2004년도 ICU부설 한국정보통신교육원지원-무선인터넷과정

유.무선 네트워크 보안

동서대학교 이훈재
hjlee@dongseo.ac.kr
http://kowon.dongseo.ac.kr/~hjlee
http://crypto.dongseo.ac.kr

정보보안 교육동영상 자료(인터넷이 되는 지역일 때만 클릭하세요!!)

당신의 정보가 유출되고 있다

인터넷 속 희망나누기
건전하고 유익한 정보공간으로 가는 길

사이버사회에서의 학부모의 역할
디지털시대의 환경오염
사이버 사회를 보호하는 법, 제도

신종범죄의 천국-사이버 공간

I. 정보 보안

- 고전 암호
- 현대 암호
- 블록 암호

고전 암호

- In Cryptography, the *meaning* of the message is hidden, not its existence
  - Kryptos = “hidden” in Greek
- Historically, and also today, encryption involves
  - *transposition* of letters
    - **Sparta’s scytale** is first cryptographic device (5th Century BC)
      - Message written on a leather strip, which is then unwound to scramble the message

  - *substitution*
    - **Kama-Sutra** suggests that women learn to encrypt their love messages by substituting pre-paired letters (4th Century AD)
      - Cipher – replace letters
      - Code – replace words

고전암호

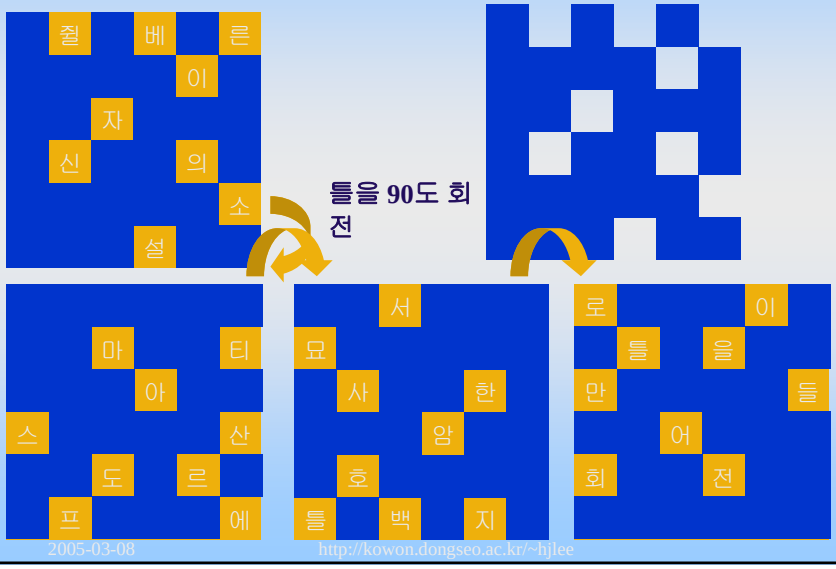
Caesar Cipher

- earliest known substitution cipher
- by Julius Caesar
- first attested use in military affairs
- replaces each letter by 3rd letter on
- example:

```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```


고전암호

- 암호틀



고전암호

- 암호틀 제작 방법
  - 마지막으로 네개의 1중 하나에 구멍을 낸다. 2부터 9까지 모두 이렇게 하면 완성.

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	6	8	7
2	5	8	9	5	4
1	4	7	3	2	1

- 제 2차 세계대전 중 남아메리카에서 활동하던 독일 스파이들은 본국으로 무선 통신할 때 이 방법을 사용하여 암호 통신을 하였다.

단순 대치식 암호

- 춤추는 난장이

「AM HERE ABE SLANEY」

(나는 여기에 왔다. 에이브 슬레이니)

「A T E L R I G E S」

「COME E L S I E」

「NEVER」

「ELSIE PREPARE TO MEET THY GOD」

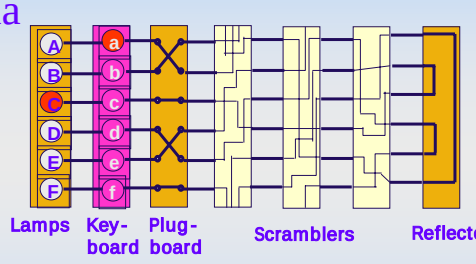
(엘시, 하느님 곁으로 갈 준비를 하라.)

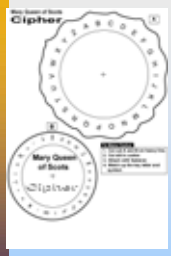
COME HERE AT ONCE

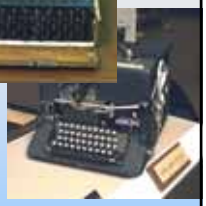
(곧 오라)

고전 암호

- Caesar's Cipher - permutation of characters
- Enigma







암호학 (Cryptology) 연구 범위

암호알고리즘

- ㅇ 블럭(Block)
- ㅇ 스트림(Stream)
- ㅇ 공개키(Public Key)
- ㅇ 확률론적 공개키 (Probabilistic Encryption)

암호 프로토콜

단순	복잡
•신분확인, 전자서명, 인증 •비밀분산 •키위탁 •특수서명 •영지식프로토콜 •전자우편	장애허용프로토콜 •전자결제 •전자화폐 •전자지불 •전자선거

키관리(Key Management System)

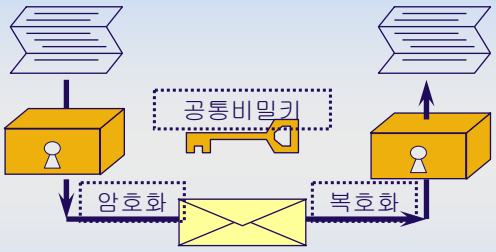
공개키디렉토리, 인증서기반, 개인식별정보기반

암호 프로토콜 응용 서비스 예

기밀성(confidentiality)	1. 소극적 공격으로 부터 전송자료를 보호 2. 트래픽 흐름분석에 대한 보호
인증(authentication)	통신의 신뢰성을 갖도록 보증함(송.수신 인증 등)
무결성(data integrity)	메시지 자체의 신뢰성을 보증함
부인 봉쇄(notorization)	송신자와 수신자의 메시지 송.수신 사실을 부정하지 못하도록 함
접근제어 (access control)	1. 시스템내의 자료의 액세스를 제어 2. 통신링크를 통한 원격 액세스 제어
가용성(availability)	정당한 사용자의 시스템 사용 요구시 사용할 수 있어야 함

대칭키 암호 (Symmetric)

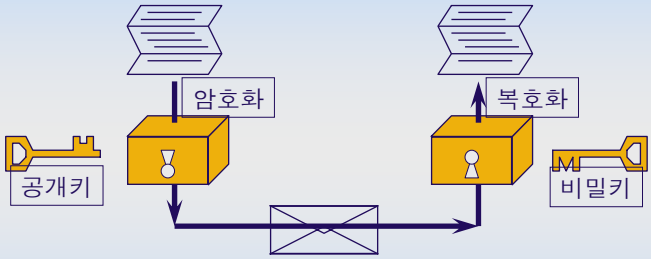
대칭키 암호시스템(관용암호, 비밀키 암호)



- 특징 : 암호화키와 복호화키가 동일
- 장점 : 암호화 및 복호화 속도가 빠름
- 단점 : 키관리의 어려움. 키분배의 문제. 다양한 응용의 어려움
- 사례 : DES, FEAL, IDEA, Skipjack, AES, SEED 등

비대칭키 암호 (Asymmetric)

비대칭형 암호시스템(공개키 암호)



- 특징 : 복호화키(=비밀키)와 암호화키(=공개키)가 다름
- 장점 : 키관리가 용이. 다양한 응용이 가능. 안전성이 뛰어남
- 단점 : 암호화 및 복호화 속도가 느림
- 사례 : RSA 등

해쉬 함수 (Hash Function)

임의의 길이를 가지는 문서

해쉬함수

고정된 길이를 가지는 문서

해 쉬 함 수

- 특징: 일방향(one-way) 함수, 메시지 압축
- 용도: 디지털서명, 메시지무결성
- 알고리즘: SHA-1, MD5 등

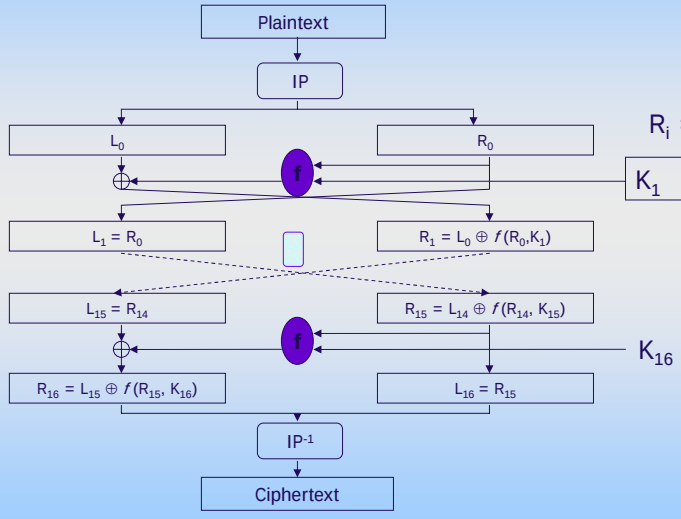
DES의 역사

- 1973년 다음 전제 조건을 전제로 표준 알고리즘을 공모
  1. 표준 암호 알고리즘은 높은 수준의 안전성을 보장할 수 있어야 한다.
  2. 표준 암호 알고리즘은 사양의 정의가 완전하여 간단히 이해할 수 있어야 한다.
  3. 표준 암호 알고리즘이 제공하는 안전성 알고리즘의 비밀성에 의존되어서는 안 된다.
  4. 표준 암호 알고리즘은 사용자나 제작자가 모두 사용 가능해야 한다.
  5. 표준 알고리즘의 응용이 다양해야 한다.
