2장. 사용자 인증
Athentication

박종혁
서울과학기술대학교 컴퓨터공학과
jhpark1@seoultech.ac.kr

목차

인증기술 영상

- 생체 인증의 진화…지문·홍채 대신 뼈·근육으로 식별 / KBS뉴스(News)
  https://youtu.be/1GjxqcNqJdI

- 분산신원확인(DID), 블록체인 대중화 이끈다 / 머니투데이방송
https://www.youtube.com/watch?v=SToydEXdRBo

- 얼굴이 신분증? LG CNS AI 안면인식(얼굴인식) 출입 서비스
https://www.youtube.com/watch?v=NTRqD-XMPgQ

- 금융권 디지털 전환 가속화…클라우드 보안 & 인증 기술 '주목' / 서울 현대 HCN
  https://youtu.be/CYBJmmkVdhg

1. 사용자 인증 개요

사용자인증정의

사용자 인증 정의

- 시스템에 접근하는 자격에 대해 신원을 확인하는 절차

  - RFC 2828

$ authentication
(I) The process of verifying an identity claimed by or for a system entity. (See: authenticate, authentication exchange, authentication information, credential, data origin authentication, peer entity authentication.)

(C) An authentication process consists of two steps:

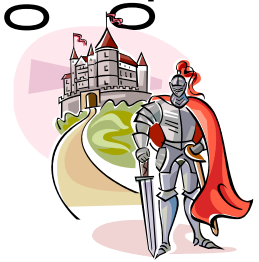
1. Identification step: Presenting an identifier to the security system. (Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service.)

2. Verification step: Presenting or generating authentication information that corroborates the binding between the entity and the identifier. (See: verification.)

(C) See: ("relationship between data integrity service and authentication services" under) data integrity service.

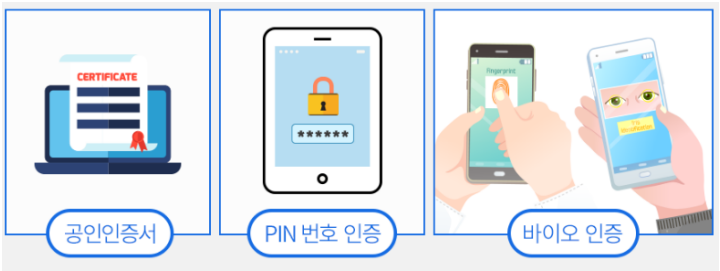
인증절차

- 인증은 정보보안의 근본적인 요소이며 주된 핵심
- 접근 제어 및 사용자 책임 기반
- 신원 확인 단계
  - 식별자가 보안 시스템에 자신의 신분을 제시
- 입증 단계
  - 개체와 식별자간의 유대를 증명하는 인증 정보를 제시 혹은 생성



사용자 인증의 4가지 수단

수 단	기 술
알고 있는 것을 통한 인증 (Something you know)	비밀번호, PIN, 질문에 대한 응답
소유물을 통한 인증 (Something you have)	토큰, 스마트 카드, 전자 키 카드, OTP, SMS
생체 조직을 통한 인증 (Something you are)	지문 ,망막, 홍채, 얼굴, 정맥
행동을 통한 인증 (Something you do)	목소리 패턴, 필적, 타이핑 리듬, 서명, 걸음걸이



전자 사용자 인증 원리

- 사용자 인증 정의
  - 전자 인증 (Electronic Authentication, EA): 전자 사용자 인증을 정보 시스템에 전자적으로 제시된 사용자 식별자들에 대한 신뢰성 수립 과정 (Electronic Authentication Guideline, NIST SP 800-63-2)

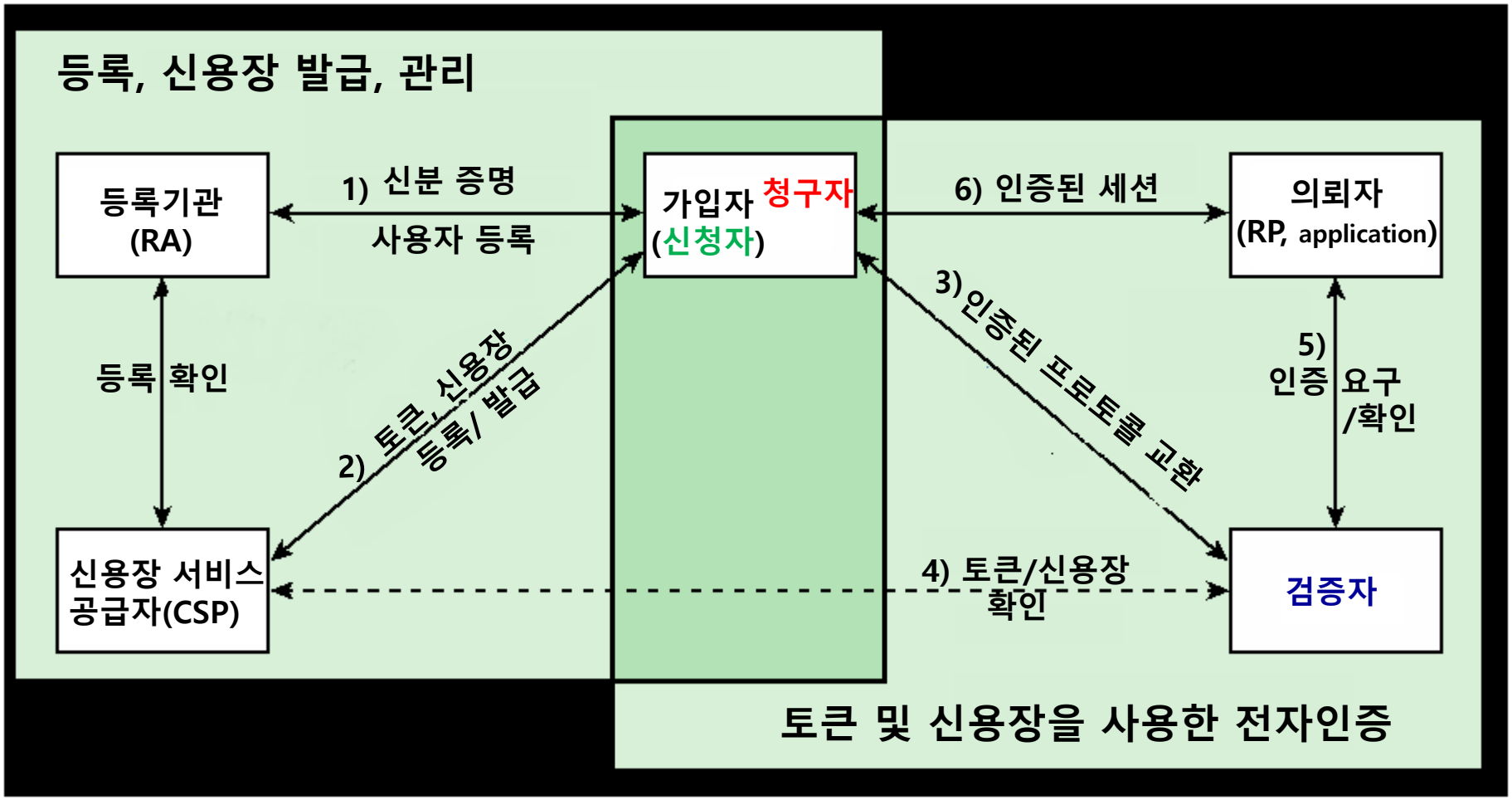
    . 2013년 공표, 2017.6 취소됨

    → NIST SP 800-63-3 Special Publication : Digital Identity Guidelines 공표, 2017. 6
  - 시스템은 인증된 개인이 데이터베이스 트랜젝션이나 시스템 자원에 대한 접근 같은 특정 기능 수행에 대한 권한을 결정하는데 인증된 식별자를 사용
  - 전자인증(EA)은 디지털 인증 (Digital Authentication)로 용어 변경 사용됨, NIST SP 800-63-3 Special Publication

> **The process of establishing confidence in user identities presented digitally to a system. In previous editions of SP 800-63, this was referred to as Electronic Authentication.**
> **- Digital Identity Guidelines, NIST Special Publication 800-63-3**

사용자 인증의 일반적 모델

NIST SP 800-63-2



인증모델 절차 설명

❖ 신청자는 등록기관의 신용장 서비스 제공자에게 가입을 신청

- 등록기관 (Registration Authority, RA) : 신용장 서비스 제공자에게 신청자의 신원을 보증하는 신뢰할 수 있는 존재
- 신용장 (Credential Service): 식별자(Identifier)와 가입자(Subscriber)가 소유한 토큰의 속성에 부여된 자료 구조이며, 인증 트랜잭션 내의 검증자가 검증

  *토큰: 암호키 혹은 가입자를 식별할 수 있는 암호화된 비밀번호

- 신용장 서비스를 위해 제공자는 가입자와 정보를 교환
- 전체 인증 시스템의 세부사항에 따라 신용장 서비스 제공자는 여러 전자 신용장을 가입자에게 발급
- 사용자가 가입자로 등록되면 실제 인증 과정이 가입자와 단수 혹은 복수의 시스템 사이에서 발생

❖ 청구자와 검증자

- 청구자(Claimant): 인증을 받고자 하는 자
  - 인증 프로토콜을 통해 검증자에게 성공적으로 토큰의 제어와 소유를 제시
- 검증자 (Verifier) : 식별을 인증하는 쪽
  - 청구자가 신용장의 가입자임을 검증
  - 검증자는 가입자의 신원에 대한 확인증을 의뢰자에 전달

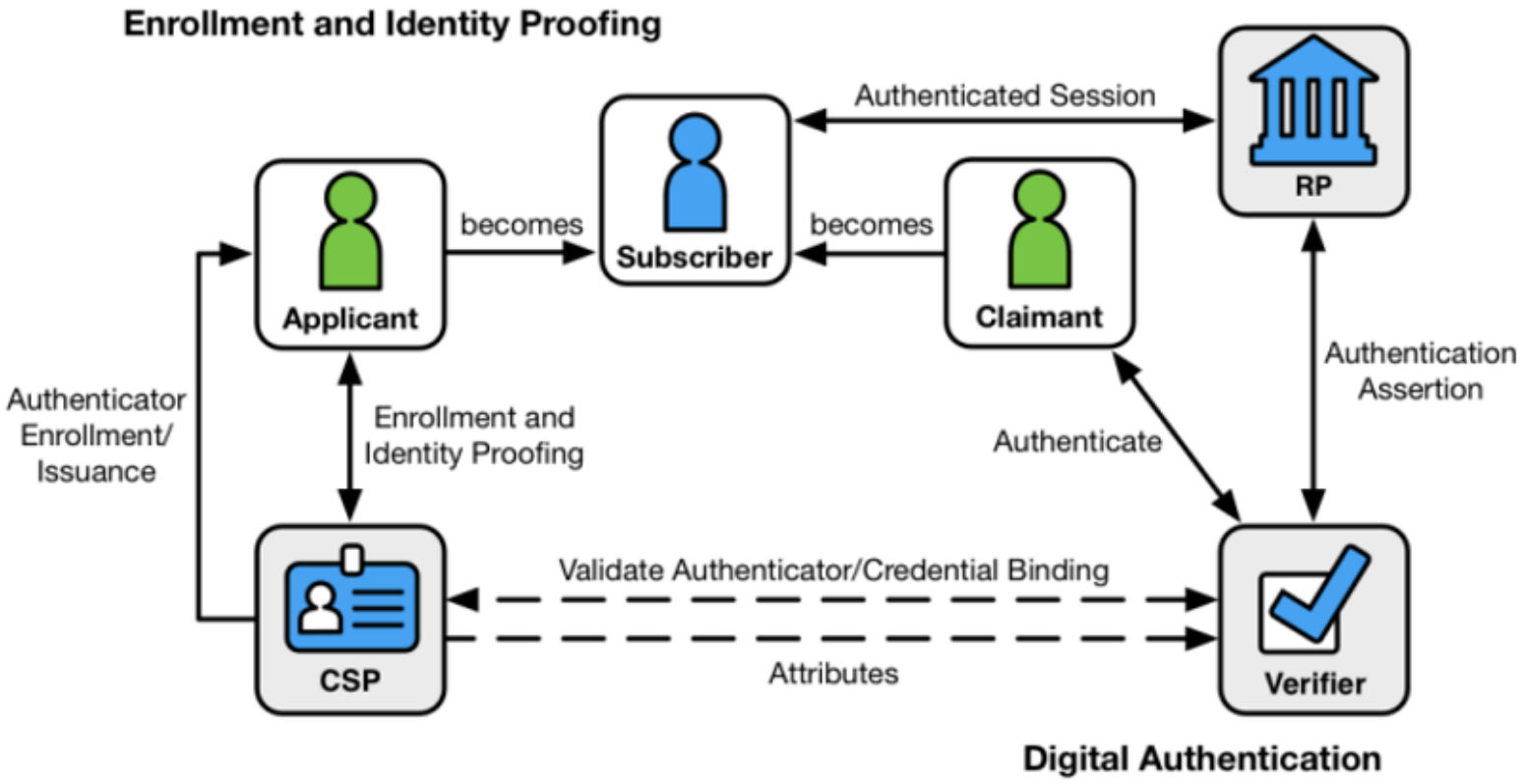
  *확인증 : 가입자 이름, 등록 시 부여된 식별자, 혹은 등록 시 검증된 가입자 속성 같은 가입자 식별 정보 등 포함

❖ 의뢰자 (RP)

- 검증자가 제공하는 인증된 정보를 접근 제어나 인증결정에 사용할 수 있음
- 신뢰기관, 식별자 등이 고려될 수 있음

- **Digital Identity Guidelines – Digital Identity Model**

- NIST Special Publication 800-63-3



2. 비밀번호 기반 인증

비밀번호 기반 인증

- 일반적으로 널리 알려진 침입자 방지 수단
  - 비슷한 서비스들이 사용자에게 이름이나 식별자(ID)뿐만 아니라 비밀번호를 요구
  - 시스템은 시스템 안에 저장된 비밀번호 파일의 사용자 ID와 대응되는 비밀번호를 입력된 비밀번호와 비교

- 비밀번호 기반의 인증 시스템은 사용자 ID로 표시되는 비밀번호 파일을 가짐
  - ID는 다음과 같은 방식으로 보안을 제공
    - ID는 사용자가 시스템에 접근이 허가되었는지 결정
    - ID는 사용자 권한을 결정함
    - ID는 임의 접근 제어(discretionary access control)로서 사용
      예) ID 목록에 있는 일반 사용자가 관리자 소유의 파일을 읽을 수 있는 권한을 부여 받은 경우

- 사용자의 비밀번호 대신 일방향 해시 함수를 사용하여 비밀번호의 해시값을 저장

비밀번호 취약점

- 오프라인 사전 공격
- 단일 사용자에 대한 암호 추측
- 단말기 강탈 하이재킹 공격
- 컴퓨터 감시 (모니터링)
- 특정 계정 공격
- 공공/알려진 암호 공격
- 사용자 실수를 이용한 공격
- 다중 비밀번호 사용을 악용

비밀번호 공격기법 및 대응방안

- 오프라인 사전 공격
  - 접근 제어가 시스템의 비밀번호 파일을 보호하는데 사용
  - 공격자 - 시스템 비밀번호 파일을 얻어 흔히 사용되는 비밀번호의 해시 함수값과 비교함
    같은 값이 발견되면, 공격자는 ID/비밀번호 값을 얻을 수 있음
  - **대응책**
    .비밀번호 파일에 대한 허가되지 않은 접근 방지
    .타협 방지를 위한 침입 탐지
    .노출된 비밀번호에 대한 빠른 재발급

