2017/01/10, 2017 보안 기초 세미나

Network Security Essentials

- Chapter_6 무선 네트워크 보안(2) -

임연주(yeonjoo@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

목 차

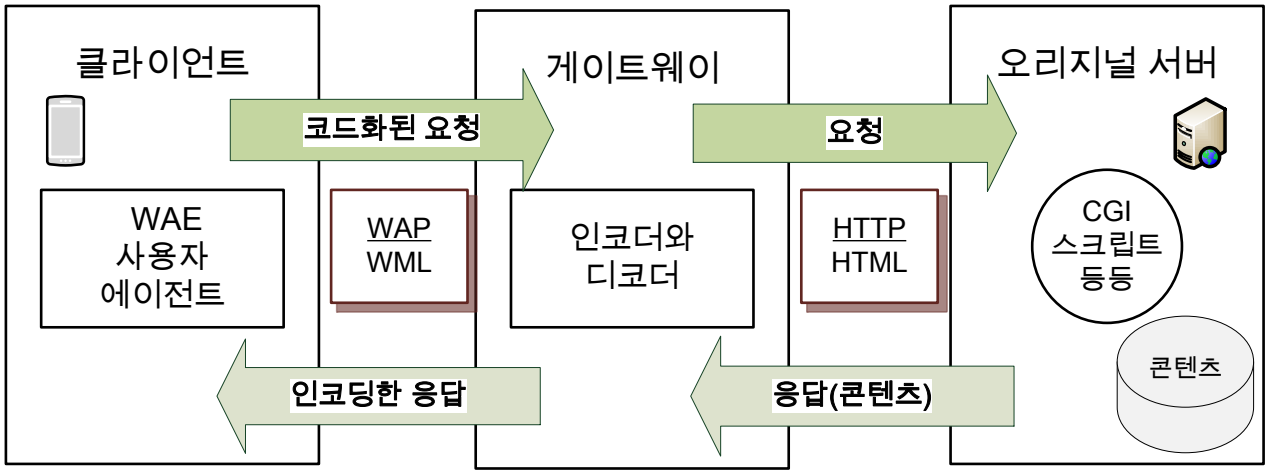
- 무선 응용 프로토콜 (WAP)
- 무선 전송 계층 보안 (WTLS)
- WAP 종단-대-종단 보안

무선 응용 프로토콜 (WAP)

- 개요
  - 무선 응용 프로토콜 (WAP, Wireless Application Protocol) 정의
    - 1989년 WAP 포럼에서 개발한 통합 표준화 하기 위한 프로토콜들의 규격
      - 휴대 전화, PDA과 같은 무선 장치를 위한 애플리케이션 프레임워크 및 네트워크 프로토콜을 표준화
  - 등장 배경
    - 무선 네트워크의 특성과 일치
      - 통신환경: 좁은 대역폭, 낮은 전송률
      - 하드웨어: 저사양 CPU, 적은 메모리 및 배터리 사양
      - 사용자 인터페이스: 입/출력 장치, 응용 프로그램의 제한

무선 응용 프로토콜 (WAP)

- 개요
  - WAP 목적
    - 무선 터미널에서 인터넷 서비스 이용
    - 무선 프로토콜 규격 개발
    - 다양한 컨텐츠와 응용 기술 개발
  - WAP 프로그래밍 모델 그림



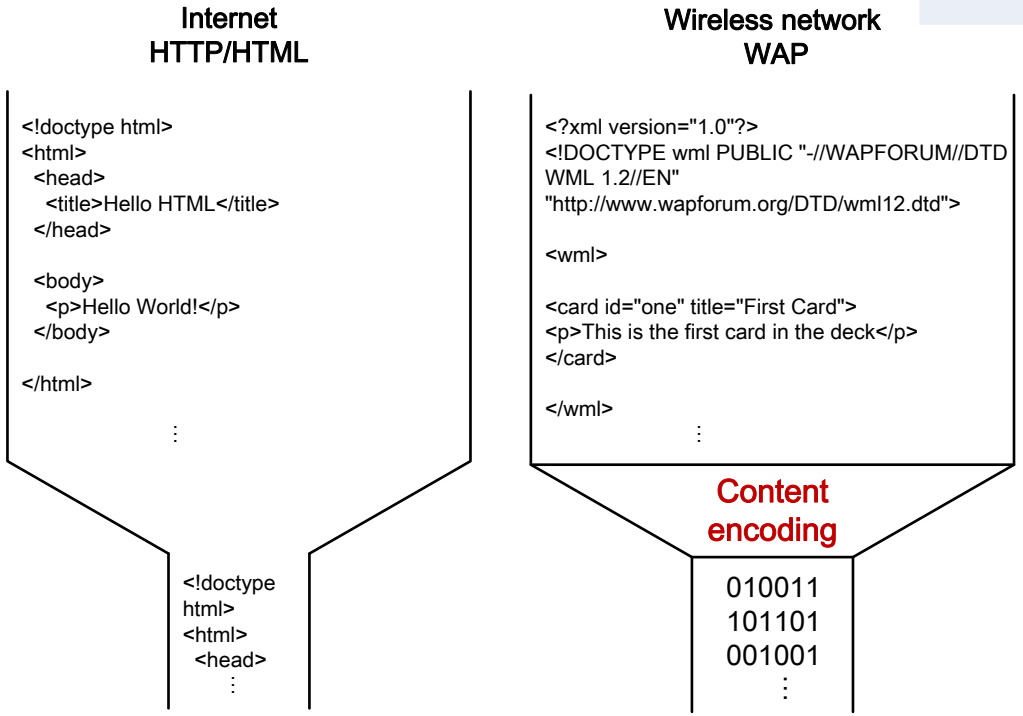
무선 응용 프로토콜 (WAP)

- WML(Wireless Markup Language)
  - 정의
    - WAP에 정의된 마크 업 언어
    - 제한된 사용자 입력 기능을 가진 모바일 장비에서 콘텐츠와 양식을 표현하기 위해 설계된 언어
    - WML 서비스에서 직접 음성통화를 가능하도록 하는 응용 인터페이스(WTAI, Wireless Telephony Application Interface)를 규정
      - WTA (Wireless Telephony Application)
        - 개발자와 사용자에게 더 나은 모바일 네트워크 서비스가 가능하게 하는 전화에 특화된 확장들의 모음

무선 응용 프로토콜 (WAP)

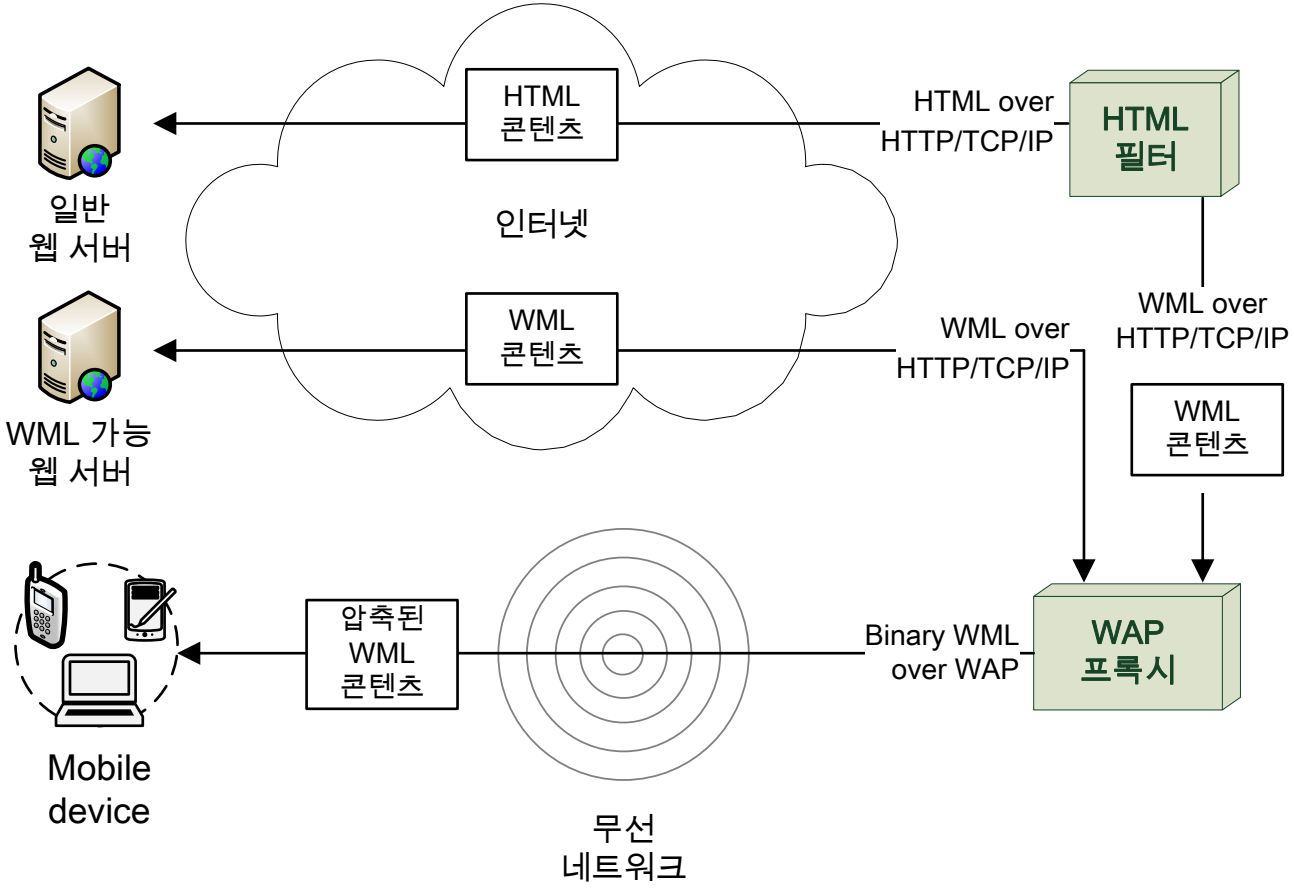
- WML(Wireless Markup Language)
  - WML과 HTML 비교 표