  6. 표준 암호 알고리즘은 전자 장치로써 제품화가 간단하고 또한, 사용이 간단해야 한다.
  7. 알고리즘의 타당성 검증에 협력해야 한다.
- 1974년 8월 2차 공모
  Water Tuchman과 Carl Meyer가 lucifer cipher를 개량한 암호 알고리즘이 위의 조건이 만족되어 표준 암호 알고리즘으로 검토되기 시작
- 1977년 1월 15일 정식 등록
- DES는 5년마다 안전성을 검토
- ANSI의 표준으로 지정되어 순수 민간용으로 사용하고 있음

DES의 기본 개념

- DES는 64비트의 키를 적용하여 64비트의 평문을 64비트의 암호문으로 암호화 시키는 대칭형 블록 암호기법
- 대체(substitution)과 치환(permutation)이라는 2개의 기본적인 암호화 함수가 반복적으로 16회 적용
  1. 혼돈(confusion) : 평문 1비트의 변화가 암호문에 어떤 변화를 초래할지를 예측할 수 없는 성질
  2. 확산(diffusion) : 평문을 구성하는 각각의 비트들의 정보가 여러 개의 암호문 비트들에 분산되어야 한다는 성질
- DES에서는 대체는 체계적으로 어떤 비트들의 유형을 다른 비트들로 전환함으로써 혼돈 성질을 제공하고, 반면에 치환은 비트들의 순서를 재배열함으로써 효과를 띄게 한다.

DES 내부 구조



$L_i = R_i\text{-}1$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

DES 내부 구조

❑ IP(Initial Permutation)

평 문

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	19	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

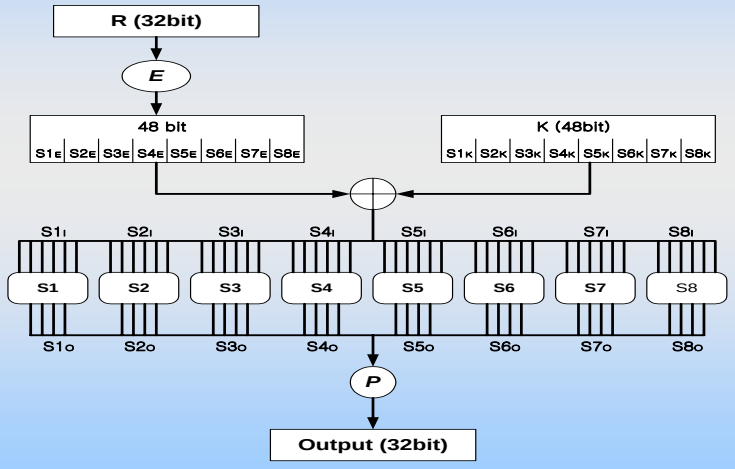
IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

- IP
  58번째 비트 -> 1번째 비트 / 50번째 비트 -> 2번째 비트
- IP^{-1}
  1번째 비트 -> 58번째 비트 / 2번째 비트 -> 50번째 비트

DES 내부 구조

❑ *f* Function



DES S-BOX 원리

(1 0 1 1 1 1) : *Input*

S1

• • • • • • • • • • • •

(0 1 1 1) : *Output*

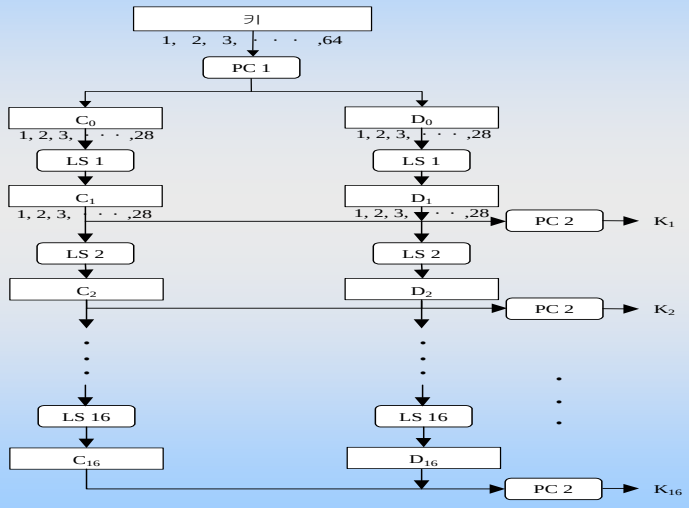
$11_{(2)}$ =3rd ROW

$0111_{(2)}$ = 7TH COLUMN

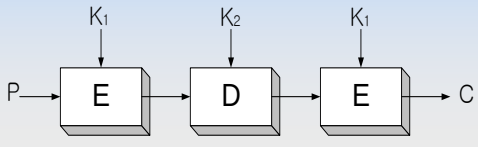
S1 box

ROW	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
11	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

DES 키 스케쥴링

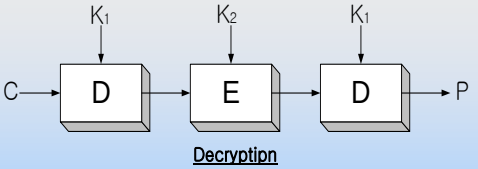


- T-DES(Triple DES with two keys)



$C = E_{K_1}[D_{K_2}[E_{K_1}[P]]]$

Encryption



$P = D_{K_1}[E_{K_2}[D_{K_1}[C]]]$

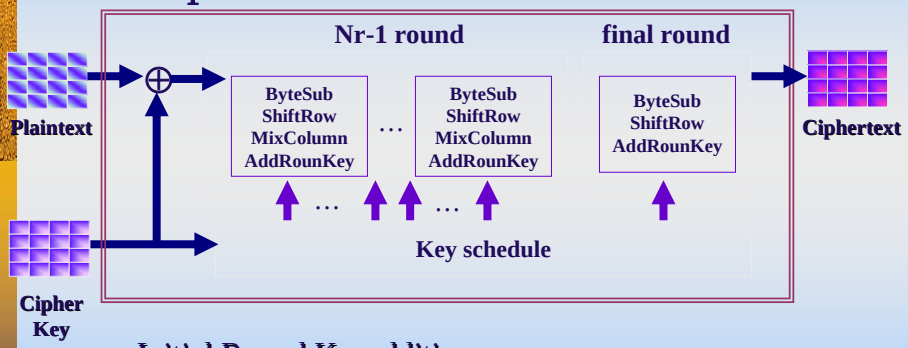
Decryptipn

Multiple Encryption

- AES 개발 배경
  - 1977년 - DES (미연방 표준)
  - 1996년 - DES의 효과적인 공격법 제안
    - DC : 2^{47}
    - LC : 2^{43}
  - 1997년 – NIST 알고리즘 공모
  - 2000년 10월 – Rijndael 채택
  - 2001년 8월 – FIPS 공식 문서로 발표

- Rijndael의 특징
  - 가변 길이 Key Length : 16,24,32 bytes
  - 가변 길이 Block Size : 16,24,32 bytes
  - 디자인의 간결성
  - 알려진 모든 공격에 안전
  - 다양한 플랫폼에서 speed 와 compact
  - SP-Network 구조
  - 블록 전체가 라운드마다 대치와 치환을 반복수행
  - 블록 code 응용
  - Operation over GF(2^8) extension field

Cipher의 구성



Initial Round Keyaddition
Nr-1 Rounds
final round

Rijndael의 Key, Block 크기

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$

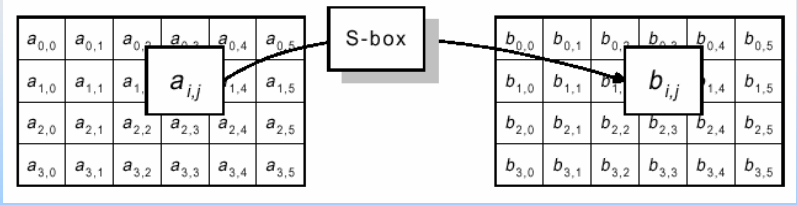
가변적 Block Size :
16 byte(128 bit)
24 byte(192 bit)
32 byte(256 bit)

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

가변적 Key Size :
16 byte(128 bit)
24 byte(192 bit)
32 byte(256 bit)

♦ Rijndael의 SubBytes – Round Step 1

✓ S-box(substitution table) 적용
- 높은 비선형성(non-linearity)
- 1-byte(State) 단위 연산
- GF(2^8)상의 연산
  역함수
  Affine (over GF(2)) transformation 적용



– Rijndael의 S-box

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

IDEA(International Data Encryption Algorithm)

- Xuejia Lai , James Massey at Swiss Federal Institute of Technology
- DES vs. IDEA
  - DES : 64bit data block, 56bit key size, 16 round
  - IDEA : 64bit data block, 128bit key size, 8 round
- Cryptographic Strength
  - Block length : 64bit, long enough to deter statistical analysis.
  - Key length : 128bit, long enough to prevent exhaustive key searches
  - Confusion : complicate the determination of how the statistics of the ciphertext depend on the statistics of the plaintext