- 특정 계정 공격
  - 공격자 - 특정 계정을 목표로 일치하는 비밀번호가 발견될 때까지 비밀번호를 추측하여 입력
  - **대응책:** 계정 폐쇄 방법 (일정 시도 횟수를 실패하면 자동 폐쇄)

- 잘 알려진 비밀번호 공격
  - 여러 사용자의 ID에 대해 잘 알려진 비밀번호를 사용해보는 것
  - 사용자는 비밀번호를 쉽게 기억하는 것으로 설정하는 경향 → 공격자도 비밀번호를 쉽게 추측 가능
  - **대응책**: 사용자가 흔한 비밀번호를 선택을 못 하도록 방지하는 정책
    인증 요청을 하는 IP 주소와 사용자 쿠키에 대한 스캐닝을 함

- 단말기 강탈
  - 공격자 - 단말기에 접속한 사람이 자리를 비울 때까지 기다림
  - **대응책**: 자동적으로 단말기에 접속하여 일정 시간 작동이 없다면 로그아웃하는 방법
    침입탐지 기법으로 사용자의 행동 변화 탐지

- 단일 사용자에 대한 비밀번호 추측
  - 공격자 - 계정 소유자에 대한 정보와 시스템 비밀번호 정책을 알아내어 비밀번호 추측
  - **대응책**: 비밀번호는 추측하기 어렵게 만드는 비밀번호 정책 및 훈련의 강화 필요
    ➔ 기밀성, 비밀번호 최소 길이, 문자 집합, 잘 알려진 사용자 식별자 사용금지, 비밀번호 사용기간 단축

- 사용자 실수 이용
  - 사용자가 기억을 위해서 비밀번호를 적어 놓았을 경우,
    ➔ 공격자들 - 사회 공학 전술 등을 사용하여 사용자 혹은 관리자에게 성공적으로 비밀번호 획득 가능
  - **대응책**: 사용자 훈련, 침입 탐지, 다른 인증 방법과 결합된 간단한 비밀번호 사용

- 다중 비밀번호 사용
  - 여러 네트워크 장치가 한 사용자에 대해 같은 비밀번호 혹은 비슷한 비밀번호를 사용
    → 공격자 - 좀 더 효율적인 방법으로 피해를 줄 수 있음
  - **대응책**: 각각의 네트워크 장치에서 같거나 혹은 비슷한 비밀번호 사용을 제한하는 정책 사용

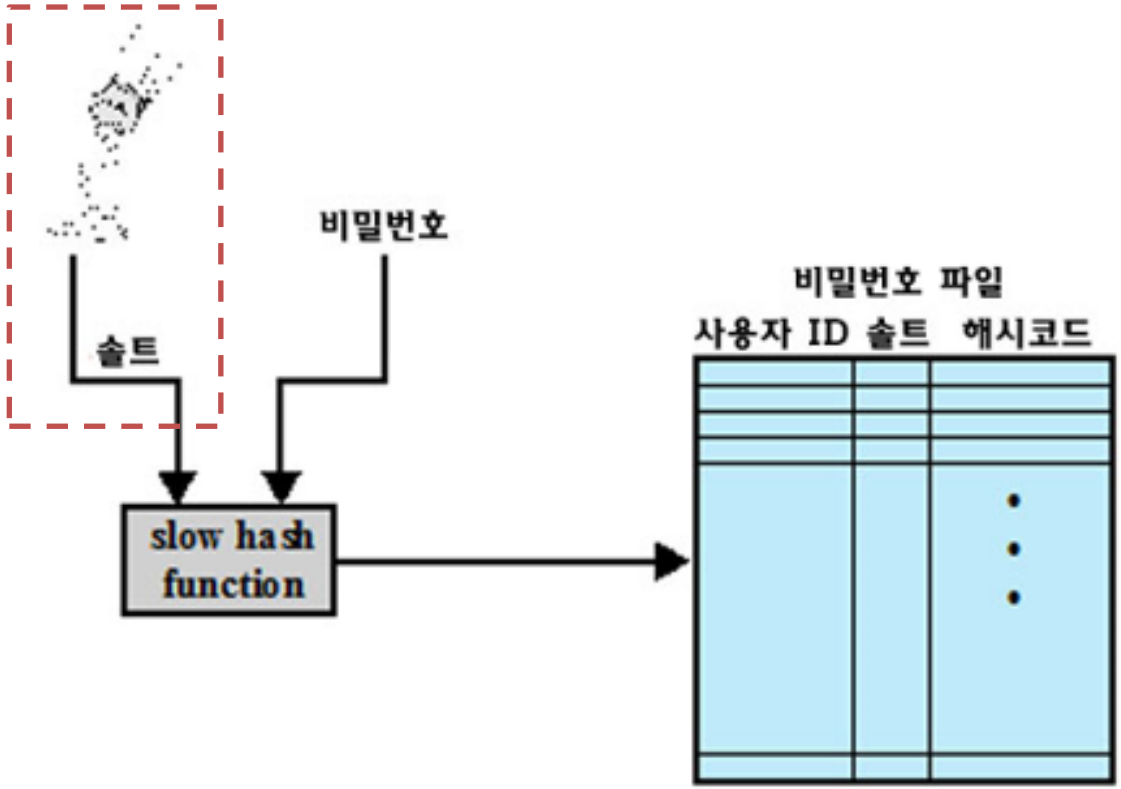
- 컴퓨터 모니터링
  - 비밀번호가 네트워크 상에서 원격으로 교환된다면 도청에 취약
  - 간단한 비밀번호 암호화는 도청 및 재사용 때문에 문제 해결책이 될 수 없음
  - **대응책**: 보다 강력한 비밀번호 암호화를 사용

해시 비밀번호의 사용

- UNIX 및 많은 운영체제에서 가장 널리 사용되는 비밀번호 기술
- 해시(Hash) 비밀번호와 솔트(salt) 값 사용
- 절차
  1. 사용자는 비밀번호를 선택하거나 부여 받음
  2. 비밀번호는 고정된 길이의 솔트값과 함께 조합
  3. 비밀번호와 솔트가 해시 알고리즘의 입력으로 제공되어 고정된 길이의 해시 값을 생성
  4. 해시된 비밀번호는 솔트값과 같이 사용자 ID에 상응하는 비밀번호 파일에 저장
  5. 사용자가 UNIX 시스템에 접근을 시도할 때, 사용자는 ID와 비밀번호를 제공
  6. 운영체제는 제공된 ID를 비밀번호 파일의 색인으로 사용, 솔트와 비밀번호를 추출
  7. 솔트와 사용자가 제공한 비밀번호는 암호화 과정의 입력으로 사용
  8. 저장된 값과 일치하면 비밀번호 허용

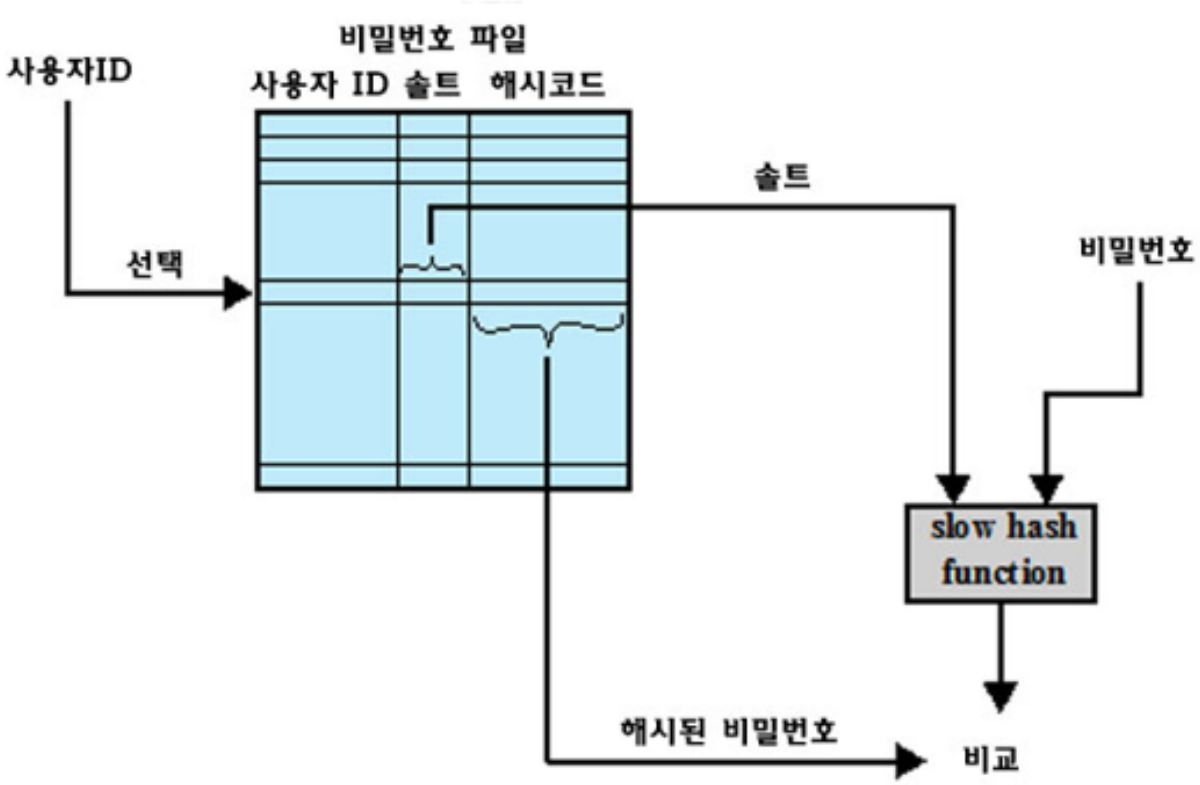
UNIX 비밀번호 방식

- 새로운 비밀 번호 적재



UNIX 비밀번호 방식

- 비밀 번호 검증



- 솔트 사용의 목적

1. 비밀번호 파일에서 중복되는 비밀번호를 방지

   - 만약 두 명의 사용자가 같은 비밀번호를 선택하더라도, 비밀번호들은 서로 다른 솔트 값을 할당 받으므로 두 명의 사용자의 해시된 비밀번호는 서로 다름

2. 오프라인 사전 공격을 획기적으로 어렵게 만듦

   - 길이가 b비트인 솔트에 대해서 가능한 비밀번호의 수는 2^b가 되며, 사전 공격에서 비밀번호 추측의 어려움이 증가

3. 둘 혹은 그 이상의 시스템에서 한 사람에 의해 사용되는 같은 비밀번호를 발견하기는 거의 불가능

사용자 선택 비밀번호 크래킹

- 전통적 접근
  - 사전 공격
    - 가능한 비밀번호를 포함한 사전을 만들고 비밀번호 파일에 모두 시도
    - 각 비밀번호를 가능한 솔트 값들로 해시해서 저장된 해시 값과 비교하는 것
    - 찾아내지 못하면, 크래킹 프로그램은 사전 내의 모든 단어의 변형들에 대해서 시도함
    - 변형 - 역방향 철자, 숫자의 추가 또는 특수 기호, 문자의 순서성 등
  - rainbow table 공격
    - 미리 해시 값을 계산하여 저장해놓는 방법
    - 공격자가 가능한 한 많은 비밀번호를 가진 사전을 생성
    - 공격자는 각 비밀번호를 각각의 솔트 값과 관련해서 해시 값을 생성
    - 그 결과가 "rainbow table"이라 알려진 매머드급 해시테이블
  - 비밀번호 크래커
    - 사람들이 추측하기 용이한 비밀번호를 선택한다는 점을 이용
    - 어떤 사용자들은 비밀번호를 고를 때 아주 짧은 것을 선택
    - 간단한 해결책

      .시스템이 6자리 이하의 비밀번호를 거부

      .모든 비밀번호를 8자리로 고정
  - John the Ripper
    - 사전의 전체 단어를 시도해보는 공격에 많이 쓰임
    - 1996년 처음 개발된 오픈 소스 비밀번호 크래커

- 현대적 접근

  - 비밀번호 크래킹 기법의 발전

    ▪두가지 방향으로 향상

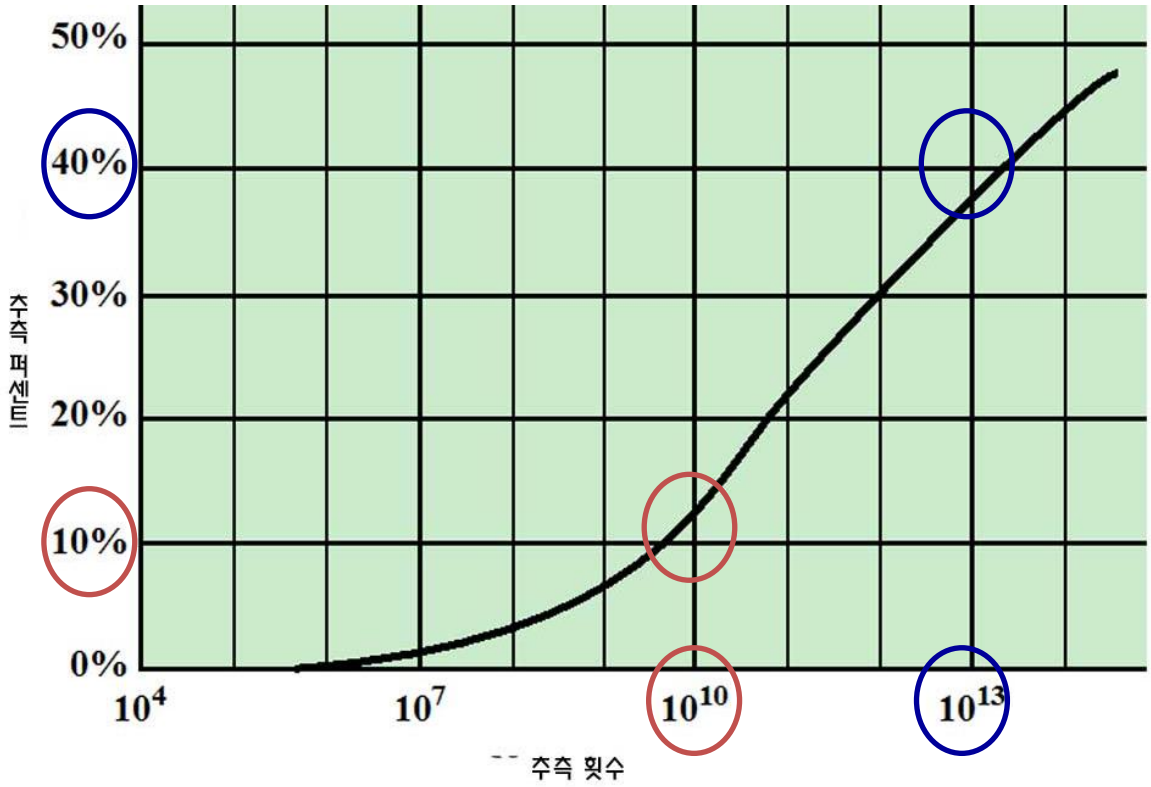
    1.비밀번호 크래킹 처리 속도가 놀랍게 향상되었음

    Ex) AMD Radeon HD7970 GPU는 평균 초당 8.2x109개 비밀번호를 시도할 수 있음

    2. 비밀번호 크래킹 기법은 잠재적 비밀번호 생성의 정교한 알고리즘을 사용

    ▪ [MAZU13]은 복잡한 비밀번호 정책을 시행하는 대학교의 학생 2,500명의 비밀번호를 분석

    - RockYou 등에서 유출된 실제 비밀번호 파일들을 데이터베이스로 구축
    - 그래프는 비밀번호당 추측 횟수에 따른 백분율을 나타냄
    - 10% 이상의 비밀번호는 1010번 추측으로 알아낼 수 있었음
    - 1013번 추측으로는 40% 이상의 비밀번호를 알아냈음