	WML	HTML
사용	Desktop	Mobile
지원하는 Tag 개수	많음	적음
출력	Device와 무관	Device에 따라 다름
구성	여러 개의 page가 하나의 site를 구성	여러 개의 card가 하나의 deck을 구성



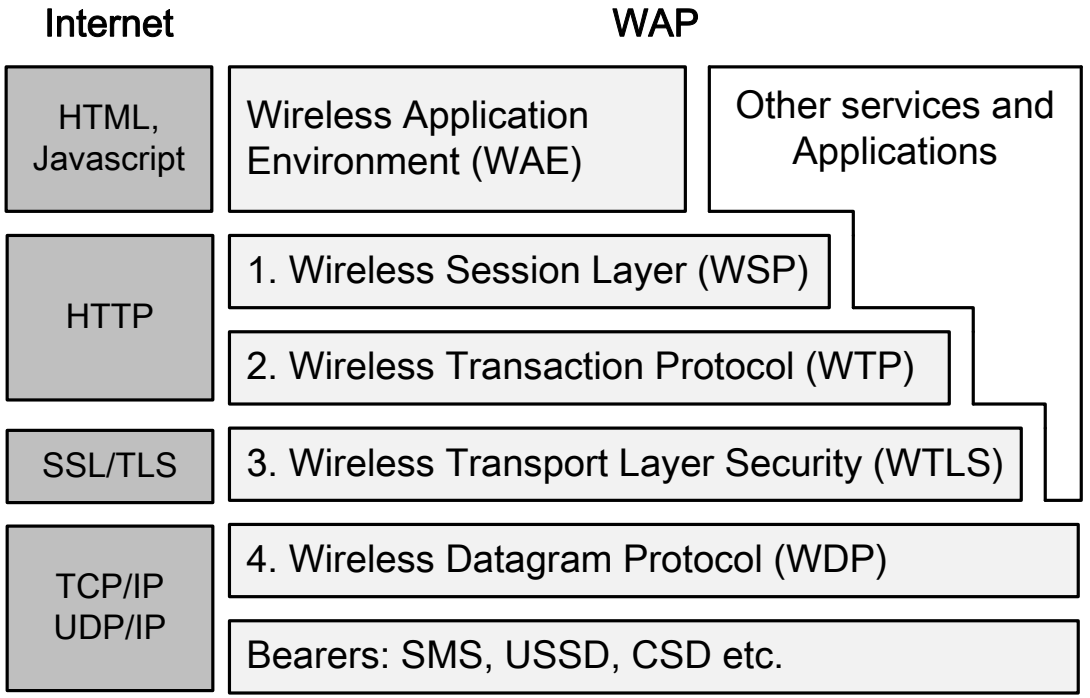
무선 응용 프로토콜 (WAP)

- 개요
  - WAP 기반 구조 그림



무선 응용 프로토콜 (WAP)

- WAP 구조 (1/4)
  - WAP 스택 구조 그림



무선 응용 프로토콜 (WAP)

- WAP 구조 (2/4)
  - WAP 스택 구조
    - Wireless Application Environment (WAE)
      - WAP 스택의 상위 계층
      - 지원하는 응용 프로그램과 장비 개발을 위한 도구와 형식의 집합
    - Wireless Session layer Protocol (WSP)
      - 세션을 생성하고, 이미 접속중인 세션을 종료하는 기능 제공
      - WAE를 두 개의 세션 서비스로 연결시키는 계층
        - 연결형 서비스 (WTP)
          - 클라이언트가 인터넷 서비스를 받는 동안 접속 상태를 유지하며 동작
        - 비연결형 서비스 (WDP)
          - 컨텐츠만 전달하고 바로 접속 종료하는 방식으로 동작

무선 응용 프로토콜 (WAP)

- WAP 구조 (3/4)
  - WAP 스택 구조
    - Wireless Transaction Protocol (WTP)
      - 트랜잭션 형태의 데이터 전송 기능을 제공
        - 유선에 비해 낮은 대역폭을 가지는 무선 통신에 알맞은 방식
      - 데이터의 송수신은 Request- replay 패킷 형태로 이루어지며, 오류가 발생한 패킷만 재전송을 요청함
        - TCP와 유사
    - Wireless Transport Layer Security (WTLS)
      - TLS을 기반으로 WAP에 적용시킴
      - 자세한 특징은 뒤에서 설명

무선 응용 프로토콜 (WAP)

- WAP 구조 (4/4)
  - WAP 스택 구조
    - Wireless Datagram Protocol (WDP)
      - 다양한 네트워크에 의해 지원되는 bearers 서비스를 이용하는 데이터 위에서 작동
      - 포트번호 주소화, 분리 및 재조립, 오류 탐지
      - UDP와 유사
    - Bearers
      - WAP G/W와 휴대폰을 연결하는 통신 망 또는 전송 방식
      - 모든 Bearer는 WDP 하위에 있음

목 차

- 무선 응용 프로토콜 (WAP)
- 무선 전송 계층 보안 (WTLS)
- WAP 종단-대-종단 보안

무선 전송 계층 보안 (WTLS)

- 개요
  - 정의
    - WAP에서 안전한 통신을 위해 정의한 보안 프로토콜
    - TLS를 바탕으로 무선 환경에 최적화된 프로토콜
    - WAP 장치와 WAP G/W 간의 보안 서비스를 제공
      - WAP G/W와 웹 서버 간의 보안은 TLS
  - 기능
    - 데이터 무결성: 메시지 인증
    - 기밀성: 암호화
    - 인증: 인증서를 통한 상호 인증

무선 전송 계층 보안 (WTLS)

- 개요
  - WTLS의 고려사항
    1. SSL/TLS는 TCP/IP 상의 연결 중심 전송 프로토콜 위에서 동작하지만 WTLS는 WDP 위에서 동작함
       - 데이터그램의 손실, 중복, 순서 바뀜을 고려해야 함
    2. 통신 속도에 제한이 있으므로 통신 데이터를 최소화해야 함
       - 인코딩 되지 않은 WTLS 인증서를 사용할 수도 있음
    3. 무선 단말기의 메모리와 프로세서의 파워가 제한적이므로, 연산이 많이 소요되는 암호 알고리즘 등의 적용이 어려울 수 있음

무선 전송 계층 보안 (WTLS)

- WTLS 파라미터 (1/2)
  - WTLS 세션상태 파라미터 정리 표

파라미터	의미
Session identifier	세션의 상태를 나타내는 임의의 바이트 열 (서버가 선택)
Protocol Version	WTLS 프로토콜 버전 번호
Peer certificate	서버와 클라이언트의 대등 X.509v3 인증서 (NULL도 가능)
Compression method	암호화 하기 전 압축에 사용되는 알고리즘
Cipherspec	MAC 계산에 사용되는 암호 또는 해시 알고리즘과 해시크기 등을 정의
Master secret	클라이언트와 서버가 공유하는 20-바이트 비밀 값
Sequence number	안전 연결에 사용되는 순서번호 붙이기 방법
Key refresh	암호화 키, MAC 비밀키, IV 등이 얼마나 자주 계산되는지 정의
Is resumable	기존 세션의 새 연결 시작가능여부를 나타내는 플래그

무선 전송 계층 보안 (WTLS)