  - Diffusion : each plaintext bit should influence every ciphertext bit, and each key bit should influence every ciphertext bit.

Implementation

- IDEA : facilitate both S/W and H/W implementation
- S/W implementation
  - Use 16bit subblocks
  - Use simple operations
- H/W implementation
  - Similarity of encryption and decryption
  - Regular structure

♦ Encryption

- 8-round
  (6 x 8 = 48 subkeys)
- output transformation
  (4 subkeys)
- Key generation
  (16-bit, 52 subkeys)

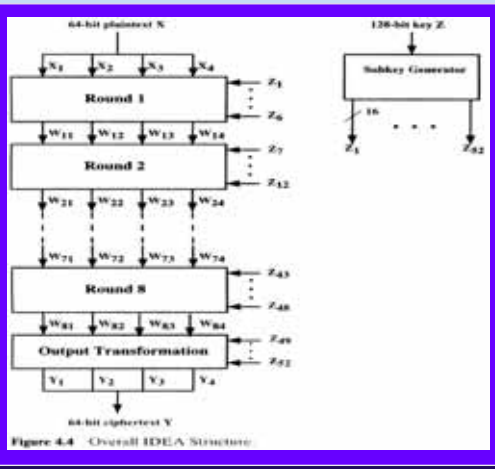
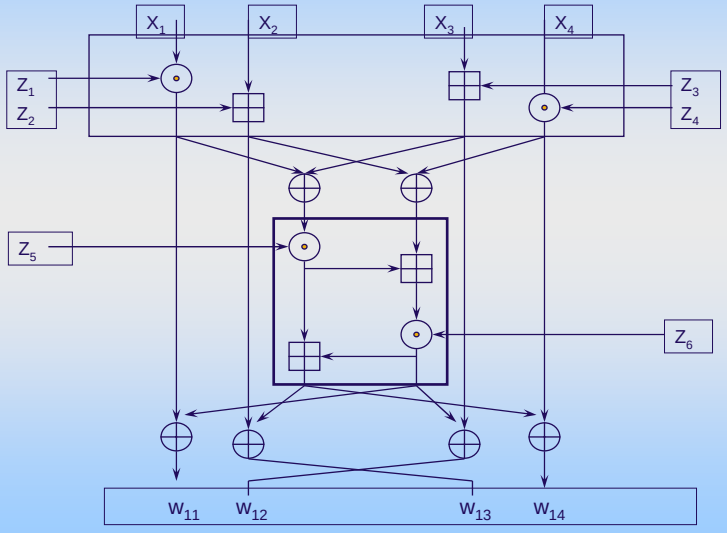


Figure 4.4 Overall IDEA Structure

❑ Single Iteration of IDEA



♦ Conf.& Diff.➔ MA(multiplication/Addition)

- three operations: two 16bit inputs, two 16bit keys → two 16bit outputs

⊕ : XOR

⊞ : Addition of integers mod(2^{16})

⊙ : Multiplication mod(2^{16} + 1)

0000000000000000
⊙ 1000000000000000
= 1000000000000001
2^{16} x 2^{15} mod (2^{16} + 1)

- Effectiveness: complete diffusion

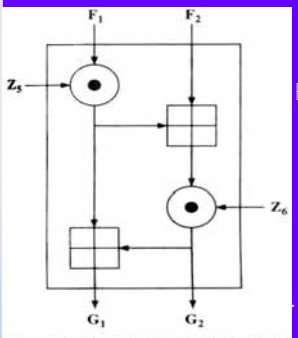


Figure 4.3 Multiplication/Addition (MA) Structure.

♦ Subkey generations : 16-bit, 52 subkeys

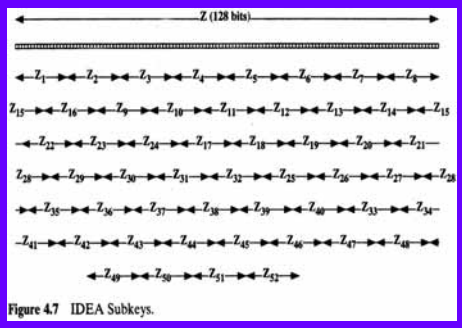


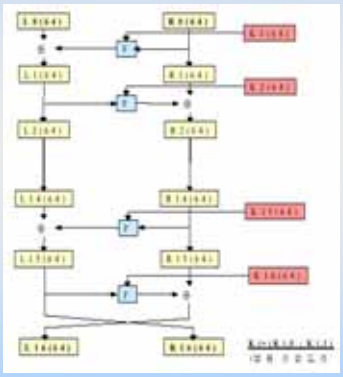
Figure 4.7 IDEA Subkeys.

- 128bit key → 16-bit 52 subkeys generated
- circular left shift of 25-bit position:

Z1 = Z[1 .... 16]
Z7 = Z[97 .... 112]
Z13 = Z[90 .... 105]
Z19 = Z[83 .... 98]
Z25 = Z[76 .... 91]
Z37 = Z[37 .... 52]
Z43 = Z[30 .... 45]

블록 암호

SEED



SEED 전체 구조도

- 국내 전자상거래의 활용 가능한 안전한 대칭키 암호알고리즘의 한국표준으로 개발되어 채택
- 구조
  전체 16round로 128비트 평문 블록을 128비트 비밀키를 이용해 암호화하는 DES와 유사한 feistal구조

  F함수의 비선형성 그 안전도를 의존
- 특징
  암복호 블록과 키 길이를 DES의 2배인 128비트로 하고 F함수의 비선형성을 높여서 안전도를 강화

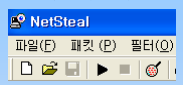
Security Solution

- Client/Server Authentication (Kerberos)
- Remote User Authentication Service (RADIUS)
- Public-Key Infrastructure (PKI)
- IP Layer Security (IPSec)
- Web Access Security (SSL)
- E-mail Confidentiality (PGP, S/MIME)
- Wireless LANs Security (802.11b)
- Cellular Phone Security (WPKI)

Wireless Security Issues

- Authentication
  - EAP-MD5, TTLS, PEAP(ID, PSWD, MAC), IEEE802.1x
  - PPP CHAP(IMSI, ESN)
  - RADIUS and DIAMETER interworking
  - Reauthentication across network roaming
- Security
  - WEP, TKIP, AES : Encrytion protocol
  - EAP authentication & Key Establishment
  - Key Exchange protocol
- Accounting
  - RFC2866 accounting
  - Flat rate, Usage based: packet, time
  - Accounting at PDSN, AP
  - IPDR brokering system

II. 인터넷 보안 ➔ 데모:



인터넷

인터넷 보안

방화벽(Firewall)

전자 메일 보안

WWW 보안

SSL/TLS

Ipsec

VPN

인터넷

- 네크워크들의 네트워크
- 네트워크의 상호연결을 위한 Defence Advanced Research Project Agency(DARPA)의 결과
- TCP/IP를 사용
- 네트워크들은 라우터에 의하여 연결됨.
- 세계 어느 곳에나 접속할 수 있음⇒ 보안문제 발생

인터넷 (계속)

- 인터넷 서비스
  - Remote log-in(telnet)
  - file transfer (anonymous file transfer, ftp)
  - E-mail
  - WWW service

인터넷(계속)

- 인터넷 접속모델

인터넷 보안

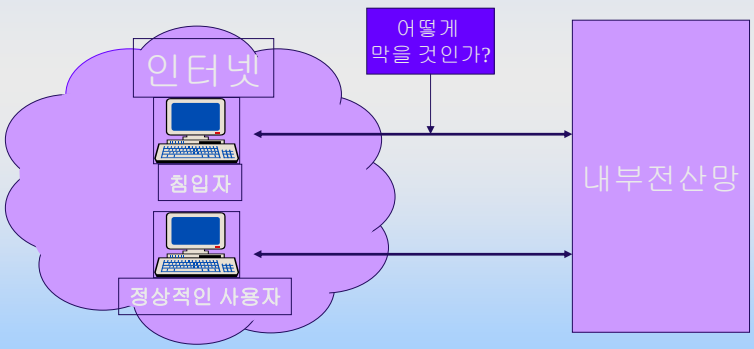
- 인터넷의 정보보호 취약성
  - 인터넷은 개방적임
  - UNIX, TCP/IP 등의 소스가 개방되어 있음
  - 침입자들의 상호 정보 교환이 쉬움
- 침입자에 의한 위협요소
  - 시스템에 대한 불법 접근 및 사용
  - 정보의 열람, 파괴 및 변조
  - 정상적인 시스템 서비스 방해

인터넷 보안(계속)

- 인터넷 보안 시스템
  - 방화벽
    - 패킷 필터링 방화벽
    - 응용게이트웨이 방화벽
  - 전자메일보안
    - PEM
    - PGP
  - WWW 보안
    - 기본인증
    - 네트워크 주소를 이용한 접근제어
    - 패스워드 검사와 네트워크 주소를 병합한 접근제어
