HTTP / HTTPS

2조
발표자: 이은상

개요

1. HTTP / HTTPS 기본 개념
2. 암호학 이론
3. HTTPS 동작 과정
4. HTTP / HTTPS, 무엇을 선택할 것인지?

주제 1. HTTP / HTTPS 기본개념

1) HTTP / HTTPS ?

* HTTP (Hypertext Transfer Protocol)
  - http 는 기본적으로 평문 텍스트(Plain Text)로 통신
  - 80번 포트

* HTTPS (HyperText Transfer Protocol Secure)
  - http 의 보안 버전 (작동 방식은 동일)
  - SSL / TLS 암호화 프로토콜을 사용하여 데이터를 안전하게 전송
  - 443번 포트

1) HTTP / HTTPS ?

HTTP 와 HTTPS 예시 이미지 삽입 예정

2) HTTP 의 문제점

* 평문 통신의 문제
  - 데이터가 노출되었을때 누구나 해석 가능
* 데이터 무결성 문제
  - 데이터가 중간에 변조되었는지 여부를 확인할 수 없음
* 신원 확인 부재의 문제
  - 클라이언트가 서버의 신원을 확인하지 않음
  - 따라서 중간자 공격자가 서버로 위장하여 클라이언트와 통신 위험성 존재

3) HTTPS 의 문제 해결 방법

* 평문 통신의 문제
  - 전송되는 데이터를 암호화
* 데이터 무결성 문제
  - 무결성 확인 매커니즘 도입
* 신원 확인 부재의 문제
  - 인증서를 사용하여 서버의 신원을 보증

3-1) HTTPS 인증서

인증서 예시 사진 삽입 예정

3-1) HTTPS 인증서

* 인증서 설명
* 인증서 포함 내용 설명

4) HTTPS 의 특장점

* 공개키 인프라 (PKI, Public Key Infrastructure)
  - 데이터의 기밀성
  - 데이터의 무결성
  - 서버의 신원 보증

* 검색 엔진 최적화(SEO, Search Engine Optimization)

4-1) HTTPS 의 단점

* 암호화/복호화 과정에서 추가적인 리소스 소모
  - 상대적으로 느린 속도

* 추가비용
  - 인증서 발급/갱신 비용
  - HTTPS 구현을 위한 추가 개발 비용

5) 공개키 인프라

* 인증기관(CA, Certification Authority)
* 디지털 인증서
  - CA는 공개키 검증, 해당 공개키에 대한 인증서 발급
* 디지털 서명
  - 개인키(Private Key)를 사용하여 서명 생성
  - 해당 서명을 공개키(Public Key)를 이용하여 검증

주제 2. 암호학 이론

주제 2. 암호학 이론

HTTPS 를 네트워크 인프라 관점으로 이해하고

공개키 인프라 개념을 이해하기 위해

1) 암호화 구분과 대표 알고리즘

* 단방향 암호화 (Hash)
  - MD5(Message Digest Algorithm 5)
  - SHA(Secure Hash Algorithm, sha-1, sha-256)

* 양방향 암호화 (대칭키 / 비대칭키)
  - 대칭키: AES
  - 비대칭키: RSA

주제 3. HTTPS 동작 과정

주제 4.

HTTP / HTTPS 무엇을 선택할 것인지?

1) 보안성, 속도, 비용 사이의 트레이드 오프

* 보안성: HTTPS 가 압도적으로 높은 보안을 보장
* 속도: 기술발전으로 퍼포먼스 측면에서의 차이는 미미
* 비용: 환경에 따라 고려해볼 여지가 있음

2) HTTPS의 성능 향상과 관련된 기술

* 보안성: HTTPS 가 압도적으로 높은 보안을 보장
* 속도: 기술발전으로 퍼포먼스 측면에서의 차이는 미미
* 비용: 환경에 따라 고려해볼 여지가 있음

참고문헌

* ChatGPT
* 생활코딩 - 암호학