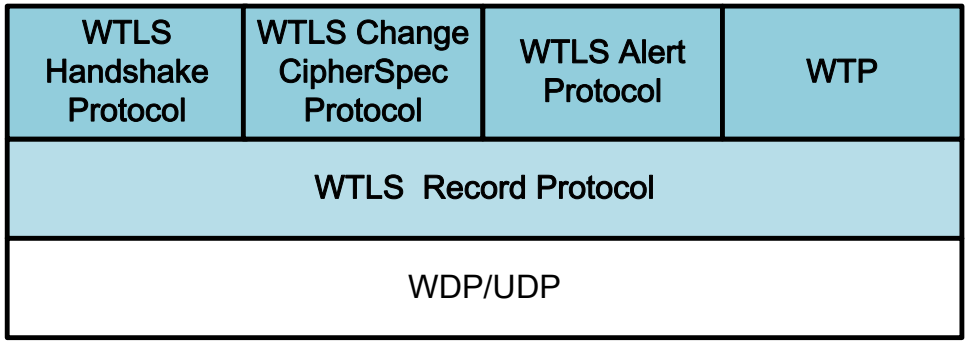
- WTLS 파라미터 (2/2)
  - WTLS 연결상태 파라미터 정리 표

파라미터	의미
Connection end	서버/클라이언트 역할을 하는가에 대한 것
Bulk cipher algorithm	알고리즘의 키 크기, 키의 어떤 부분이 비밀인지, 블록/스트림 암호 여부, 암호 블록 크기 등의 정보
MAC algorithm	MAC 계산에 사용할 키의 크기와 해시 값 크기 정보
Master secret	클라이언트와 서버가 공유하는 20-바이트 비밀 값
server/client random	각각 제공하는 16비트의 랜덤 값
Sequence number	안전 연결에 사용되는 순서번호 붙이기 방법
Key refresh	암호화 키, MAC 비밀키, IV 등이 얼마나 자주 업데이트 되는지 정의 (새로운 키 값 **n = $2^{key\_refresh}$**번의 메시지가 전송될 때마다 업데이트)

무선 전송 계층 보안 (WTLS)

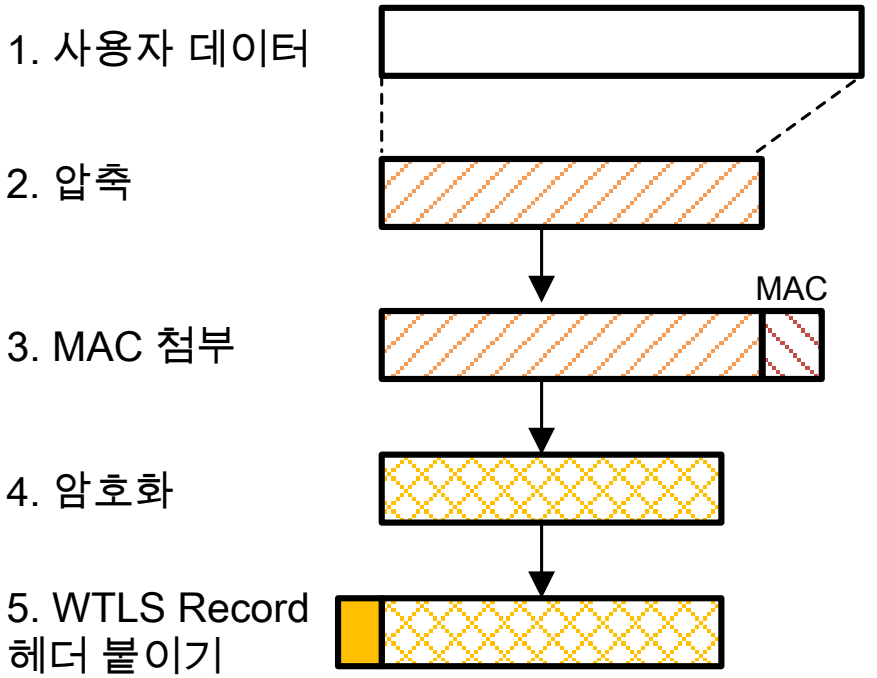
- WTLS 구조

1. WTLS Handshake Protocol
   - 통신의 이전에 필요한 보안속성 협상을 수행
     - 세션 키, 암호화 알고리즘, 인증 등을 파라미터 정의
2. WTLS Change CipherSpec Protocol
   - 협상의 적용상태를 알림
3. WTLS Alert Protocol
   - 세션의 종료 또는 오류 발생시 알림
4. WTLS Record Protocol
   - 데이터를 암/복호화
     - 무결성 제공



무선 전송 계층 보안 (WTLS)

- WTLS Record Protocol (1/3)
  - 정의 및 기능
    - 상위 계층으로부터 사용자 데이터를 받아서 PDU 안에 캡슐화를 실행
    - 기밀성, 무결성 제공
  - 전반적인 동작 그림



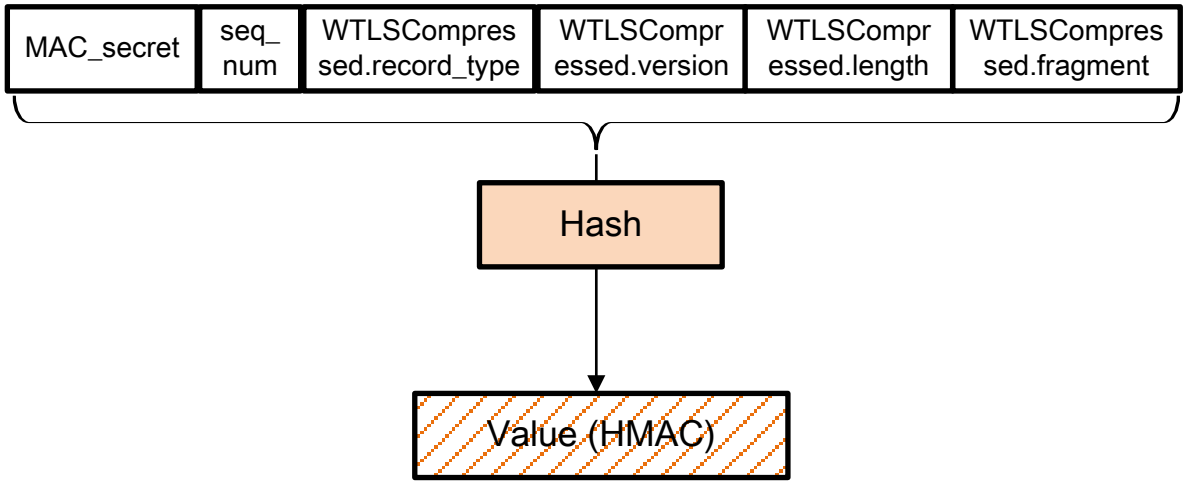
무선 전송 계층 보안 (WTLS)

- WTLS Record Protocol (2/3)
  1. 압축
     - 협상한 비손실 압축 알고리즘으로 압축
  2. MAC 첨부
     - HMAC 알고리즘을 사용해 MAC 값 계산
       - MD5/SHA-1
     - 압축된 데이터 뒤에 덧붙임
  3. 암호화
     - 협상한 알고리즘을 이용해 암호화
       - DES, 3DES, RC5, IDEA을 지원

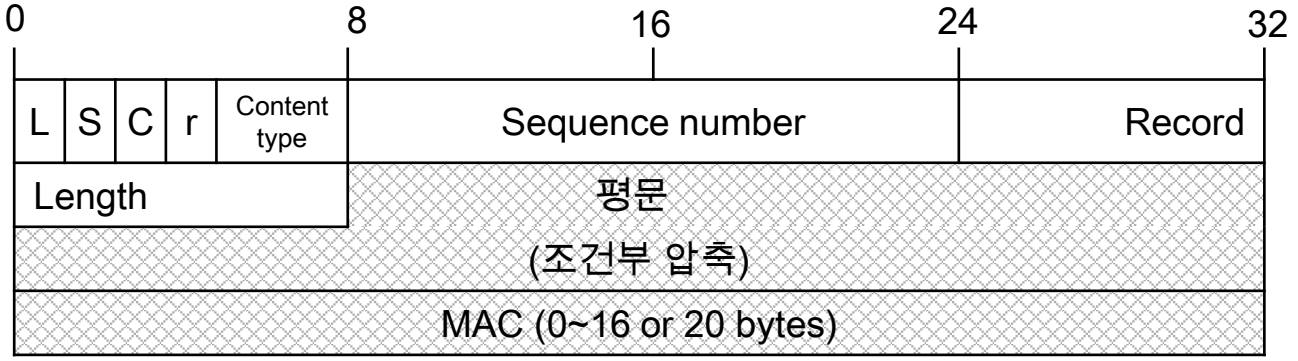
  ✓ WTLS에서 단편화는 이루어지지 않음
     - UDP/WDP 계층에서 단편화가 이루어지기 때문

