Part 3. 접근통제

Section 8. 접근통제 개요 (출제빈도 0.7%)

Section 9. ★ 사용자 인증 (출제빈도 4.8% / 매회 4-5문제 출제)

[1] 인증

(1) 메시지 인증

- 메시지의 무결성을 검증
- 메시지 암호화 방식, MAC, 해시 함수

> 💡 1) 메시지 암호화 방식
> Caes 1) 대칭키
> - 기밀성+부분적 인증(송수신 부인방지)
> Case 2) 비대칭키
> - 수신자의 공개키로 암호화 : 기밀성
> - 송신자의 개인키로 암호화 : 인증과 부인방지
>
> 2) 메시지 인증코드(MAC)
> - 메시지와 대칭키를 입력으로 만들어진 코드
> - 사전에 송신자와 수신자 간에 대칭키의 공유가 필요
>
> 3) 해시함수
> - 데이터를 정해진 크기의 Message Digest로 만드는 일방향 함수
> - MAC과 달리 대칭키를 사용하지 않으며, 결과값 자체는 기밀성이 없음

(2) 사용자 인증

- 사용자 인증
- 개인 식별 : 내부 직원이 외부인과 공모하여 고객의 돈을 인출하는 경우를 불가능하게 하는 법

[2] 사용자 인증 기법

(1) 지식 기반 인증 (What you Know)

[패스워드]

(1) 고정된 패스워드

- 크래킹 툴 : NTCrack, John the Ripper, Pwdump, Wfuzz, Cain and Abel, THC Hydra

(2) 일회용 패스워드(OTP)

(1) 질의응답 방식 = 시도응답 방식(Challenge-Response)

- 사용자가 ID를 서버 호스트에 보내면, 서버 호스트는 난수를 생성하여 클라이언트에게 보낸다.
- 단점 : 네트워크 모니터링에 의해 값 노출될 경우 취약, 서버와 클라 사이의 통신 횟수

(2) 시간과 이벤트 동기화 방식

- 시간 동기화 방식 : 클라이언트는 현재 시간을 입력값으로 OTP를 생성해 서버로 전송, 서버 역시 같은 방식으로 생성
- 이벤트 동기화 방식 : OTP 토큰과 OTP 인증서버의 동기화된 인증횟수(Counter) 기준으로 사용자가 인증 요청시마다 OTP 값 생성

(3) S/KEY 방식

- 벨 통신 연구소에서 개발, UNIX 운영체제 인증에서 사용, 해시 함수의 역연산을 하기 어렵다는 점에서 착안

[시도-응답 개인 식별 프로토콜] (Challenge Handshake Authentication)

[특징]

- 공개키 및 비밀키 암호 기반
- 패스워드 방식이 '도청이 용이하지 않은 환경'에서 안전하다면, 이 방식은 '**도청이 가능한 환경'에서 안전**한 방식
- 자신의 비밀 정보를 서버에게 제공
- 시도(challenge)로 사용하는 값 : 가변적인 난수, 순번, 시각표 등을 사용

[분류]

- 일방향 개인 식별 프로토콜
- 상호 개인 식별 프로토콜

[시도-응답 개인 식별 프로토콜] (zero-knowledge identification)

[특징]

- 시도-응답 개인 식별 프로토콜과 달리 **자신의 비밀 정보를 서버에게 제공하지 않고** 자신의 신분을 증명하는 방식

[분류]

- Flat-Shamir 프로토콜
  - 매우 큰 두 소수의 곱을 법으로 하는 어떤 수에 대한 제곱근 계산의 어려움에 기반
- Dchnorr 개인식별 프로토콜
  - 매우 큰 소수를 법으로 하는 이산대수 문제의 어려움에 기반

(2) 소유 기반 인증 (What you Have)

1. 메모리 카드(토큰)
2. 스마트 카드
3. 일회용 비밀번호(OTP)

(3) 개체(생물학적) 특성 기반 인증 (What you Are)

1. 생체인증(biometics)

[3] 통합 인증 체계

(1) 통합 인증 체계(SSO, Single Sign On)

1. 정의
2. 구성요소
3. 장단점

- 장점
  - 사용자 편의성 증가, 중앙 집중 관리를 통한 효율적 관리

4. 기타
   - EAM(Extranet Access Management)

     ✔️ 인트라넷, 엑스트라넷 및 일반 클라이언트/서버 환경에서 자원의 접근 인증과 이를 기반으로 자원에 대한 접근 권한을 부여, 관리하는 통합 인증 관리 솔루션

     ✔️ 하나의 ID와 암호 입력으로 다양한 시스템에 접근할 수 있도, 각 ID에 따라 **사용 권한 차등 부여** 가능

     ✔️ SSO 기술을 포함하며, 사용자 권한을 중앙에서 모니터링하고 제어하는 통합 인증 관리용 시스템

     ✔️ 로그인 세션의 보안기술 적용을 통해 Replay Attack 또는 네트워크상의 위변조를 방지해준다.

     ✔️ PKI와 연동하여 암호화 및 전자서명 지원이 가능하다.

