5.4 HTTPS

5장. 전송레벨 보안

개요 (1)

- HTTPS(SSL을 이용하는 HTTP)
  - 웹브라우저와 웹서버 간의 안전통신 구현을 위한 HTTPS와 SSL의 결합
  - 모든 웹브라우저에 내장
  - HTTPS 통신을 지원하는 웹 서버에 따라 달리 사용
    - 예) 검색엔진은 HTTPS를 지원하지 않음
- 사용자 관점
  - URL주소가 https://로 시작
  - HTTPS는 443번 포트로 SSL을 호출
    - HTTP는 80번 포트

개요 (2)

- HTTPS에서 암호화 요소
  - 요청 문서 URL
  - 문서 내용
  - (브라우저 사용자가 입력한) 브라우저 양식 내용
  - 브라우저가 서버에게 보낸 쿠키와 서버가 브라우저로 보낸 쿠키
  - HTTP 헤더 내용
- RFC 2818 “HTTP Over TLS”
  - Updated by RFC5785, RFC7230
  - RFC 5785 “Defining Well-Known Uniform Resource Identifiers (URIs)”
  - RFC 7230 “Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing”
- HTTPS 입장에서는 SSL이나 TLS 상관 없음

연결 개시 (1)

- HTTPS 클라이언트
  - TLS 클라이언트 역할 수행
  - 적절한 포트를 통해 서버에 연결 시작
  - TLS 핸드셰이크 시작을 위해 TLS ClientHello를 전송
  - TLS 핸드셰이크가 마무리되면 첫 번째 HTTP 요청을 전송
  - 모든 HTTP 데이터는 TLS응용 데이터로 전송

연결 개시 (2)

- HTTPS 연결 수준
  - HTTP 수준
    - 하위계층으로 연결 요청 메시지 전달
  - TLS 수준
    - TLS 클라이언트와 TLS 서버 사이의 세션 설정
    - 하나 이상의 연결 지원
  - TCP 수준
    - 클라이언트 측 TCP와 서버 측 TCP 연결

연결 종료 (1)

- HTTP 클라이언트나 서버
  - HTTP 레코드 안에 “Connection: close” 를 삽입해서 연결 종료
  - 이 레코드 전달 후 연결이 종료된다는 의미
- HTTPS 연결 종료를 위해 TLS가 원격 TLS와 연결을 종료해야 함
  - 하위 TCP 연결을 먼저 종료
  - TLS 경보 프로토콜 close_notify 사용
  - TLS 종료 전 종료 경보 교환을 시작해야 함

연결 종료 (2)

- 불완전 종료(incomplete close)
  - TLS는 종료 경보를 보낸 뒤에 상대방이 종료 경보를 보낼 때까지 기다리지 않고 연결을 종료할 때 발생
  - 세션 재사용은 모든 메시지를 수신했을 때에만 허용되어야 함
  - HTTP는 하위 TCP 연결이 사전 close_notify 경보와 Connection: close 지시자 없이 종료되는 상황에 대처할 수 있어야 함
    - 원인
      - 서버 프로그램 오류
      - TCP 연결중단을 일으키는 통신오류
        - 모종의 공격
        - 보안경고 발령 필요