무선 전송 계층 보안 (WTLS)

- WTLS Record Protocol (3/3)
  - MAC 계산과정 그림



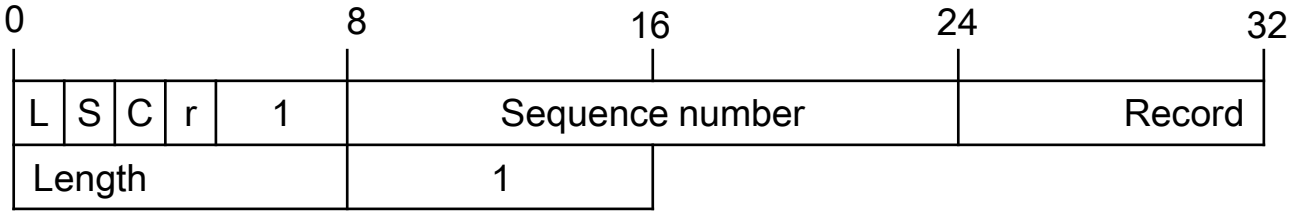
  - 포맷 그림



- L: 레코드 길이 필드 존재 여부
- S: 순서번호 필드 존재 여부
- C: 압축, MAC 및 암호화 사용여부
- r: 예약

무선 전송 계층 보안 (WTLS)

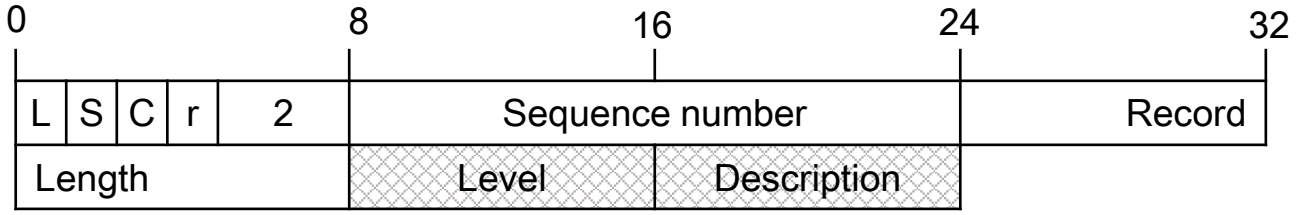
- WTLS Change CipherSpec Protocol
  - 주요 기능
    - Handshake 프로토콜로 협상된 내용이 이후 통신부터 적용됨을 알림
  - 포맷 그림



- L: 레코드 길이 필드 존재 여부
- S: 순서번호 필드 존재 여부
- C: 압축, MAC 및 암호화 사용여부
- r: 예약

무선 전송 계층 보안 (WTLS)

- WTLS Alert Protocol (1/1)
  - 주요 기능
    - 암호 오류, 압축 오류, 메시지 인증 오류, 인증 실패 등을 경고필드에 표기한 뒤 전송
  - 포맷 그림



- L: 레코드 길이 필드 존재 여부
- S: 순서번호 필드 존재 여부
- C: 압축, MAC 및 암호화 사용여부
- r: 예약

무선 전송 계층 보안 (WTLS)

- WTLS Alert Protocol (2/2)
  - 항상 심각(Always Fatal) 경고의 종류 표

유형	의미
session_close_notifiy	송신자가 현재 연결 상태나 안전 세션을 통해 더 이상 메시지를 보내지 않겠다는 것
unexpected_message	적합하지 않은 메시지의 수신
bad_record_MAC	부정확한 MAC 수신
decompressed_failure	압축해제 함수에 적합하지 않은 입력 (압축풀기 불가 또는 최대 허용길이보다 큰 경우 등)
handshake_failure	사용할 수 있는 옵션이 주어졌지만 송신자와 협상 불가

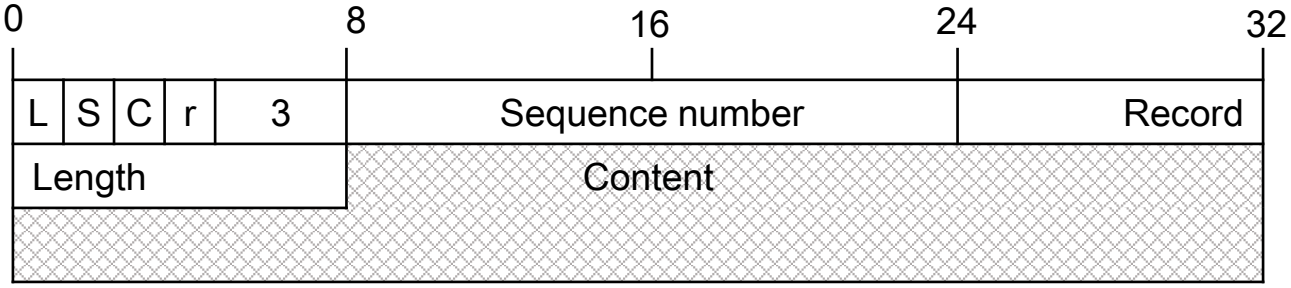
  - 일반적인 경고의 종류 표

유형	의미
connection_close_notify	송신자가 현재 연결 상태로는 더 이상 메시지를 보내지 않겠다는 것
오류_certificate	bad, unsupported등 의 수신된 인증서에 대한 경고
certificate_상태	revoked, expired, unknown 등의 인증서 문제가 발생

무선 전송 계층 보안 (WTLS)

- WTLS Handshake Protocol (1/15)
  - 정의 및 기능
    - 한 세션 동안 이용되는 파라미터 생성
      - 사용되는 비밀정보를 고유
    - 서버와 클라이언트간의 상호 인증 수행
    - 사용할 암호 및 MAC 알고리즘과 암호 키를 결정
    - 최적화된 완전-핸드셰이크(Optimized Full-Handshake)가 추가되어 사용
  - 포맷 그림

- L: 레코드 길이 필드 존재 여부
- S: 순서번호 필드 존재 여부
- C: 압축, MAC 및 암호화 사용여부
- r: 예약



무선 전송 계층 보안 (WTLS)

- WTLS Handshake Protocol (2/15)
  - 종류
    1. 완전-핸드셰이크 (Full-Handshake)
       - 새로운 세션을 시작할 때 사용
    2. 최적화된 완전-핸드셰이크 (Optimized Full-Handshake)
       - WTLS에서 추가된 것
       - 서버는 클라이언트 인증을 위해 클라이언트 인증서를 요청하지 않고, 서버 내에 보관된 클라이언트 인증서를 가지고 인증을 수행
    3. 단축-핸드셰이크 (Abbreviated-Handshake)
       - 기존 세션을 재개해서 다시 이용할 경우에 사용

무선 전송 계층 보안 (WTLS)

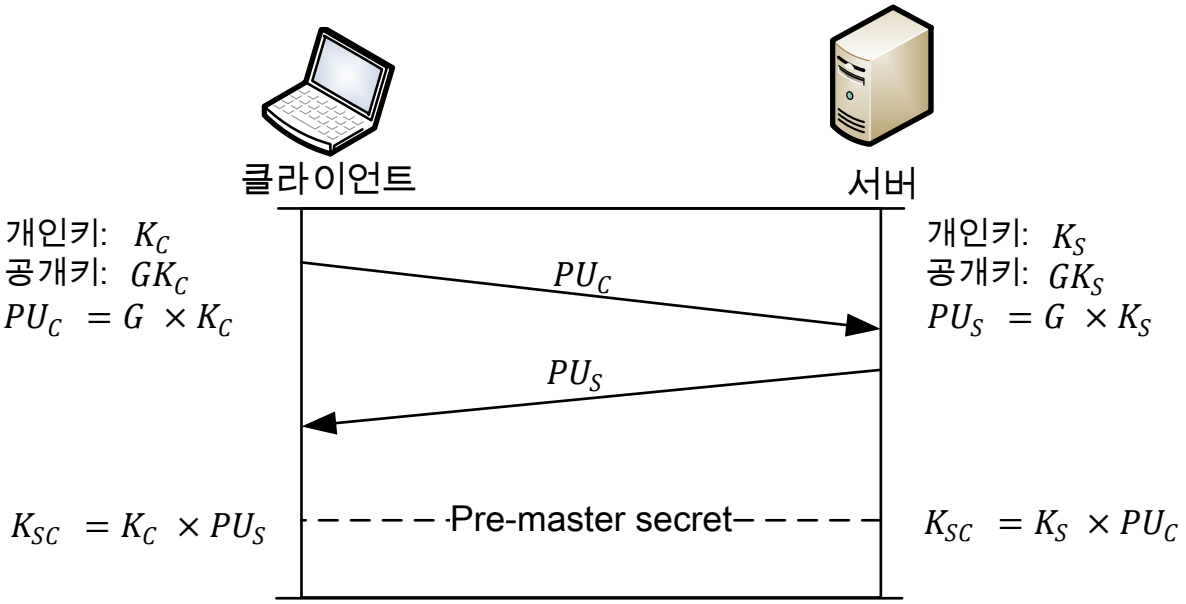
- WTLS Handshake Protocol (3/15)
  - 키 교환 알고리즘 (1/2)
    - 기존의 세션을 이용하는 경우
      - 이전에 계산된 master secre를 사용해 세션 다시 시작
      - 새롭게 교환된 서버/클라이언트 난수 값이 키 블록 계산 시 반영되어 이전 연결과 다른 키 블록 생성

