정보보안론 10주차 강의

! 시험 !

전자 상거래 공격 유형

인증 공격

네트워크로 접근한 사용자가 적절치 않은 인증으로 다른 사용자로 위장하는 것

(피싱 사이트를 만들어서 상대방의 인증서를 탈취한 뒤 그 사람인 것 처럼 공격하는 방식)

송수신 부인 공격

네트워크를 통해 수행한 인증 및 거래 내역을 부인하는 것

기밀성 공격

네트워크로 전달되는 인증 정보 및 주요 거래 정보가 유출되는 것

무결성에 대한 공격

네트워크 도중에 거래 정보 등이 변조되는 것

! 시험 !

공개 키 기반 구조 (PKI)

메시지의 암호화 및 전자 서명을 제공하는 복합적인 보안 시스템 환경

트리형 공개 키 기반 구조

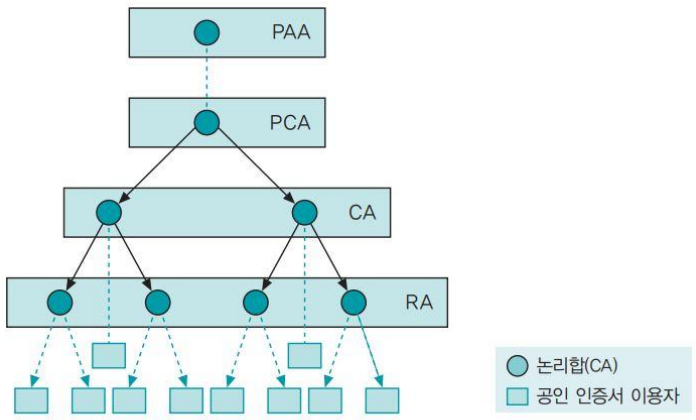

그림 8-6 트리형 공개 키 기반 구조

PAA : 우리나라 정부

PCA : KISA 트리형 공개 키 기반 구조

CA : 인증서 발급 기관

RA : 실제 은행들

! 시험 - 공인 인증서 !

■ 공인 인증서

▪ 공인인증서의 구성

① 버전: 공인 인증서의 형식을 구분
(우리가 사용하는 대부분의 공인 인증서는 버전 3)

② 일련 번호: 공인 인증서를 발급한 인증 기관 내의 인증서 일련번호

③ 서명 알고리즘: 공인 인증서를 발급할 때 사용한 알고리즘

④ 발급자: 공인 인증서를 발급한 인증 기관의 DN, DN은
X.500 표준에 따라 명명된 이름으로 cn, ou, o, c 필드로 구성

⑤ 유효 기간: 공인 인증서를 사용할 수 있는 시작일과 만료일로
초 단위까지 표기

⑥ 주체: 공인 인증서 소유자의 DN

⑦ 공개 키: 공인 인증서의 모든 영역을 해시하여 인증 기관의
개인 키로 서명한 값

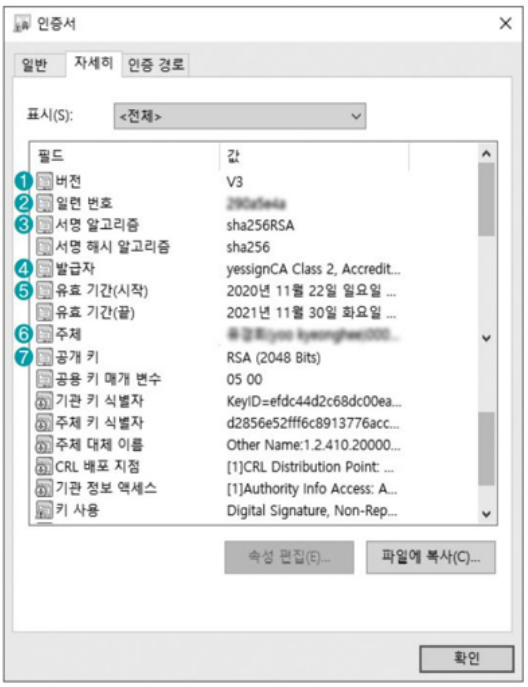

그림 8-8 공인 인증서 구성(ch09-09_new)

! 시험 - 전자서명 구현 원리 !

