Computer Science 정리

3. 보안

1. 암호화 방식

- 대칭 암호화 방식

DES(Data Encryption Standard) 알고리즘	- DES는 64비트의 블록 암호화 알고리즘으로 56비트 크기의 암호화 키로 암호화.
트리플(triple) DES 알고리즘	- 암호화 및 복호화 과정 DES와 달리 암호화키 2개 사용
AES(Advanced Encrytion Standard) 알고리즘	- DES의 암호화 강도가 점점 약해지면서 새롭게 개발된 것 - 향후 30년 정도 사용 가능 보안성, 128비트 암호화 블록 - 다양한 키 길이를 갖출 것이라는 공모 조건으로 선정
SEED 알고리즘	- 전자상거래, 금융, 무선통신 등에서 전송되는 중요한 정보 보호를 목적으로 순수 국내 기술로 개발 - 128비트 블록의 암호화 알고리즘
ARIA 알고리즘	- 전자정부 구현을 목적으로 개발 - AES 알고리즘과 같이 128/192/256 비트 암호화 키 지원
기타 대칭형 알고리즘	- IDEA /RCS /skipjack / LEA 알고리즘

- 비대칭 암호화 방식

- 암호화 키 전달을 위한 비대칭 키의 동작 아이디어

RSA 알고리즘 (연구자 3인의 이름)	- RSA 암호는 기본적인 정수론,즉 소수를 이용하는 것 - RSA 암호의 아이디어는 중요 정보를 소수 2개로 표현한 후 두 소수의 곱을 힌트와 함께 전송하여 암호로 사용 - RSA 알고리이 나오면서 정립된 비대칭 암호화 알고리즘은 각 개인이 공개 키와 개인 키를 공유하는 구조.
특징	- 비대칭 암호화 알고리즘에서는 언제나 한 쌍의 개인 키와 공개 키로 암호화와 복호화가 이루어짐
기능	- 기밀성 : 비대칭 암호화 알고리즘은 대칭 암호화 알고리즘 보다 더 엄밀한 기밀성을 제공 - 부인 방지 : 비대칭 암호화 알고리즘은 대칭 암호화 알고리즘에 없는 부인 방지(nonrepudiation) 기능 제공

- 해시(hash)

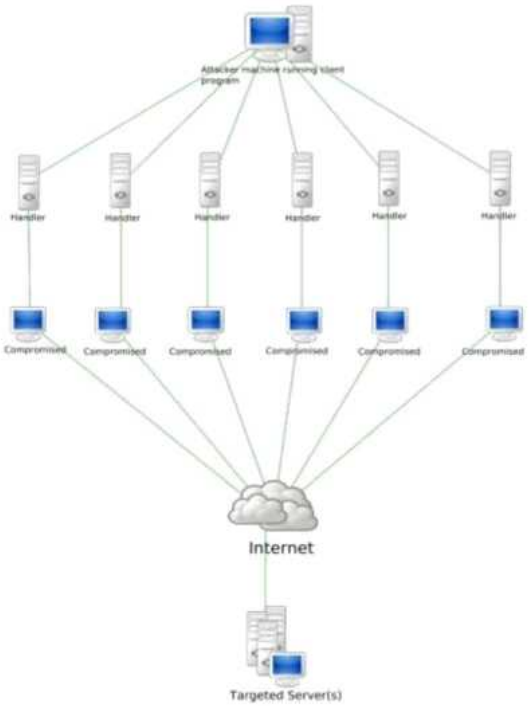
특징	- 해시(hash)는 하나의 문자열을 더 짧은 길이의 값이나 키로 변환하는 것 - 암호가 정보를 숨기기 위한 것이라면 해시는 정보의 위조/변조를 확인 - 즉, 정보의 무결성을 확인하기 위한 것 - 해시를 사용하여 전자서명,전자봉투,전자화폐 등 다양한 전자상거래 구현 - 대표적인 해시 알고리즘은 MDS가 있다.
역할	- 해시는 데이터베이스의 탐색을 효과적으로 구현하기 위해 만들어진 것. - 보안에서는 해시가 완전히 똑같은 데이터만 해시 값이 같고 조금만 달라도 해시가 전혀 다르다는 점을 이용 - 데이터가 임의로 변경되지 않았다는 데이터 무결성을 확인하기 위한 도구
종류	- MD 알고리즘 - MD(Message Design function 95) 알고리즘은 로널드 리베스트가 공개 키 기반 구조를 만들기 위해 RSA와 함께 개발한 것 - MD2 , MD4, MD5 가 있음 - SHA - SHA(Secure Hash Algorithm)는 160비트 값을 생성하는 해시 함수 - MD5보다 조금 느리지만 좀 더 안전하다고 알려져 있음 - SHA에 입력하는 데이터는 512비트 크기의 블록임 - SHA 알고리즘은 SHA-1 , SHA-2 로 나눌 수 있음