1. RSA
   - 클라이언트가 생성한 Pre-master secret(20byte)를 서버의 공개키로 암호화해서 서버에게 전송

2. Diffie-Hellman
   - Pre-master secret: : $g^{cs} \ mod \ p$
   - DH 계산 수행

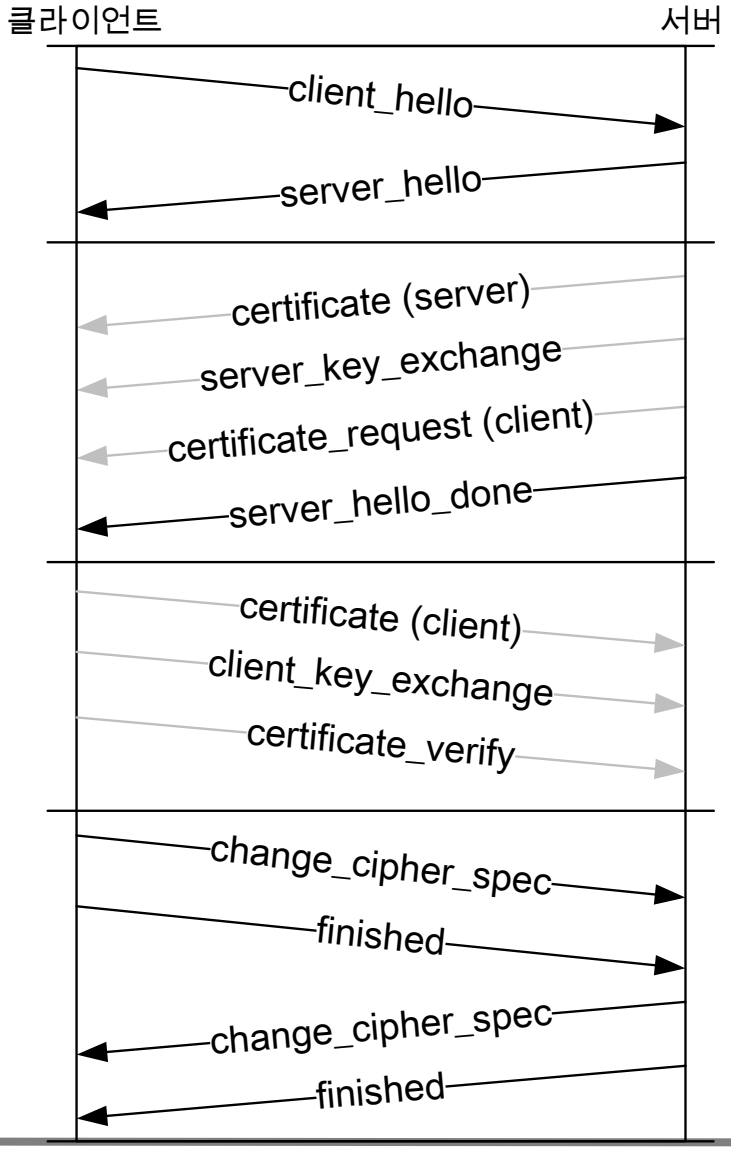
무선 전송 계층 보안 (WTLS)

- WTLS Handshake Protocol (4/15)
  - 키 교환 알고리즘(2/2)
    3. EC Diffie-Hellman
       - Pre-master secret: : K_{SC}
       - ECDH 계산 수행
         - 타원 곡선 상의 G 공유



무선 전송 계층 보안 (WTLS)

- WTLS Handshake Protocol (5/15)
  - 전반적인 동작 그림



단계 1
보안 기능 수집: 프로토콜 버전, 세션 ID, 암호 조합, 압축 방법, 초기 랜덤 넘버를 구성

단계 2
서버는 인증서를 보내고 키를 교환하고 인증서를 요청
서버는 hello message 단계의 종료를 알림

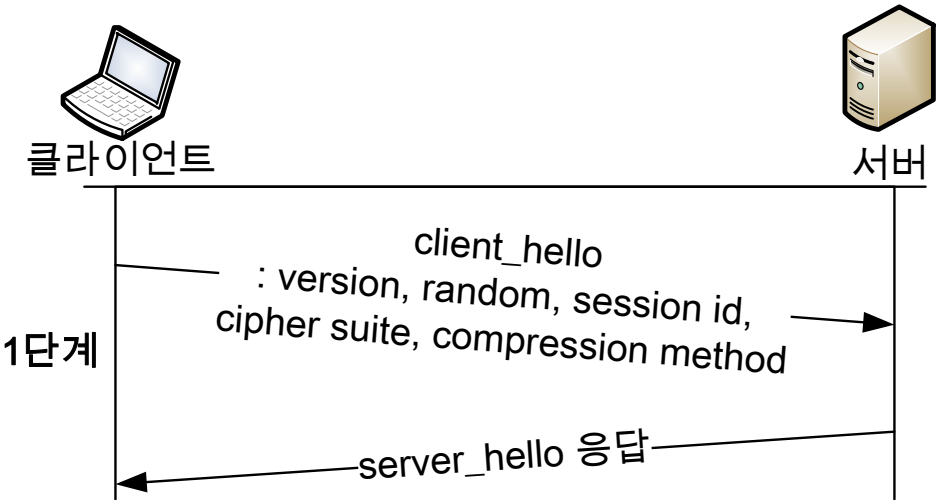
단계 3
클라이언트는 요청이 있을 경우, 인증서를 보냄, 키를 교환, 클라이언트는 인증서 확인사항을 보냄

단계 4
암호 조합을 변경하고 핸드셰이크 프로토콜을 종료

- 음영이 들어간 화살표는 옵션이거나 상황에 따라 필요한 경우만 씀

무선 전송 계층 보안 (WTLS)

- Handshake Protocol (6/15)
  - 1단계: 보안 기능 설정

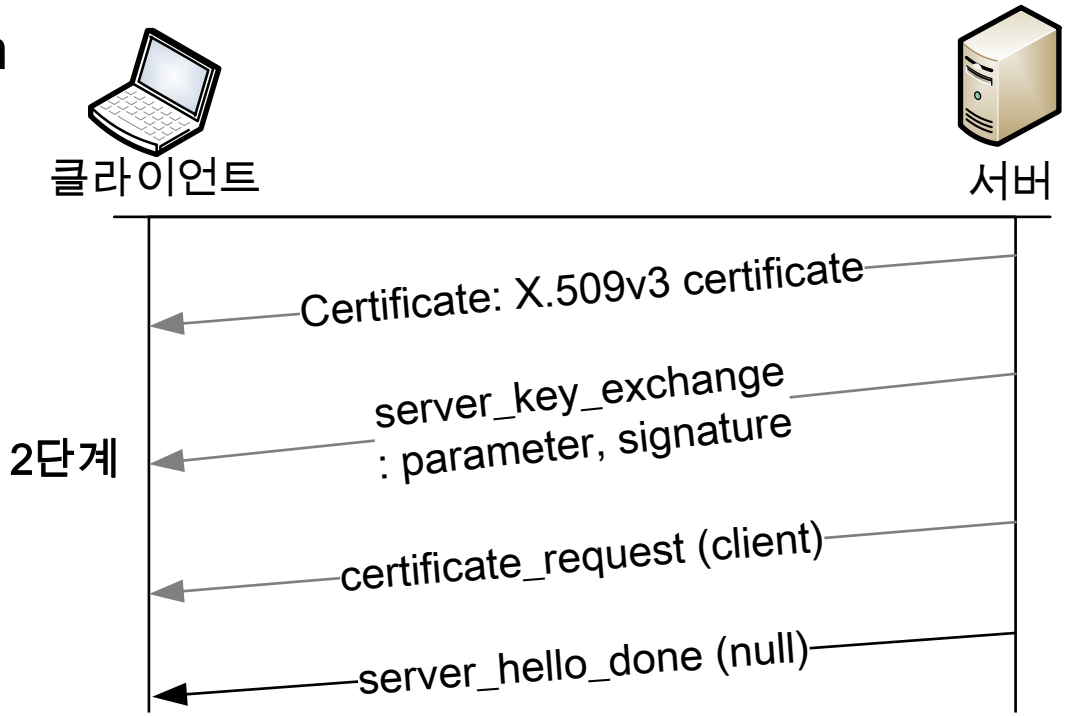


암호 명세	의미
Cipher algorithm	RC4, DES 등
MAC Algorithm	MD5 또는 SHA-1
Cipher type	스트림 또는 블록
Is exportable	참 또는 거짓
Hash size	0, 16(MD5) 또는 20(SHA-1) bytes
Key material	Write 키 생성에 사용할 데이터를 포함하는 데이터 열