전자서명은 원본의 해시 값을 구한 뒤 부인 방지 기능을 부여하기 위해 공개 키 방법을 사용

복호화한 해시 값과 편지에서 구한 해시 값이 일치하면 위조 되지 않았다고 확신할 수 있음

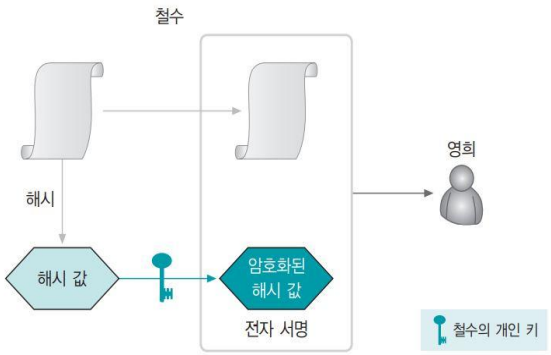

그림 8-11 전자 서명 생성

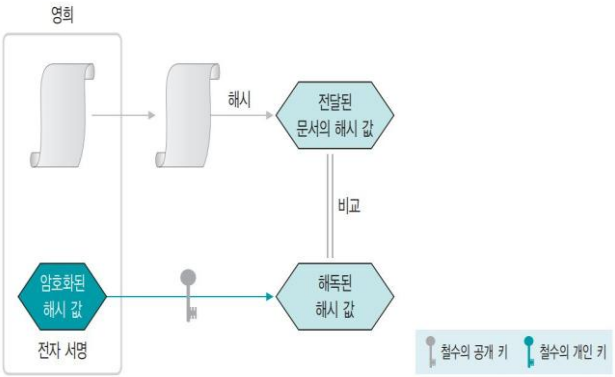

그림 8-12 전자 서명이 된 전송 문서 확인

! 시험 !

전자 서명이 제공하는 기능 (비밀키가 공개가 안되었을 때)

위조 불가

인증

재사용 불가

변경 불가

부인 방지

!! 시험 – 전자 봉투 암호화/복호화 과정 설명 !!

