출석수업 과제물(평가결과물) 표지(온라인제출용)

**교과목명 : 컴퓨터보안**

**학 번 : 202034-153746**

**성 명 : 이동열**

**강 의 실 : 경기지역대학 온라인수업**

**연 락 처 : 010-5254-5565**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

기밀성은 데이터에 대해 인가 받은 사용자만이 접근할 수 있도록 하는 것을 의미한다. 중요한 데이터를 외부에 무분별하게 노출하지 않기 위해 지켜야하는 핵심 요소로 데이터에 대해 승인이나 인가를 받지 못한 사용자에 대해서는 접근을 제한해야 한다.

예를 들어 웹사이트나 은행 등에 저장되어 있는 휴대폰번호나 계좌번호와 같은 개인 식별정보가 악의적인 사용자에게 넘어간다면 큰 피해가 발생될 수 있다. 이런 일을 방지 하기 위해 기밀성을 달성해야 한다.

기밀성을 해치는 주요 공격은 인증 레이어를 우회하거나 네트워크로 전송되는 패킷을 중간에서 탈취하는 스니핑 공격, 암호화되어 있는 데이터들을 분석해 이후 행동을 예측하고 다른 정보를 획득하는 트래픽 분석 공격이 있다.

기밀성을 달성하기 위해서는 인가된 사용자만 데이터에 접근할 수 있도록 인증 및 접근 통제 시스템을 구축하거나 디스크 암호화, 패킷 암호화 등을 통해 정상적으로 인가받지 않은 사용자가 데이터에 접근하거나 탈취하더라도 내용을 확인하지 못하게 하는 방법이 있다.

무결성은 데이터의 생명주기동안 의도와 다르게 데이터가 변경 및 손상되지 않고 완전성과 정확성, 일관성을 보장하는 것을 의미한다. 이는 승인된 사용자, 절차에 의해서만 데이터가 변경될 수 있다는 것을 의미한다.

무결성을 해치는 대표적인 공격은 데이터를 탈취해 변조 후 사용자에게 전달하는 스푸핑 공격이다. 이렇게 의도되지 않은 데이터 변조로 인해 사용자에게 피해가 발생할 수 있다.

무결성을 보장하기 위해서는 전자서명을 통해 데이터가 변조되지 않았음을 검증하거나 승인되지 않은 사용자에 의해 데이터가 변조됐을 경우 알림을 발생시키는 방법이 있다.

가용성은 데이터에 정상적으로 접근할 수 있음을 보장하는 것을 의미한다. 이는 의도치 않게 서버나 데이터가 파괴되지 않아야 하며 인가받은 사용자가 데이터에 접근하고자 할 때 정상적으로 접근이 가능해야 함을 의미한다.

가용성을 해치는 요인은 자연재해, 화재와 같은 외부 요인과 서버 자원 과부화와 같은 내부 요인이 있으며 이외에도 서버 노후화, 불안정한 네트워크와 같은 요인들도 있다.

가용성을 보장하기 위해서는 예상치 못한 중단에 대비해 서버를 이중화하거나 재해 복구 계획을 세워 각종 재해에 대비하는 방법이 있다. 또한 서버 장비를 주기적으로 교체해 장비 고장을 방지하고 소프트웨어를 최적화해 자원 낭비를 방지하는 방법도 있다.

대칭키 암호는 암호화할 때와 복호화할 때 동일한 키를 사용하는 방식이다. 이때 사용하는 키를 비밀 키 또는 대칭 키라고 부른다. 대칭키 방식은 서버 자원을 적게 소모하고 암호화 및 복화 속도가 빠르기 때문에 디스크 암호화와 같은 곳에 사용된다.

대칭키를 사용해 암호화 통신을 해야할 경우 상대방도 동일한 키를 가지고 있어야 하기 때문에 키를 전달하는 과정에서 키 탈취와 같은 공격에 노출될 수 있다. 또한 해당 키를 여러 사용자가 사용할 경우 키 교체와 같은 부분 때문에 관리가 어려워 진다는 단점이 있다.

대칭키 암호화는 블록 암호 방식과 스트림 암호 방식이 있다. 블록 암호 방식 평문 데이터를 블록 단위로 나눠서 암호화하는 방식이다. 평문을 여러개의 작은 블록으로 나눈 다음 각 블록을 암호화하고 암호화된 블록은 다음 암호화의 입력 블록이 된다. 이런 방식은 병렬 수행이 가능하기 때문에 성능면에서 이점이 있다. 블록 암호 방식에 사용되는 알고리즘에는 AES, SEED, ARIA, IDEA 등이 있다. 스트림 암호 방식은 암호화할 평문과 동일한 길이의 키를 생성해 암호화할 평문과 비트 단위의 XOR 연산을 통해 암호화하는 방식이다. 이때 연산에 사용할 키로는 규칙이 없는 랜덤 수열을 사용하는 것이 가장 안전하다.

