정보 보안

유튜브 주소 : https://youtu.be/3rbfjjS-SDU

전자 문서

사용자 인증

침입 탐지

전자 문서

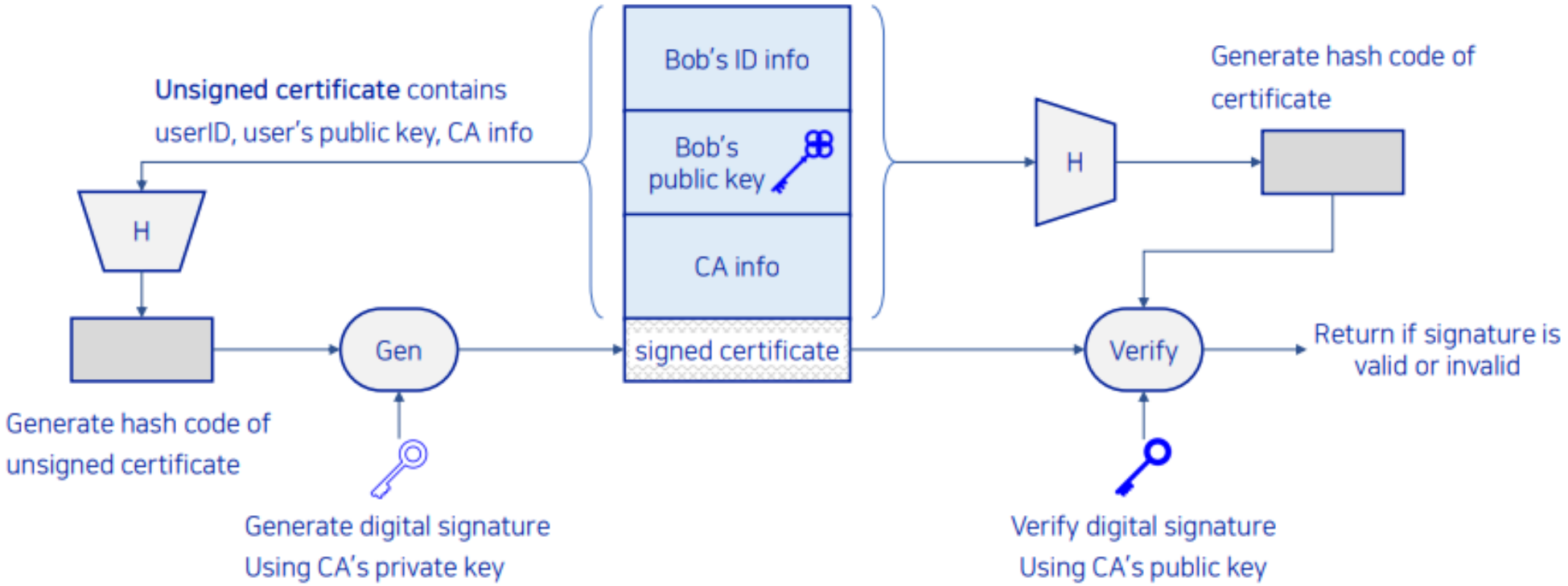
전자 서명

- 서명자가 전자 문서에 서명했다는 사실을 나타내기 위함
- 데이터의 무결성 증명 및 인증과 부인 방지를 위하여 사용
- 기본 개념
  - 송신자의 개인키로 서명하고 공개키로 검증
- 조건
  - 위조 불가
  - 서명자 인증
  - 부인 방지
  - 변경 불가
  - 재사용 불가

