11주차 3차시 인증

【학습목표】

1. 암호화 기법을 통한 인증에 대해 설명할 수 있다.
2. 인증 기법에 대해 설명할 수 있다.

학습내용1 : 암호화 기법

1. 암호 시스템

암호 기법을 적용한 암호화 및 복호화 과정으로 구성된 시스템

* 암호 시스템의 분류

① 암호 방법에 따른 분류
비밀키 시스템 : 대칭키 시스템, 암호화 및 복호화 할 때 개인키 사용
공개키 시스템 : 암호화 할 때 공개키, 복호화 할 때 개인키 사용.

② 암호 형태에 따른 분류
블록 암호 : 평문을 질정길이의 블록으로 잘라서 암호 알고리즘에 따라 암호화 하는 방식
스트림 암호 : 문자 단위 혹은 비트 단위로 암호화 하는 방식

2. 암호화

데이터를 주고받을 때 송신자와 수신자 이외에는 그 내용을 알아보지 못하도록 평문을 암호문으로 변환하는 것이다.

3. 복호화

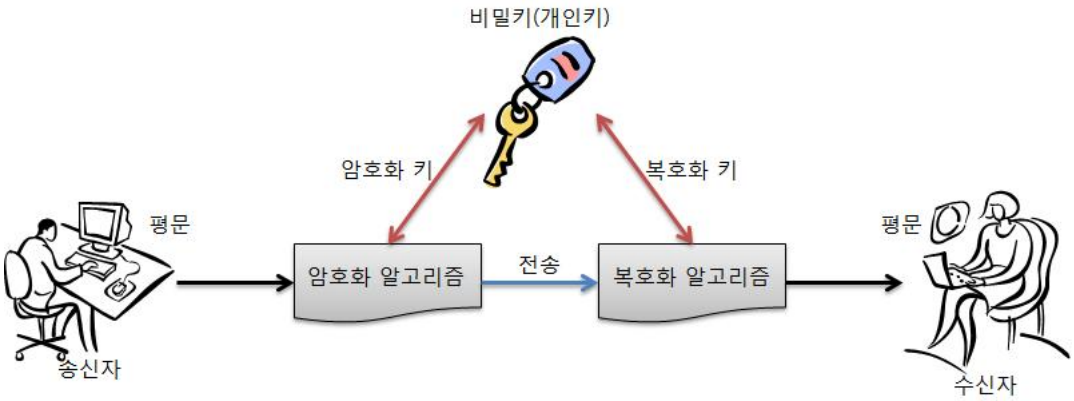
암호화되어 전송된 암호문을 원래의 평문으로 되돌려 복구하는 것이다.

4. 암호의 기능

무결성(Integrity) : 송신자의 내용이 변경되지 않고 수신자에게 전달되었다는 것을 보장하는 것.(변경은 삽입, 삭제, 대체, 수정을 말한다)
기밀성(Confidentiality) : 정보를 전달할 때 다른 사람들이 도청하지 못하도록 노출을 막아서 의도된 수신자만이 메시지를 해독할 수 있도록 하는 것
인증(Authentication) : 송신자가 데이터를 보내면 수신자가 송신자의 신원을 확인하는 것
부인방지(Non-repudiation)/서명 : 송신자가 의사를 표시한 내용이 수신자에게 전달이 된 후에 임의로 부정할 수 없는 것 (서명 함께 전달 필요)

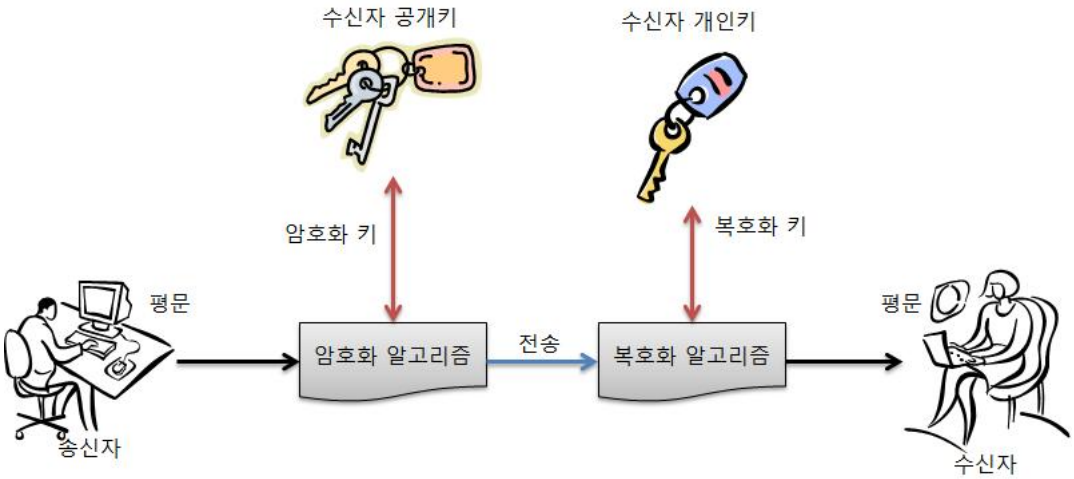
5. 비밀키 시스템

Private Key System(개인키 시스템)
대칭형 암호화 기법
가장 널리 사용하는 암호화 알고리즘
암호/복호 알고리즘에 사용할 비밀키를 하나만 사용한다.