추측 횟수에 따른 비밀번호 획득 확률

비밀번호 파일 접근 제어

- 비밀번호 공격을 막기 위해 공격자의 비밀번호 파일에 대한 접근 거부
  - 특별한 권한 소유자만 파일의 해시된 비밀번호 접근이 가능
    - 공격자가 사용자의 비밀번호를 알지 못한다면 비밀번호 파일을 읽을 수 없음
  - 해시된 비밀번호는 사용자 ID와 격리되어 "Shadow password file" 역할
- 비밀번호 보호 정책
  - 기술을 바탕으로 한 완벽한 접근 제어 수단과 예측하기 어려운 사용자의 비밀번호 선택을 병행해야 함

- 비밀번호 파일의 취약점은 여전히 존재
  - 대부분의 UNIX 시스템을 포함한 많은 시스템들은 예상치 못한 시스템 정지에 취약
  - 해커
    - 운영체제의 이러한 소프트웨어 취약점을 이용해 접근 제어 시스템을 우회하여 비밀번호 파일을 추출 가능
    - 파일 시스템 또는 데이터베이스 관리 시스템의 취약점을 찾아 파일에 접근 가능
  - 보안 사고는 우발적으로 비밀번호 파일을 읽을 수 있도록 할 수 있으며, 모든 계정의 손상이 발생할 수 있음
  - 몇몇 사용자들은 다른 기억보호 정의 영역에 다른 기기에 대한 계정을 가지고 있으며, 동일한 비밀번호를 사용
  - 물리적 보안의 취약점은 해커에게 기회를 제공할 수 있음
  - 때때로 비밀번호를 여분의 디스크 또는 기록용 디스크에 위급 상황에 대비해 백업함
  - 이러한 백업을 공격자가 접근하여 비밀번호 파일을 읽을 수 있음
  - 사용자가 리눅스 같은 다른 OS로 부팅하여 비밀번호 파일에 접근할 수 있음
  - 시스템 비밀번호 파일 대신 네트워크 트래픽 스니핑 같은 다른 접근 방식으로 사용자의 ID와 비밀번호를 수집할 수 있음

비밀번호 선택 전략

- 사용자들이 무작위로 선택된 8개의 문자로 구성된 비밀번호를 부여 받는다면 비밀번호 크래킹은 매우 어려움
  - 대부분의 사용자들은 비밀번호를 기억하지 못함

- 목표: 사용자가 기억하기 쉬운 비밀번호를 선택하되 추측하기 쉬운 비밀번호 제거

- 기본적인 네 가지 기술
  - 사용자 교육
  - 컴퓨터에 의한 비밀번호 생성
  - 반응적 비밀번호 확인
  - 복잡한 비밀번호 정책

- 반응적 비밀번호 확인 전략
  - 시스템이 정기적으로 시스템 내부의 비밀번호 크래커를 작동시켜 추측 가능한 비밀번호를 시스템 자체적으로 발견
  - 시스템은 비밀번호가 추측 가능한 것이라면 사용자에게 이를 알리고 재설정 요구
  - 문제점
    1. 자원 소비가 큼
       - 비밀번호파일을 훔칠 수 있는 공격자는 이러한 작업을 위해서 몇 시간 또는 심지어 며칠 동안 최대 CPU 시간을 투자할 수 있기 때문
    2. 비밀번호 반응 확인 시스템이 문제점을 발견하기 전까지 취약점이 계속 존재

- 사전적 비밀번호 정책
  - 비밀번호 보안을 향상하기 위한 가장 좋은 접근 방법
  - 사용자가 자신의 비밀번호를 선택할 때 시스템 허락을 받도록 하는 방식
  - 사용자에게 충분한 안내와 추측에 의한 사전 공격 가능성이 없는 비밀번호 중에서 사용자가 기억할 수 있는 비밀번호를 선택 유도

사전적 비밀번호 정책

비밀번호 크래커
사용하지 않는 사전기반으로 암호를 재확인

규칙 적용
- 암호가 준수해야 하는 특정 규칙

Bloom filter
- 해시를 사용한 사전 기반으로 테이블을 작성
- 테이블에 대해 원하는 비밀번호 확인

3. 토큰 기반 인증

토큰 기반 인증

- 토큰: 사용자 인증 목적을 위해 사용자가 소유한 객체
- 토큰으로 사용되는 카드 유형

카드 유형	특징	예
금형 도안	앞면 표지	구형 신용카드
전자기 띠	뒷면 전자기 띠, 앞면 문자	은행 카드
메모리	메모리 내장	선불 전화카드
스마트 접촉형 비접촉형	내부 메모리와 프로세서 표면의 전기적 접촉 내장된 라디오 안테나	생체 ID 카드

메모리 카드

- 데이터 저장 기능 (처리는 못 함)
  예) 뒷면에 전자기 띠(마그네틱 라인)를 가진 은행 카드
  전자기 띠는 판독기가 읽을 수 있는 간단한 보안 코드만 저장

- 개인 식별 번호 (PIN) 또는 비밀번호와 결합하여 강력한 보안성을 제공

- 잠재적 약점
  - 특수 판독기 필요: 토큰 사용 비용과 판독기의 하드웨어 및 소프트웨어의 보안성 관리가 유지되어야 하는 필요성이 발생
  - 토큰 손실: 토큰을 잃어버린 경우 일시적으로 사용자의 시스템 접근이 제한
  - 토큰이 위조되거나 도용된다면, 공격자는 PIN만 알아내면 접근이 가능
  - 사용자 불만: 사용자가 ATM 사용을 위한 메모리 카드 사용에 어려움이 없더라도, 컴퓨터 접근을 위한 메모리 카드의 사용은 불편한 것으로 간주됨

스마트 카드

- **프로세서, 메모리, 입출력 포트를 포함한 전체 마이크로프로세서를 포함**
- **스마트 카드**
  1. 물리적 특징
     - 내장 마이크로 소프트웨어를 포함하고 있는 스마트 토큰, 은행 카드와 비슷한 스마트 토큰은 스마트카드라 불림
  2. 사용자 인터페이스
     - 사용자와 토큰 간의 인터페이스는 키패드와 화면이 포함됨
  3. 전자적 인터페이스
     - 스마트카드나 다른 토큰들은 호환되는 판독기/기록기와 통신을 위해서 전자적 인터페이스를 요구
     - 인터페이스 유형

     1. 접촉형
        - 표면을 스마트카드 판독기에 직접 접촉해야 함
        - 명령어, 데이터, 카드 상태 정보 등은 물리적 접촉면에서 발생

     2. 비접촉형
        - 스마트카드 판독기에 가까이 대기만 하면 됨
        - 판독기와 카드는 안테나를 가지고 있으며 라디오 주파수를 통해 교신
        - 대부분의 비접촉형 카드는 전자기적 신호에서 내부 칩을 위한 전원도 전달

- **스마트 토큰을 이용한 인증 프로토콜**

1. 정적
   - 사용자 - 자신을 토큰에 인증, 토큰 - 사용자를 컴퓨터에 인증

2. 동적 비밀번호 생성기
   - 토큰 - 고유의 비밀번호를 주기적으로 생성
   - 생성된 비밀번호 - 수동으로 사용자에 의해서 또는 토큰을 통해 인증을 위해 컴퓨터 시스템에 입력
   - 토큰과 컴퓨터 시스템- 초기화 및 동기화가 되어 컴퓨터가 현재 토큰의 비밀번호를 알고 있어야 함

3. 시도 응답
   - 컴퓨터 시스템은 랜덤 숫자들로 이루어진 문장 생성
   - 스마트 토큰 - 컴퓨터 시스템이 생성한 문장에 대한 응답을 생성

- **스마트 카드의 세 가지 메모리 타입**

1. 읽기 전용 메모리(ROM)
   - 카드 번호와 카드 주인의 이름 정보 등이 사용 기간 동안 변하지 않고 저장 유지됨

2. 전기적으로 삭제가 가능하고 프로그래밍이 가능한 ROM(EEPROM)
   - 프로토콜 같은 응용프로그램 데이터 및 프로그램만 저장함
   - 매 시간 변화하는 데이터를 저장하기도 함

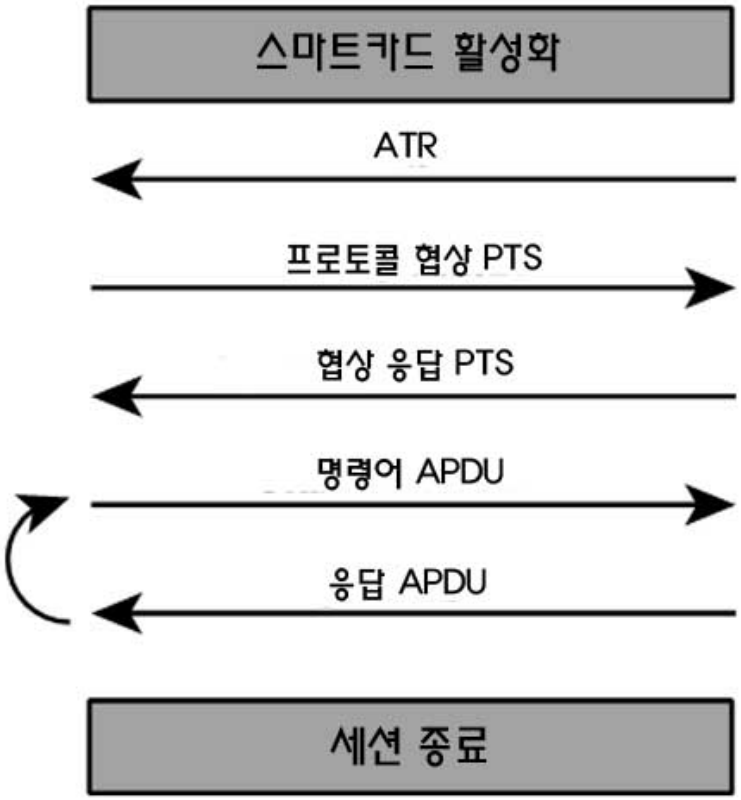
   Ex) 전화카드 안의 EEPROM은 통화 시간을 저장 및 유지함

3. RAM
   - 응용프로그램이 실행되는 동안 일시적인 데이터를 저장함

스마트 카드/판독기 동작

스마트카드

스마트 단말기



APDU = Application protocal data unit

ATR = Answer to reset

PTS = Protocal type selection

전자식별카드

- 전자식별 카드
  - 국가 전자식별 카드(eID)는 운전면허증 같은 다른 국가 ID 카드처럼 정부나 상업적 용도로 사용될 수 있음
  - eID 카드는 다양한 프로그램에서 보다 강력한 신원 증명을 제공함
  - 최근에 개발되어 사용되는 독일의 neuerPersonalausweis: 표면에 인간이 판독할 수 있는 다음 데이터를 포함
    1. 개인 데이터
       - 이름, 생년월일, 주소: 여권과 운전면허증과 같은 형태
    2. 문서 번호
       - 9자리의 고유 카드 식별 문자열
    3. 카드 접근 번호(CAN)
       - 6자리의 숫자가 표면에 인쇄됨
       - 비밀번호로 사용됨
    4. 기계 판독 영역(MRZ)
       - 3줄의 인간과 기계가 판독할 수 있는 텍스트
       - 비밀번호로 사용 가능

전자 ID [eID]

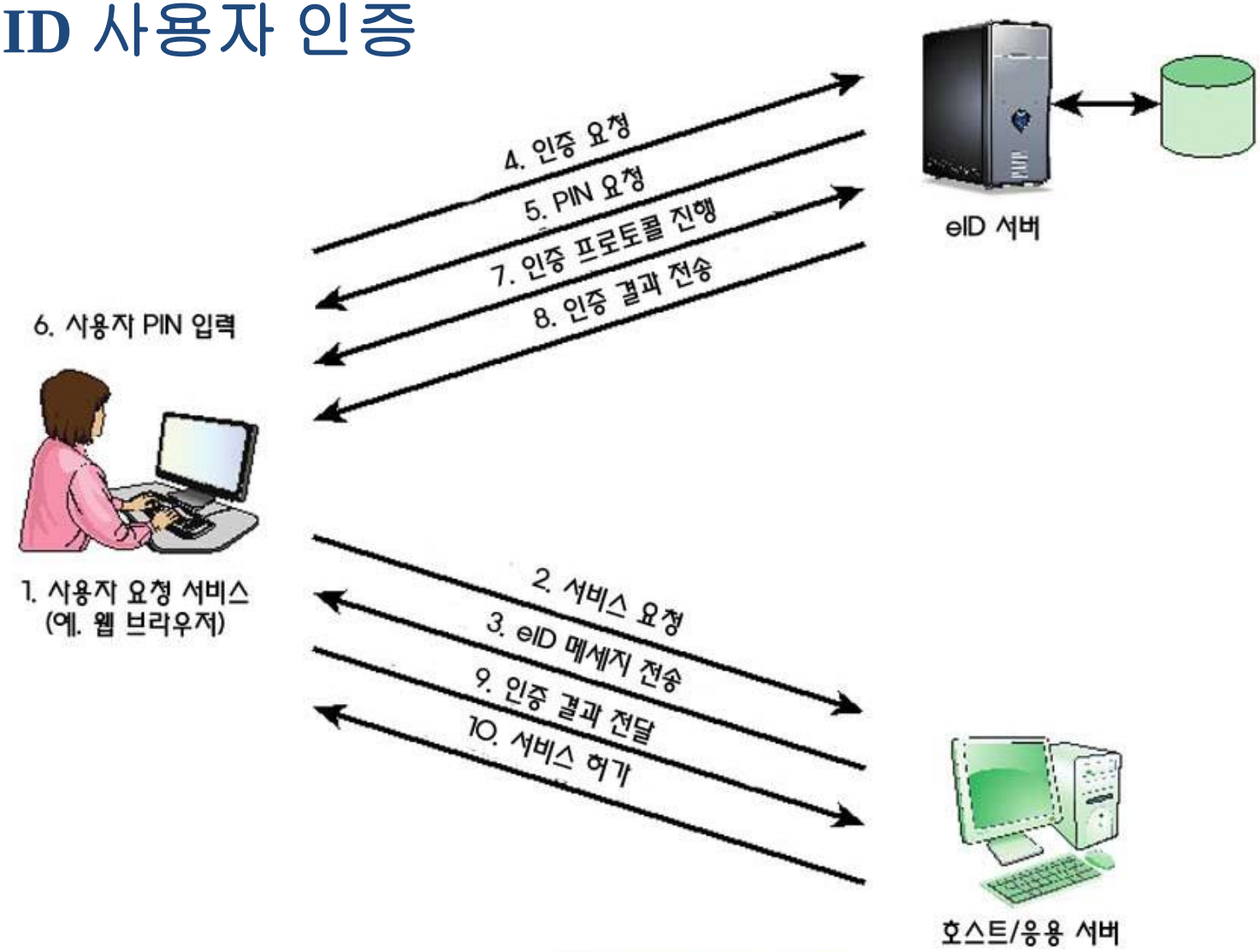
- eID 기능
  1. ePass
     - 정부의 사용을 위한 기능, 카드 소유자의 신원을 나타내는 계수를 저장
     - 다른 서비스도 ePass를 사용할 수 있으며, ePass 기능은 카드에 구현되어야 함
     - 오프라인 기능
  2. eID
     - 다양한 정부와 상용 응용프로그램에서 일반적인 용도로 사용
     - 인가된 서비스가 카드 소유자의 허가 후 접근할 수 있는 신원 기록을 저장
     - 오프라인과 온라인 서비스에 모두 사용 가능
  3. eSign
     - 선택적 기능이며 개인키와 키를 검증하여 전자 서명을 생성하는 보증서를 저장