(2) 커버로스(kerberos)

1. 개요
   - 1980년대 중반 MIT의 Athena 프로젝트 일환
   - 대칭키 암호기법에 바탕을 둔 티켓 기반 인증 프르토콜
   - 타임스탬프를 이용하여 위장을 통한 티켓 사용을 막음
   - 네트워크 상에서 클라,서버,KDC 세 통신주체 간에 인증 받은 사용자만이 적절한 통신을 할 수 있게 함
   - 사전에 알지 못하던 송신자와 수신자간의 대칭키를 교환하는데 적합하다. (X)

     → 해설) 네트워크상에서 Clinet, Server, KDC 세 통신주체 간에 인증 받은 사용자만이 적절한 통신을 할 수 있게 한다.
   - 기밀성, 가용성, 무결성과 같은 보안 서비스를 제공한다. (X)

     → 해설) 가용성과는 거리가 멀다
2. 구성도
3. 취약성
   - 장점

        - 데이터의 기밀성과 무결성 보장
        - 재생공격 예방
        - SSO
        - 대칭키를 이용해 도청으로부터 보호
    - 단점
        - 패스워드 사전공격(dictionary attack)에 약함
        - 비밀키, 세션키가 임시로 단말기에 저장되어 있어 침입자에 의해 탈취당할 수 있음
        - Timestamp 로 인해 시간동기화 프로토콜이 필요
        - KDC가 단일실패지점(SPoF)이 될 수 있음.
4. 버전4와 버전5의 차이점

(3) 세사미(SESAME, Secure European System for Application in a Multi-vendor Environment)

1. 개요
    - Kerberos의 기능을 확장하고 약점을 보완하기 위해 개발된 SSO 기술
    - 대칭 및 비대칭 암호화 기법을 사용
    - Kerberos는 주체를 객체에 인증하기 위해 '티켓'을 사용하는 반면, SESAME은 PAC(Privileged Attribute Certificate)를 사용

Section 10. 접근통제 보안 모델 (출제빈도 2.4%)

1. 접근 통제의 모델

[1] 강제적 접근통제(MAC, Mandatory Access Control)

- Rule based, Administratively directed
- 관리자만이 접근제어의 규칙 설정 및 변경 (중앙집중)
- 주체와 객체의 보안 레벨을 비교하여 접근 권한 부여 (군사용)

[2] 임의적 접근통제(DAC, Discretionary Access Control)

- Identity, User directed,
- 주체 신분에 따라 접근권한 부여 (분산형)
- ACL을 사용해서 구현하는 것이 일반적

  [분류]

  - 접근제어 행렬(matrix) : 주체를 행, 객체를 열로 구성
  - 접근제어 목록(ACL) : 객체의 관점에서 주체에 권한을 부여
  - 자격목록(Capability List = Capability Tickets = Capability Table) : 주체의 관점에서 객체에 권한 부여

  [문제]

  - 한 주체 당 객체 목록과 허용되는 접근모드를 리스트로 관리하는 것을 ACL이라고 한다.

    → (X) `한 주체` 당 객체 목록은 `CL`이다.

[3] 역할기반 접근통제(RBAC, Role Based Access Control)

- 주체와 객체 사이에 역할을 두어 역할에 따라 접근 통제 (non-DAC)
- 특권의 최소화
- 직무의 분리
- 데이터 추상화
- 사용자에게 지나친 권한이 부여될 우려가 다. (X)

[4] 벨라파듈라 모델(BLP, Bell-Lapadula Confidentiality Model)

- 기밀성을 강조한 MAC 모델
- 낮은 보안 레벨의 권한을 가진 이가 높은 보안 레벨의 문서를 읽고 쓸수 없지만, 낮은 레벨의 문서는 읽고 쓸 수 있다.

[5] 비바 무결성 모델(Biba Integrity Mdoel)

- 무결성 레벨에 따라서 정보에 대한 접근을 제어하는 모델

2. 접근통제 기술과 기술론

[1] 제한된 사용자 인터페이스

[2] 임의적 접근 통제 (DAC)

1. 접근제어 행렬(access control matrix)
2. 자격 목록(Capability List, TIckets, Table)
    - 한 주체 당 객체 목록과 허용되는 접근모드를 리스트로 관리
3. 접근제어 목록(ACL, Access Control Lists)

3. 보안 모델

[1] 벨라파듈라 모델(BLP, Bell-LaPadula Confidentiality Model)

[2] 비바 무결성 모델(Biba Integrity Mdoel)

- 데이터 무결성에 초점을 둔 상업용 접근 통제 보안 모델

[3] 클락-윌슨 무결성 모델(Clark-Wilson Integrity Model)

[4] 기타 접근통제 보안 모델

1. 정보흐름 모델
2. 상태 기계 모델
3. 만리장성 모델

Section 11. 접근통제 보안위협 및 대응책 (출제빈도 0.3%)

1. 접근통제 보안위협 및 대응책

[1] 패스워드 크래커

1. 사전 공격(Dictionary Attack)
2. 무차별 공격(Brtue-force Attack)
    - 모든 조합의 경우의 수를 시도
    - EX : 워다이얼링(wardialing), John the Ripper, Wfuzz, Cain and Abel, THC Hydra

3. 레인보우 테이블 공격

[2] 사회공학(Social Engineering)

[3] 피싱, 파밍, 스미싱

[4] 은닉채널(Covert Channel)

[5] 방사(Emanation)