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.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

텍스트, 폰트, 화이트, 영수증이(가) 표시된 사진

자동 생성된 설명