6. 공개키 시스템(Public Key System()

공용키 시스템
디피-헬먼(Diffie-Hellman)에 의해 발표
송신자/수신자 모두 공개키와 개인키를 각각 소유하고 있다.
공개키는 평문을 암호화 할 때 사용
개인키는 암호문을 받아서 평문으로 변환할 때 각 개인이 다르게 소유한 개인키를 이용하여 암호문을 평문으로 복구



학습내용2 : 보안 기법의 종류

1. 정보보안 기법

① 디지털 서명 기법
손으로 쓰는 서명과 같이 전자서명으로 송신자가 문서를 전송했음을 증명하는 기법
송신/수신 하는 과정에서 암호문이 변조되지 않았음을 증명하는 기법
송신자는 송신자의 개인키를 이용하여 디지털 서명 후 문서를 송신한다.
수신자는 송신자의 공개키를 이용하여 디지털 서명과 문서를 확인한다.

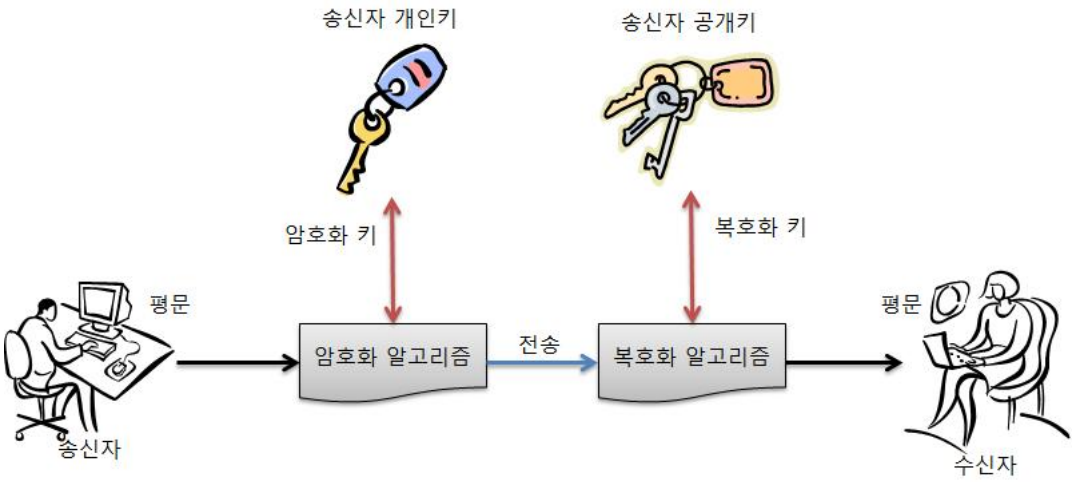
② 여분 정보 삽입 기법
정상적인 데이터에 여분의 거짓 데이터를 삽입하여 불법적인 방법으로 데이터에 접근하는 공격으로부터 보호하는 기법
정상적인 데이터와 거짓 데이터가 구분되지 않도록 한다.

2. 인증교환 기법

송신자/수신자 가 메시지를 주고받는 중간에 변경되지 않았음을 확인하는 기법이다.

① 메시지 인증 기법
송신자가 메시지를 전송할 때 전자 서명과 문서를 함께 전송한다.
수신자는 메시지를 수신할 때 전자 서명과 문서를 함께 수신 받는다
메시지 인증을 위해서 송신자/수신자 가 공통된 비밀키를 가지고 있어야 한다.

② 사용자 인증 기법
컴퓨터 시스템의 특정한 구역(폴더/디렉터리)을 사용자의 아이디와 암호로 보호하는 기법
구역에 접근을 허락 하도록 하려면 사용자의 아이디와 암호를 사용하여 사용자를 확인하는 기법
송신자는 송신자의 개인키로 암호문을 작성하여 수신자에게 보내주면, 수신자는 송신자의 공개키를 이용하여 암호문을 평문으로 복구한다.
송신자의 개인키를 이용하여 암호문을 만들었고, 수신자가 송신자의 공개키를 가지고 복호화 했으므로 송신자를 확인할 수 있다.



3. 접근 제어 기법

데이터에 접근이 허가된 사람에게만 데이터 사용을 허용하는 정책을 강화하기 위한 기법

4. 데이터 무결성 기법

한 단위 데이터의 무결성에 사용되는 방법과 접속점에서 전달되는 데이터 시퀀스 전체의 무결성을 위한 방법
불법 변경 탐지 방법을 이용하면 공격 탐지는 가능하지만 사전 방지는 불가능.

5. 경로 제어 기법

데이터 전송 전에 경로 과정을 구체적으로 지정함으로써 데이터를 안전한 채널만을 통하여 전달

6. 공증기법

통신 개체 사이에 전달되는 정보의 발신처, 정보의 무결성, 보내진 시간, 받은 시간 등을 공증하는 제3의 기관에 의존

7. 물리적 보안 유지와 인적자원의 보안 관리

모든 시스템은 어떤 형태로든 물리적으로 보안 유지
시스템을 운용하는 인적자원의 신뢰 요구

8. 하드웨어와 소프트웨어의 신임성

객체의 정확한 기능 수행을 확인하는 방법
형식적인 증명방식, 증명과 검증, 사전 예고된 공격의 탐지와 운영록 작성, 비밀장소에서 신임된 인적자원의 직접 제작

【학습정리】

1. 암호화
데이터를 주고 받을 때 송신자와 수신자 이외에는 그 내용을 알아보지 못하도록 평문을 암호문으로 변환하는 것이고, 암호화되어 전송된 암호문을 원래의 평문으로 되돌려 복구하는 것이 복호화다.

2. 암호의 기능
무결성, 기밀성, 인증, 서명

3. 암호화 기법
비밀키 시스템(개인키 시스템, 대칭키 시스템)
공개키 시스템

4. 정보 보안 기법
디지털 서명 기법, 여분 정보 삽인 기법

5. 인증 교환 기법
메이지 인증, 사용자 인증, 접근 제어 기법