전자 문서

공개키 인증서

- 공개키의 소유권을 증명하는 데 사용되는 전자 문서

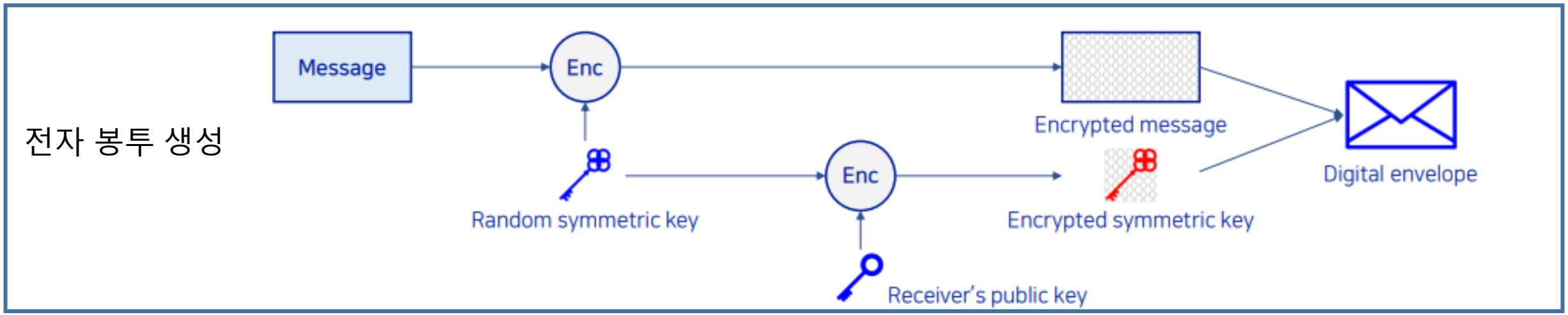


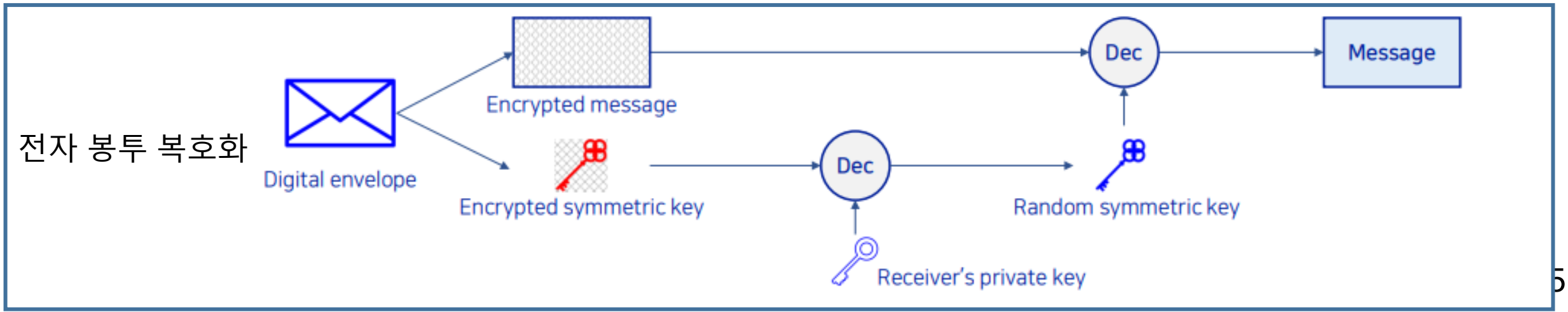
서명된 디지털
인증서 생성

Bob의 공개키를
이용한 인증서 검증

전자 문서

- 전자 봉투
- 송신자의 비밀키를 암호화한 전자 문서





사용자 인증

- 인증 수단

범주	예시
알고 있는 것	비밀번호, 개인 식별 번호(PIN), 사용자가 미리 정한 질문에 대한 답변 등
소유하고 있는 것 (토큰)	전자키 카드, 스마트 카드, 물리적 키 등
개인인 것 (정적 생체 인식)	지문, 망막, 홍채 인식, 안면 인식 등
개인이 하는 것 (동적 생체 인식)	음성 패턴, 필적, 보행 패턴, 립 무브먼트, 타이핑 패턴 등

