정보보호

정보보안

무결성

> 메시지 변조 방지

- 정보가 허가되지 않은 방식으로 바뀌지 않는 성질

기밀성

> 허가된 사용자 이외에 암호 해독 불가

- 암호화는 기밀성을 위한 기술

가용성

부인방지

> 송수신 사실 부정 방지

- 전자서명은 부인방지를 위한 기술

인증성

- MAC은 인증을 위한 기술

암호학

암호시스템

- 세 가지 충족 요건
    - 암호화 키에 의해 암호화 및 복호화가 효과적
    - 암호화 키는 반드시 블록 암호나 스트림 암호로 구성되어 있어야 한다.
    - 암호 시스템은 사용이 쉬워야
    - 알고리즘 자체보다는 암호화 키에 의해 보안이 이루어져야

대칭키(=비밀키=관용암호) 암호 시스템(DES: Data Encryption Standard)

- 키의 교환 문제 발생
- SSL과 같은 키 교환 방식 사용.
- DES 암호 알고리즘
    - 1970년대 초 IBM 사가 개발한 알고리즘
    - 64비트 블록 암호 알고리즘
    - NIST + NSA가 개발에 참여
    - 암호화 방식의 전자 코드북과 암호피드백으로 이루어졌다.
- AES 암호 알고리즘
    - SPN방식 사용

비대칭키(=공개키) 암호 시스템

- 하나의 알고리즘으로 암호화 복호화 키 쌍을 수행한다.
- 송신자는 공개키, 수신자는 개인키를 알고 있어야 함.
- 전송할 때는 공개키, 해독할 때는 개인키(=비밀키)
- 부인 방지 서비스 제공
- 대표적인 예는 전자서명

RSA

- Rivest 암호화, Adleman이 개발함
- 전자 서명에 이용
- 계산량이 많음
- 키 길이가 길어지면 암,복호화 속도가 느려진다

구분	대칭키(비밀키)	비대칭키(공개키)
암호화 키와 복호화 키의 관계	동일	서로 다름
암호화 키	비밀	공개
복호화 키	비밀	비밀
키 분배	필요	불필요
키 개수	N(N-1)/2	2N
암호화 속도	고속	저속
경제성	높음	낮음
서비스	기밀성	기밀성, 부인 방지 인증
목적	데이터 암호화	대칭키 교환
전자 서명	복잡	간단
단점	키 교환	중간자 공격, 속도 느림
대표 알고리즘	DES, 3DES, AES, IDEA	RSA, ECC, RC4, NTRU
키의 길이	짧다	길다

	AES	RSA
암,복호화 속도	빠르다	느리다
키 길이에 따른 속도		키길이가 길어지면 느려짐

보안 기법

전자 서명

- 위조 불가
  - 서명자만이 서명문 생성
- 재사용 불가
  - 서명문의 서명은 다른 문서의 서명으로 사용 불가능
- 변경 불가
  - 서명된 문서의 내용 변경 불가능
- 부인 불가
  - 서명자는 서명한 사실을 부인
- 전자 서명의 서명자를 누구든지 검증할 수 있어야

디지털 서명

- 부인방지를 위해 사용
- 디지털 서명 생성에는 개인키를 이용하고 검증할 때는 공개키를 사용

기타 보안 기술

스테가노그래피

- 암호화와 함께 이 기법을 사용해 보안 수준을 높이는 데 의의가 있음
- 기밀 정보를 그래픽, 사진, 영화, 소리 파일 등에 암호화해 숨기는 심층 암호 기술
- 전송하고자하는 정보를 작은 글자로 위장하여 숨겨 전송하는 데 주로 이용

워터마크

- 지폐 위조 방지, 불빛에 비추었을 때 그림이나 문자 확인 가능
- 저작권 정보를 인식하지 못하게 디지털 콘텐츠에 삽입

핑거프린팅

악성코드 및 해킹 기법

악성코드 = 말웨어

> 악의적 목적으로 만들어진 모든 프로그램(프로그램, 매크로, 스크립트 등)

- 사회 공학적 공격

  > 시스템이 아닌 사람의 감성이나 특성을 자극하는 공격. 즉 사람의 취약점을 공격하는 기술이다.

  - 피싱
  - 파밍
  - 스미싱
  - APT(Advanced Persistent Threat) 공격

- 트로이목마

  > 어떤 침입 행위를 하기 위해 일정 시간 위장 상태로 유지하며, 코드 형태로 시스템의 특정 프로그램 내부에 존재하는 것.
  >
  > 해킹 기능을 가진 악성 프로그램

- 스파이웨어/에드웨어

  > 사용자의 허가 없이 사용자의 컴퓨터에 설치되어 사용자의 정보를 빼가거나 컴퓨터의 입출력을 읽어서 정보를 수집.

- 랜섬웨어
- 스미싱

  > 사용자를 속이는 문구에 링크를 포함하여 클릭하면 사용자의 정보를 탈취하거나 소액결제를 유도함

- 피싱

  > 유명 기관이나 금융기관을 사칭한 채 웹 사이트나 이메일 등으로 사용자의 금융 정보를 빼내어 예금 인출 및 다른 범죄에 이용하는 행위.