    - Secure HTTP (S-HTTP)
    - Secure Socket Layer(SSL)

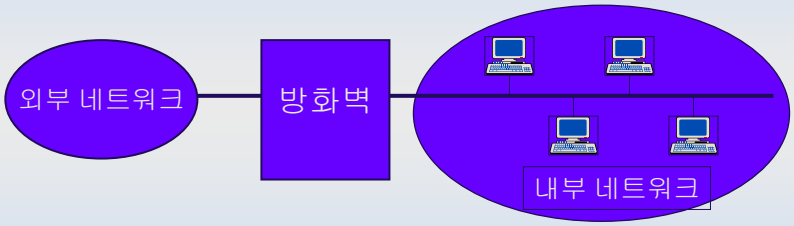
인터넷 보안(계속)

- 인터넷 보안 모델



방화벽

- 방화벽



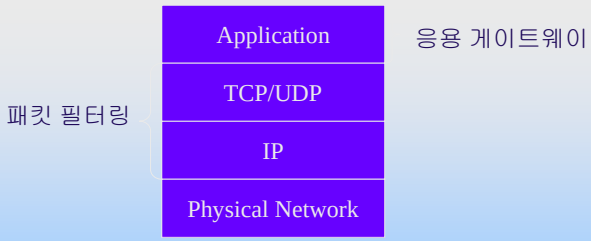
  - 내부 네트워크에 대한 접속제어나 외부 네트워크로부터의 보호
  - 라우터나 응용 게이트웨이에서 구현됨.
  - 외부 네트워크와 내부 네트워크 사이에 허가된 트래픽만을 통과

방화벽(계속)

- 방화벽 시스템 정보보호 서비스
  - 사용자 인증
    - 정보를 교환하는 상대 확인, 접근 자격 유무를 확인하는 절차
  - 접근제어
    - 불법 침입자에 의한 불법적인 자원 접근 및 파괴 방지
  - 트래픽 암호화
    - 트래픽의 노출을 방지하기 위해 전송되는 트래픽을 암호화
  - 트래픽 로그
    - 외부 네트워크과 내부 네트워크 사이의 모든 트래픽 기록
  - 감사추적기능
    - 누가, 언제, 어떤 호스트에 접근하여, 어떤 정보를, 어떻게 얼마동안 접근하였는가를 기록

방화벽(계속)

- 방화벽의 유형
  - 패킷 필터링 방화벽 (네트워크 계층)
  - 응용 게이트웨이 방화벽 (응용 계층)

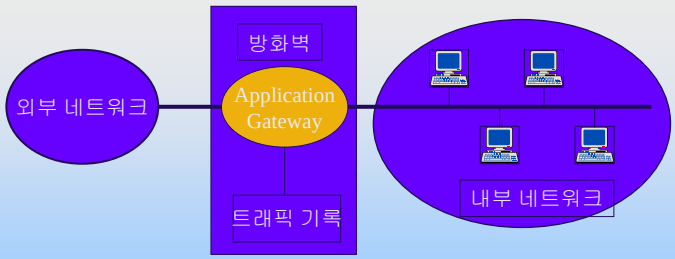


방화벽(계속)

- 패킷 필터링 방화벽
  - 네트워크 계층에서 다음의 정보에 의해 허가된 트래픽만을 통과시킴
    - 패킷의 송신자 IP 주소와 포트
    - 패킷의 수신자 IP 주소와 포트
    - 프로토콜 필드 : TCP 또는 UDP
    - TCP 프로토콜 플래그 : SYN와 ACK
  - 많은 상용 라우터들과 방화벽 시스템들은 패킷 필터링 기능을 가짐.

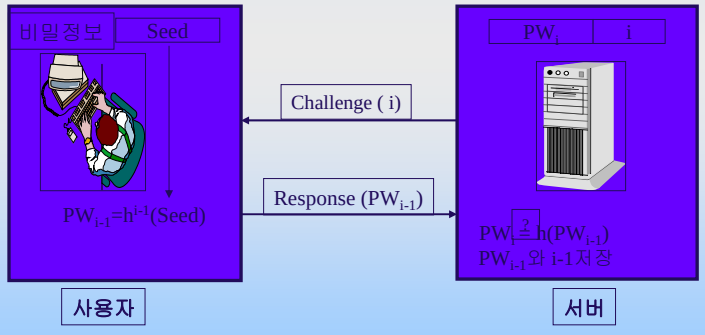
방화벽(계속)

- 응용 게이트웨이 방화벽
  - 응용계층에서 인증, 내용 보안등을 수행
  - 응용계층에서 사용에 대한 기록유지 및 감사추적
  - One-Time Password, Kerberos 등을 사용하여 인증



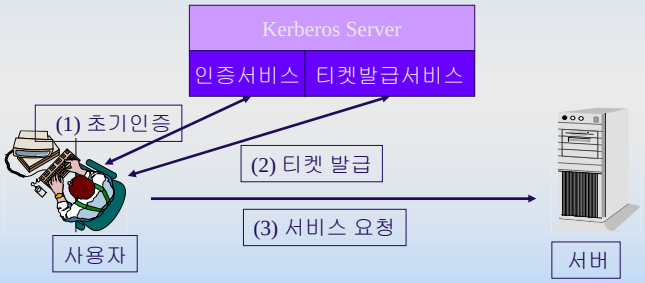
방화벽(계속)

- 인증기법
  - **One-Time Password (S/KEY)**



방화벽(계속)

- **Kerberos**

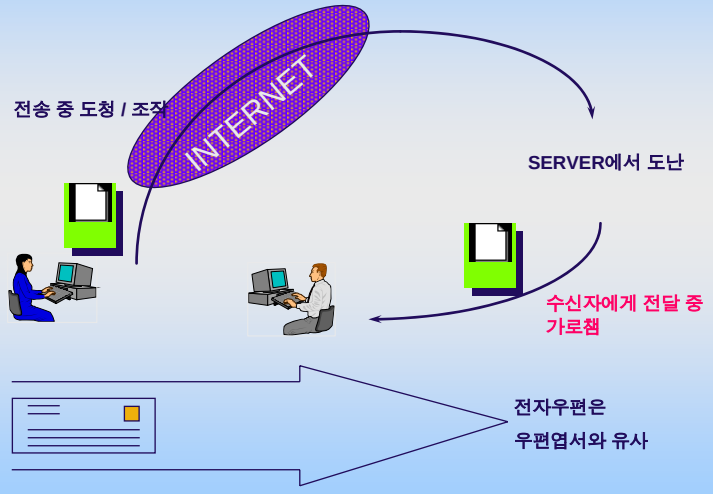


  - 특징
    - MIT에서 개발된 네트워크 인증 시스템
    - 종단 사용자를 인증하기 위하여 설계

방화벽(계속) ➔ 데모: ZONE ALARM

- 방화벽의 장•단점
  - 장점
    - 내부 시스템들이 각각 보안 대책이 없더라도 방화벽으로 인해 내부 네트워크에 연결된 모든 시스템을 외부로부터 보호
    - 방화벽 시스템 운영자가 지정한 사용자만이 내부 네트워크로 들어올 수 있도록 설정 가능
  - 단점
    - 방화벽이 설치된 게이트웨이가 침입당하면 내부 네트워크에 연결된 모든 시스템의 보안을 보장 못함
    - 내부 네트워크에서 외부 네트워크로의 통신에 제한을 받을 수 있음.
    - 방화벽에서 병목현상이 생길 수 있음

전자우편 보안



전자우편 보안

- 전자우편 보안 요구사항
  - 기밀성 (Confidentiality)
  - 무결성 (Integrity)
  - 데이터의 출처 인증(Data Origin Authentication)
  - 송신 부인 방지 (Nonrepudiation of origin)
  - 수신 부인 방지 (Nonrepudiation of receipt)

❑ 전자우편 보안 서비스

- ❑ 메시지 기밀성
- ❑ 송신자에 대한 실체인증
- ❑ 메시지 무결성
- ❑ 부인봉쇄

- ❑ **PEM** (Privacy Enhanced Mail)
- ❑ **PGP (Pretty Good Privacy)**
- ❑ **S/MIME(Secure/Multipurpose Internet Mail Extensions) , by RSA 사**
- ❑ **MOSS(MIME Object Security Service)**

♦ Privacy Enhanced Mail (PEM)

– PEM 기능과 알고리즘

기 능		사용된 알고리즘
기밀성		DES-CBC(메시지), RSA(세션키)
송신자 인증		RSA, MD2 or MD5
메시지 무결성		MD2 or MD5, DES-ECB or DES-EDE
세션키 분 배	대칭 암호	DES-ECB or DES-EDE
	비대칭암호	RSA, MD2

– 특징

- 키관리 기반체제를 이용한 전자우편 시스템
- 기밀성, 송신자 인증, 메시지 무결성, 발신자 부인봉쇄 제공
- 전자우편에 정보보호 관련기능을 제공하는 인터넷 표준

- Pretty Good Privacy (PGP)
  - PGP 기능과 알고리즘

기 능	사용된 알고리즘
기밀성	IDEA(메시지), RSA(세션키)
송신자 인증	RSA, MD5
압 축	ZIP

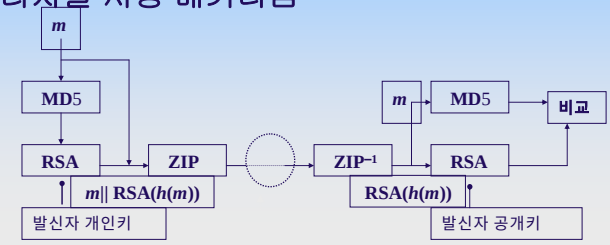
  - 특징
    - Phil R. Zimmerman이 개발
    - 다양한 운영체제에서 사용
    - 기밀성과 인증 기능을 가짐.

PGP

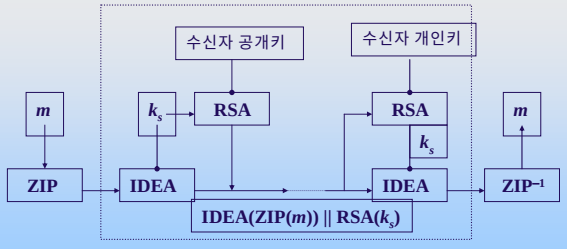
- Phil Zimmerman
- 전세계적으로 다양한 기종에서 실행되는 공개 소프트웨어
- 공개적인 검토 작업을 통해서 대단히 안전하다고 할 수 있는 알고리즘을 기반
  - 공개키 암호 **RSA**, 대칭형 암호 **IDEA**, 해쉬 함수 **MD5**
- 파일과 메시지를 암호화하는 표준화된 방법

기능	알고리즘
메시지 암호화	**RSA, IDEA**
디지털 서명	**RSA, MD5**
압축	**ZIP**
전자우편 호환성	**기수–64 변환**

PGP 디지털 서명 메커니즘

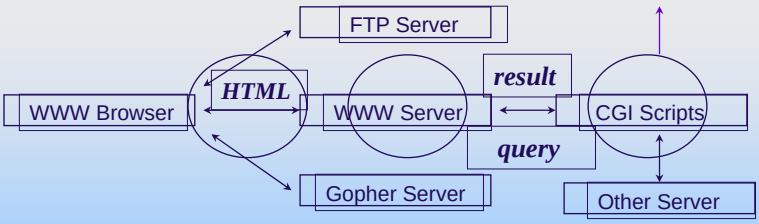


PGP 기밀성 메커니즘



WWW 보안

- Browser (Explorer, Netscape) Server (NCSA HTTP, httpd)
- URL (Uniform Resource Locator)
- HTML (HyperText Manipulation Language)
- CGI (Common Gateway Interface) - e.g. form processing



❑ WWW 보안 요구사항

- ❑ Client / Server 상호인증
- ❑ 교환되는 메시지 / 문서의 무결성
- ❑ 기밀성

❑ WWW 보안 프로토콜

- ❑ 채널보안기법
  - ❑ SSL (Secure Socket Layer)