이름	역할
version	클라이언트가 수용할 수 있는 가장 높은 버전
random	클라이언트/서버가 제공하는 16 비트 난수 (nonce)
session ID	값이 0이 아니면 동일한 암호 값을 사용, 0이면 새로운 세션을 위한 값을 설정
cipher suite	클라이언트가 지원하는 암호 알고리즘 목록과 교환 방식을 나열
compression method	압축 방법

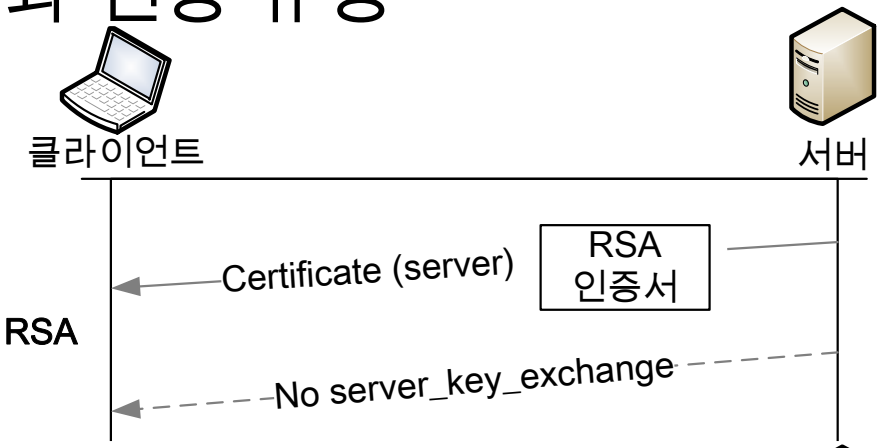
무선 전송 계층 보안 (WTLS)

- Handshake Protocol (7/15)
  - 2단계: 서버 인증과 키 교환 (1/3)
    - 대표적 키 교환 알고리즘 (3가지)
      1. RSA
      2. 익명 Diffie-Hellman
      3. EC Diffie-Hellman

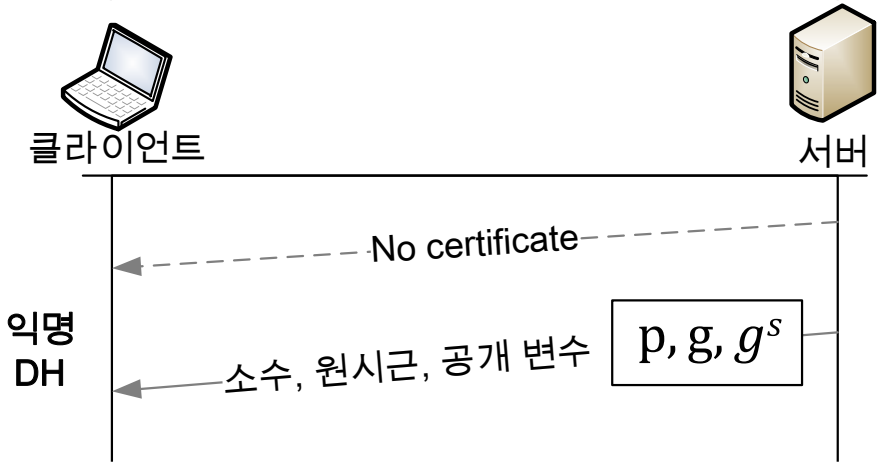


무선 전송 계층 보안 (WTLS)

- Handshake Protocol (8/15)
  - 2단계: 서버 인증과 키 교환 (2/3)
    - 3가지 키 교환과 인증 유형
      1. RSA

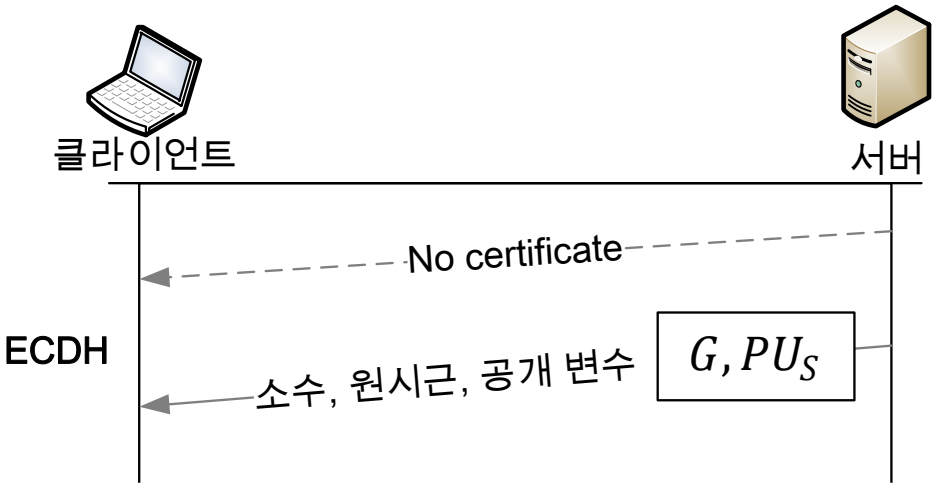


      2. 익명 DH



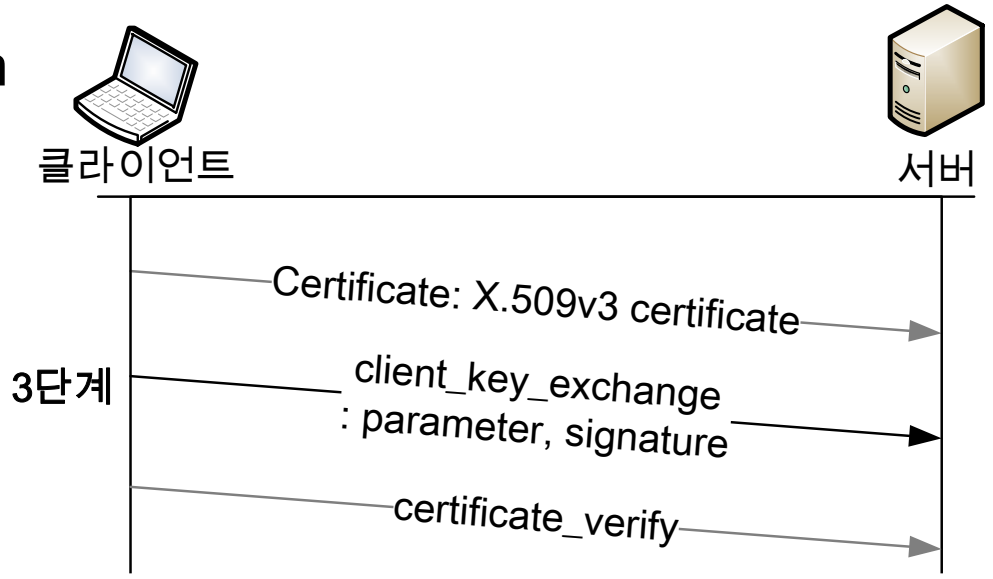
무선 전송 계층 보안 (WTLS)

- Handshake Protocol (9/15)
  - 2단계: 서버 인증과 키 교환 (3/3)
    - 3가지 키 교환과 인증 유형
      3. EC Diffie-Hellman