- 비밀번호 인증 연결 수립(PACE)
  - eID 카드 내의 비접촉형 RF 칩이 접근 제어 없이 판독되지 않도록 함
  - 온라인 응용프로그램의 경우 : 카드 소유자만이 알고 있는 6자리의 PIN을 입력함으로써 접근이 수립
  - 오프라인 응용프로그램의 경우 : 카드 뒷면에 인쇄된 MRZ 혹은 앞면에 인쇄된 6자리 카드 접근 번호가 사용

eID 카드의 전자적 기능과 데이터

기능	목적	PACE 비밀번호	데이터	사용
ePass (의무)	인가된 오프라인 검사 시스템이 데이터 판독	CAN,MRZ	얼굴 사진; 2개 지문 (선택); MRZ 데이터	오프라인 생체 신원 검증을 정부 사용으로 예약
eID (활성화 선택)	온라인 응용프로그램의 데이터 판독 혹은 기능 접근	eID PIN	성; 예명 학위; 생년월일; 출생지; 주소; 커뮤니티 ID; 만료일	식별; 나이 검증; 커뮤니티 ID 검증; 제한적 식별(가명) 철희 요청
	오프라인 검사 시스템이 데이터를 판독하고 주소와 커뮤니티 ID를 업데이트	CAN, MRZ		
eSign (증명 선택)	인증 기관은 온라인으로 서명 보증	eID PIN	서명키; X.509 certificate	전자 서명 생성
	시민은 eSign PIN으로 전자 서명 생성	CAN		

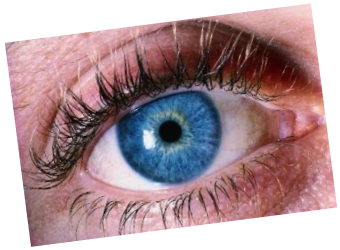
- **eID 사용자 인증**

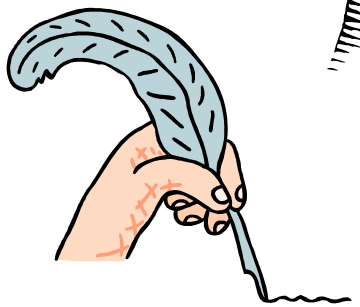

4. 인증 요청
5. PIN 요청
7. 인증 프로토콜 진행
8. 인증 결과 전송
eID 서버
6. 사용자 PIN 입력
1. 사용자 요청 서비스
(예. 웹 브라우저)
2. 서비스 요청
3. eID 메세지 전송
9. 인증 결과 전달
10. 서비스 허가
호스트/응용 서버

4. 생체 인식 인증

4. 생체 인식 인증

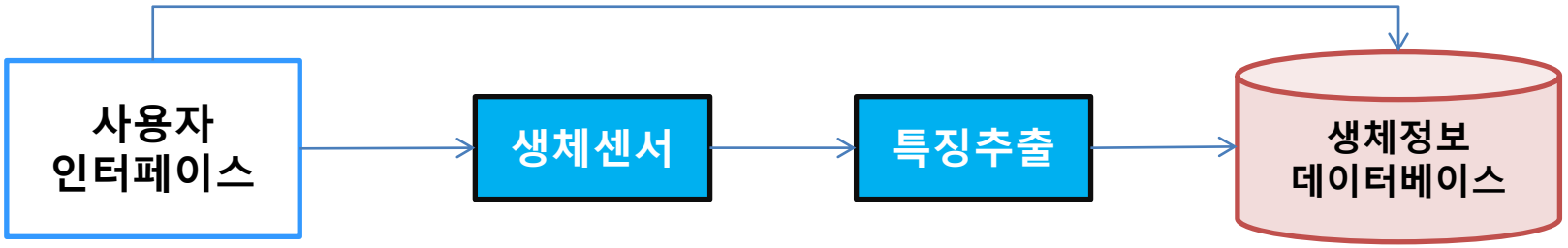
- 생체 인식 인증 시스템
  - 신체의 특징을 이용한 개인 인증
  - 지문, 손 모양, 얼굴 특성, 망막, 홍채 패턴 등과 같은 정적 특성과 음성과 서명 등과 같은 동적 특성 포함
  - 기본적으로 패턴 인식을 기반으로 함



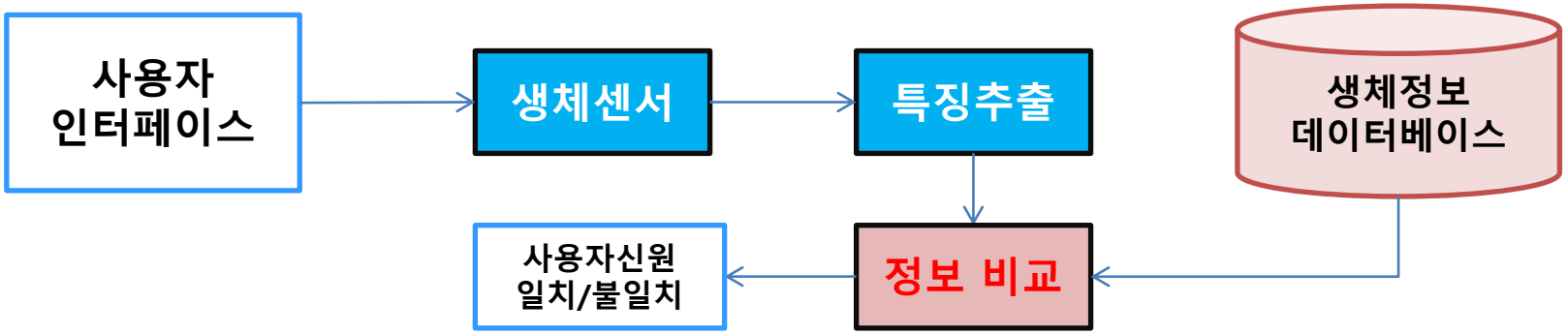


- 생체인식 인증의 비용과 정확도의 상관관계 (개략적인 지표)
  - 정확도는 스마트 카드 및 비밀번호 사용자 인증은 적용하지 않음
    예) 사용자가 비밀번호를 입력하면, 사용자가 맞는지 아닌지, 입력된 비밀번호와 예상된 비밀번호가 정확히 맞는지 확인함
- 생체인식 인증 시스템은 입력된 생체 인식 특징과 저장된 특징을 비교 후 인증
  - 생체 인식 정확도 개념 이전의 작동하는지 알아야 함

- 일반적 생체 시스템
  - 사용자 개개인의 생체 인식 정보가 먼저 공인 데이터베이스에 등록되어야 함
  - 데이터베이스 등록은 사용자에게 비밀번호를 할당하는 것과 유사함



생체 정보 등록 절차



생체인식 인증 절차

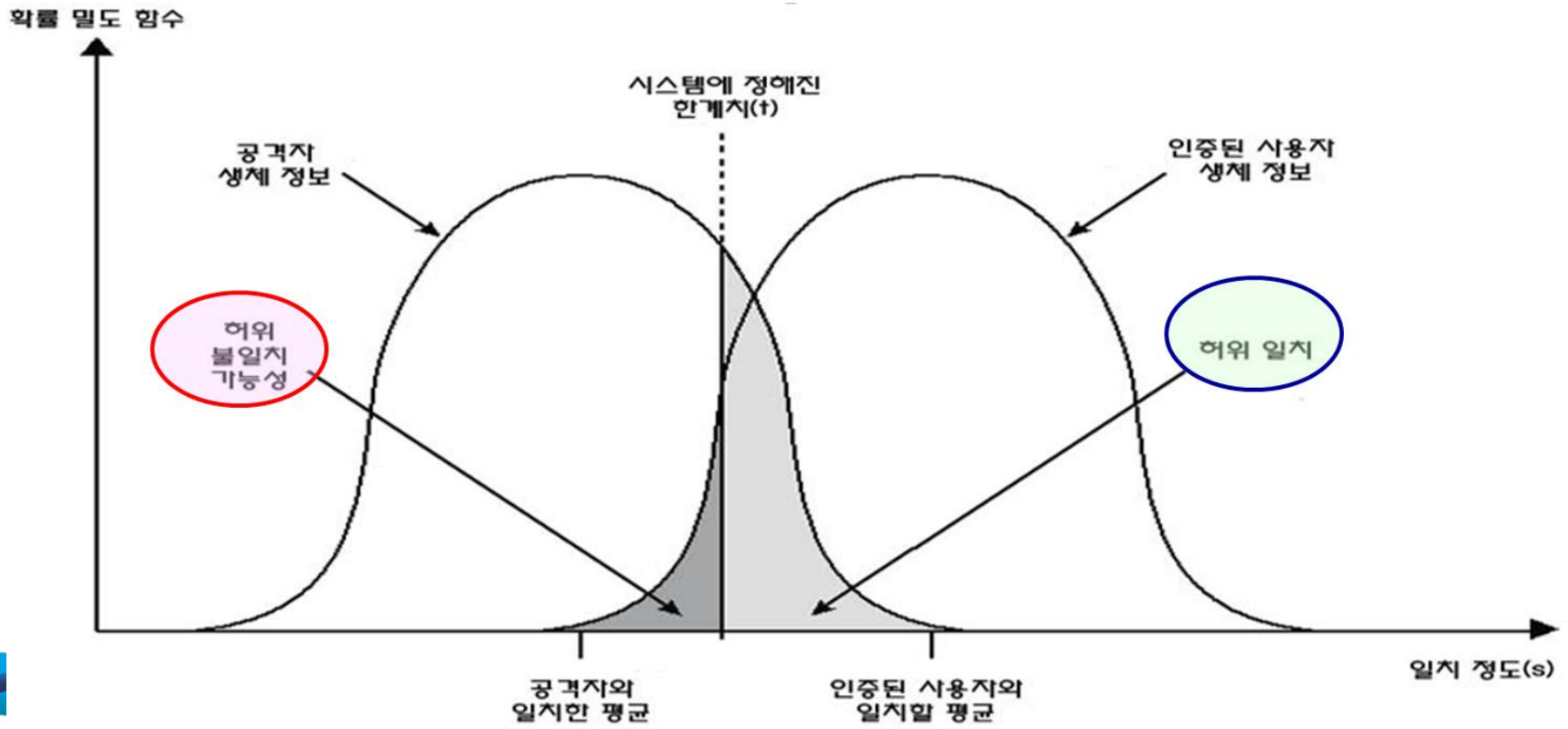
- 생체인식기술에 활용되기 위한 일반적으로 갖추어야할 특성

특 성	설 명
보편성(Universality)	모든 사람이 가지고 있는 생체 특성이 있어야 함
유일성(Uniqueness)	같은 특성을 가진 사람이 없어야 함
영구성(Permanence)	절대 변화하거나 변경되지 않아야 함
획득성(Collectability)	센서로부터 생체 특성 정보 추출 및 정량화가 용이해야 함

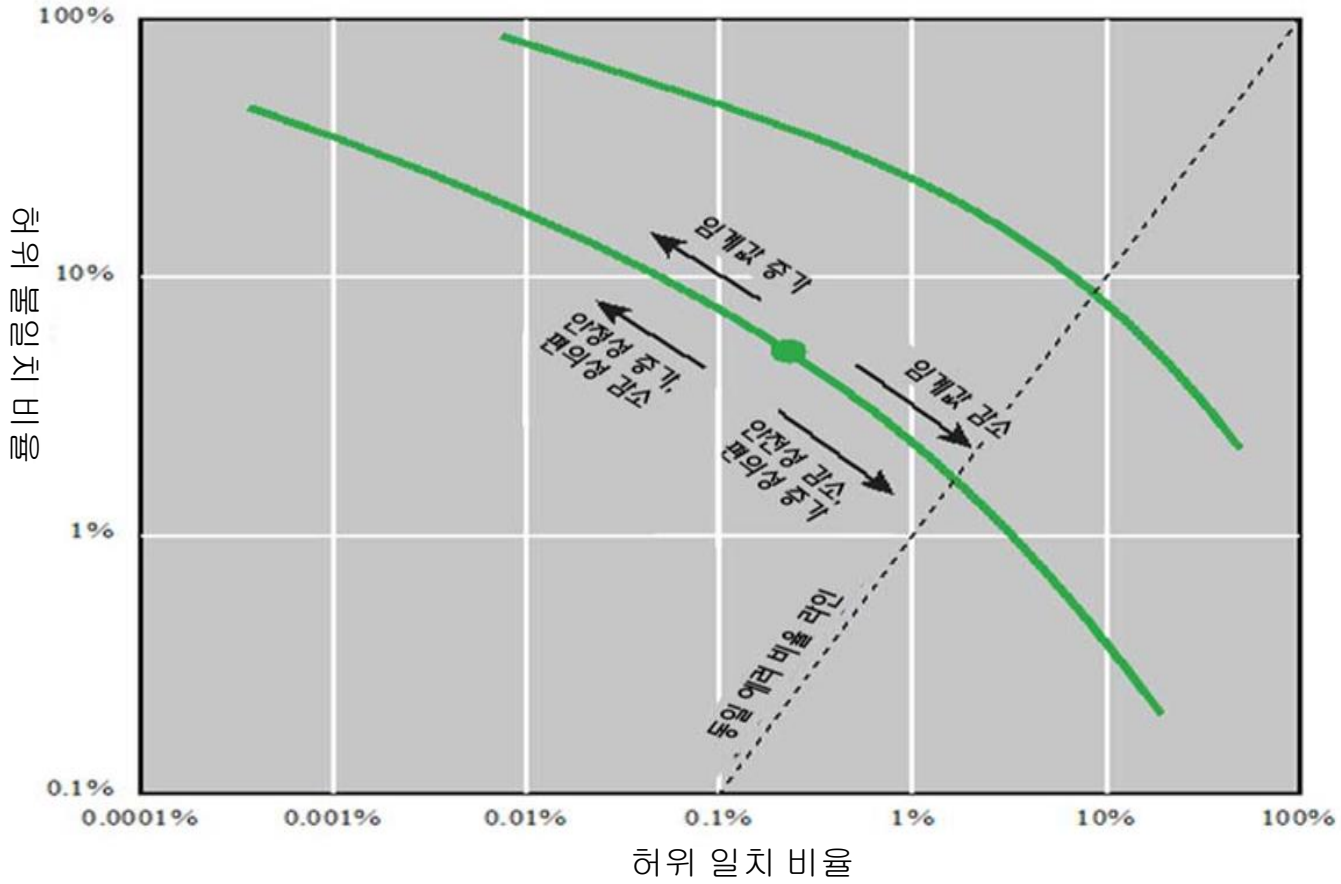
- 생체 인식 정확도
  - 생체 인식에서는 개인의 물리적 특성은 디지털 정보로 표현되고 개인별로 단일 디지털 표현 혹은 템플릿을 컴퓨터에 저장
  - 사용자가 인증하려 할 때, 시스템은 저장된 정보 집합과 제공된 정보 집합을 비교하게 되고 주어진 복잡한 생체 정보를 사람은 저장된 정보와 정확히 일치하는지 예측할 수 없음
  - 시스템은 일치되는 정보(matching score, 일반적으로 숫자로 표현)를 생성하는 알고리즘을 이용하여 저장된 정보와 입력된 정보 사이의 유사한 정도를 측정
    - 허위 일치 비율(false match rate) : 같은 출처의 생체 샘플이 제대로 인식되는 횟수와 다른 출처로 오인되는 횟수의 비율
    - 허위 불일치 비율(false non-match rate) : 같은 출처의 샘플이 다른 출처로 오인되는 비율