  - ❑ PCT (Privacy Communication Technology)
- ❑ 메시지 보안기법
  - ❑ S-HTTP

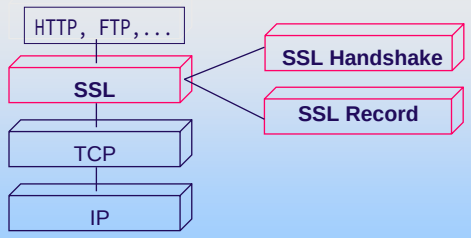
WWW 보안

- WWW 보안 요구사항
  - HTTP 트랜잭션의 기밀성
    - WWW의 통신에서 사용자와 서버만이 통신하는 내용을 알 수 있음
      ⇒ HTTP 해더와 본문 내용을 암호화한 후 수신자를 나타내는 해더를 암호문에 붙여줌.
  - 서버와 클라이언트에 대한 인증
    - HTTP 트랜잭션이 일어나기 전에 상대방에 대한 인증
      ⇒ 특정 메시지에 디지털 서명을 붙여줌.
  - HTTP 트랜잭션의 무결성
    - 클라이언트의 request와 서버의 response가 전송도중 변경되지 않았다는 것을 확인
      ⇒ 메시지에 해쉬값을 함께 보냄.

WWW 보안 (계속)

- WWW 보안 방법들
  - 기본인증
    - 사용자의 ID와 패스워드를 이용하여 인증
  - 네트워크 주소를 이용한 접근제어
    - 허가된 네트워크 주소에서 접근한 사용자만 접근을 허용
  - 패스워드 검사와 네트워크 주소를 병합한 접근제어
    - 허가된 네트워크 주소의 허가된 사용자만 접근을 허용
  - Secure HTTP (S-HTTP)
    - 응용 레벨에서의 메시지의 암호화를 제공
  - Secure Socket Layer(SSL)
    - 응용계층과 TCP/IP계층의 사이에서 암호화된 채널을 제공

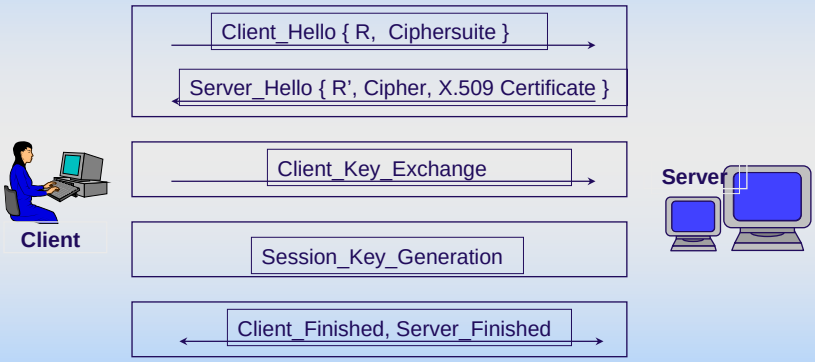
- **SSL (secure socket layer)** ➔ 데모 : 우리은행
- Netscape Communications
- Privacy, Data Integerity, Server [Client] Authentication,
- RSA, Diffie-Hellman, Fortezza for Key Exchange
- DES, 3DES, IDEA, RC2, RC4[stream cipher] for Data Encryption
- MD5, SHA for Hash Function (MAC)



Algorithm Negotiation,
Key Exchange,
Authentication

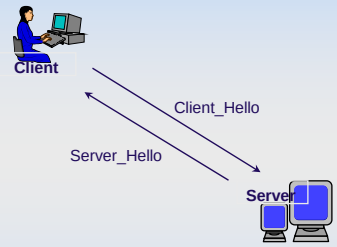
Data Encapsulation
for data protection

SSL Handshake Protocol



SSL Client Hello Phase

- client SSL version
- 28-byte random number R
- session ID
- cipher_suites
- compression methods



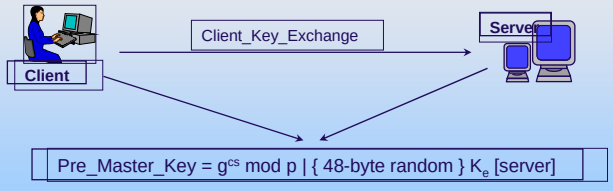
SSL Server Hello Phase

- server SSL version
- 28-byte random number R'
- session ID -> If a new session, server's certificate
- cipher_suite { key exchange algorithm }
- compression method

SSL Client Key Exchange

- Key Exchange Algorithm's Parameter in Certificate
  - RSA : public exponent k_e, modulus n
  - Diffie-Hellman : g, modulus p, g^s mod p
- From *Pre_Master_Key* To *Mater-Key* [MD5, SHA, R, R']

Master_Key = MD5 (Pre_Master_Key || SHA ('A' || Pre_Master_Key || R || R')) ||
MD5 (Pre_Master_Key || SHA ('BB'|| Pre_Master_Key || R || R'))||
MD5 (Pre_Master_Key || SHA ('CCC'|| Pre_Master_Key || R | R'))



SSL Session Key Generation

- Keys for data encryption and data integrity

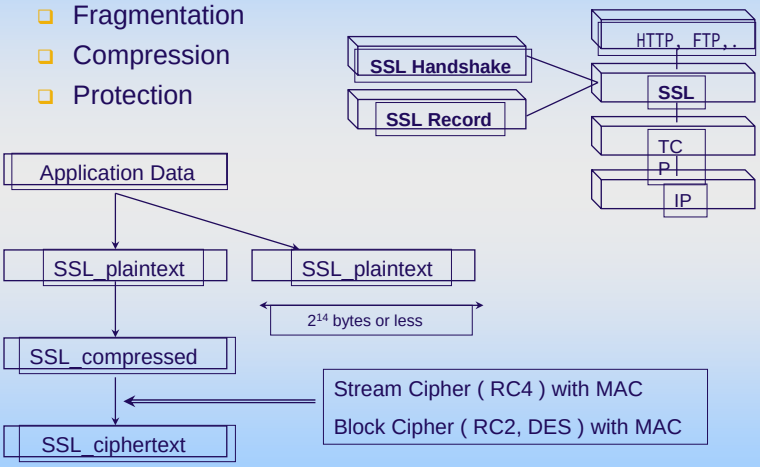
Key_Block = MD5 (Master_Key || SHA ('A' || Master_Key || R || R')) ||
MD5 (Master_Key || SHA ('BB' || Master_Key || R || R')) ||
MD5 (Master_Key || SHA ('CCC' || Master_Key || R || R')) || .....

SSL Client-Server Finished

- Key Exchange, Authentication 확인
- Negotiated Algorithm, Parameter
- All Handshaked Messages
- Sender's value { client[0x434C4E54], server[0x53525652] }

SSL Record Protocol

- Fragmentation
- Compression
- Protection



Change cipher spec 프로토콜

- Change cipher spec 메시지는 이후의 레코드에 대해 cipherspec에 정의된 알고리즘과 키를 이용해 보호될 수 있도록 수신측에 알리기 위해 사용된다.
- 클라이언트는 키 교환메시지와 인증서 확인 메시지를 전송한 후에 보냄
- 서버는 클라이언트로부터 받은 키 교환 메시지를 성공적으로 처리한 후에 보냄

Alert 프로토콜

- SSL 레코드 계층에서 제공되는 컨텐츠 타입 중 하나
- 각종 오류에 대한 메시지와 설명을 전송하는데 이용

(압축 및 암호화 오류, MAC 오류, 인증서 오류, 프로토콜 실패 등)

SSL/TLS

❑ SSL/TLS란?

► End-to-End 서비스에서 인증이나 암호화 기술, 압축기술 등을 이용하여 트랜스포트 계층 위에서 적용되는 보안 프로토콜

► TCP를 이용하여 신뢰할 수 있고 안전한 End-to-End 서비스 제공

► SSL은 미국의 Netscape사에 의하여 개발되었고, TLS v1.0은 IETF에서 개발한 표준 프로토콜로 SSL v3.0과 유사

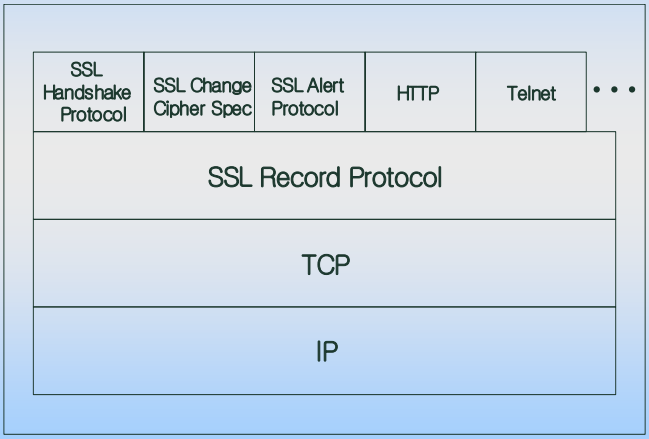
SSL/TLS

❑ SSL/TLS의 계층

<table>
<tr><td>HTTP</td><td>FTP</td><td>SMTP</td></tr>
<tr><td colspan="3">SSL or TLS</td></tr>