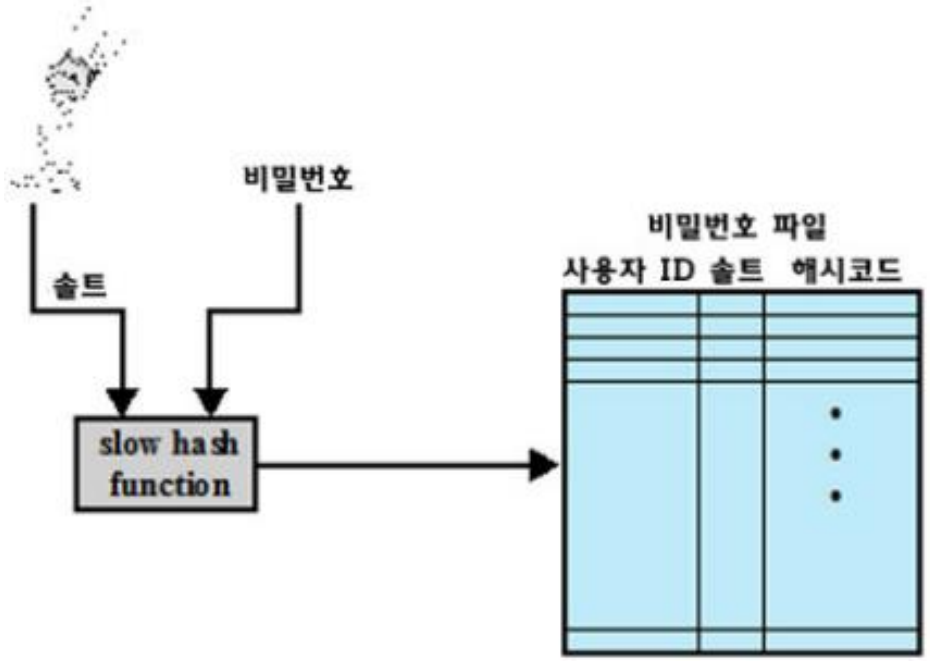
사용자 인증

- 비밀번호 기반 인증
  - 일반적으로 널리 알려진 침입자 방지 수단
  - 시스템에 저장된 비밀번호를 입력된 비밀번호와 비교하여 인증
  - 비밀번호 서버는 시스템에 접속하는 사용자의 ID를 인증
  - ID 보안
    - 사용자가 시스템에 접근이 허가되었는지 결정
    - 사용자 권한을 결정
    - 임의 접속 제어로서 사용(접근 여부를 관리)

