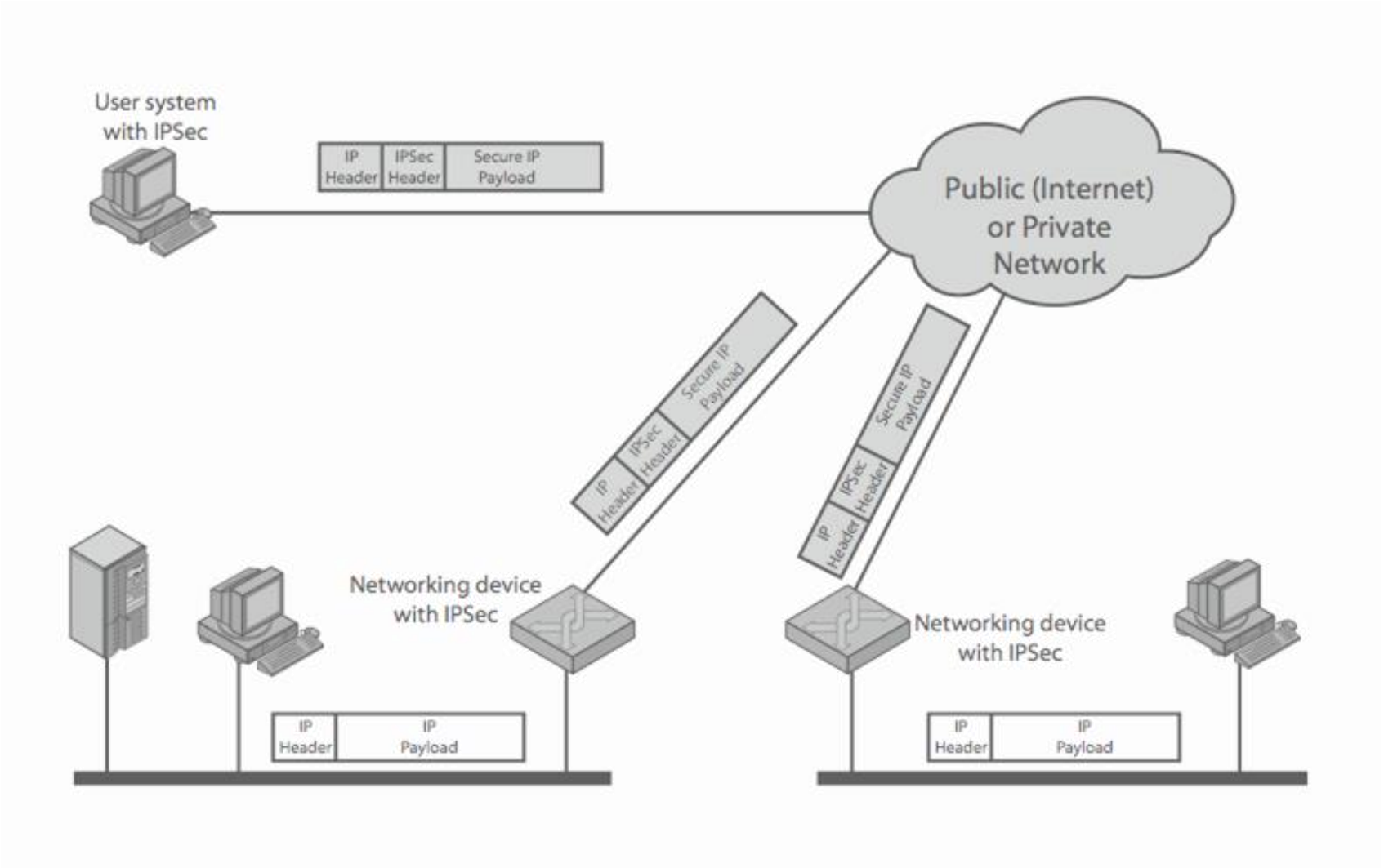
기밀성

- 암호화 메시지와 통신하는 노드가 제 3자에 의해 도청되는 것을 막아줌

키 관리

- 안전한 키 교환과 관련
- 인터넷 교환 표준 IKEv2가 제공

IPsec의 사용


User system
with IPSec
IP
Header
IPSec
Header
Secure IP
Payload
Public (Internet)
or Private
Network
Secure IP
Payload
IPSec
Header
IP
Header
Secure IP
Payload
IPSec
Header
IP
Header
Networking device
with IPSec
Networking device
with IPSec
IP
Header
IP
Payload
IP
Header
IP
Payload