- **생체인식 인증 시스템의 딜레마**
  - 한 사용자가 여러 번 시스템에 의해서 인증
    - 일치되는 정도(matching score) s값은 다양하게 측정되어 확률 밀도 함수는 종 모양을 띠게 됨
    - 예) 지문 인식에서, 결과 값은 센서 잡음, 측정 시 손가락 팽창 정도, 건조한 상태 정도, 손가락 배치 위치 등으로 인해 추출된 값이 변하게 됨
    - 평균적으로 추출된 결과값은 일치되는 정도가 같고, 재측정을 할수록 확률 밀도 함수는 종 모양 형태를 띠게 됨

    ➔ 주어진 진짜 정보 와 거짓 정보 집합 범위 안에서 제공된 정보를 비교하는 것이 매우 어려움

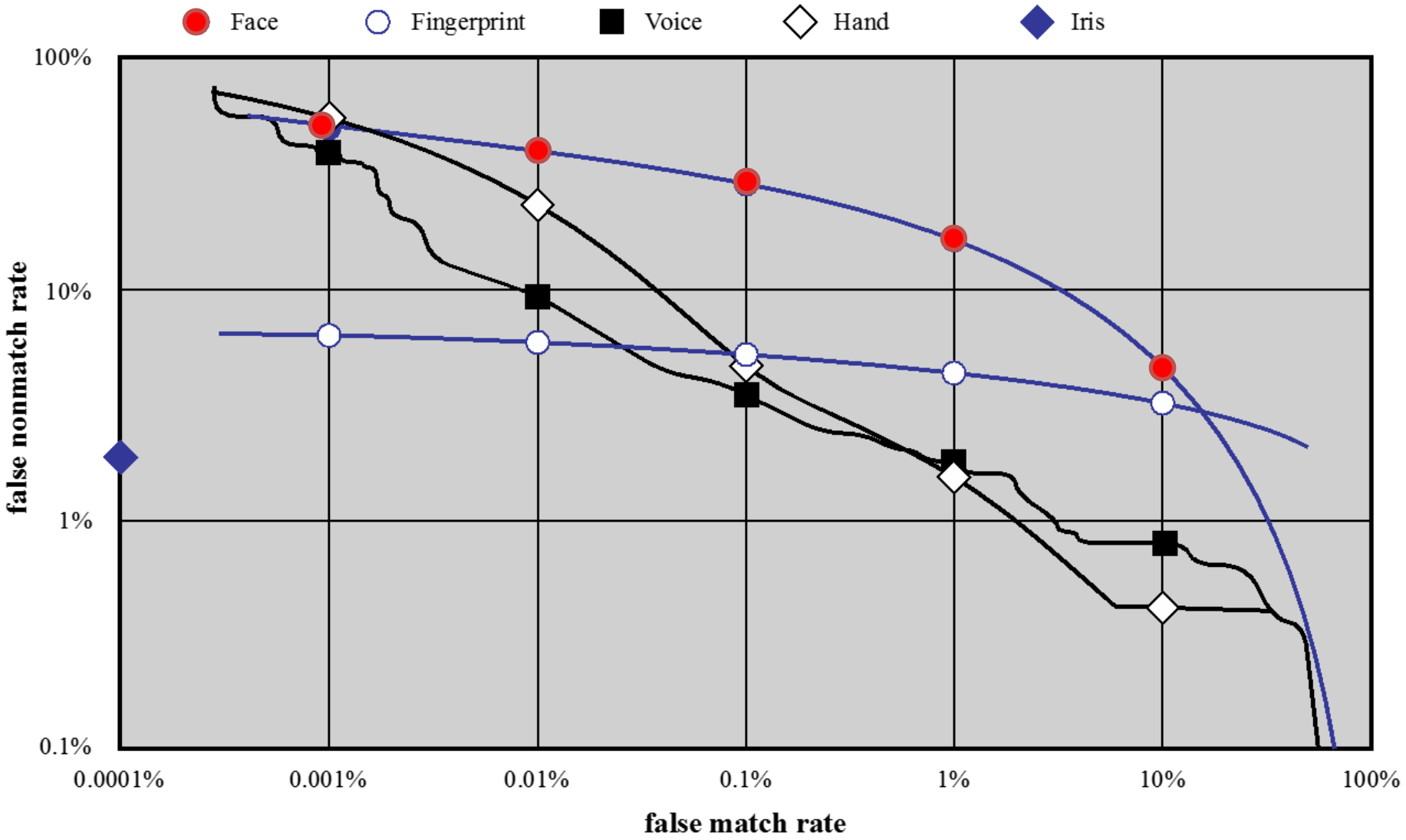


- 이상적인 생체 인식 측정 운영특성 곡선



- 생체 인식 시스템의 허위 일치 범위와 허위 불일치의 대조된 양상으로 구성
- 서로 다른 두 시스템에 대한 이상적인 곡선, **곡선이 낮고 왼쪽일수록 이상적임**

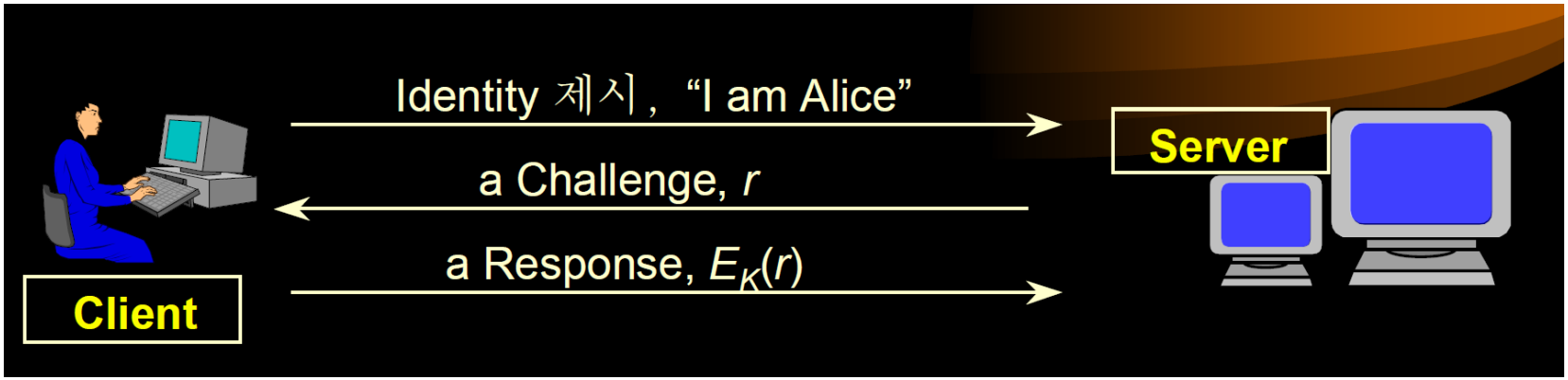
- 실제 제품 테스트에서 얻은 특성 곡선
  - **홍채 인식** 시스템은 200만 이상의 상호 비교에서 허위 일치 비율이 없으며 넓은 허위 일치 비율에 대해 얼굴 생체 인식은 최악의 성능을 보임



5. 원격 사용자 인증

Challenge-Response 개인식별 프로토콜

- 시도-응답 개인식별 프로토콜
- Client와 Server가 공통된 secret key K 를 공유
- E is a public encryption function e.g. DES ; hash function
- 비밀정보(secret information)의 상호교환은 없음
- key database 보호
- 매번 상이한 Response 값; E 함수의 안전성에 기반



비밀번호 프로토콜

- 비밀번호를 통한 간단한 시도-응답 프로토콜의 예
  - 사용자 : 자신의 신분을 증명할 수 있는 정보를 원격 호스트로 보냄
  - 원격호스트 : 일회성 랜덤 숫자 (nonce) 생성, 이 값을 사용자에게 전송
    - 호스트 쪽에선 두 함수 h()와 f()를 명시하여 전송
  - **사용자의 응답** : f(r′, h(P′))을 계산한 값
    - r′=r, P′: 사용자의 비밀번호, h(): 해시 함수
  - 비밀번호와 함수 f를 통해 생성한 랜덤 숫자를 조합한 값을 해시 연산 값으로 출력
  - 호스트 : 등록된 사용자 비밀번호를 해시함수를 이용해서 저장
  - 사용자 U: h(P(U))으로 표현
  - 사용자로부터 응답이 오면, 호스트는 f(r′, h(P′))값과 계산된 f(r, h(P(U))) 값을 비교하여 값이 일치하면 사용자 인증 성공

Client

Host

U, User

U

r, random number
h(), *f*(), functions

(*r*, *h*(), *f*())

P′
r′, return of *r*

f(*r*′, *h*(*P*′))

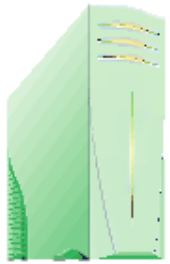
if *f*(*r*′, *h*(*P*′)) =
f(*r*, *h*(*P*(*U*)))
then yes else no

yes/no

토큰 프로토콜

- 토큰 기반 인증 프로토콜 예
  - 사용자: 자신의 신분을 증명할 수 있는 정보를 원격 호스트로 전송
  - 호스트: 무작위로 선정한 숫자와 식별함수 f()와 h()를 사용한 응답
  - 토큰 : 정적 패스코드를 저장하거나 일회성으로 무작위 패스코드를 생성
    - 일회성 무작위 생성 패스코드 - 어떤 방식으로든 호스트 쪽과 서버 쪽의 동기화가 이루어져야 함
    - 예) 사용자가 비밀번호 P′를 입력하여 패스코드를 활성화 시키는 방법
  - 비밀번호: 사용자와 토큰 사이에서만 공유, 원격호스트는 제외
  - 토큰 f(r′, h(W′))으로 호스트에 응답,
    - 정적 패스코드 - 원격호스트 쪽에서 h(W(U))의 해시 연산된 값을 저장
    - 동적 패스코드 - 원격 호스트가 일회성 패스코드를 생성하고 해시 값을 가짐

Client



Host

U, User

U

r, random number
h(), *f*(), functions

(*r*, *h*(), *f*())

P′ → *W*′
password to
passcode via token
r′, return of *r*

f(*r*′, *h*(*W*′))