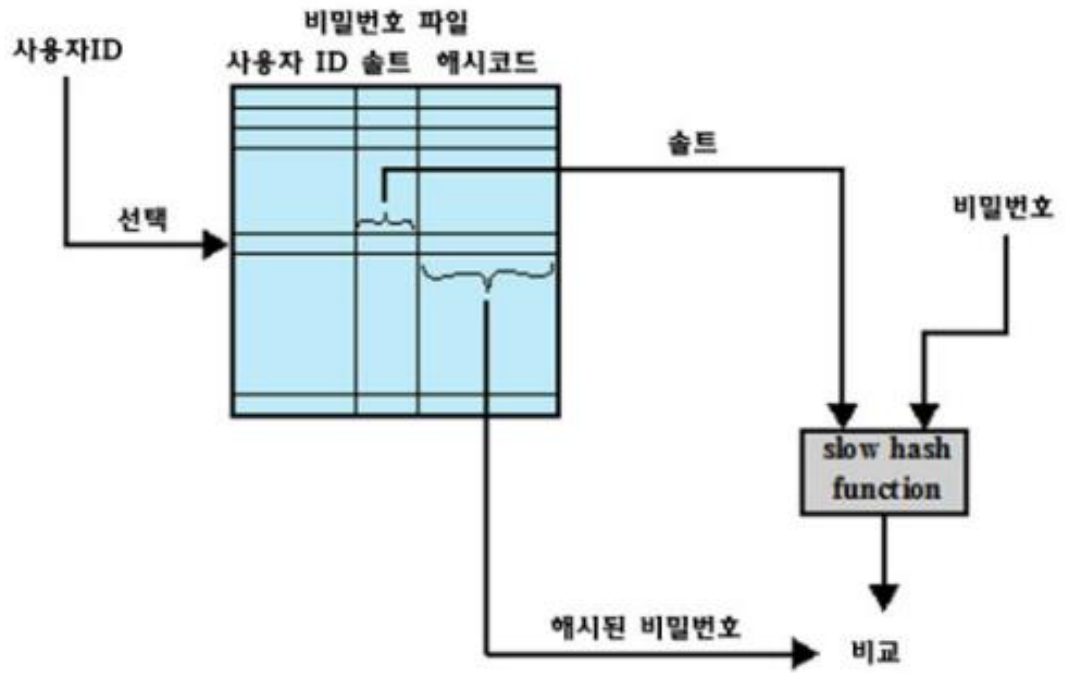
사용자 인증

- 비밀번호 기반 인증

UNIX 비밀번호 방식



새로운 비밀번호 적재



비밀번호 검증

사용자 인증

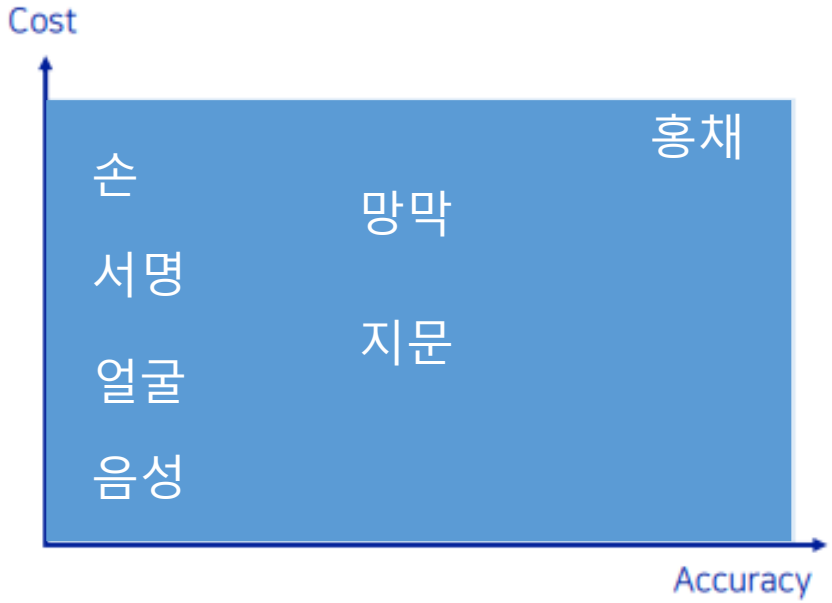
- 토큰 기반 인증
  - 토큰 -> 사용자 인증 목적을 위해 사용자가 소유한 객체