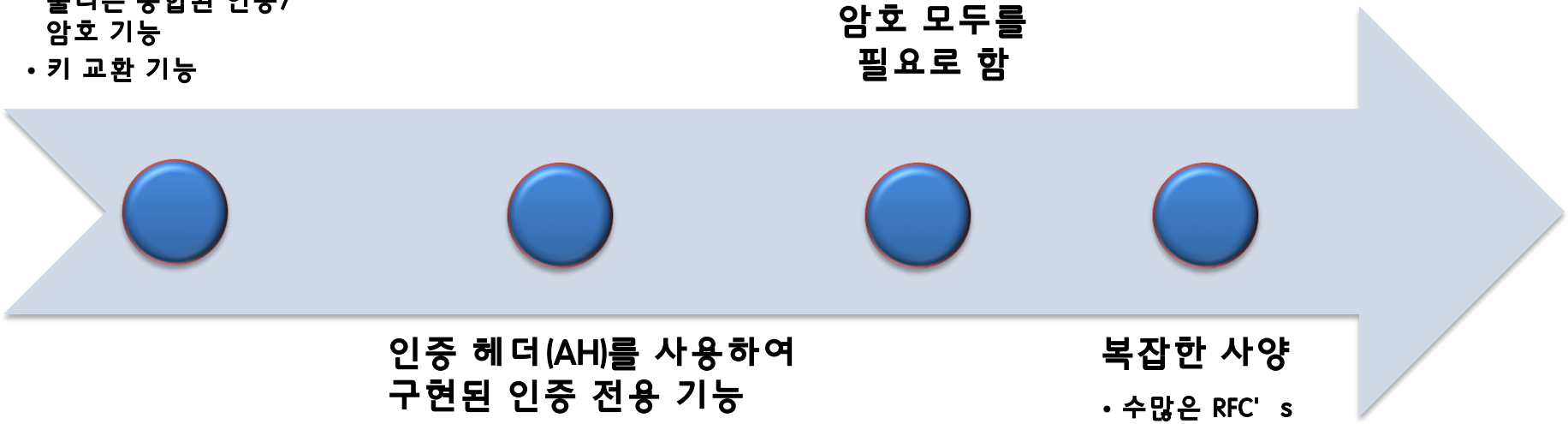
IPsec의 이점

- 방화벽이나 라우터에 구현될 경우, 이는 트래픽 경계간에 강력한 보안을 제공함
- 방화벽 우회 차단
- 전송 계층 하에 있으므로 어플리케이션에 대한 투명성 보장
- 엔드 유저에 대한 투명성
- 개인 사용자에 대한 보안 제공
- 안전한 라우팅 아키텍쳐

IPsec의 범위

두 가지 기능 제공:

- ESP(Encapsulating Security Payload)라고 불리는 통합된 인증/암호 기능
- 키 교환 기능



인증 헤더(AH)를 사용하여 구현된 인증 전용 기능

- 메시지 인증은 ESP가 제공되기 때문에, AH의 사용은 IPsecv3로의 하위 호환이 가능하지만 새 어플리케이션에서는 사용될 수 없음

VPNs는 인증과 암호 모두를 필요로 함

복잡한 사양

- 수많은 RFC' s 2401/4302/4303 /4306

보안 연관
(SA: Security Associations)

- 트래픽의 흐름을 안전하게 하는 송신자와 수신자간의 단 방향 관계
  - 대등한 관계가 2-방향식 보안 교환으로 요구될 경우, 2개의 보안 관련(SA)이 필요
- IPv4나 IPv6 헤더에 있는 목적 주소와 동봉된 확장 헤더(AH 또는 ESP)에 있는 SPI 에 의해 고유하게 식별

3가지 파라미터로 정의됨:

- Security Parameter Index (SPI)
- IP Destination Address
- Protocol Identifier

보안 페이로드 캡슐화(ESP)