전자 봉투

전달하려는 메시지를 암호화하여 한 사람을 통해 보내고 암호화 키는 다른 사람이 가져가도록 암호학적으로 구현

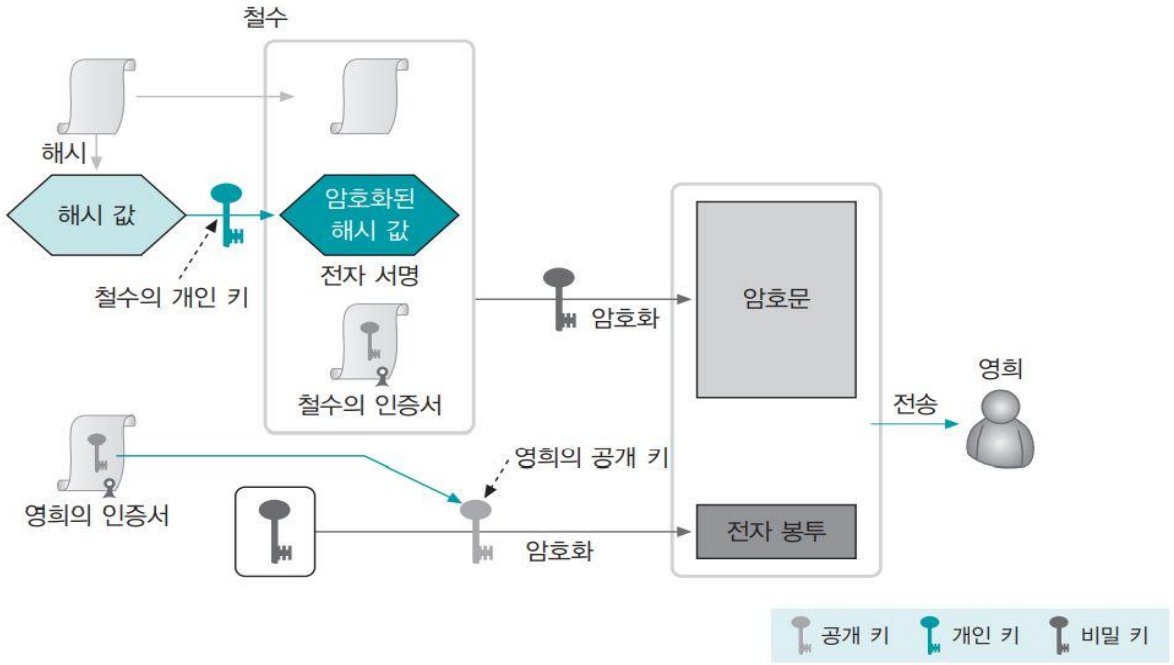

그림 8-13 전자 봉투를 이용한 암호 전송

- 철수는 전자 봉투를 사용하기 위해 먼저 전자 서명을 생성

- 전자 서명과 원문, 자신의 공개 키가 들어 있는 인증서를 비밀 키(DES 알고리즘 등에 사용되는 대칭 키)로 암호화

- 전자 서명 세트와 인증서, 암호화한 비밀 키가 영희의 공개 키로 암호화

- 최종적으로 철수는 비밀 키로 암호화한 결과와 비밀 키가 암호화된 전자 봉투를 영희에게 전송

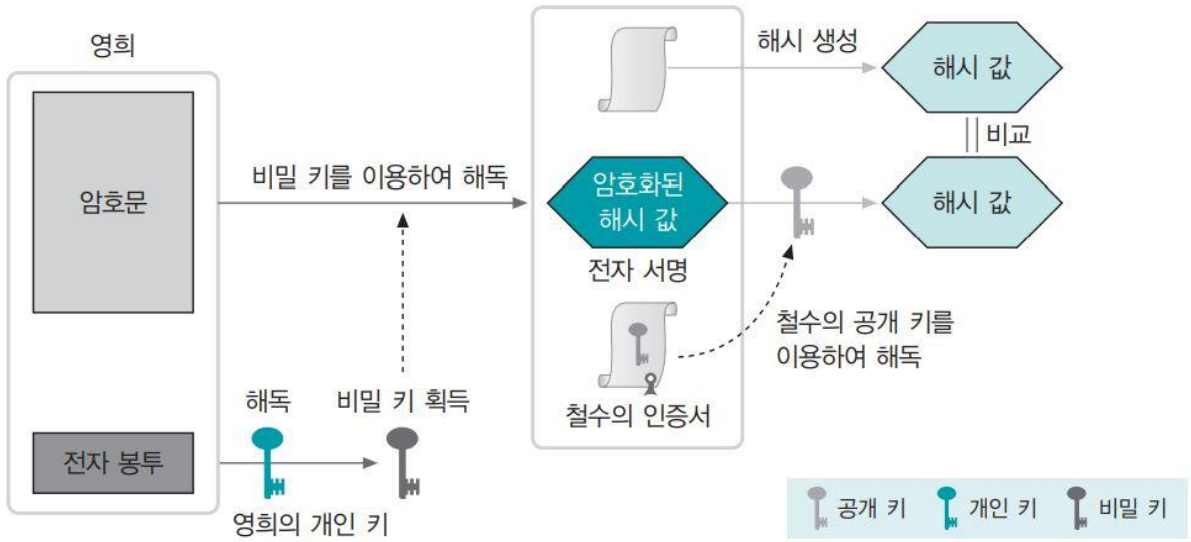

그림 8-14 전자 봉투의 복호화

- 전달받은 영희는 전자 봉투를 자신의 개인 키로 복호화하여 비밀 키를 획득

- 비밀 키를 이용하여 전자 서명과 편지, 철수의 인증서를 복호화(해독)

- 복호화한 인증서에서 철수의 공개 키를 얻어 전자 서명을 복호화하고 이를 편지의 해시 결과와 비교

! 시험 - 스마트카드 인증 !

정적 데이터 인증 (SDA)

개념 : 카드에 저장된 고정된 서명 데이터를 검증하는 방식

절차 : - 카드에 저장된 인증 데이터를 단말기가 읽음

- 단말기는 카드 발급기관의 공개키로 서명을 검증

특징 : - 서명 데이터가 고정되어 있어 복제 위험 존재

- 오프라인 환경에서도 사용 가능

- 구현이 간단하고 비용이 저렴

단점 : - 위조 카드에 취약 (서명 데이터 복사 가능)

- 보안 수준이 낮아 고위험 거래에는 부적합

동적 데이터 인증 (DDA)

개념 : 카드가 실시간으로 서명 데이터를 생성하여 검증하는 방식

절차 : - 단말기가 카드에 인증 요청

- 카드가 내부 개인키로 동적 서명 생성

- 단말기는 발급기관의 공개키로 서명 검증

특징 : - 서명 데이터가 매번 달라짐 -> 복제 불가능

- 카드에 암호 연산 기능 (MPU) 필요

- 보안성이 매우 높음

단점 : - SDA보다 구현 복잡, 비용 증가

- 일부 구형 단말기에는 지원되지 않음

! 시험 – 가상 화폐 (비트코인) !

블록체인: 보안

실물이 없는 비트코인은 입출금 내역인 장부로만 존재, 그 장부에 나타난 금액 합계가 잔액이 됨

거래 내역을 조작한다면 그것은 바로 장부를 조작하는 일

장부를 조작한다는 것은 변조된 블록을 생성하여 전파시키는 데 성공한다는 의미지만 현실적으로 불가능

! 시험 – 네트워크 암호화 !

4계층의 암호화 프로토콜

SSL : 40비트와 128비트 키를 가진 암호화 통신 가능

L2TP, IPSec보다 상위 수준에서 암호화 통신 기능을 제공하여 4계층(전송 계층)과 5계층(세션 계층) 사이의 프로토콜

SSL의 기능

클라이언트 인증: 클라이언트의 인증서를 확인하여 서버 에 접속할 자격이 있는지 확인하는 작업

암호화 세션: 암호화된 통신, 40비트와 128비트의 암호화 세션을 형성

서버 인증: 클라이언트가 자신이 신뢰할 만한 서버에 접속을 시도하고 있는지 확인하는 것

그림 8-37 OSI에서 SSL의 동작 위치