<tr><td colspan="3">TCP</td></tr>
<tr><td colspan="3">IP</td></tr>
</table>

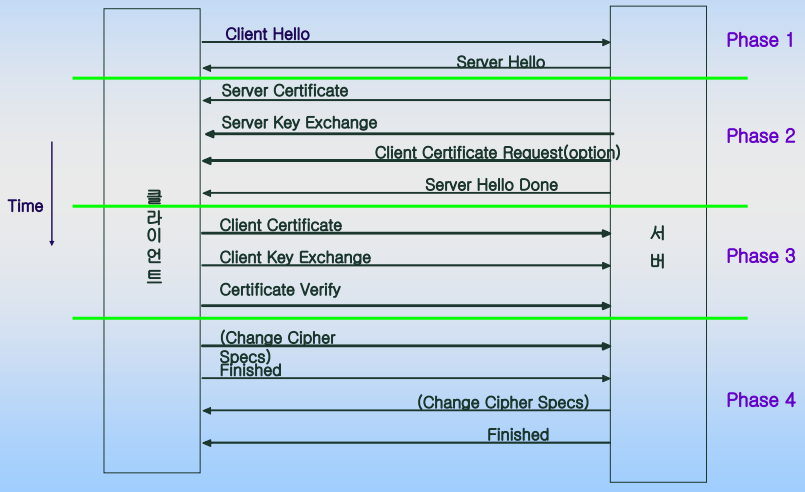
SSL/TLS

❑ SSL/TLS의 구성도



SSL/TLS

❑ Handshake Protocol



SSL/TLS

❑ Change Cipher Spec

► 암호 알고리즘이나 해쉬함수, 압축방법 등의 변경 설정

► 1 Byte(value: 1)로 구성

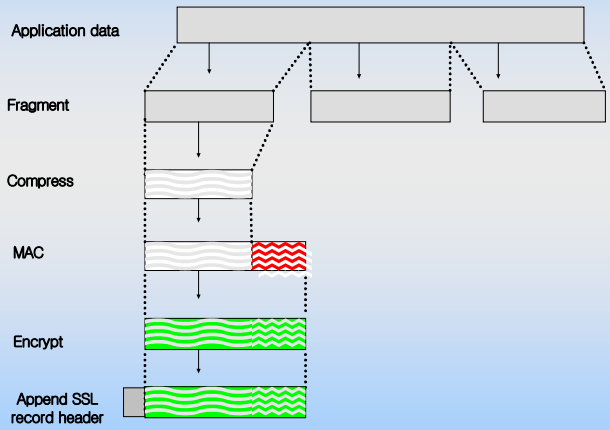
❑ Alert Protocol

► 압축이나 암호화 오류, MAC 오류, SSLHP 실패, 인증서 오류 등에 대한 메시지 처리

► 2 Byte(Level, Alert)로 구성

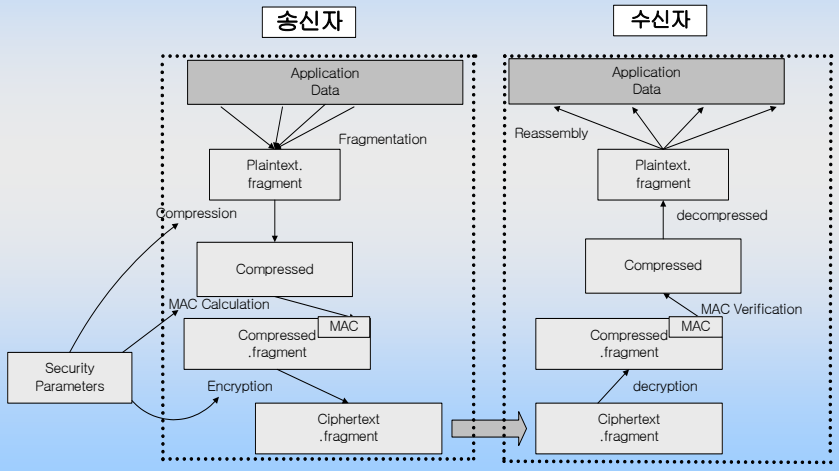
SSL/TLS

❑ Record Protocol 동작



SSL/TLS

❑ 송•수신 시 Record Protocol 동작



IPSEC

❑ IPsec이란?

► 인증, 무결성, 기밀성, 접근제어, 재전송 방지 기능 제공

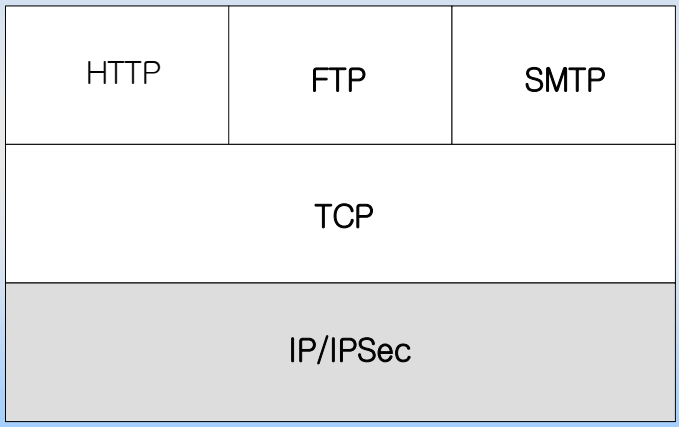
► PPTP(Point-to-Point Tunneling Protocol) 와 L2TP(L2 Tunneling Protocol)의 결합 구조

► 인터넷 프로토콜 계층에서 동작하므로 Application Program이나 Protocol의 보안 부담 감소

► IPv4와 IPv6에 모두 적용

IPSEC

❑ IPsec 레벨



IPSEC

❑ IPsec 구성

보안 프로토콜	데이터 관리기술	키관리 메커니즘
AH (Authentication Header) ESP (Encapsulating Security Protocol)	SPD (Security Policy Database) SAD (Security Association Database)	IKE (Internet Key Exchange)

IPSEC

❑ IKE

► 인증과 암호화에 필요한 암호알고리즘 키를 생성하고, 분배하기 위한 것으로 ISAKMP/Oakley 표준에 따라 클라이언트와 서버에서 모두 SA를 생성

❑ SA(Security Association)

► 보안 서비스를 제공하기 위한 보안 매개 변수들의 집합(알고리즘 식별자나 모드, 키 등)으로, 개념적으로 SSL/TLS의 Cipher Change Spec과 유사

IPSEC

❑ AH(Authentication Heder)

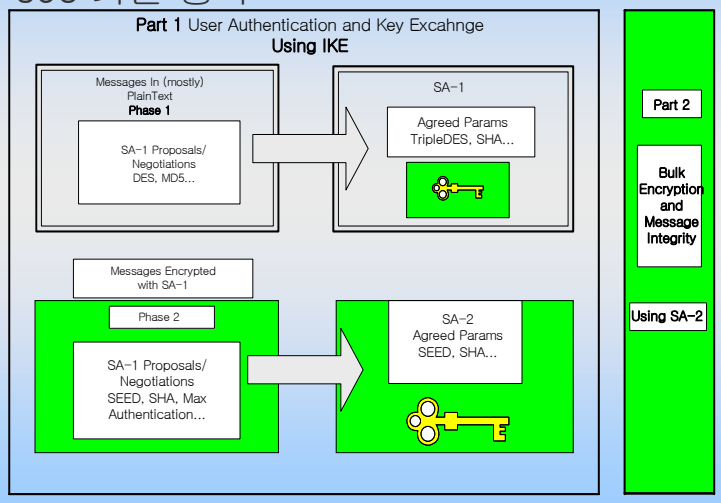
► IP 데이터그램에 대하여 무결성과 인증, 재전송 공격 방지 등의 보안 서비스 제공

❑ ESP(Encapsulating Security Protection)

► IP 데이터그램에 기밀성과 무결성, 인증, 재전송 공격 방지 등의 보안 서비스 제공

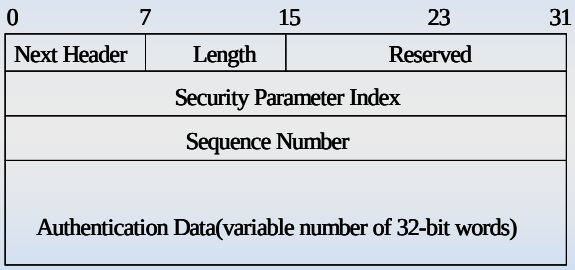
IPSEC

❑ IPsec 기본 동작



IPSEC

❑ AH



IPSEC

❑ IPv4 Header

0	8	16	24	31
Version	Hlen	Service Type	Total Length	
Identification			Flags(3)	Fragment Offset(13)
Time To Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
IP Option(If any)				Padding
Data(variable)				

IPSEC

❑ IPv6 Header

0	8	16	24	31
Version	Priority	Flow Label		
Payload Length			Next Header	Hop Limit
Source IP Address				
Destination IP Address				

10 * 32 bit = 40 octects

IPSEC

❑ IP Extension Header

0	Hop-by-Hop Header
43	Routing Header
44	Fragment Header
51	Authentication Header
59	No Next Header
60	Destination Options Header

IPSEC

❑ IPsec 적용전 패킷

IPV4

Origin IP header	TCP	Data

IPV6

Origin IP header	Extention header(option)	TCP	Data

IPSEC

❑ Transport mode에서의 AH

IPV4

Origin IP header	AH	TCP	Data

IPV6

Origin IP header	Extention header(option)	AH	E-header(option)	TCP	Data

IPSEC

❑ Tunnel mode에서의 AH

IPV4

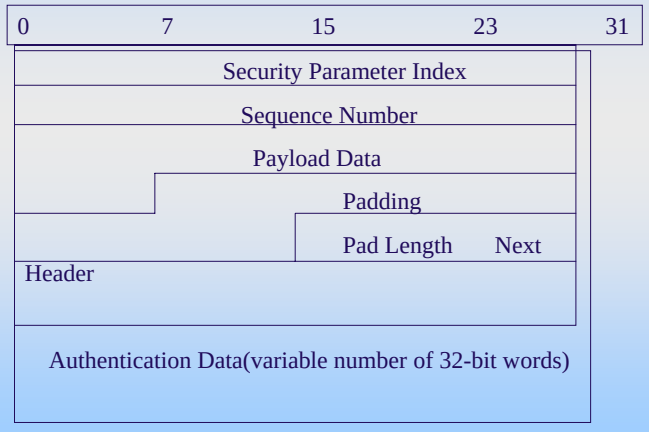
New IP header	AH	Origin IP header	TCP	Data

IPV6

New IP header	Extention header(option)	AH	Origin IP header	Extention header(option)	TCP	Data

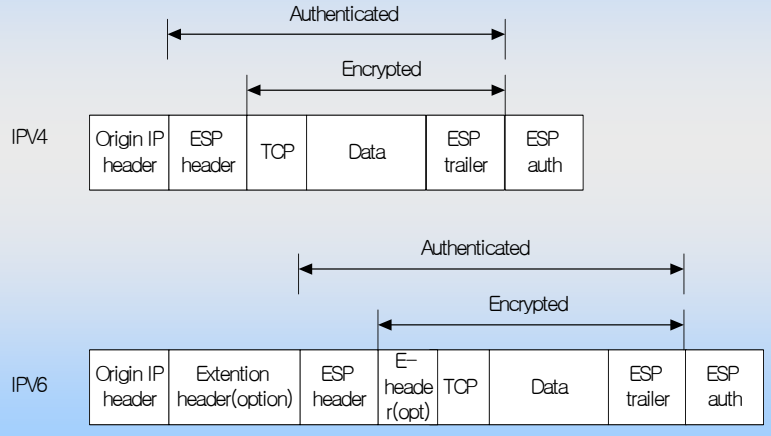
IPSEC

ESP Header



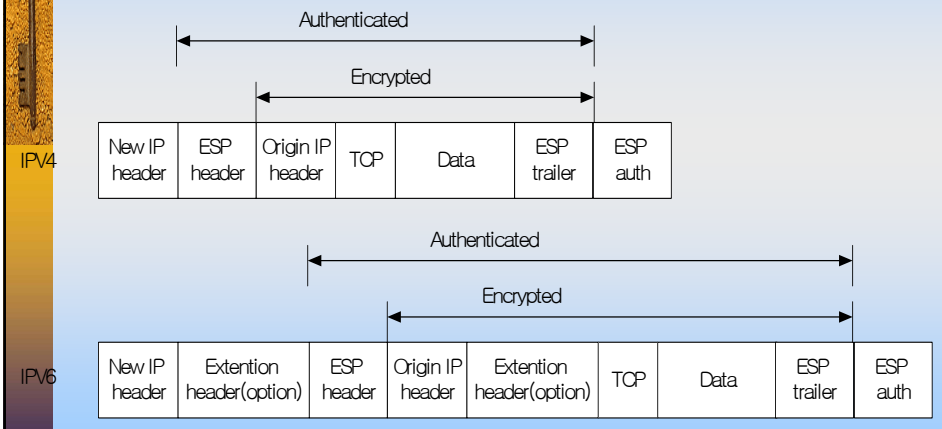
IPSEC

Transport mode에서의 ESP



IPSEC

❑ Tunnel mode에서의 ESP



VPN

❑ 가상사설망의 일반적인 특징

► 값비싼 전용선이나 임차선대신 공중망인 인터넷 이용을 이용하여 네트워크 비용 감소

► 공중망인 인터넷 이용에 따른 접속 내용의 노출에 따른 보안성 강화를 위하여 안전한 원격 접속 프로토콜 필요

► 모든 보안 지침서에서 직원들의 안전한 원격서비스를 지원하기 위하여 설치 권고

VPN

❑ 가상사설망의 일반적인 특징(계속)

► 원격 접속에 사용되는 디바이스 인증이 중요하기 때문에 원격작업을 원하는 직원들에게 회사에서 인증한 디바이스를 개별적으로 공급해야 하는 불편과 금전적인 부담 초래

► 고정된 원격 접속 지점에 따라 본점-지점간 접속처럼 서로 신뢰할 수 있는 지점에서만 원격 접속이 가능

VPN

❑ 하드웨어형 가상사설망

► 라우터기반 가상사설망

► 모든 트래픽을 Tunneling

► 라우터의 성능 감소를 줄이기 위하여 하드웨어로 구현

► 업데이트나 변경이 어려움

► 기밀성과 인증, 무결성 등의 보안을 위하여 IPSEC 이용

VPN

❑ 방화벽형 가상사설망