공개키 암호는 암호화 및 복호화에 공개키, 개인키 두개를 사용하는 방식이다. 개인키는 자신이 안전하게 보관하고 공개키는 사용자에게 공개한다. 대칭키 암호화 통신은 송신하는 사람이 평문을 공개키로 암호화해서 수신 받는 사람에게 전달하면 수신 받는 사람은 비공개 키를 사용해 암호문을 복호화한다. 공개키 암호화의 대표적인 알고리즘은 RSA, ECC, ElGamal과 전자서명에 사용되는 DSA, KCDSA 등이 있다.

공개키 방식은 암호문을 개인키로만 복호화할 수 있기 때문에 공개 키를 상대방에게 전달할 때 탈취로부터 매우 안전하다. 하지만 공개키 암호화는 대칭키 방식에 비해 속도가 매우 느려 실시간 암호화 통신에는 사용하기 힘들고 전자서명 정도로만 활용할 수 있다. 이러한 특징 때문에 SSL/TLS와 같이 암호화 통신시에는 대칭키를 암호화해서 상대방에게 전달하는 용도로만 사용하고 실제 암호화 통신은 대칭키를 사용한다.

RSA 알고리즘은 소인수분해를 기반으로 하는 알고리즘으로 큰 정수의 소인수분해가 힘든 점을 이용하는 방식이다. 구체적으로는 큰 정수 이 있다고 할 때 아래 수식을 만족하는 이 있다면와 을 알고 있어도 를 찾기 힘든 점을 이용한 것이다.

mod

RSA 알고리즘은 비슷한 자릿수의 차이가 큰 를 사용하며 전체 과정은 키 생성, 키 분배, 암호화, 복호화로 총 4단계로 진행된다.

먼저 키 생성을 보면, 비슷한 자릿수의 를 곱해 을 구한다. 이때 을 이진수로 변경했을 때의 길이가 Key의 길이가 된다. 을 구했다면 키마이클 함수를 사용해 아래 수식을 계산한다.

위 수식으로 계산한 결과값은 개인키에 사용된다. 키마이클 함수 외에도 오일러의 피함수를 사용해도 되지만 오일러의 피함수는 가 지나치게 커져버리는 경우가 발생할 수 있어 키마이클 함수를 주로 사용한다. 이후 아래 두 조건을 만족하는 정수 를 선택한다.

1 < e < , , 와 은 서로소

마지막으로 를 사용해 아래 수식을 계산한다.

이렇게 구한 값들은 공개키()와 개인키()의 구성요소가 된다. 키 생성 과정 중 주의해야할 점은 개인키의 구성요소인 와 계산에 사용되는 는 외부에 노출되면 안된다는 것이다.

그 다음 키 분배 과정을 보면 키 생성 과정을 통해 생성한 키를 암호화하려는 사용자에게 전달해야 한다. 메세지를 전달하려는 사용자는 공개키가 있어야만 암호화가 가능하기 때문에 메세지를 전달받을 사용자는 신뢰할 수 있는 경로를 통해 공개키를 상대방에게 전달해야 한다.

암호화 과정은 공개키와 변환법을 사용해서 진행한다. 공개키의 를 사용해 아래 수식을 계산하면 암호화된 를 얻을 수 있다.

복호화 과정은 개인키를 사용해서 수행한다. 개인키 를 사용해 아래 수식을 계산하면 c를 복호화할 수 있다.

전자서명은 메세지를 전달한 서명자의 신원과 내용 변조를 보증하는 정보를 의미한다. 전자서명을 만족하기 위해서는 5가지 조건을 만족해야 한다. 합법적인 사용자만이 문서에 서명이 가능해야 하는 위조 불가 조건, 공개키로 누구든지 서명자를 검증할 수 있어야 하는 서명자 인증 조건, 서명한 후 서명한 사실을 부인할 수 없는 부인 불가 조건, 문서 내용을 변경할 수 없는 변경 불가 조건 서명은 서명한 문서에서만 사용해야 하는 재사용 불가 조건이 있다.

전자서명은 서명 생성을 위한 해시함수, 서명 암호화를 위한 개인키, 암호문을 복호화하기 위한 공개키가 필요하며 전체적인 동작방식은 다음과 같다.

텍스트, 도표, 평면도, 개략도이(가) 표시된 사진

자동 생성된 설명

먼저 송신자는 서명 암호화 및 복호화에 사용할 개인키/공개키 키 쌍을 생성한다. 그 다음 해시함수를 사용해 메세지를 다이제스트로 변환한다. 이 다이제스트가 전자서명에서 서명 역할을 하게 된다. 이렇게 생성한 다이제스트를 개인키로 암호화한 뒤 메세지와 같이 첨부해서 수신자에게 전달한다.

수신자는 전자서명이 포함된 전체 메세지 중 암호화된 전자서명을 공개키로 복호화하고 메세지 본문을 해시함수를 사용해 다이제스트로 변환한다. 그 다음 복호화된 다이제스트(전자서명)와 새로 만든 다이제스트를 비교한다. 이 때 두 다이제스트가 일치하면 전자서명은 유효한 것이 되며 서명자와 메세지 내용을 보증하게 된다.