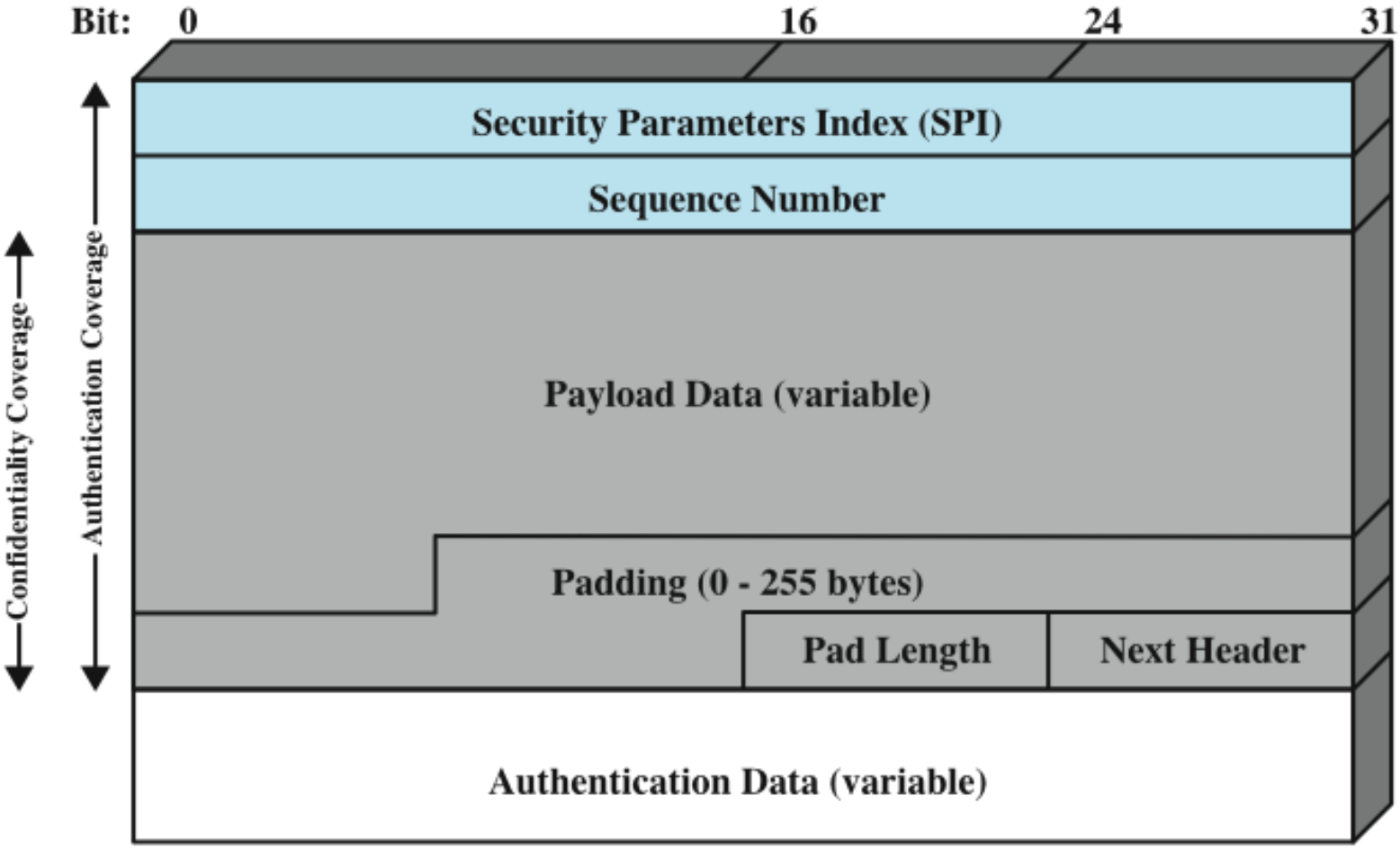


Figure 22.7 IPSec ESP Format

전송 모드와 터널 모드

- 전송모드 보호는 IP 패킷의 페이로드까지 확장
- 일반적으로 두 호스트 간의 end-to-end형 통신이 사용됨
- 전송 모드의 ESP는IP 페이로드를 암호화 하고 선택적으로 인증을 수행하지만 IP헤더는 이에 포함되지 않음

- 터널 모드는 전체 IP패킷에 대하여 보호를 제공
- 전체 원본 패킷은 터널을 통하여 IP 네트워크의 한 지점에서 또 다른 지점으로 이동
- 하나 또는 하나 이상의 보안 연관(SA)이 IPsec을 구현하는 방화벽이나 라우터와 같은 보안 게이트웨이일 때 사용됨

- 터널 모드의 방화벽 뒤의 많은 네트워크 호스트들은 IPsec의 구현 없이도 보안 커뮤니케이션에 참여 가능