- DoS

  > 분산 서비스 공격

  - 특정 서버의 서비스 기능을 마비시켜서 다른 정당한 클라이언트가 서비스 제공을 받지 못함
  - 공격의 원인이나 공격자를 추적하기 힘듦
  - 사용자의 실수로 발생할 수도
  - 시스템의 자원을 부족하게 함
  - 라우터, 웹, 전자 우편, DNS 서버 등 모든 네트워크 장비를 대상으로 이루어질 수 있다.
  - 취약점 공격형
    - Boink
    - Bonk
    - TearDrop 공격
    - Land 공격
  - 자원 고갈 공격형
    - Ping Of Death 공격
    - SNY Flooding 공격
    - Smurf 공격
    - Mail Bomb 공격
  - DDoS 공격형
    - 여러 지점의 pc좀비를 만들어 특정 시간에 한 지점 서버에 공격.

- DDoS

  > 다수의 시스템을 통한 DoS 공격

- 루트킷

  > 루트 권한을 획득하여 시스템 장악

- SYN 플러딩

> TCP 프로토콜의 3 Ways Handshaking 방식으로 통신을 수행하는데 이때 SNY만 수행하고 SNY+ACK을 수행하지 않아 Half Open 상태로 만들어 백로그 큐를 증가시켜 특정 포트의 서비스를 거부 상태로 만드는 공격.

- 스머프 공격

  > 네트워크 상에서 어떤 호스트의 서비스를 방해하는 서비스 거부 공격 방법.

- 백도어

  > 시스템 정보 유출과 루트 권한 획득

  - 넷버스
  - 백오리피스
  - 루트킷

    > 공격자가 시스템에 사용자 몰래 침입하기 위해 설치해 둔 프로그램으로, 백도어, 원격 접근 프로그램, 침입 흔적 로그 삭제 프로그램 등으로 구성.

- 스푸핑(=Spoofing)

  > 속이다, 사기치다라는 뜻. 외부의 악의적 네트워크 침입자가 웹 사이트를 구현해 해당 방문을 유도하여 웹 사이트 사용자의 정보를 빼가는 수법.

- IP Spoofing

  > 인터넷 프로토콜인 TCP/IP 프로토콜의 결함.
  >
  > 즉, TCP 시퀀스 번호, 소스 라우팅, 소스 주소를 이용한 인증 메커니즘을 통한 방법. 인증 기능이 있는 시스템에 침입하기 위해 침입자가 사용하는 시스템을 원래의 호스트로 위장하는 방법.

- 스니핑(Sniffing)

  > 지나가는 패킷 흐름에 로그인, 패스워드 등을 유출

- 파밍

  > 피싱 기법 중 하나. 사용자가 자신의 웹 브라우저에 정확한 주소를 입력해도 가짜 웹 주소로 접속하게 하여 개인정보 탈취

- TCP 래퍼(Wrapper)

  > 네트워크 서비스에 관련한 트래픽을 제어하고 모니터링을 할 수 있는 unix 기반의 방화벽, 서비스를 요청해 오면 접속 가능한지 확인하여 로그를 남기고, 허가되지 않은 접근일 경우 차단.

- Exploit 공격 = 취약점 공격

  > 소프트웨어나 하드웨어에 공격자가 설계해 놓은 버그를 수행하도록 만들어진 절차나 명령어

- SQL Injection

  > 웹 서비스가 예외적인 문자열을 필터링 하지 못하도록 sql을 변경하거나 조작함

- XSS(Cross Site Scripting) 공격

  > 공격자에 의해 작성된 악의적 스크립트가 게시물을 열람하는 다른 사용자에게 전달되어 실행되는 취약점을 이용한 공격.

- KRACK

> WPA2를 공격하기 위한 방식. WPA2의 4-way 핸드셰이크 과정에서 메시지를 조작하고 재전송하여 정보를 획득하는 공격 방식

- SSL stripping

> Moxie Marlinspike가 제안한 공격방식, 중간자 공격을 통해 사용자와 서버 사이에 https 통신을 http로 변경해서 비밀번호 등을 탈취해서 공격하는 방식

번외

- 개인정보 보호법
  - 개인정보
    - 살아있는 개인에 관한 정보, 성명, 주민등록번호 및 영상 등을 통해 개인을 알 수 있는 정보
  - 정보주체
    - 처리되는 정보로 알아볼수 있는 사람으로서 그 정보의 주체가 되는 사람
  - 처리
    - 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그밖에 유사한 행위
  - 개인정보 처리자
    - 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통해 개인정보를 처리하는 공공기관, 법인, 단체 및 개인
- FDS(=이상금융거래탐지시스템)
  - 전자금융거래에서 사용되는 단말기 정보, 접속 정보, 거래 내용 등을 종합적으로 분석하여 이상 거래를 탐지하고 이상금융거래 차단
  - 보안 프로그램에서 방지하지 못하는 전자금융사기에 대한 이상거래를 탐지하여 조치를 취할 수 있도록 함
- 망분리 기술
  - OS 커널 분리
  - VDI
  - 가상화기술