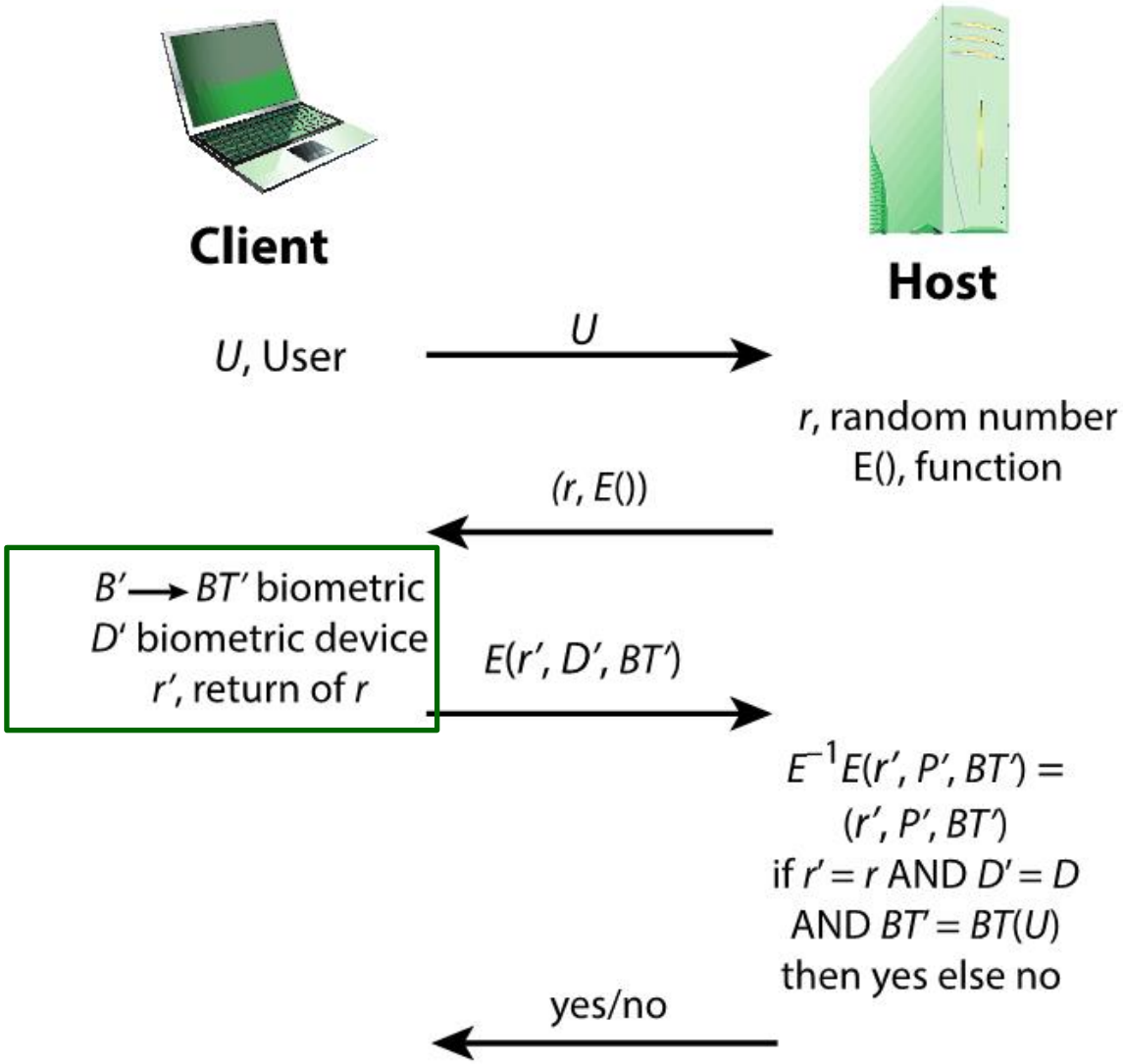
-패스코드 W' 제공

if *f*(*r*′, *h*(*W*′)) =
f(*r*, *h*(*W*(*U*)))
then yes else no

yes/no

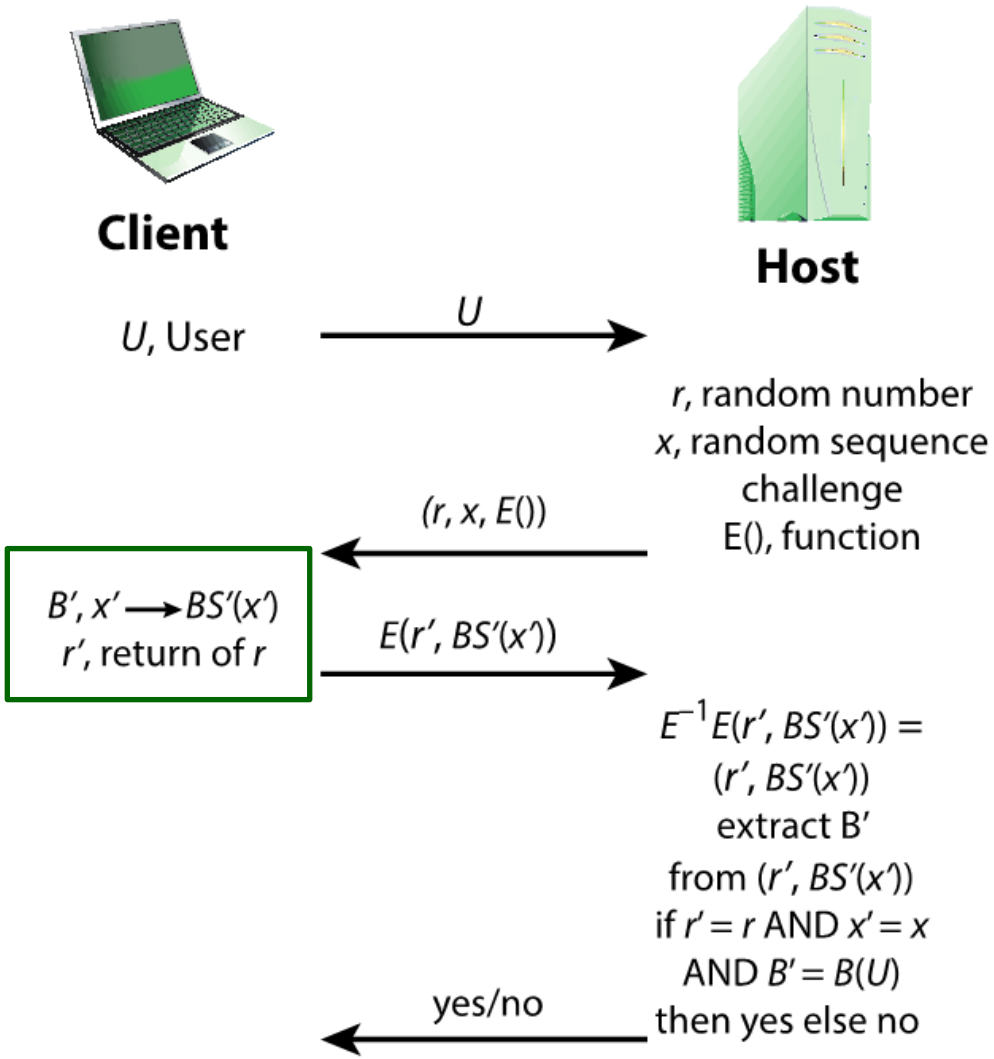
정적 생체 인식 프로토콜

- 정적인 생체정보를 통한 프로토콜의 예
  - 사용자 : ID를 호스트에게 전송
  - 호스트 : 무작위로 선정한 숫자 r과 암호화를 위한 E()의 식별자를 사용자에게 전송
  - 사용자측, 클라이언트 시스템에서는 생체 인식 장치를 제어
    - 사용자의 생체 인식 B′로부터 생체 인식 정보 집합인 BT′를 생성, 암호문 E(r′, D′, BT′)를 반환
    - D′ 식별자 : 특정 생체 인식 장비를 식별할 수 있는 인수
  - 호스트 : 사용자로부터 들어오는 메시지를 복호화하여 세 번째 인자를 확인하여 호스트 쪽에 저장된 값과 비교
    - 일치한다면, 호스트는 r′ = r을 확인
    - BT′값과 저장된 값 사이의 일치되는 정도를 확인하여 미리 정의된 임계값을 초과하는지 확인
  - 호스트 : 호스트 데이터베이스에 등록된 기기목록의 수신장치 ID를 비교하여 생체인식 캡처 장치의 간단한 인증은 제공


Client
Host
U, User
U
r, random number
E(), function
(r, E())
B′ → BT′ biometric
D′ biometric device
r′, return of r
E(r′, D′, BT′)
E⁻¹E(r′, P′, BT′) =
(r′, P′, BT′)
if r′ = r AND D′ = D
AND BT′ = BT(U)
then yes else no
yes/no

동적 생체 인식 프로토콜

- 동적인 생체 인식 프로토콜의 예
  - 정적 생체 인식과 주요 차이점: 인증 시 호스트가 임의의 숫자뿐만 아니라 *임의의 순서까지 제공*
    - **순서인증**: 숫자 순서, 문자 순서, 또는 단어 순서
    - BS′(x′) 생성: 클라이언트에서 사용자는 순서를 입으로 소리 내고, 순서를 타이핑, 또는 손으로 써서 생체 인식신호
  - 클라이언트에서는 받은 메시지를 복호화
  - 숫자 r′과 호스트 쪽에서 생성한 r과 일치하는지 확인
  - 생체 인식 정보 BS(x′)를 바탕으로 저장된 BT(U)와 비교하여 사용자과 x값이 각각 일치하는지 확인
  - 비교 값이 미리 정의한 임계 값을 초과하면 사용자 인증 성공


Client
Host
U, User
U
r, random number
x, random sequence
challenge
E(), function
(r, x, E())
B′, x′ → BS′(x′)
r′, return of r
E(r′, BS′(x′))
E⁻¹E(r′, BS′(x′)) =
(r′, BS′(x′))
extract B′
from (r′, BS′(x′))
if r′ = r AND x′ = x
AND B′ = B(U)
then yes else no
yes/no

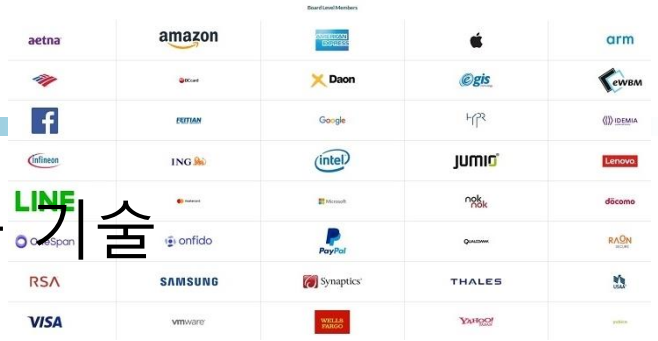
6. 인증 보안 이슈

사용자 인증의 일반적인 공격과 방어

공 격	인증자	예	통상적 방어
클라이언트 공격	비밀번호	전수 검색	시도 제한, 많은 후보자군
	토큰	전수검색	시도 제한, 많은 후보자군
	생체	False match	시도 제한, 많은 후보자군
호스트 공격	비밀번호	평문 도난, 사전적/전수 검색	해시; 많은 후보자군, 비밀번호 데이터베이스 보호
	토큰	비밀번호 도난	위와 같음; 1회용패스워드
	생체	템플릿 도난	장비 인증 캡처; 시도 응답 프로토콜
도청, 도난, 복사	비밀번호	shoulder surfing	사용자의 비밀 유지 노력: 문제 있는 비밀번호에 대한 관리자의 빠른 대응; 다중 요소 인증
	토큰	하드웨어 도난, 위조	다중 요소 인증; 위조 변조 방지
	생체	생체 복제(스푸핑)	동적 패턴 변화 분석, 생체특성분석

공 격	인증자	예	통상적 방어
재생 (재사용)	비밀번호	도난 된 비밀번호 응답재생	시도 응답 프로토콜
	토큰	도난 된 비밀번호 응답재생	시도 응답 프로토콜; 1회용패스워드
	생체	도난 된 생체 템플릿 응답 재생	시도 응답 프로토콜 이용 복사 탐지
트로이 목마	비밀번호, 토큰, 생체	가짜 클라이언트 생성 및 장비 도난	신뢰하는 보안 영역에서 클라이언트와 장비 인증
서비스 거부	비밀번호, 토큰, 생체	다수의 오류인증으로 인한 잠김	행위 기반 대응; 실시간 모니터링-탐지 및 차단

FIDO 인증 기술



- FIDO(Fast IDentity Online) 바이오 인증 기술
- FIDO Alliance, https://fidoalliance.org
- FIDO 얼라이언스가 추구하는 인증방식
  - 온라인상의 빠른 신원 확인을 위해 간단하고(Simpler), 강력한 (Stronger) 인증방식을 개발
  - 최근 카드 결제, 금융거래, 사용자 인증 강화 및 편의성 향상이 필요한 핀테크 비즈니스, 회사 내부결제 등 사용

- FIDO 2.0
  - 모바일뿐만 아니라 PC환경을 포함한 모든 온라인 환경에서 생체 인증을 사용할 수 있도록 하는 기술

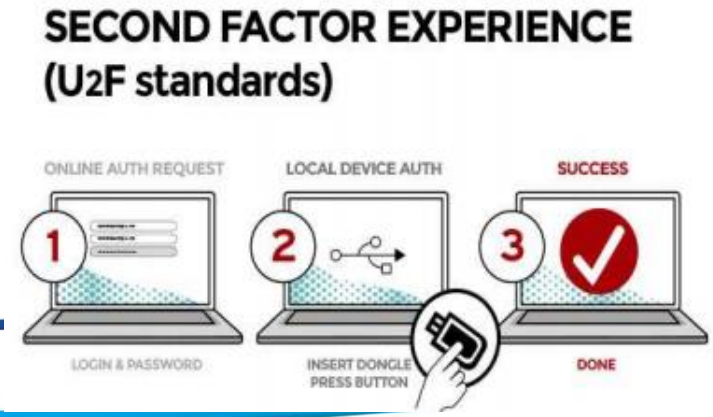
    (FIDO 1.0: 모바일 환경에서 생체 인증을 사용할 수 있는 표준)

- IoT 디바이스를 위한 자동화된 온보딩 프로토콜 발표, 2021

FIDO의 두가지 프로토콜

- UAF(Universal Authentication Framework) Protocol
  - 사용자의 디바이스에서 제공하는 인증방법을 온라인 서비스와 연동하여 사용자를 인증하는 기술

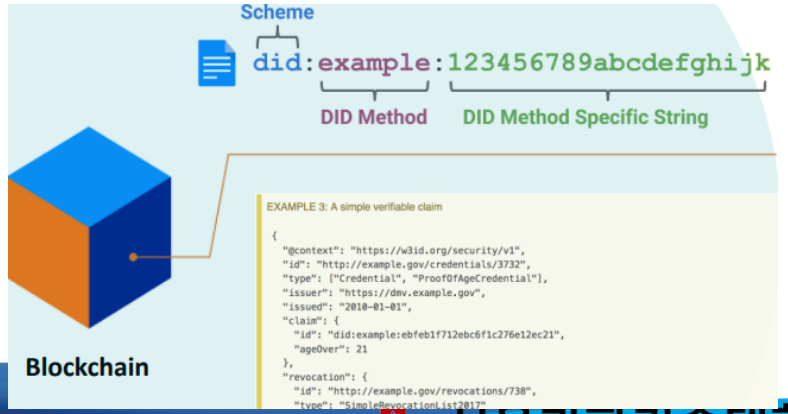
- U2F(Universal 2nd Factor) Protocol
  - 기존 패스워드를 사용하는 온라인 서비스에서 두번째 인증요소로 강한 인증을 사용자 로그인 시에 추가할 수 있는 프로토콜



DIDs (디지털 신원 증명) 기술

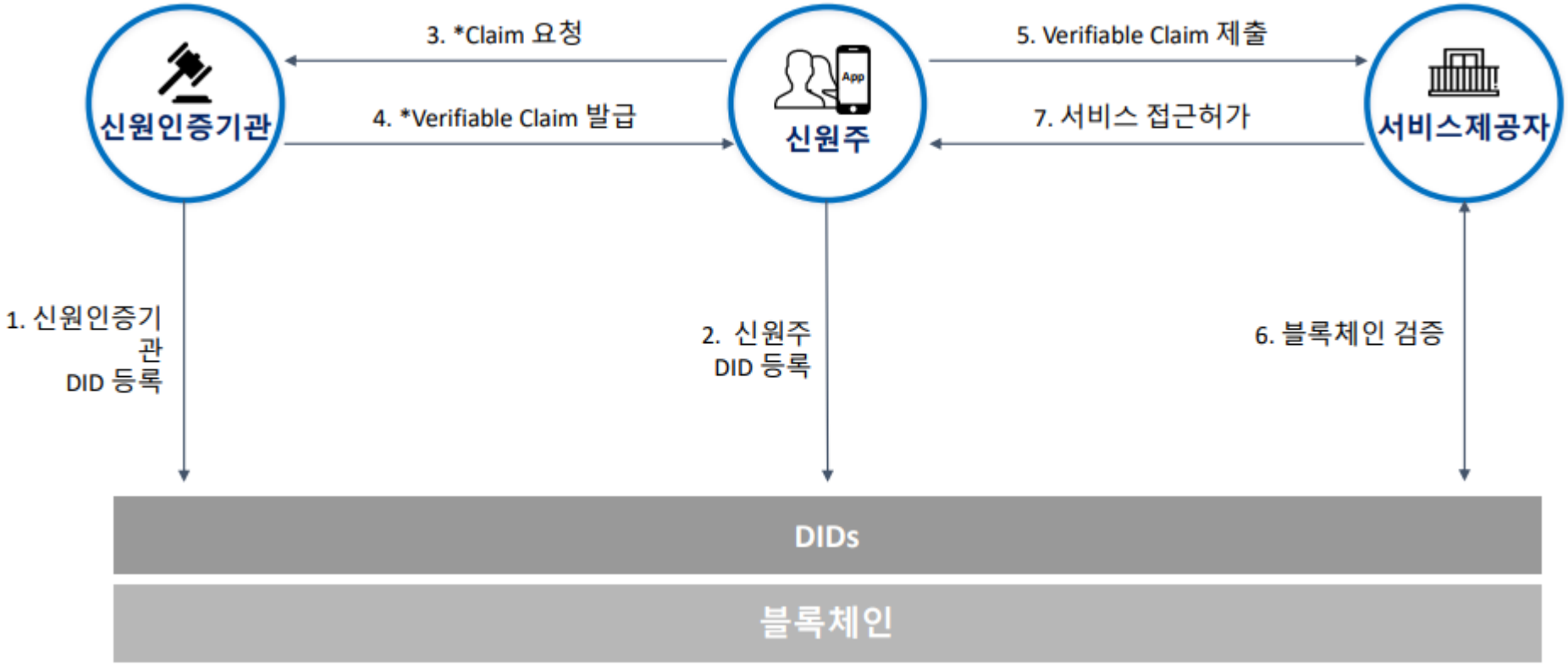
- 탈중앙 식별자 (Decentralized IDentifiers)
  - 분산 원장 기술 또는 네트워크에 등록되어 있어 중앙집중 형 등록 기관을 필요로 하지 않는 전 세계적 유일한 식별자
  - 중앙기관이 아닌 개인이 자신의 데이터를 직접 관리하는 구조로 기존 방식과 달리 서비스 이용과정에서 모든 개인정보를 제공하지 않음
- 중요 특성
  - 영속성 (Persistent): 변경 및 조작되지 않음
  - 해석가능성 (Resolvable): 메타데이터로 조회할 수 있음
  - 암호학적 증명(Cryptographically verifiable): 암호학적으로 소유권을 증명할 수 있음
  - 탈중앙성 (Decentralized): 중앙화된 기관이 필요하지 않음

- W3C(World Wide Web Consortium)가 주도하여 블록체인을 이용한 ID 인증 구조 논의 시작
  - DID Document Syntax를 정의하고 오픈소스 화



DID 서비스 흐름

- 누구의 소유도 아닌 블록체인에서 탈중앙화 식별자 DID가 관리되고, 누구나 이를 확인할 수 있음



*Claim: 신원주가 제출한 주민등록번호, 성별 등의 신원 정보에 대한 주장
*Verifiable Claim: 신원인증기관에 의해 인증되어 증명 가능한 신원 단위