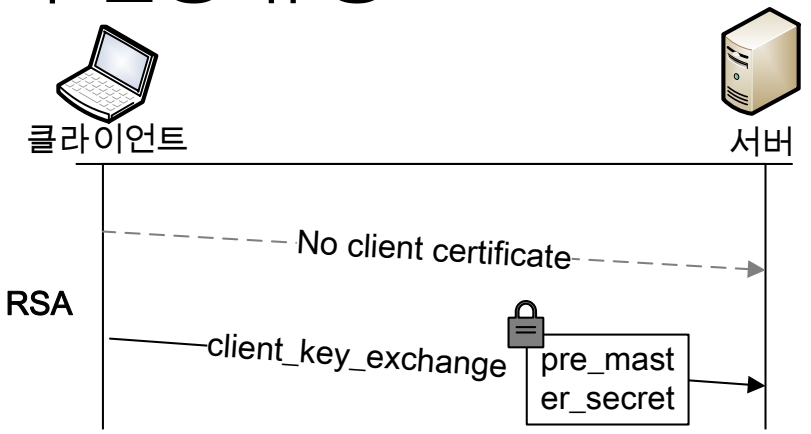
무선 전송 계층 보안 (WTLS)

- Handshake Protocol (10/15)
  - 3단계: 클라이언트 인증과 키 교환 (1/3)
    - 클라이언트가 자신의 인증서가 유효함을 스스로 검증
    - 대표적 키 교환 알고리즘 (3가지)
      1. RSA
      2. 익명 Diffie-Hellman
      3. EC Diffie-Hellman

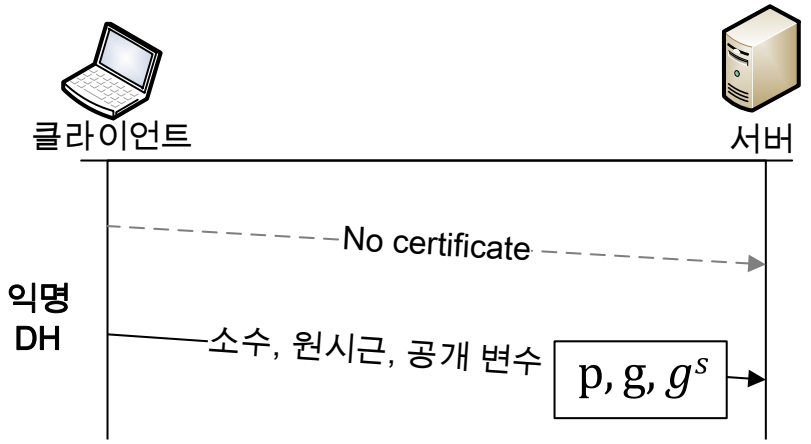


무선 전송 계층 보안 (WTLS)

- Handshake Protocol (11/15)
  - 3단계: 클라이언트 인증과 키 교환 (2/3)
    - 4가지 키 교환과 인증 유형
      1. RSA

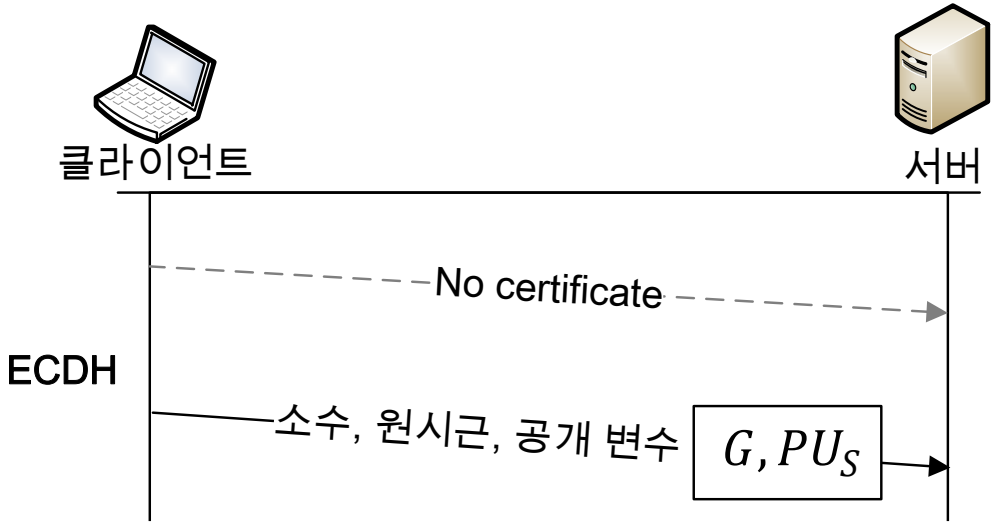


      2. 익명 DH



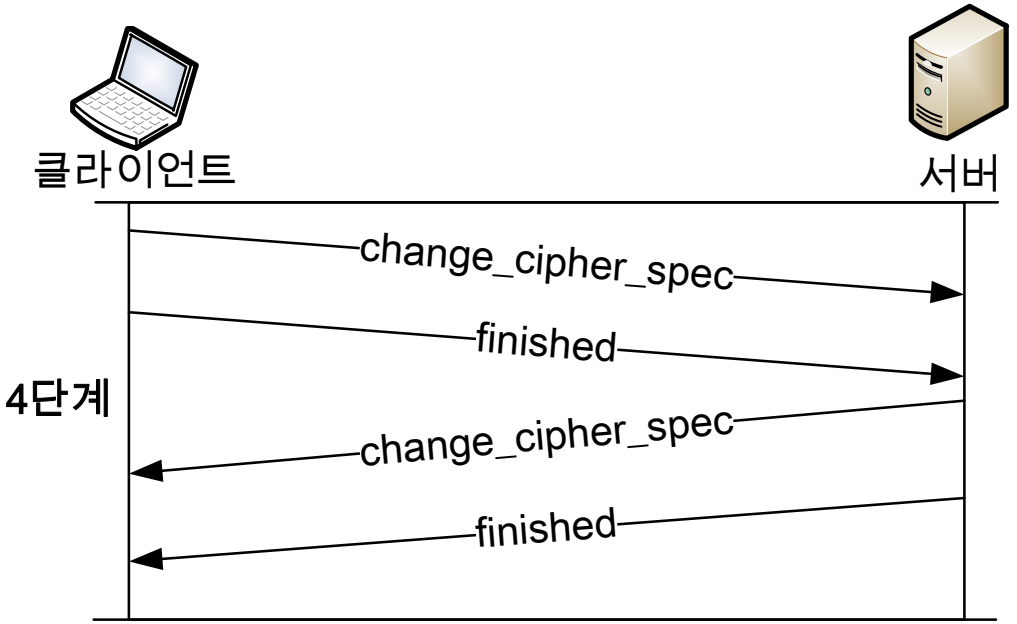
무선 전송 계층 보안 (WTLS)

- Handshake Protocol (12/15)
  - 3단계: 클라이언트 인증과 키 교환 (3/3)
    - 4가지 키 교환과 인증 유형
      3. EC Diffie-Hellman



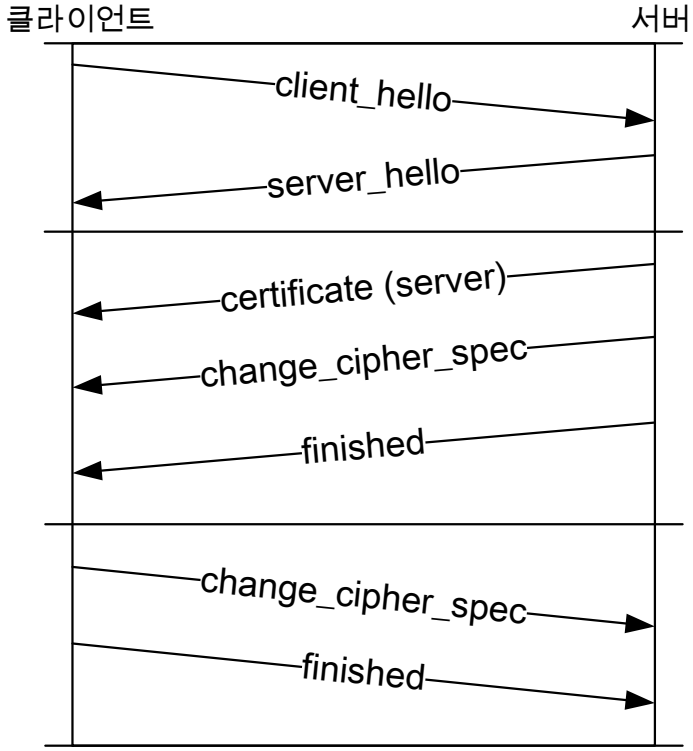
무선 전송 계층 보안 (WTLS)

- Handshake Protocol (13/15)
  - 4단계: 종료
    - 안전한 연결 종료
    - Finished 메시지는 키 교환과 인증 과정이 성공적임을 확인