► 방화벽 기능과 VPN 기능의 결합

► 모든 트래픽을 Tunneling

► 방화벽에 대한 무결성과 보안 보장

► VPN을 위한 별도의 방화벽 룰셋 설정 필요

► 방화벽의 성능 감소를 줄이기 위하여 하드웨어로 구현

► 업데이트나 변경의 어려움

► 기밀성과 인증, 무결성 등의 보안를 위하여 IPSEC 이용

VPN

❑ 전용 디바이스형 가상사설망

► 라우터나 방화벽 성능에 영향을 주지 않음

► IP 주소나 IP Protocol에 기반한 Tunneling

► 네트워크 내에 설치되기 때문에 관리자 관리에 용이

► 새로운 Layer 역할을 하기 때문에 공격을 당하더라도 다른 네트워크 디바이스에 영향을 주지 않음

► 소프트웨어로 구현되기 때문에 유연성이 뛰어남

► 타 VPN에 비해 Scalable

► 확장 규모와 소요 예산간 비례관계

VPNS

❑ 사용자 인증기반 서비스플랫폼형 가상사설망

► VPN의 사용자 인증 및 권한 통제 부재로 인한 취약성 보완

► VPN의 하드웨어화에 따른 비용 증가과 유연성 부족 보완

► 유비쿼터스형 원격 접속이 가능하기 때문에 언제 어디서나 원격서비스 가능

► 전용 디바이스형 VPN 개념과 서비스 플랫폼 기술, two-factor 사용자 인증기술의 결합

► TLS기반 가상사설망서비스

VPNS

► 소프트웨어로 구현되기 때문에 유연성이 뛰어남

► 회사 구성원 여부에 대한 인증과 내부자 공격 방지를 위한 사용자 인증 및 권한 제어

► 용도에 따라 세분화된 구성이나 구축 가능(Customize 용이)

► 경제적이고 사용자 편이성 강화

III. 무선인터넷 보안

- 무선인터넷 보안
- Handshake Protocol
- Other protocols
- WAP
- WTLS Protocols

무선 인터넷 보안

❑ 필요성

► 무선인터넷에서는 단말 간 무선통신 상에서 여러 위협 요소가 존재하기 때문에 무선인터넷 상에서의 도청이나 메시지 변조, 신분 위장 등의 방지 필요

무선 인터넷 보안

❑ 무선 인터넷의 보안기술 적용

► 사용자 인증을 위한 패스워드기반 인증과 공개키기반 인증

► 데이터의 전송 도중 내용의 변조를 방지하기 위한 해쉬 또는 MAC

► 전송로 상의 도청방지를 위한 암호화(대칭키 암호 또는 공개키 암호)

► 데이터의 송신 및 수신 부인 방지를 위한 전자서명

무선 인터넷 보안

❑ 안전한 무선랜 운영

► 소규모 조직에서 안전한 무선랜 운영

- AP의 전파가 건물 내로 한정되도록 전파 출력 조정
- 외부에 접한 벽이나 창문으로부터 먼 건물 안쪽에 AP 설치
- AP의 ID나 패스워드를 자주 변경
- 관리자 이외의 사람들이 추측 불가
- AP와 무선단말기의 SSID(Service Set Identifier)를 자주 변경

무선 인터넷 보안

- AP에 MAC 주소 필터링 기능을 설정하고 무선랜 카드의 주소를 AP에 등록
- WEP 키를 주기적으로 변경
- 128 비트 이상의 WEP 키를 제공하는 장비 사용

무선 인터넷 보안

► 대규모 조직에서 안전한 무선랜 운영

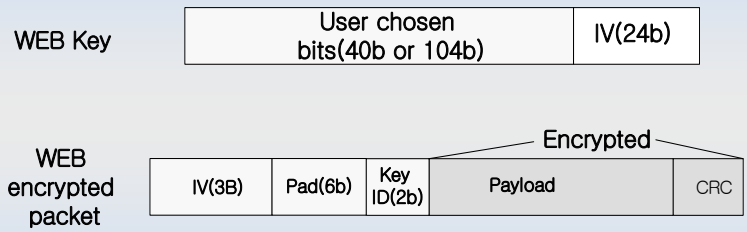
- 용도에 적합한 보안정책 수립 및 시행
- 무선랜 사용자와 장비 현황을 기록한 관리대장 비치
- AP 전파가 건물 내에 한정되도록 전파 출력 조정
- 외부 벽이나 창문에서 가급적 먼 건물 안쪽에 AP 설치
- 민감한 정보를 다루는 경우, 전파가 외부로 유출되지 않도록 전파차폐 시설이나 전파 불투과성 외벽도료 사용

무선 인터넷 보안

- WEP 키를 주기적으로 자동으로 변경시키는 Dynamic

  WEP 키를 사용하거나 TKIP(패킷 전송 시 일정한 간격으로 암호 키를 새로 생성)을 이용하여 데이터 암호화
- 내부 네트워크를 보호하기 위해서 AP와 내부 네트워크 사이에 스위치를 설치하여 내부 네트워크에서 호스트 간에 주고받는 트래픽이 무선네트워크를 통하여 외부로 나가지 않도록 설정

무선 인터넷 보안



무선 인터넷 보안

❑ IEEE 802.11의 인증 서비스

► 암호기반 방식

- AP는 난수를 생성하여 무선단말기로 보내고, 무선단말기는 WEP 키를 사용하여 난수를 암호화하여 AP로 돌려 보냄
- AP는 돌려받은 암호값을 복호화한 후, 복호화된 값이 AP가 보낸 난수와 일치할 경우에만 무선단말기 접근 허용
- 단방향 인증으로서 무선단말기는 AP를 인증할 수 없어, Man-in-the-Middle 공격 등에 취약

무선 인터넷 보안

► 비암호기반 방식

- Open System 인증 방식: 빈 스트링으로 된 SSID로 무선단말기를 인증하는 Null 인증
- Closed System 인증 방식: 무선단말기가 0~32 바이트의 스트링으로 된 SSID를 AP로 전송하고 AP는 이 값을 받아서 사용자의 접근을 허용하는 단순한 식별 수준

무선 인터넷 보안

❑ IEEE 802.11의 기밀성 서비스

► RC4 스트림 암호 이용

► 40비트 RC4 암호키는 Brute Force Attack에 취약

► 104비트 RC4 암호키도 Brute Force Attack에 여전히 취약(40비트와 80비트간의 해독 시간 차이는 거의 두 배 수준)

무선 인터넷 보안

❑ IEEE 802.11의 무결성 서비스

► CRC 기술을 사용하여 무선단말기와 AP 사이에 전송되는 메시지의 무결성 제공

► 송신 측에서는 각 페이로드에 대하여 CRC값을 계산하여 페이로드와 CRC를 WEP키로 암호화하여 송신하고, 수신 측에서는 복호화된 페이로드에 대한 CRC 값과 복호화된 CRC 값을 비교하여 무결성 여부 판단

무선 인터넷 보안

❑ IEEE 802.11의 추가적인 보안 취약성

► 사용자가 초기화 벡터의 설정이나 변경할 수 없어, 동일 제조사가 개발한 각 무선 NIC에 초기화 벡터가 동일할 경우, 공격자가 네트워크 트래픽을 분석하여 WEP키 해독 가능

► 초기화 벡터는 RC4 암호화키의 일부이기 때문에 공격자가 초기화 벡터 24비트를 알면, RC4 키 스케줄링의 취약점을 이용하여 쉽게 WEP키 해독 가능

무선 인터넷 보안

► 키 관리 기능 부재

► 하나의 AP에 많은 사용자들이 공유 WEP키를 사용 -> 공유된 암호키 세트를 Rotate -> 한번에 여러 개의 키를 사용자에게 발행 : 사전에 발행되는 공유키 노출 가능성은 여전히 존재

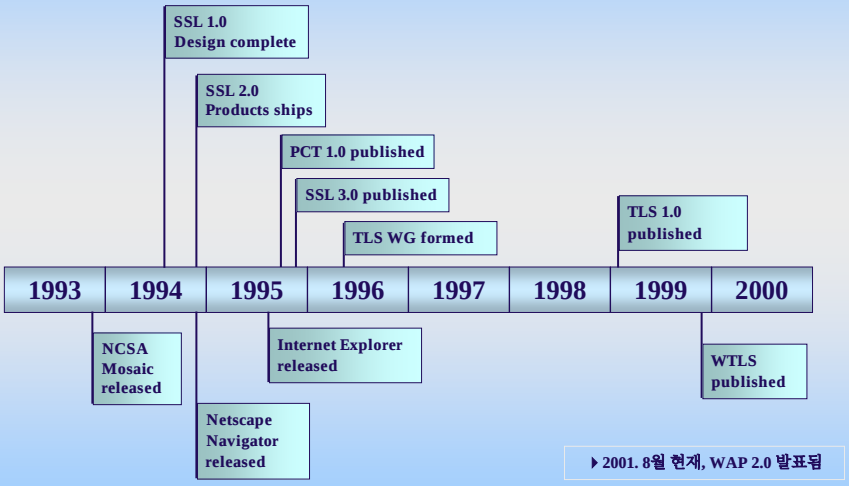
무선 인터넷 보안

❑ IEEE 802.11의 보안 취약성 해결 방안

► WEP의 RC4 스트림 암호를 128비트 블록 암호인 AES로 교체하는 방안

► 802.1X를 기반한 EAP (Extensible Authentication Protocol) 이용하여 인증 때마다 새로운 WEP 키 전송

