2019 정보보안 중간

텍스트, 영수증, 폰트, 화이트이(가) 표시된 사진

자동 생성된 설명

1. 보안에서 사용되는 공격 기법 중 하나 이다. 이 공격은 모든 가능한 조합을 시도하여 암호를 해독하거나 암호화된 데이터에 접근하기 위해서 사용된다. 원리는 가능한 모든 입력 또는 키 조합을 순차적으로 병렬로 시도하면서 조합을 찾을 때 까지 진행한다. 매우 강력하지만 시간과 자원을 많이 소모하는 공격이다.
2. 메시지 무결성은 메시지가 전송 중에 변경되지 않았음을 보장하는 보안 속성이다. 해시 함수를 사용하면 메시지를 해시함수에 입력하여 해시 값을 생성하고 메시지와 함께 전송한다. 수신측은 이 메시지와 해시함수를 계산해 송신측이 보낸 해시 값과 비교해 같다면 메시지가 중간에 변경되지 않았다고 판단하고, 다른 경우는 메시지가 중간에 변경되었다고 판단한다.
3. 디피 – 헬만 알고리즘은 비대칭키 암호화 알고리즘의 방법 중 하나로 송수신측은 각각의 공유키와 비밀키 사용한다. 기본적으로 송수신측이 안전하게 비밀키를 공유하고 이를 사용하기 위해서 만들어졌다. 안전하게 비밀키를 공유하는 과정은 다음과 같다.  
   1. 암호화 과정에서 사용한 변수들을 정의한다. ( p, g )

2. A와 B은 각각 비밀 수 a와 b를 선택

3. 다음 계산을 수행하여 공개 수를 계산

* Alice: A = g^a mod p
* Bob: B = g^b mod p

4. Alice와 Bob은 공개 수 A와 B를 서로에게 전달

5. 이제 Alice와 Bob은 비밀 수 a와 b를 사용하여 동일한 비밀 키를 계산할 수 있다.

* Alice: K = B^a mod p
* Bob: K = A^b mod p

이로써 A와 B는 서로 비밀 키를 공유하게 된다. 이때 공격자는 양측이 송수신하는 메시지를 보더라도, 공격자는 키를 생성할 수 없다.

1. 블록 암호를 사용하여 데이터를 암호화하는 대칭 암호화 모드 중 하나이다. 병렬처리에 용이하다. Initialization vector를 생성해서 이 IV를 기반으로 카운터를 생성한다. 카운터는 블럭마다 증가시키며 카운터와 키값을 가지고 암호화 하고 이를 사용해 평문과 XOR연산을 한다. 복호화 과정이 이와 같이 흐름으로 복호화 된다. CTR모드는 데이터 무결성을 지원하지 않기 때문에 HMAC과 같은 무결성 검사를 사용하는게 좋다.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

1. HMAC : 대칭 알고리즘으로, 인증 또는 무결성을 확인하기 위해 동일한 비밀 대킹키를 사용.  
   RSA : 비대칭 알고리즘으로 공개키와 개인키 쌍을 사용. 서명을 생성하는데 개인키를 사용하며 서명을 확인하는 데에는 공개키가 사용된다.
2. HMAC : 대칭키 암호화에서는 일반적으로 128비트에서 256비트의 길이의 키를 사용한다.  
   RSA : 비대칭키 알고리즘을 사용하기 때문에 대칭키보다 긴 키를 사용한다. 일반적으로 2048비트에서 4096비트의 길이를 사용한다.
3. HMAC : 대칭 알고리즘을 사용하므로 처리속도가 빠르고, 대칭키를 사용함으로 암호화 및 복호화가 빠르다.  
   RSA : 비대칭 알고리즘으로 키 길이가 길 수록 처리 속도가 감소한다. 서명 생성 및 확인 작업에는 많은 계산이 필요하기 때문에 상대적으로 느리다.
4. HMAC : 대칭 알고리즘으로 암호화/ 복호화를 하는데 같은 키가 사용된다. 그래서 키를 가진 모든 사용자가 암호화 복호화가 가능하다. A와 B가 비밀키를 공유한다면 A가 만든 암호문을 B도 만들어낼 수 있다. 때문에 A가 만든 암호문을 A가 거짓으로 만들지 않았다고 주장하면 B도 만들어낼 수 있는 암호문이기 때문에 B가 A가 만든 암호문임을 증명 할 수 없다.  
   RSA : 비대칭 알고리즘으로 암호화 / 복호화 하는데 공개키, 개인키 쌍을 사용한다. 그렇기 때문에 A가 만든 암호문은 A만 복호화 할 수 있기 때문에 부인 방지 기능을 제공한다.

텍스트, 폰트, 화이트, 영수증이(가) 표시된 사진

자동 생성된 설명

1. m(메시지)을 hash 함수(sha2,sha3)를 사용해 message digest로 만든 뒤 송신측의 private key로 암호화해 Digital signature을 만들어낸다. 만들어진 Digital signature는 m와 함께 송신된다.  
    텍스트, 도표, 스크린샷, 원이(가) 표시된 사진

   자동 생성된 설명
2. 수신측은 m(메시지)와 암호화된 Digital signature를 수신한다. m은 hash 함수(sha2,sha3)를 사용해 message digest로 만들고 암호화된 Digital signature를 public key를 사용해 복호화 한다. 복호화된 값과 message digest을 비교해 같다면 데이터가 공격 받지 않고 변경, 위조되지 않았다고 생각할 수 있다.   
   텍스트, 스크린샷, 도표, 폰트이(가) 표시된 사진

   자동 생성된 설명