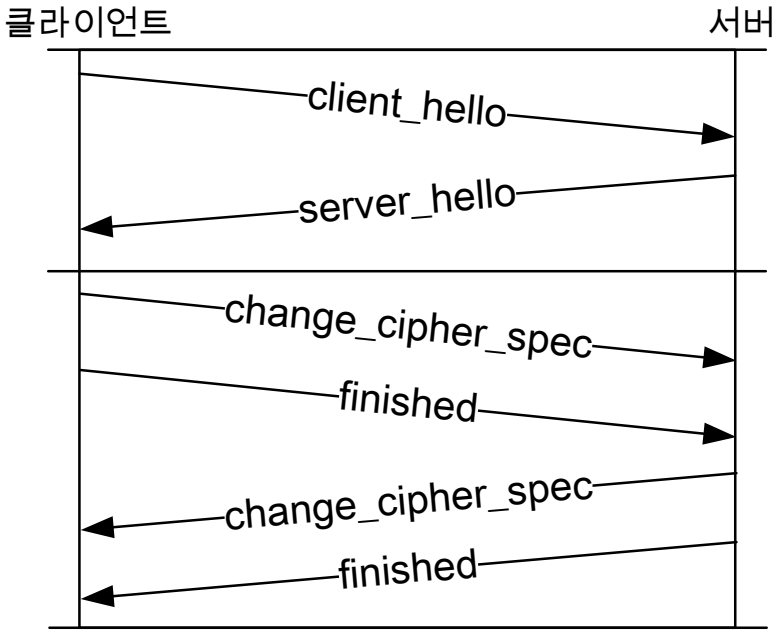
무선 전송 계층 보안 (WTLS)

- Handshake Protocol (14/15)
  - 최적화된 완전-핸드셰이크 (Optimized Full-Handshake)
    - 서버가 클라이언트의 인증서를 다른 경로를 통해 가지고 있는 경우
      - 과거에 통신했던 경우/공개되어 있는 경우 등
    - 동작 그림



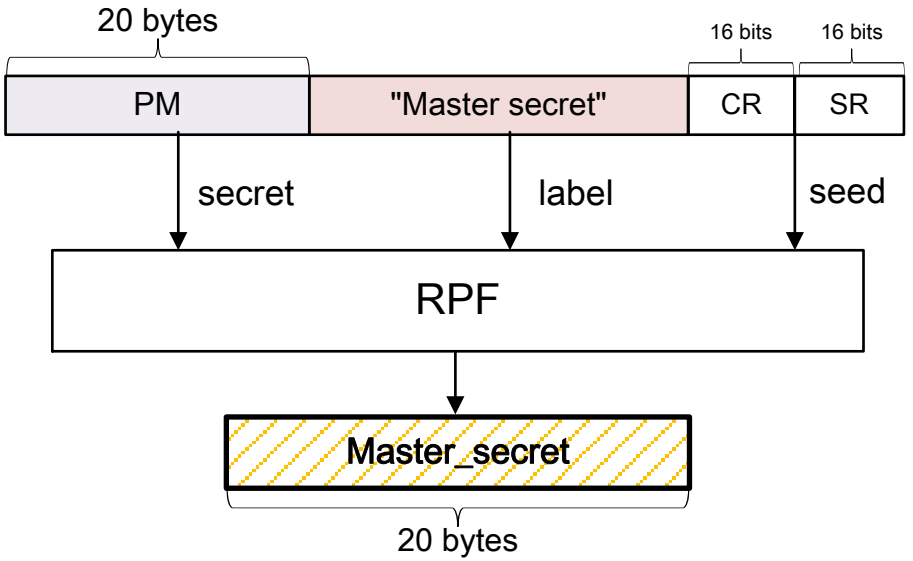
무선 전송 계층 보안 (WTLS)

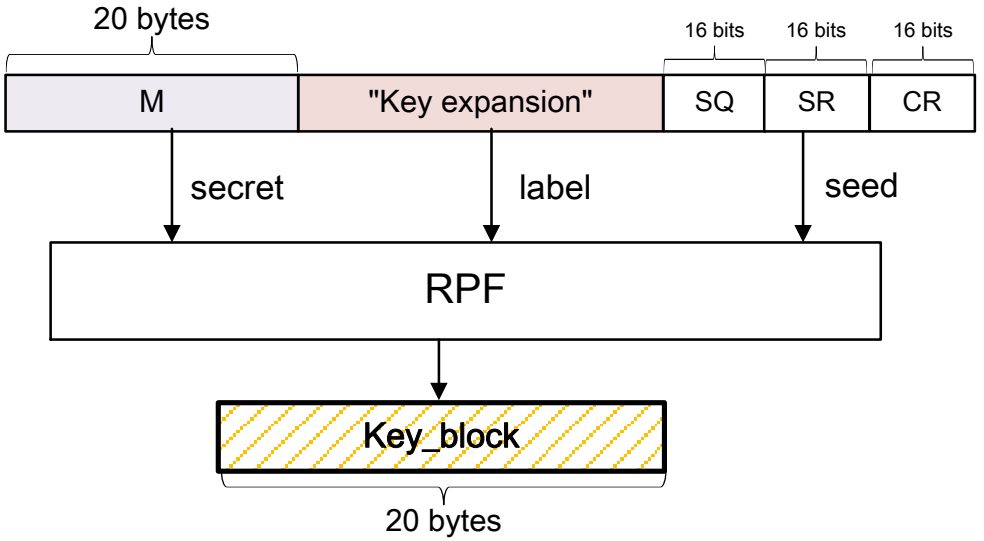
- Handshake Protocol (15/15)
  - 단축-핸드셰이크 (Abbreviated-Handshake)
    - 인증서 교환과 같은 서버와 클라이언트 인증을 위한 정보는 교환하지 않음
    - 이전 세션에서 Master secret과 현재 교환한 난수 값을 이용해 파라미터 재생성
  - 동작 그림



무선 전송 계층 보안 (WTLS)

- 암호계산
  - Master Secret , Key_block 암호 계싼 과정 그림





목 차

- 무선 응용 프로토콜 (WAP)
- 무선 전송 계층 보안 (WTLS)
- WAP 종단-대-종단 보안

WAP 종단-대-종단 보안

- WAP 종단-대-종단 보안의 필요성

1. WTLS의 취약점
   - TLS를 무선 환경에 최적화하여 수정한 프로토콜
     - 제약된 환경으로 인해 일부 알고리즘 사용이 제한됨

2. WAP 종단간 안정성
   - WAP이 사용하는 프로토콜과 인터넷 프로토콜이 서로 다름
     - 두 프로토콜의 연결을 위한 WAP G/W의 사용으로 인해 발생하는 취약점이 존재

WAP 종단-대-종단 보안

- WAP 종단-대-종단 보안 방법
  - 2가지 방법
    - TLS-기반 보안
      - 두 종단 사이에 안전한 TLS 세션 설치
      - WAP G/W는 TCP 계층의 G/W로 동작
        - G/W를 통과하는 동안 TCP 데이터는 암호화 되어있기 때문에 종단-대-종단 보안유지 가능
    - IPsec-기반 보안
      - 클라이언트나 G/W에서 IPsec을 사용하면 모든 과정에서 데이터가 암호화되기 때문에 종단-대-종단 보안 유지 가능

감사합니다!

백업 1: 국제 네트워킹 표준 기구

- 대표적 국제 네트워킹 표준 기구 정리 표

기관명	역할
국제 표준화 기구(ISO, International Organization for Standardization)	전 세계에서 가장 큰 표준 기구, OSI 참조 모델을 개발
미국 표준 협회(ANSI, American National Standards Institute)	표준을 만드는 기구에게 자격을 주고 이들 기구를 감독
정보 기술 산업 협의회(ITIC, Information Technology Industry Council)	정보 기술 분여의 여러 회사 모임, 표준을 개발
국가 정보 기술 위원회(NCITS, National Committee for Information Technology)	ITIC가 만든 위원회로, 정보 기술 분야와 관련된 표준을 개발하고 관리
미국 전기 전자 학회(IEEE, Institute of Electrical and Electronics Engineers)	전기, 전자 분야 전문 기구, IEEE 802 프로젝트로 이더넷 등 여러 유명 네트워킹 기술을 개발
미국 전자 공업 협회(EIA, Electronic Industries Alliance)	전기 결선과 전송 표준을 출판한 국제 산업 협회
미국 통신 산업 협회(TIA, Telecommunications Industry Association)	EIA의 통신 부문으로 통신 표준을 개발
국제 전기통신 연합-통신 표준 부문(ITU-T, International Telecommunication Union-Telecommunication Standardization Sector)	통신 산업 표준을 개발하는 국제 기구
유럽 전기 통신 표준 협회(ETSI, European Telecommunications Standards Institute)	유럽 시장을 위한 통신 표준을 개발, 라디오 대역폭 사용을 규제

백업 2: 인터넷 표준 기구

- 인터넷 표준 기구 관계 그림