2. 분산 서비스 거부 공격(DDoS)

- 분산 서비스 거부 공격의 기본 구성

- 공격자(attacker) : 공격을 주도하는 해커 컴퓨터
- 마스터(master) : 공격자에게 직접 명령을 받는 시스템 , 여러대의 에이전트 관리
- 핸들러(handler)프로그램 : 마스터 시스템의 역할을 수행하는 프로그램
- 에이전트(agent) : 직접 공격을 가하는 시스템
- 데몬(demon)프로그램 : 에이전트 시스템의 역할을 수행하는 프로그램

*DDoS구성



*출처 : https://en.wikipedia.org/wiki/Denial-of-service_attack

3. 스니핑

- 스니핑 공격의 원리
  - 데이터 속에서 정보를 찾는 것으로 공격 시 아무것도 하지 않고 조용히 있는 것만으로도 충분하여 수동적 공격이라 함.
  - 스니핑 공격자는 가지지 말아야 할 정보까지 모두 볼 수 있어야 하므로 랜 카드의 프러미스큐어스(promiscuous)모드를 이용해 데이터 링크 계층과 네트워크 계층의 정보를 이용한 필터링을 해제함

- 스니핑 공격의 종류

스위치 재밍 공격	- 스위치가 MAC 주소 테이블을 기반으로 포트에 패킷을 스위칭할 때 정상적인 스위칭 기능을 마비시키는 공격, MACOF 공격이라고도함 - 고가의 스위치는 MAC 테이블의 캐시와 연산자가 쓰는 캐시가 독립적으로 나뉘어 있어 스위치 재밍 공격이 통하지 않음
SPAN 포트 태핑 공격	- 스위치의 포트 미러링(port mirroring)기능을 이용한 공격 - 포트 미러링 : 각 포트에 전송되는 데이터를 미러링하는 포트에도 똑같이 보내는 것 침입 탐지 시스템이나 네트워크 모니터링 또는 로그 시스템을 설치할 때 사용

- 스니핑 공격의 탐지

  - ping을 이용한 탐지
  - ARP를 이용한 탐지
  - DNS를 이용한 탐지
  - 유인을 이용한 탐지
  - ARP watch를 이용한 탐지

4. 스푸핑

- 스푸핑 공격의 종류

ARP 스푸핑 공격	- ARP 스푸핑은 MAC 주소를 속이는 것 - 로컬에서 통신하는 서버와 클라이언트의 IP주소에 대한 데이터 링크 계층의 MAC 주소를 공격자의 MAC 주소로 속여 클라이언트에서 서버로 가는 패킷이나 서버에서 클라이언트로 가는 패킷이 공격자에게 향하게 하여 랜의 통신 흐름을 왜곡하는 공격
IP 스푸핑 공격	- 트러스트 관계(신뢰 관계)를 맺고 잇는 서버와 클라이언트를 확인한 후 클라이언트에 서비스 거부 공격을 하여 연결을 끊은 뒤 클라이언트의 IP주소를 확보한 공격자는 실제 클라이언트처럼 패스워드 없이 서버에 접근하는 공격
ICMP 리다이렉트 공격	- 네트워크 계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알려 패킷의 흐름을 바꾸는 공격
DNS 스푸핑 공격	- 실제 DNS 서버보다 빨리 DNS response 패킷을 보내어 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격

5. 방화벽

- 방화벽 특징 및 설명

네트워크의 방화벽	- 보안을 높이기 위한 일차적인 방법 - 신뢰하지 않는 외부 네트워크와 신뢰하는 내부 네트워크 사이를 지나는 패킷 미리 정한 규칙에 따라 차단하거나 보내주는 기능을 하는 HW/SW
접근 제어	- 관리자가 통과시킬 접근과 거부할 접근을 명시하면 방화벽이 그에 따라 수행 - 구현 방법에 따라 패킷 필터링(packet filtering)방식 , 프록시(proxy)방식 - 접근 제어를 수행하는 룰셋(rule set)은 방화벽을 기준으로 보호하려는 네트워크의 외부와 내부에 존재하는 시스템의 IP주소와 포트로 구성
로깅과 감사 추적	- 방화벽은 룰셋 설정과 변경, 관리자 접근, 네트워크 트래픽의 허용 또는 차단과 관련한 사항을 로그로 남김
인증	- 방화벽에서는 메시지 인증, 사용자 인증, 클라이언트 인증 방법 사용 - 메시지 인증, 사용자 인증, 클라이언트 인증
데이터 암호화	- 한 방화벽에서 다른 방화벽으로 데이터를 암호화해서 보내는 방식
방화벽의 한계	- 바이러스는 파일 등을 통해 감염되므로 근본적으로 방화벽이 영향을 미치기 어려움 - 일부 웜은 막을 수 있지만 정상적인 서비스 포트에 대해 웜이 공격을 시도할 때는 막을 수 없음