- 국내 DID 컨소시엄 현황

구분	이니셜 DID 얼라이언스	DID 얼라이언스	마이아이디 얼라이언스
특성	통신과 은행이 주도	금융결제원, 은행, 카드 등 다양한 기업이 참여	금융투자협회 중심으로 주요 증권사 참여
참여사	SK텔레콤, KT, LG유플러스, 삼성전자, 코스콤, 현대카드, BC카드, KEB하나은행, 우리은행, NH농협은행, 신한은행, KB국민은행, CJ올리브네크웍스, 삼성SDS 총 14개사	금융결제원, NH농협은행, 신한은행, 광주은행, 전북은행, 신한카드, 삼성카드, KB국민은행, KB국민카드, 롯데카드, 병무청, 한국투자증권, RAON, 삼성SDS, 코인플러그, NICE평가정보, 군인공제회 C&C 등 총 64개사	금융투자협회, 신한은행, BNK부산은행, 삼성증권, 미래에셋대우, KB증권, KB생명, 유안타증권, 유진투자증권, 한화투자증권, 하이투자증권, POSCO, 삼성전자, STX, 김&장, 아이콘루프 등 총 47개사
주요 기반기술	SK텔레콤 블록체인(이니셜)	라온시큐어 블록체인 신원인증 플랫폼 옴니원(Omnione)	아이콘루프 블록체인 마이아이디(MyID)
컨소시엄 주요(제안) 서비스	모바일운전면허증(통신3사), 모바일신분증(SK), 계좌보유증명(KEB하나은행), 재직증명서 및 모바일사원증 발급(공동)	제안서비스 없음	'쯩(비대면 실명인증 서비스)'을 통해 신한은행 실명인증 서비스 중(8.26) (NH, IBK 또한 쯩 실명인증 발급기관으로 연내 서비스 오픈 예정)

참고문헌

- Stallings, 컴퓨터보안 (Computer Security), 한티미디어, 2016
- FIDO를 활용한 IoT 단말기 및 사용자 보안인증 기술, 한국FIDO산업포럼, 주간기술동향, 2017
- FIDO 소개, 한국정보인증, https://fido.kica.co.kr, 2017
- FIDO Alliance, 2021, https://fidoalliance.org
- 전자서명 기반의 디지털 신분증 구현 방안과 활용 사례, KISA, 2019
- 최근 생체인식 산업 동향과 시사점, 이슈분석 188호, IITP, 2021
- 전자서명 기반의 디지털 신분증 구현 방안과 활용 사례, ICONLOOP, KISA, 2019
- 개인정보의 주권회복을 위한 솔루션,탈중앙화 신원증명(DID), KB지식비타민, KB경영연구소, 2020

Q & A

69

추가자료

70

- 사용자 신원에 따른 인증 수단의 문제점
  - 공격자는 비밀번호를 추측하거나 훔칠 수 있음
  - 토큰을 위조하거나 훔칠 수 있음
  - 사용자는 비밀번호를 잊거나, 토큰을 잃어버릴 수 있음
  - 비밀번호와 토큰 정보를 관리하는 데 상당한 비용이듬
  - 생체인식 인증은 거짓된 긍정 또는 거짓된 부정, 사용자 수락, 비용, 편의 등이 해당됨

- [SP800-63-2]의 4단계 보증 레벨
  - 레벨1: 확인된 신원의 유효성이 거의 없음
    - 예) 회사 웹 사이트의 게시판에 고객이 참여하는 경우를 들 수 있고, 일반적으로 사용자ID와 비밀번호만 인증에 사용함
  - 레벨2: 확인된 신원의 유효성이 조금 없음
    - 신용장은 기관에서 공개적으로 초기 식별 보증이 요구되는 많은 경우의 비즈니스에 적합하고, 이 레벨에서는 위에 기술된 여러 인증 수단들과 여러 보안 인증 프로토콜이 필요함
  - 레벨3: 높게 확인된 신원의 유효성.
    - 고객이나 고용인이 제한된 고가의 서비스에 접근하도록 하는 데 적합함
    - 예) 변리사가 특허 신용 정보를 특허국에 전자 제출하는 경우이고, 부적절한 노출은 경쟁자에게 유리함. 이 레벨에서 인증의 여러 기술적 요소들이 사용되어야 하고, 최소한 두 개 이상의 독립적인 인증 기술을 사용해야 함
  - 레벨4: 매우 높게 확인된 신원의 유효성
    - 고객이나 고용인이 제한된 매우 고가의 서비스에 접근하도록 하거나 부적절한 접근이 매우 위험할 경우에 적합함
    - 예) 법 집행자가 범죄 기록 데이터베이스에 접근하는 경우이고, 허가되지 않은 접근은 개인 정보 문제를 야기할 수 있고, 일반적으로 레벨 4 인증은 다수의 잘 알려진 개인적인 등록 요소들을 요구함

- 잠재적 영향
  - 잠재적 영향은 보증 레벨에 밀접하게 관련된 개념
  - FIPS 199(Standards for Security Categorization of Federal Information and Information Systems, 2004)에서는 보안 침해에 대한 3 레벨의 기관이나 개인의 잠재적 영향을 정의함(1/2)

    - 낮음: 인증 오류가 기관 작동, 기관 자산, 혹은 개인에 제한된 역효과를 미치는 경우
      (1) 기관의 주요 기능 수행에 어느 정도 지장을 주는 경우
      (2) 기관의 자산에 사소한 손실을 주는 경우
      (3) 기관이나 개인에게 사소한 경제적 손실을 주는 경우
      (4) 개인에게 사소한 유해를 주는 경우

    - 보통: 인증 오류가 심각한 역효과를 미치는 경우
      (1) 기관의 주요 기능 수행은 가능하나 효율성이 심각하게 감소하는 경우
      (2) 기관의 자산에 중대한 손실을 주는 경우
      (3) 기관이나 개인에게 중대한 경제적 손실을 주는 경우
      (4) 개인에게 생명에 심각한 유해를 가하거나 부상 위협은 없지만 심각한 지장을 주는 경우.

- 잠재적 영향
  - 잠재적 영향은 보증 레벨에 밀접하게 관련된 개념
  - FIPS 199(Standards for Security Categorization of Federal Information and Information Systems, 2004)에서는 보안 침해에 대한 3 레벨의 기관이나 개인의 잠재적 영향을 정의함(2/2)

    - 높음: 인증 오류가 치명적인 역효과를 미치는 경우
      (1) 기관의 주요기능 수행이 불가능할 정도의 손실을 주는 경우
      (2) 기관의 자산에 치명적 손실을 주는 경우
      (3) 기관이나 개인에게 치명적인 경제적 손실을 주는 경우
      (4) 개인에게 생명에 심각한 유해를 가하거나 부상 위협을 주는 경우

- 위험영역
  - 잠재적 영향과 적절한 보증 레벨의 대응은 상황에 따라 결정됨.
  - 주어진 정보 시스템이나 기관의 서비스 자산에 대해, 기관은 인증 실패가 발생 했을 때의 영향 정도를 영향의 종류와 위험영역을 이용하여 결정할 필요가 있음
  - 예를 들어, 데이터베이스에 허가되지 않은 접근을 발생하는 인증 오류에 의한 잠재적 경제손실을 생각 할때, 데이터베이스 영향은 다음과 같음
    - 낮음

    최악의 경우, 부분 혹은 기관의 책임에 사소한, 복구되지 않은 경제적 손실
    - 보통

    최악의 경우, 부분 혹은 기관의 책임에 심각한, 복구되지 않은 경제적 손실
    - 높은

    부분 혹은 기관의 책임에 치명적인, 복구되지 않은 경제적 손실

• 각 보증 레벨의 최대 잠재적 영향

	보증 레벨 영향 프로파일			
인증 오류에 대한 잠재적 영향 카테고리	1	2	3	4
지위나 평판에 대한 불편 혹은 손실	낮음	보통	보통	높음
경제적 손실 혹은 기관 책임	낮음	보통	보통	높음
기관의 프로그램이나 관심에 유해	해당없음	낮음	보통	높음
민감한 정보의 허가되지 않은 유출	해당없음	낮음	보통	높음
개인 안전	해당없음	해당없음	낮음	보통/높음
민사 혹은 형사위반	해당없음	낮음	보통	높음

비밀번호 기반 인증

비밀번호 선택전략: 블룸 필터

- 효율적이고 효과적인 비밀번호 사전 검색 기술
- 거절 대상이 되는 단어들의 리스트를 바탕으로 리눅스 운영체제와 같은 다수의 시스템상에서 구현된 기술
- 블룸 필터의 작동 방식

  k블룸 필터는 k개의 독립적인 해시 함수 $H_1(x)$, $H_2(x)$, ... , $H_k(x)$로 구성

  각 함수는 비밀번호를 0 ~ N-1의 해시 값으로 매핑 함

$$H_j(X_j) = y \quad 1 \le i \le k; \quad 1 \le j \le D; \quad 0 \le y \le N-1;$$

  X_j = 비밀번호 사전의 j번째 단어, D = 비밀번호 사전에 있는 단어 수

- 비밀번호 사전에 대해 다음과 같은 과정이 적용됨
  1. 0으로 초기화된 N 비트의 해시 테이블을 정의
  2. 각각의 비밀번호에 대해서 k개 해시 값이 계산, 이에 해당하는 해시 테이블의 비트가 1로 설정
  3. 만약 $H_j(X_j)$ = 67이라면, 해시 테이블에서 67번째 비트는 1로 설정
  4. 만약 해당 비트가 이미 1로 설정되어 있다면 1인 상태로 계속 남아 있게 됨

- 새로운 비밀번호가 확인될 때, k개 해시 값을 계산함
  - 만약 해시 테이블의 해당되는 비트의 값이 1이면, 해당 비밀번호는 거절됨
- 사전 내의 모든 비밀번호는 거절될 수도 있지만, False Positives도존재 할 수도 있음
  - False Positives: 비밀번호가 사전에 포함되지는 않지만 해시 테이블상에서는 일치하는 경우

- 비밀번호 undertaker와 hulkhogan은 사전에 포함되어 있다고 추측할 수 있지만, xG%#jj98은 그렇지 않음

H_1(undertaker) = 25 H_1(hulkhogan) = 83 H_1(xG%#jj98) = 665
H_2(undertaker) = 998 H_2(hulkhogan) = 665 H_2(xG%#jj98) = 998

- 비밀번호 xG%#jj98가 시스템에 제안되면, 비록 사전에 존재하지 않더라도 해당 비밀번호는 거절됨

- 만약 False Positives가 많다면, 사용자의 비밀번호 선택은 어려움
- False Positives 확률 P는 다음과 같이 추정할 수 있음

$$P \approx \left(1 - e^{-kD/N}\right)^k = \left(1 - e^{-k/R}\right)^k$$

또는

$$R \approx \frac{-k}{\ln(1 - p^{1/k})}$$

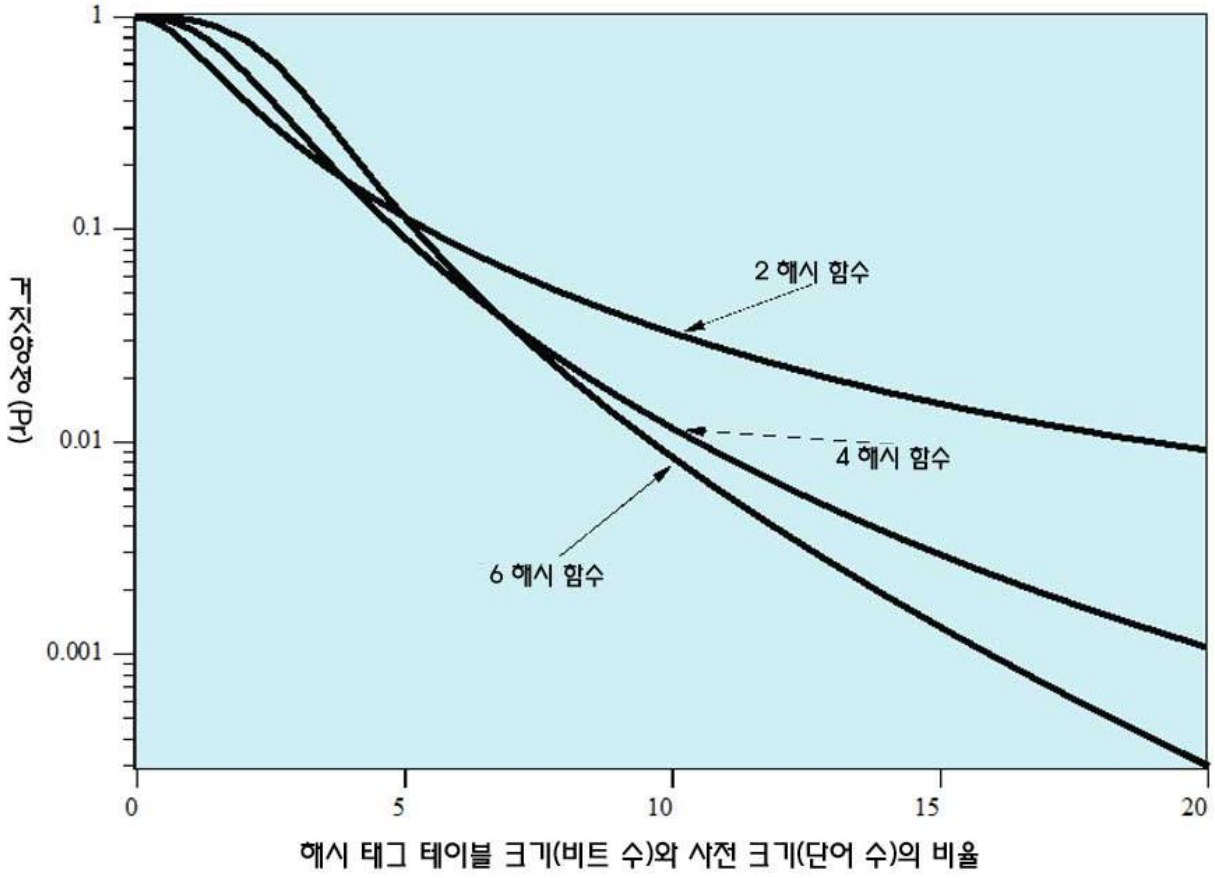
k = 해시 함수의 수

N = 해시 테이블 비트 수

D = 사전의 단어 수

R = N/D. 해시 테이블 크기(비트)와 사전 크기(단어 수)의 비율

- P를 k값의 변화에 따른 R함수로 표현함
- 100만 개의 단어를 포함하고 있는 사전과 사전에 포함되지 않은 거절해야 하는 비밀번호에 대해 0.01 확률을 기대한다고 가정함
  - 만약 6개의 해시 함수를 선택한다면, R = 9.6의 비율이 필요함
  - 9.6 x 10^6비트, 1.2MB 크기의 가용 저장 공간의 해시 테이블이 필요하게 됨
- 전체 사전 용량은 8MB 이상 필요하게 됨
- 결과적으로 7배로 압축 가능


1
0.1
0.01
0.001
0
5
10
15
20
2 해시 함수
4 해시 함수
6 해시 함수
해시 테그 테이블 크기(비트 수)와 사전 크기(단어 수)의 비율

생체 인식 인증

- 생체 인식 응용프로그램의 물리적 특성
  - 얼굴 특징 : 사람과 사람을 구별하는 가장 흔한 방법이므로 컴퓨터에서의 식별도 자연스럽게 고려됨
    - 가장 보편적인 접근 방법은 상대적 위치와 눈, 눈썹, 코, 입술, 턱과 같은 주요 얼굴 특징의 모양 등을 기반으로 하는 것임
    - 다른 접근법은 인간의 얼굴을 기본 혈관 시스템과 상호 얼굴 형상을 생산하기 위해 적외선 카메라를 사용하는 방법임
  - 지문 : 수 세기 동안 식별을 위한 도구로 사용되어왔고, 이러한 과정은 체계화되고 법의 집행 목적에 대해서 부분적으로 자동화됨
    - 산등성이 패턴과 손가락 끝 표면의 밭고랑 패턴으로 이루어짐
    - 자동 지문 인식기와 비교분석 시스템은 모든 지문 인식 패턴 중 수치 대리로 저장하기 위해 지문의 기능 번호를 추출함
  - 손 모양 : 모양, 길이, 손가락 너비 등 손의 특징을 구별함

