쇼단(Shodan)

웹 사이트를 검색한 결과를 보여주는 일반적인 검색엔진과 달리 인터넷에 연결된 기기의 다양한 정보를 제공하는 검색엔진
라우터, 스위치, 특정 웹서버, CCTV 등 다양한 장비와 서비스에 대한 정보를 수집해 사용자에게 IP정보, 국가 정보, OS 정보, 포트 정보 등의 결과를 알려주는 검색엔진
각 기관에서 관리하는 장비와 서비스의 보안 취약점을 쉽게 파악할 수 있도록하기 위함이지만 이를 악의적인 목적으로 활용하는 문제점도 있다

인터넷(웹) 공간의 분류

1) 표층웹 : 일반적으로 사용하는 웹 브라우저를 통해 구글, 네이버 등의 검색엔진에 접속하여 검색어를 입력한 후 접근할 수 있는 일반인에게 공개된 웹 사이트 공간

2) 딥웹 : 표층웹과 달리 일반적인 검색엔진 사이트를 통해 검색되지 않는 비공개 인터넷 영역으로 개인 이메일, 회사 내부망, 유료 DB 사이트 등이 해당

3) 다크웹 : 딥웹의 일종으로 Tor, I2P 등 특수한 브라우저(소프트웨어)를 통해서만 접근이 가능한 웹으로 익명성 보장은 물론 IP주소 추적이 불가능하도록 고안된 인터넷 영역

PKI(공개키 기반 구조)

CRL(인증서 폐지 목록) : 인증서 유효기간 만료 전 폐지나 효력이 정지된 인증서 목록으로 사용자가 인증서의 유효성을 확인할 수 있도록 인증기관이 배포

OCSP : 사용자가 온라인으로 실시간 인증서 상태 정보를 확인할 수 있는 인증기관이 제공하는 서비스

<인증서 폐지 사유>
- 주체의 개인키가 유출되거나 손상되었을 때 주체의 요청 또는 인증기관의 직권으로 폐지
- 인증기관(CA)의 개인키가 유출되거나 손상되었을 때 인증기관은 서명한 인증서를 모두 폐지
- 인증기관이 주체를 더 이상 인증하지 않는 경우 인증서를 폐지

일련번호 : 인증기관별로 각 인증서를 식별하기위한 일련번호

서명 알고리즘 식별자 : 인증기관이 인증서 내용을 서명할 때 사용한 알고리즘 ID

주체 : 인증서 소유자에 대한 DN(Distinguish Name) 정보

발급자 : 인증서를 발급한 인증기관의 DN(Distinguish Name) 정보

서명 : 인증기관이 서명한 서명값

전자서명을 통해 제공할 수 있는 보안 서비스

1) 메시지 무결성 : 서명자가 작성한 메시지가 위변조되지 않았음을 보장

2) 메시지 인증 : 메시지가 올바른 상대방이 보낸 것임을 보장

3) 부인 방지 : 메시지를 보낸 상대방이 나중에 자신이 보낸 메시지가 아니라고 부인하지 못하도록 보장

전자서명/디지털서명의 요구 조건

1) 위조 불가 : 서명자 외에는 서명값을 생성할 수 없어야 한다

2) 변경 불가 : 서명한 메시지의 내용을 변경할 수 없어야 한다

3) 서명자 인증 : 서명값을 통해서 서명자를 확인할 수 있어야 한다

4) 부인방지 : 서명자가 나중에 서명한 사실을 부인할 수 없어야 한다

5) 재사용 불가 : 생성한 서명값을 다른 메기지의 서명값으로 사용할 수 없어야 한다

스마트 OTP를 통한 인증방식의 동작 원리

스마트폰과 IC카드을 이용해 인증

고객은 거래 중인 은행에서 비밀번호 생성에 필요한 정보가 담김 IC카드를 발급받는다

금융 거래 시 기존의 보안카드나 OTP를 통해 생성된 숫자를 입력하는 대신, 거래 은행에서 발급받은 IC카드를 스마트폰에 접촉하면 자동으로 숫자가 생성되어 입력된다
이때 스마트폰은 전용 앱이 설치되어야 하고, NFC(근거리 무선통신)가 지원되어야 한다

용어

토르(Tor) : 분산 네트워크 기반의 익명의 인터넷 서비스

프록시(Proxy) : 클라이언트와 서버 사이에서 자신을 통해 다른 네트워크 서비스에 간접적으로 접속할 수 있도록 중계해주는 방식