  - 토큰으로 사용되는 카드 유형

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

사용자 인증

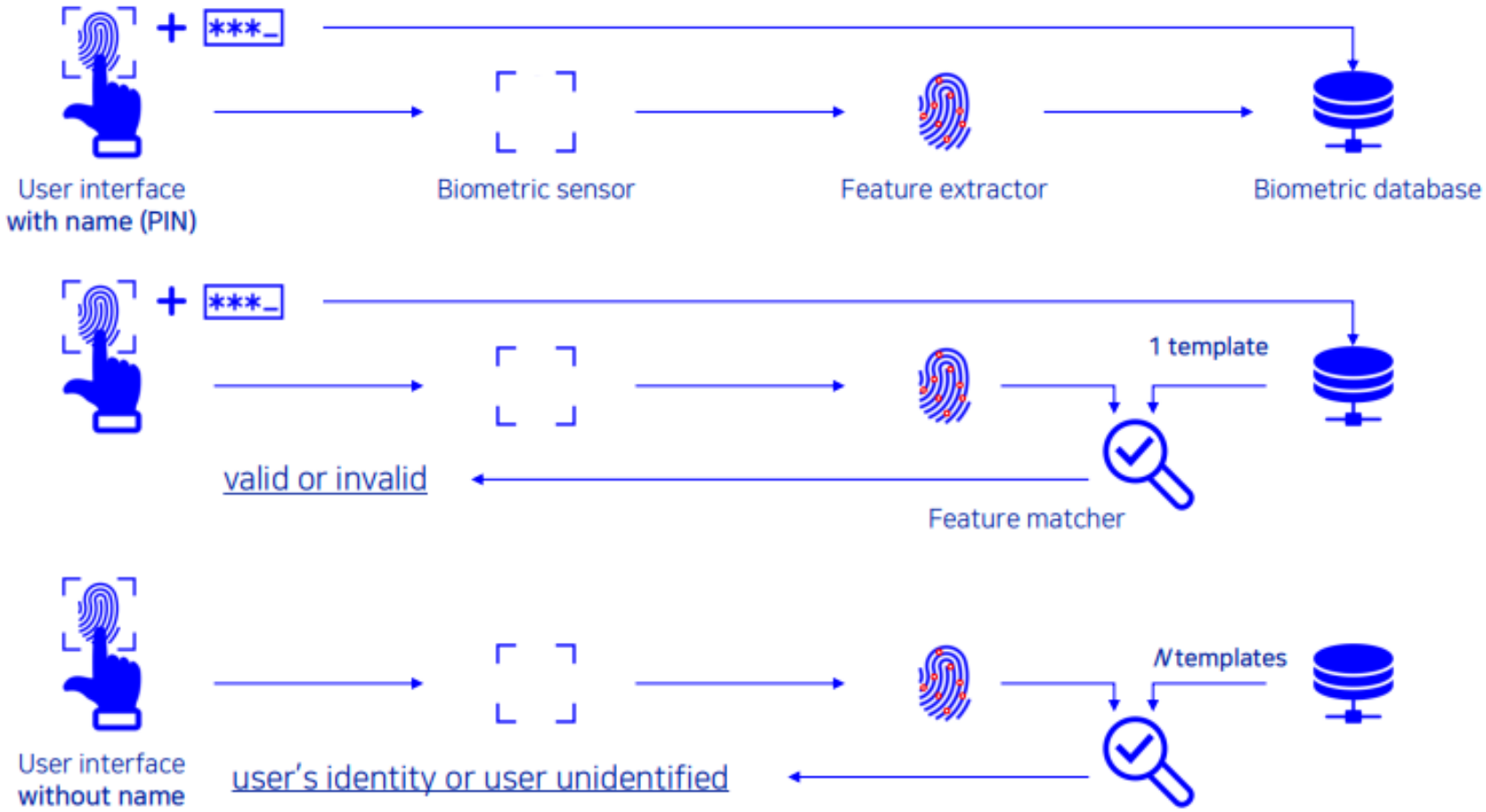
- 생체 인식 인증
  - 신체의 특징을 사용해 개인을 인증
  - 비밀번호, 토큰과 비교했을 때 기술이 복잡하고 비용이 많이 듦
  - 최근엔 정확성 많이 높아짐
  - 주로 다른 인증 방법과 섞어 보안성을 높이는 데에 사용