- 망막 패턴 : 망막 표면 바로 아래 혈관에 의해 형성된 패턴은 고유하므로 인증에 적합함
  - 망막 인식 시스템은 눈의 시각이나 적외선 빛을 낮은 강도 광선을 추측하여 망막 패턴의 디지털 이미지를 얻음

- 홍채 : 홍채의 세부 구조는 또 다른 독특한 신체적 특징임

- 서명 : 각각의 필기는 독특한 스타일을 가지고 있어, 이것을 이용하여 특히 서명에 반영됨
  - 그러나 개인의 여러 서명 샘플이 동일하지 않고 미래의 샘플과 일치시킬 수 있는 서명의 컴퓨터 표현을 구현하는 단계는 복잡함

- 음성 : 개인의 서명 스타일이 쓴 사람의 독특한 신체적 특성뿐만 아니라 습관도 반영됨
  - 그러나 한 사람에게 시간에 따라서 다양한 샘플이 존재하며, 생체 인식 작업을 복잡하게 함

- 클라이언트 공격
  - 공격자가 호스트에 대한 접속이나 통신 경로에 대한 개입 없이 사용자 인증을 시도하는 것을 말함
  - 공격자는 합법적인 사용자로 가장하여 시스템에 접근을 시도하고, 비밀번호 기반 시스템에서, 공격자는 사용자의 비밀번호 를 추측하여 접속을 시도하고 수 많은 시도 끝에 비밀번호를 얻을 수 있음
  - 공격자는 모든 가능한 비밀번호를 확인하는 방법을 통해 시스템에 성공적으로 접근할 수도 있음
  - 해결방법
    - 이러한 공격을 막기 위해서는 길고 예측 불가능한 비밀번호를 사용하여야 함. 하지만 많은 수의 비트가 필요하기 때문에 비밀번호 예측이 불가능함
    - 프로그램 자체에서 서비스에 접근하기 위한 비밀번호 입력에 대한 일정시간 동안 제한을 두는 방법이 있음

- 호스트 공격
  - 직접적으로 호스트 시스템상의 사용자 파일의 비밀번호, 토큰 패스코드 또는 생체 인식 정보에 접속하는 방법
  - 토큰 방식의 경우 호스트상에 저장되지 않은 일회성 패스코드를 생성함
  - 생체 인식의 경우, 사용자의 신체적 특징으로 인해 생체 인식정보를 확보하기 어려움
  - 정적인 특징을 사용하는 경우, 생체 인식 장치에 대한 추가 인증이 필요함
  - 동적인 특징을 사용하는 경우, 시도-응답 프로토콜 형식의 보안대책이 필요

- 재사용 공격
  - 캡처된 사용자 응답의 반복을 통한 공격을 포함하고, 가장 쉬운 대응책으로 시도-응답 프로토콜이 있음

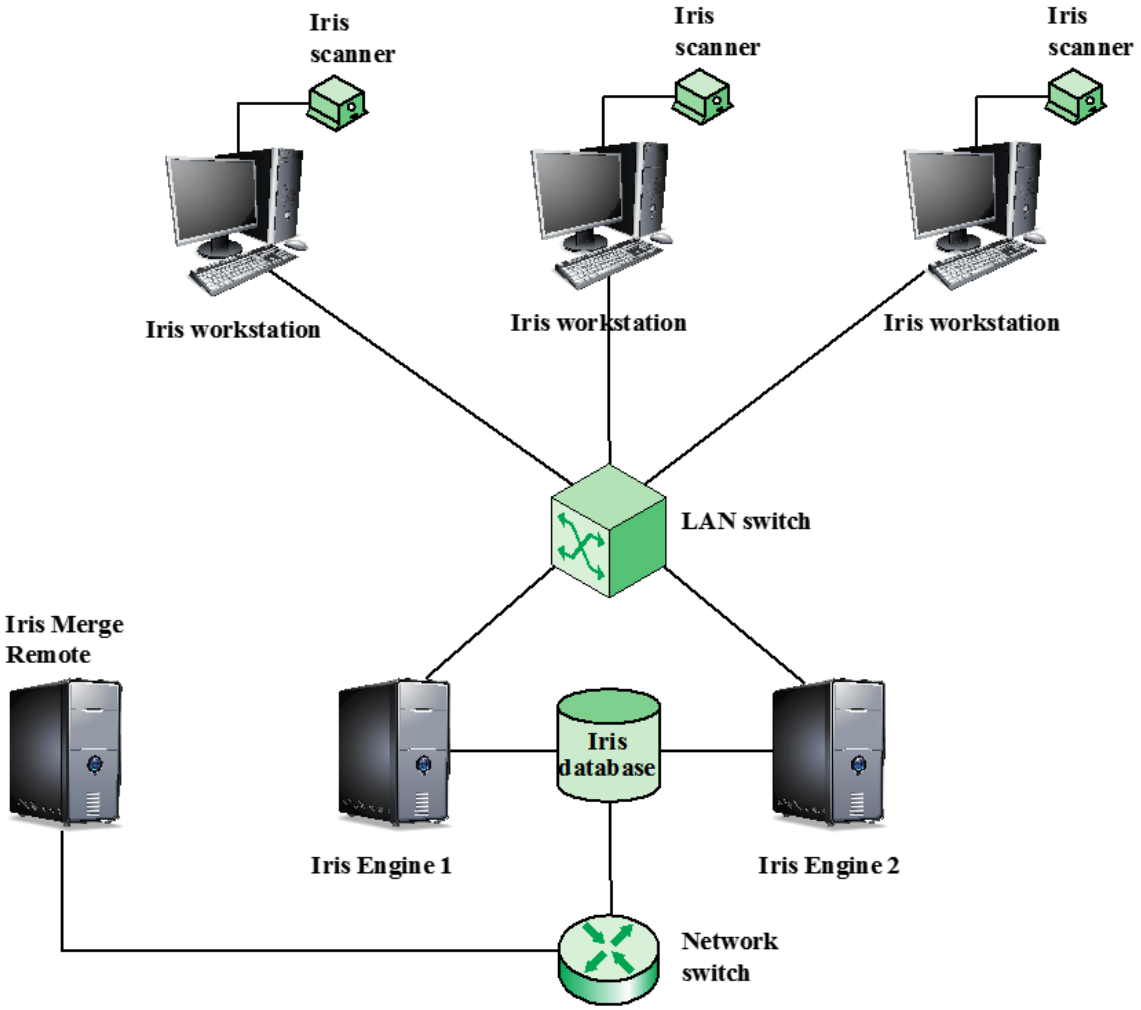
- 트로이 목마 공격
  - 같은 응용프로그램 및 하드웨어 장치에 대한 공격은 사용자의 입력 정보를 캡처하는 방식을 사용함
  - 공격자는 확보한 정보를 사용해 합법적인 사용자로 가장해 시스템에 접근이 가능함

- 서비스 거부 공격
  - 다량의 인증 시도를 발생시켜 사용자 인증서비스를 마비시키는 공격임
  - 발전된 공격은 특정 사용자의 로그인 오류를 임계 값 이상으로 발생시켜 해당 사용자가 로그아웃 되도록 만듦
  - 토큰을 포함한 여러 요소의 인증 프로토콜이 이러한 공격을 약화 시킬 수 있음

실용 응용프로그램: 홍채 인식 시스템

- 아랍에미리트(UAE)에서 개발, 국경 검문소에서 사용하는 홍채 인식 시스템
  - 생체 인식 시스템의 요구사항
  - 많은 사람들 중에서 특정 사람 식별
  - 시간에 따라 변하지 않은 생체 특징 사용
  - 사용이 용이함
  - 많은 응용프로그램에 대해 실시간으로 반응
  - 억 단위 비교가 가능하고 최고의 성능을 유지
  - 비용이 경제적

- 홍채 인식 스캔 사이트 구조

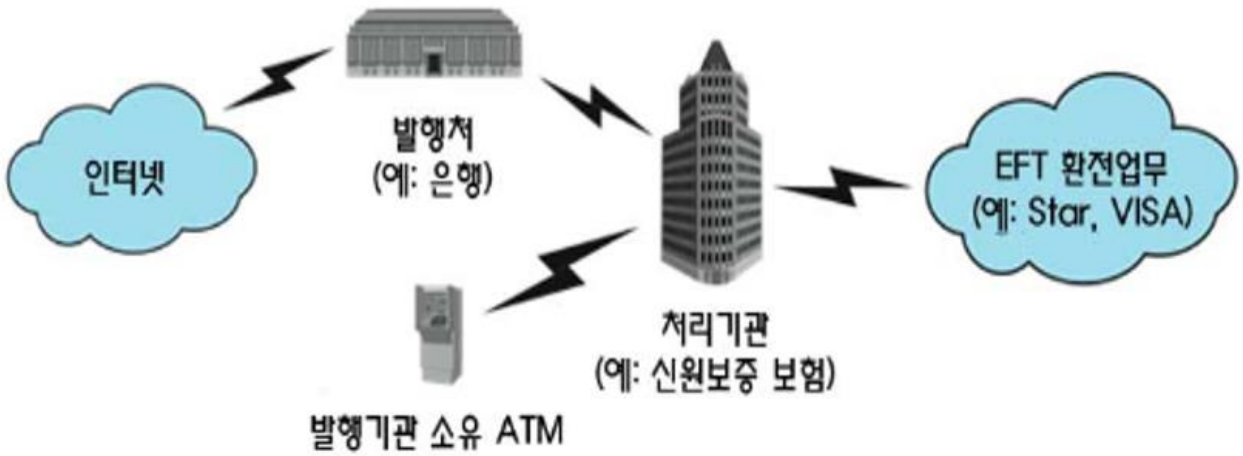


- 홍채 인식 시스템의 원리
  - 시스템 구현은 등록과 신원검사를 포함, 추방된 외국인은 등록 센터에서 홍채 스캔
  - 스캔 정보는 중앙의 데이터베이스 집결
  - 홍채 인식 카메라는 5~24인치의 흑백사진을 찍고, TV원격제어와 유사한 침해되지 않은 적외선 조명을 사용
  - 사진 소프트웨어
    - 우선 홍채 부분 추출 - 내외부 경계, 눈꺼풀의 형태를 찾아냄
  - 홍채 표면에 대해 DNA순서 코드와 유사한 상 코드를 생성
  - 홍채의 고유한 특성은 이 코드에 담겨 있으며 스캔된 홍채들의 데이터베이스에서 검색됨
  - 분산된 네트워크를 통해 모든 방문자의 홍채 코드는 실시간으로 중앙의 데이터베이스에서 검색됨

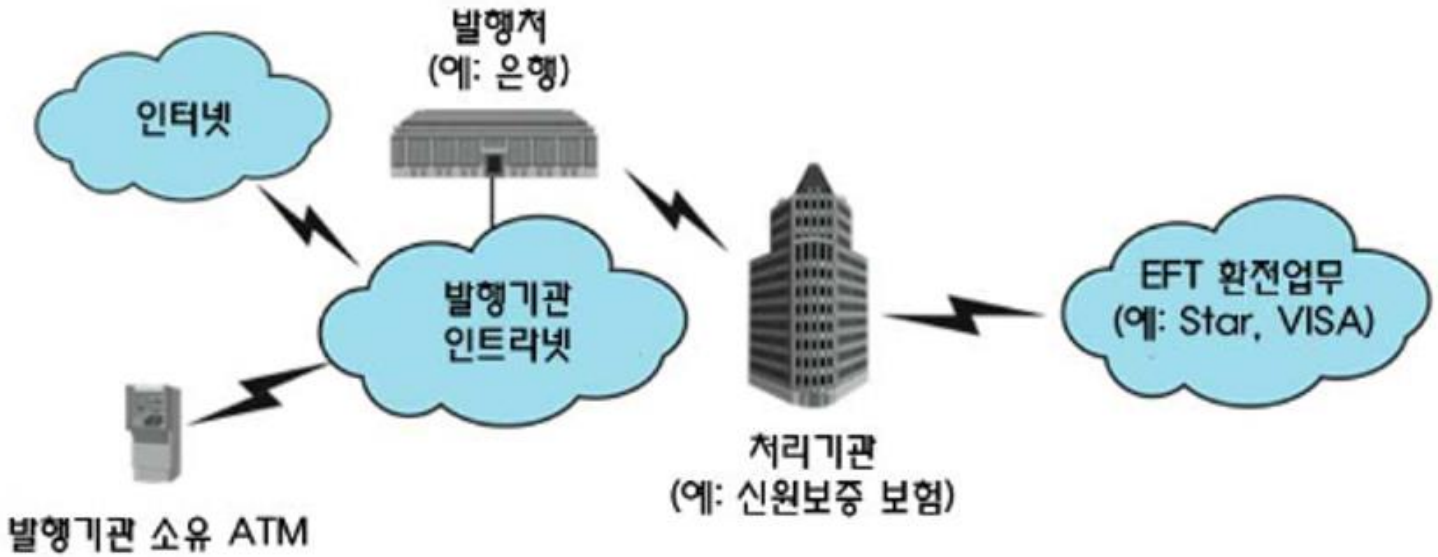
사례 연구: ATM 시스템 보안 문제

- Redspin사의 ATM(automated teller machine)사용 보안 취약점 설명 보고서
  - 카드소유자: 직불카드가 발행된 개인, 일반적인 카드 사용에 따른 지불에 대한 책임이 있음
  - 발행자: 카드소유자에게 직불카드를 발행하는 기관
  - 발행기관: 카드 사용자의 계좌와 모든 은행 관련 업무에 대한 책임
  - 처리자: 핵심 데이터 의 처리 및 전자송금(EFT)같은 핵심 데이터 처리 서비스를 발행자에게 제공하는 기관
    - EFT는 발행자가 POS장비와 ATM들을 연결하는 지역과 국가 네트워크에 접근가능

- ATM 시스템의 구성



  - ATM은 ATM을 소유한 발행자 보다 처리자와 임대 혹은 가상 라인으로 직접 연결
  - 전용 라인 사용 : 유해한 데이터로부터 가로채기를 어렵게 하고 보안성을 위해 추가적으로 메시지의 PIN부분이 ATM장비로부터 처리자로 DES로 암호화되어 전송
  - 처리자는 카드 사용자가 어떤 ATM에서도 계좌에 접근 할 수 있도록 EFT와 연결
  - 사용자가 자신의 카드를 사용하고 PIN을 입력
  - ATM은 PIN을 암호화하고 허가요청의 일부로 처리자에게 전송
  - 처리자는 고객의 정보를 갱신하고 응답을 보냄



- 발행자는 통상적으로 자신의 인터넷이 연결된 TCP/IP를 사용하는 랜과 인트라넷을 운용

- ATM을 발행자 네트워크 연결하고 처리까지 단일 전용 라인을 유지
  - 발행자가 매달 비싼 회선 비용을 절약하고 발행자가 ATM관리를 용이하게 함

- ATM시스템의 취약점
  - 기밀성: 카드 번호, 만료일, 계좌 잔액 등은 온라인 구매나 서명 기반의 트랜젝션을 위한 복제카드 생성에 사용될 수 있음
  - 무결성: 데이터 변조 같은 공격자의 공격을 차단할 수단이 없음
  - 만약 공격자가 전송되는 메시지를 캡처할 수 있다면,
    - 공격자는 ATM이나 처리자로 가정 가능
    - 공격자는 처리자가 트랜젝션이 발생했다는 사실을 모르게 ATM이 돈을 지급 할 수도 있음
  - 공격자가 사용자 계좌 정보와 암호화된 PIN을 캡처 한다면,
    - ATM 장비의 암호화 KEY가 변경되기 전까지 공격자는 계좌 잔액을 수정하거나 수정된 정보 전송 가능