무선인터넷 보안

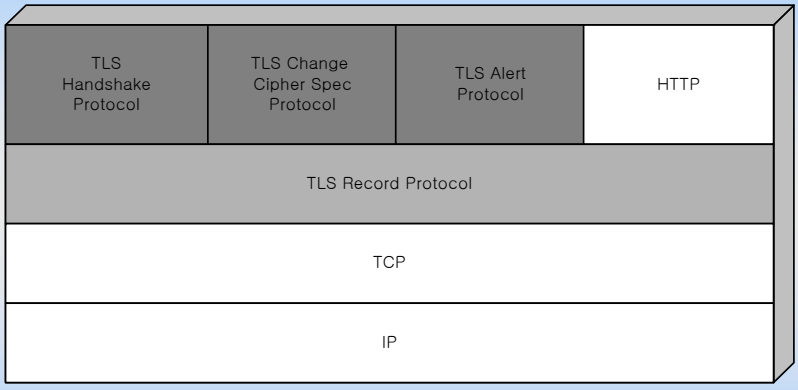


무선인터넷 보안

- TLS(Transport Layer Security)의 개요
  - TLS는 Netscape社에서 개발한 SSL(Secure Socket Layer)의 표준화 버전이다. – **IETF RFC2246** – 1999
  - 서버와 클라이언트 사이의 통신과정에서 비밀성(privacy)과 데이터 무결성(integrity)을 제공한다.
  - 네트워크 계층의 암호화 방식이기 때문에 HTTP뿐 아니라 NNTP, FTP등에서도 사용할 수 있다.
  - 표준화 홈페이지

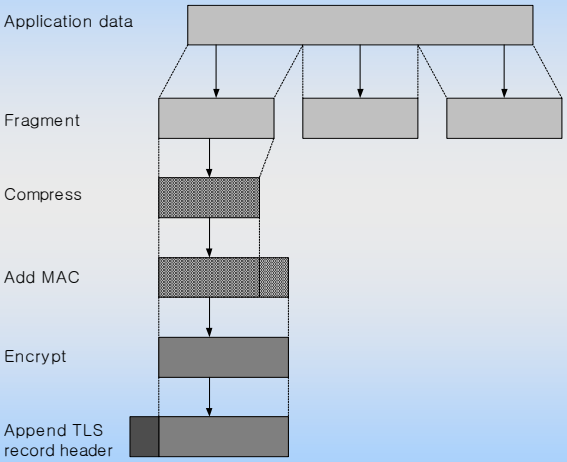
http://www.ietf.org/html.charters/tls-charter.html

❑ TLS Architecture



※ TLS는 두 개의 계층, 네 개의 프로토콜로 이뤄져 있다.

❑ TLS Record Protocol



❑ Handshake Protocol

(1) Handshake protocol의 기능 및 절차

- 서버와 클라이언트간의 상호 인증을 수행한다.
- 실질적 보안 프로토콜인 Record protocol에서 사용될 암호 알고리듬, 키 등을 협상한다.
- Handshake protocol은 크게 4단계의 절차를 가진다.
  - Phase 1. Establish Security Capabilities
  - Phase 2. Server Authentication and Key Exchange
  - Phase 3. Client Authentication and Key Exchange
  - Phase 4. Finish

Other protocols

(1) Change Cipher Spec 프로토콜

- 현재의 연결에서 사용할 Cipher Suite을 갱신하기 위해 사용된다.

(2) Alert 프로토콜

- TLS 프로토콜 사용시 발생하는 경고 메시지를 peer 개체에게 전송하기 위해서 사용된다.
- 발생하는 경고메시지의 종류
  - 메시지의 부적절함이나 전송상태의 오류
  - MAC의 부정확/복호시의 오류
  - 인증서에 관련된 오류
  - 암호 스펙의 협상과정에서의 오류 등

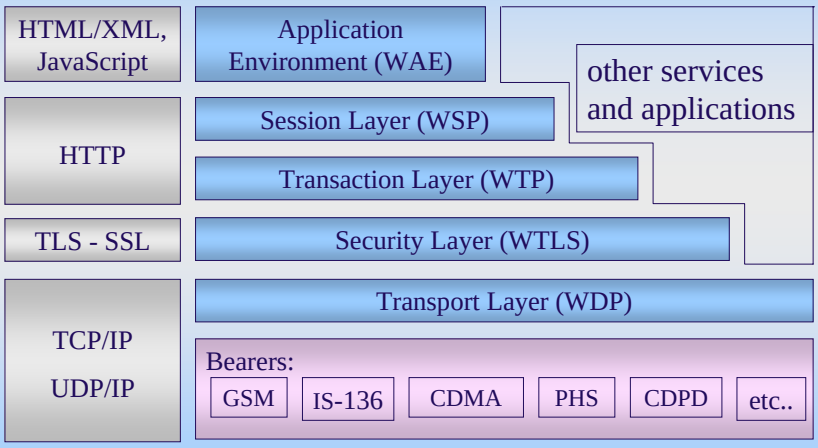
WAP (Wireless Application Protocol)

(1) 무선 통신 환경에서의 어플리케이션을 개발하기 위해 산업 규격을 제정하는 WAP Forum의 연구 결과

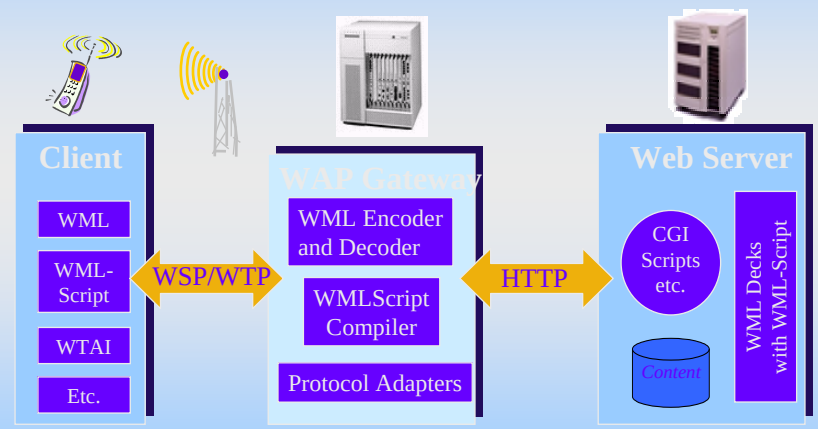
(2) 네트워크 기술, 무선 데이터 기술, 인터넷 기술 등의 빠른 발전으로 생겨난 기술

(3) 휴대용 단말기 하나만으로 무선 인터넷에 접속(양방향통신)할 수 있도록 브라우저 개발 및 표준 언어의 개발의 필요성 대두로 WAP이 탄생

WAP Architecture



WAP programming model



WAP Gateway

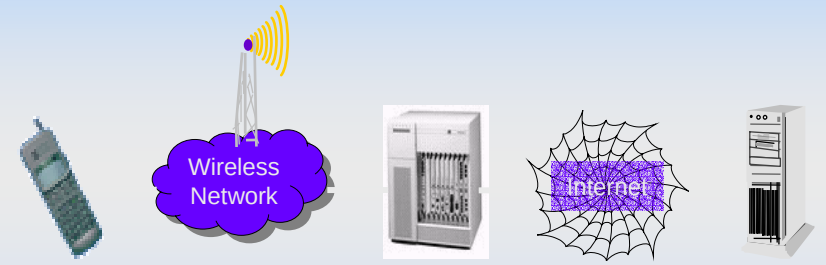
(1) Gateway와 WAP 브라우저 사이에 보안제공을 위해 WTLS사용
- 무선환경에 적합하도록 SSL(TLS) 에 비해 datagram support, optimized handshake, dynamic key refresh 지원

(2) SSL과 WTLS 보안 프로토콜 사이의 상호 변환
- 유선에서 SSL-encrypted message를 무선 네트웍에서의 WAP WTLS 로 변환

(3) Secondary media에서 decrypted contents가 저장되어서는 안 된다.

(4) Gateway를 인증된 사람만이 접근 할 수 있도록 해야 한다.

Security in a WAP environment



WTLS (Wireless Transport Layer Security)

(1) SSL, TLS와 같은 인터넷 보안 프로토콜에 기초한 안전한 접속을 위한 framework 규정

(2) Confidentiality, Authentication, Integrity 같은 보안 서비스 제공

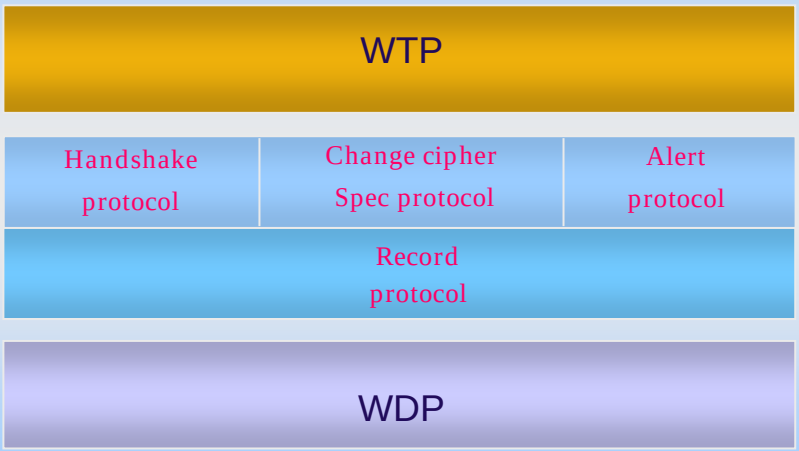
(3) node-to-node security 제공

(4) 무선 환경에 적합하도록 대역폭, 메모리, 소요 전력을 고려한 효율적인 프로토콜

(5) SSL보다 protocol overhead를 최소화하고 데이터 압축을 더 많이 함

(6) 무선 환경에 적합한 security algorithm을 포함

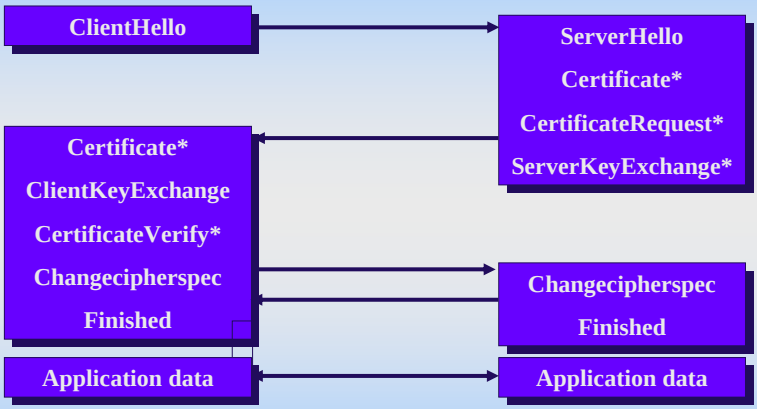
Architecture of WTLS



WTLS Protocols

Handshake protocol	서버와 클라이언트 간의 인증 수행 사용할 암호 알고리즘 및 키 분배
Change cipher spec protocol	설정된 세션 정보와 연결 정보를 사용한다는 것을 상대방에게 알린다
Alert protocol	오류 메시지 전송 (암호, 압축, MAC 오류, 인증서 실패, etc)
Record protocol	전송되는 메시지의 기밀성과 무결성 제공

WTLS Full Handshake Protocol



❖ TLS와 달리 인증서의 형식으로 X.509형식 뿐 아니라, WTLS 인증서, X9.68 인증서 중 하나를 선택해서 사용 가능

❑ Abbreviated/Optimized Handshake

(1) Abbreviated Handshake Protocol

- 새로운 세션을 시작하지 않고 이전 세션 정보를 이용해 세션을 재사용 할 경우
- 인증서를 위한 정보들이 교환되지 않고, 암호 파라메터들도 처음부터 재 생성되지 않는다.

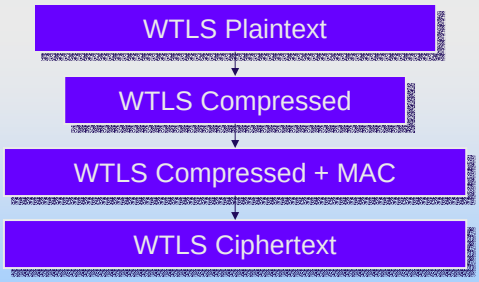
(2) Optimized Handshake Protocol

- 서버나 다른 저장소에 저장되어 있는 클라이언트 인증서를 통해 클라이언트를 인증하고자 할 경우

❑ WTLS Record Protocol

(1) TLS와의 차이점

- TLS 에서 이루어지는 데이터 fragmentation(단편화)는 WTLS 에서 이루어지지 않음
  (하위 계층인 WDP/UDP 계층에서 단편화가 이루어 짐)



정보보안 교육동영상 자료(인터넷이 되는 지역일 때만 클릭하세요!!)

당신의 정보가 유출되고 있다

인터넷 속 희망나누기
건전하고 유익한 정보공간으로 가는 길

사이버사회에서의 학부모의 역할
디지털시대의 환경오염
사이버 사회를 보호하는 법, 제도

신종범죄의 천국-사이버 공간

함께 만들어요, 즐거운 네트워크