생체 특성들의 비용 대 정확도

사용자 인증

- 생체 인식 인증

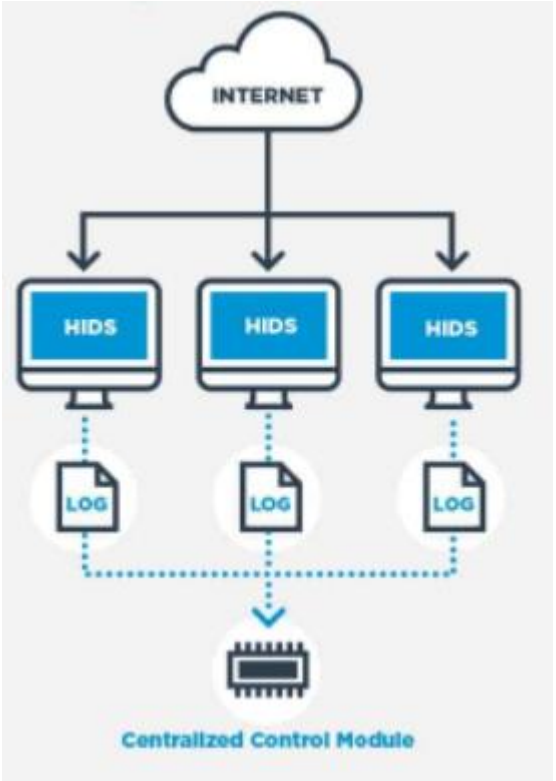


침입 탐지

- 침입자에 의한 해킹 –> 보안 위협 중 하나
- 침입 탐지 –> 해커에 의한 침입 공격을 탐지
- 센서 –> 데이터 수집 역할(침입 탐지의 기본적인 구성 요소)
- IDS -> 침입 탐지 시스템(Instrusion Detection System)
- 침입 탐지 대상에 따른 IDS 분류
  - 호스트 기반 IDS (HIDS)
  - 네트워크 기반 IDS (NIDS)
  - 분산 또는 하이브리드 IDS (Hybrid IDS)

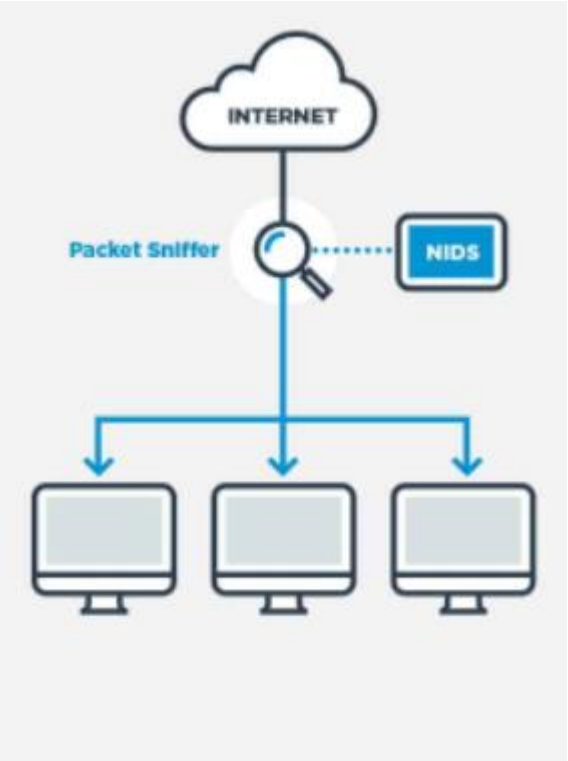
침입 탐지

- 호스트 기반 침입 탐지(HIDS)
- 호스트 자체에 설치되는 침입 탐지 시스템
- 대상 호스트만 분석 가능(네트워크 탐지X)
- 로그 분석, 프로세스 모니터링을 통해 침입 탐지
- 트로이목마 등의 탐지가 가능
- 보통은 NIDS와 섞어서 사용



