Http 완벽가이드 #14(~p390)
보안 HTTP

2023.11.04

1. 다음 설명 중 틀린 것은?

1. 어려운 인코딩,디코딩 작업은 대부분 ssl 라이브러리 안에서 일어나기 때문에, 보안 HTTP를 사용하기 위해 웹클라이언트와 서버가 프로토콜을 처리하는 로직을 크게 변경할 필요는 없다.
2. 비밀메세지를 전달하는 수백만대의 컴퓨터를 쉽게 만들수 있는 시스템을 공개키 암호법이라고 한다.
3. 잘 알려진 대칭키 알고리즘으로는 DES, Triple-DES, RC2, RC4 등이 있다.
4. 대부분 인코딩, 디코딩 알고리즘이 공개적으로 알려져 있으므로 키만이 유일한 비밀이다.
5. 95년기준 10만달러 비용으로128비트 DES 암호를 깨뜨리는데, 7만년이 걸린다.

정답 : 5 (10의 19승 년)
1. p357
2. p358
3. p362 4. p362

2. 다음 설명 중 맞는 것은?

1. 128비트 암호화 소프트웨어는 활발히 수출되고 있다.
2. 대칭키 암호의 장점 중 하나는 발송자와 수신자가 대화하려면 둘 다 공유키를 가진다는 점이다.
3. 공개키 알고리즘 체계 중 RSA 알고리즘이 유명하며, MIT에서 발명되었다.
4. 공개키 알고리즘은 그 빠른 계산 방식으로 널리 쓰인다.
5. 신뢰할 수 있는 기관으로 부터 보증받은 사용자나 회사의 정보는 디지털 서명으로 보관한다.

정답 : 3
1. p363 수출업체가 벌금 맞았다.
2. 단점
4. 공개키 암호방식의 알고리즘은 느린 경향이 있다.
5. 디지털 인증서

3. 다음 설명 중 틀린 것은?

1. 인증서 내부에는 대상의 이름, 유효기간, 인증서발급자, 디지털 서명이 들어 있다.
2. 디지털 인증서에 대한 단일표준은 1992년, 시애틀에서 만들어 졌다.
3. 대부분의 인증서는 그들 정보는 x.509라 불리는 표준화 된 서식에 저장하고 있다.
4. 인증서 발급자는 서명한 기관의 이름 x.500 포맷으로 기록되어 있다.
5. 서버인증서는 웹사이트이름, 호스트명, 공개키, 서명기관의 이름과 서명을 가진다.

정답 : 2
1. p369
3. p370
4. p370표
5. p371

4. 다음 설명 중 맞는 것은?

1. HTTP 는 분산된 웹앱의 광역 보안 관리에 있어 대단히 중요하다.
2. 오늘날 HTTP의 보안계층은 TLS과 그것의 현대적인 대체품인 SSL로 구현된다.
3. URL이 https 스킴을 가지고 있다면 클라이언트는 서버에 442번 포트로 연결한다.
4. SSL은 바이너리 프로토콜이기 때문에 HTTP와는 완전히 다르다.
5. HTTPS 핸드셰이크 과정에는 임시 세션키 생성 단계가 있다.

정답 : 4

1. https
2. p373 (바뀜)
3. 443번
5. p376

5. 다음 설명 중 틀린 것은?

1. SSL은 서버 인증서를 클라이언트로 나르고, 다시 클라이언트 인증서를 서버로 날라주는 상호 인증을 지원한다.
2. 서버 인증서는 조직이름, 주소, 서버DNS도메인 이름, 그외 정보를 보여주는 X.509 v3에서 파생된 인증서이다.
3. HTTPS 인증서는 사이트 정보가 더해진 X 509 인증서이다.
4. 웹서버 인증서 검사를 위한 알고리즘에는 사이트 신원검사를 포함한다.
5. 몇몇 인기 있는 웹 서버 프로그램은 여러개의 인증서를 지원한다.

정답 : 5

1. p377
2. p377
3. p377 그림 아래
4. p378
5. 오직 하나의 인증서 만을 지원한다.

6. 다음 설명 중 틀린 것은?

1. SSL은 복잡한 바이너리 프로토콜이다.
2. 클라이언트와 서버는 DES-CBC3-MD5 대량 암호화를 쓰는 것에 합의 했다.
3. 클라이언트가 서버로 보낼 데이터를 서버의 공개키로 암호화하기 시작했다면, 프락시는 더 이상 HTTP 헤더를 읽을수 없다.
4. HTTPS 터널링 프로토콜을 사용하기 위해서 HTTPS는 CONNECT 라 불리는 새로운 확장메서드를 이용해 평문으로 된 종단 정보 제공을 위해 사용된다.
5. SSLeay는 OpenSSL을 계승 하였다.

정답 : 5

4. 387
5. 반대임