정보보안의 핵심 3요소(CIA)

* 기밀성(Confidentility) : 정보는 인증된 대상만 접근할 수 있어야 한다.
* 무결성(Integrity) : 정보의 변경은 허가된 사람이 인가된 매커니즘을 통해서만 이루어져야 한다.
* 가용성(Availability) : 정보는 필요할 때 언제든지 사용할 수 있어야 한다.(정해진 방법대로 처리되었을 때)[이를 악용한 것이 DDoS]

정보 보안 서비스

* CIA(기밀성, 무결성, 가용성)
* 인증(Authentication)
  + 컴퓨터 보안에서 허가된 사람이 맞는지 확인하는 시도
  + 인증의 수단 : 지식(비밀번호), 소유(OTP), 신체(지문, 홍채, 정맥 등등)
  + 2단계 인증(2 Step Authentication)
* 부인 방지
  + 전제 : 메시지의 송수신이나 교환 후 또는 통신이나 처리가 실행된 후
  + 그 사실을 사후에 증명함으로써 사실 부인을 방지하는 서비스

공격 기법

[3가지 길을 통해 하나의 세션을 만들게끔 함]

* 세션 하이제킹 : 로그인 된 상태를 가로채 별도의 인증 없이 시스템에 접근하는 공격 / 기밀성, 무결성 훼손
* DDoS(Distributed Denial of Service)
  + 서비스 거부 공격의 일종 / 가용성 훼손
  + 악성 코드나 바이러스 등의 악의적인 프로그램들을 통해서 많은 수의 일반 사용자 PC를 감염시켜 좀비PC로 만든 다음 한번에 시스템에 서비스를 요청하여 시스템의 가용성을 떨어트려 원래 의도된 용도로 사용하지 못하게 하는 공격이다.

에러 검출

* 패리티 비트
* 전송하는 데이터에 1bit를 패리티비트로 설정해 미리 결정해놓은 홀짝과 맞을 경우 데이터가 정상적으로 전송된 것으로 간주

체크섬(CheckSum)

* 데이터를 일정 크기로 분리한 다음 그 합계값을 이용해 데이터의 무결성을 보장한다.

해시 함수(Hash)

* 데이터를 정해진 크기의 유니크한 요약본으로 만들어주는 함수

해시 함수의 요구 사항

* 같은 데이터에 대해서는 항상 같은 결과가 나와야 한다.
* 원본 데이터의 약간의 변화만 있어도 완전히 다른 결과가 나와야 한다.
* 해시 함수의 결과로 원본 데이터의 복구가 불가능해야 한다.

해시 충돌

* 서로 다른 입력 값을 넣었음에도 불구하고 같은 출력 값이 나온 경우

암호화 용어

* 평문(Plain Text) : 암호화되지 않은 데이터
* 암호문(Cipher Text) : 평문을 암호화 처리해서 다른 사람이 알아보지 못하게 만든 데이터
* 암호화(Encryption) : 평문을 암호문으로 변경하는 처리
* 복호화(Decryption) : 암호문을 평문으로 변경하는 처리

암호화 알고리즘

* 대칭키 알고리즘
  + 데이터를 암호화/복호화 할 때 특정한 키값을 사용하여 암호화하고 복호화 할 수 있다.
  + DES, TripleDES, AES 등등
  + 키 배포문제
* 공개키 알고리즘
  + 암호화에 사용하는 키와 복호화에 사용되는 키가 서로 다르다.
  + 개인키와 공개키
  + 암호화 및 부인방지에 사용된다.
  + 개인키 : 본인만 알고 있는 값
  + 공개키 : 모두가 알고 있는 키 값
* RSA : 컴퓨터로 소인수분해가 어렵다는 것에 기반을 둔 공개키 기반의 암호화 알고리즘
  + 암호화, 디지털 서명을 통한 부인방지 제공
  + 대표적인 트랩도어 알고리즘