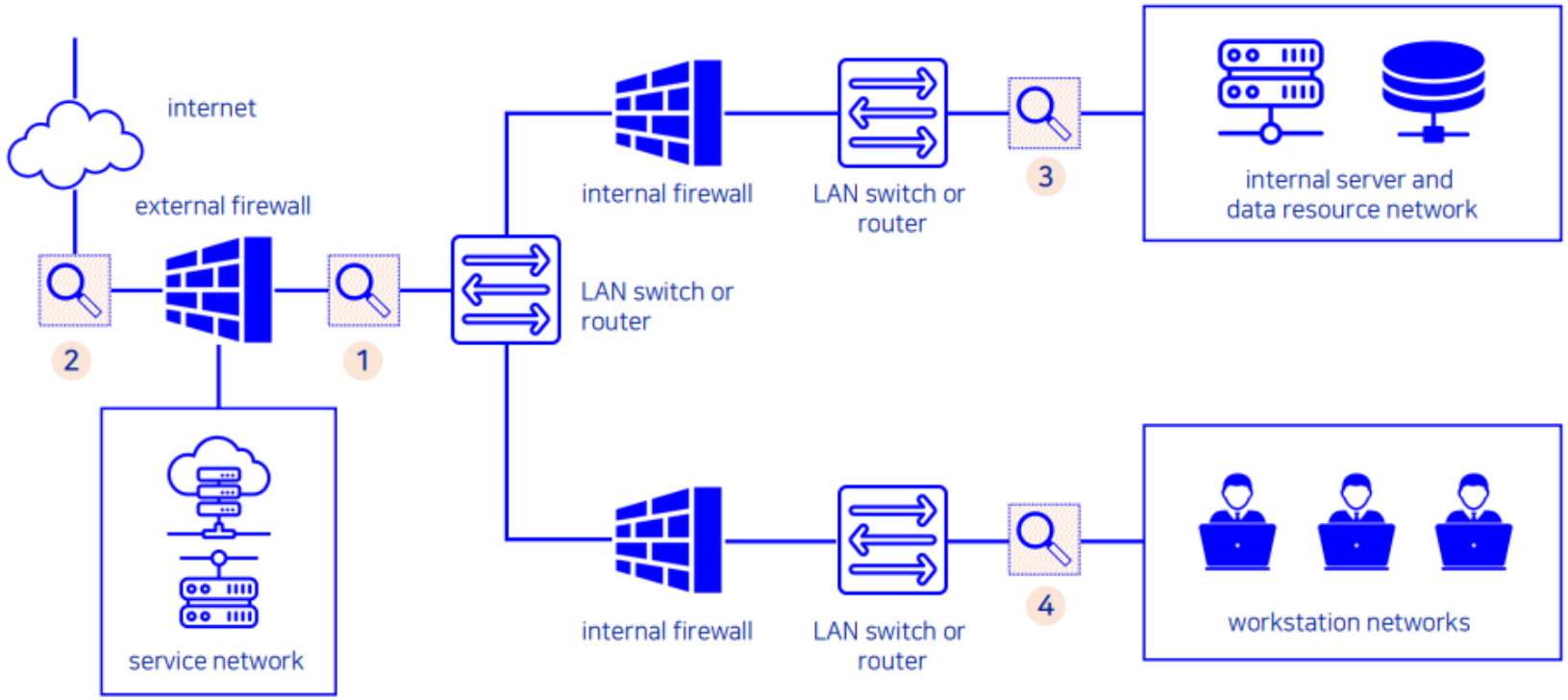
침입 탐지

- 네트워크 기반 침입 탐지(NIDS)
- 네트워크 패킷을 분석하여 침입 탐지
- 네트워크 침입에 대해 실시간 탐지 가능
- 3,4,5계층까지 폭 넓게 로그 수집
- NIDS 센서를 네트워크 상의 다양한 경로에 설치



침입 탐지

- 네트워크 상에서의 위치 별 NIDS 센서 배포 예시
  - 1. 외부 방화벽의 안쪽
  - 2. 외부 방화벽과 인터넷(혹은 WAN)의 사이
  - 3. 내부 방화벽의 안쪽 – 내부 서버나 DB 보호 목적
  - 4. 내부 방화벽의 안쪽 – 사적, 금융 네트워크 등 중요 시스템 추가 보호 목적



Q & A