16 정보보안

Section 1. SW개발 보안 설계

1. 정보보안

(1) 정보보안 개념

- 기업의 정보 및 정보 시스템에 대해서 허가되지 않은 접근, 변경, 삭제 등으로부터 보호하는 것
- 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적(정책, ISMS, PIMS), 기술적 방법(암호화, 접근통제, 데이터 백업)을 의미한다.

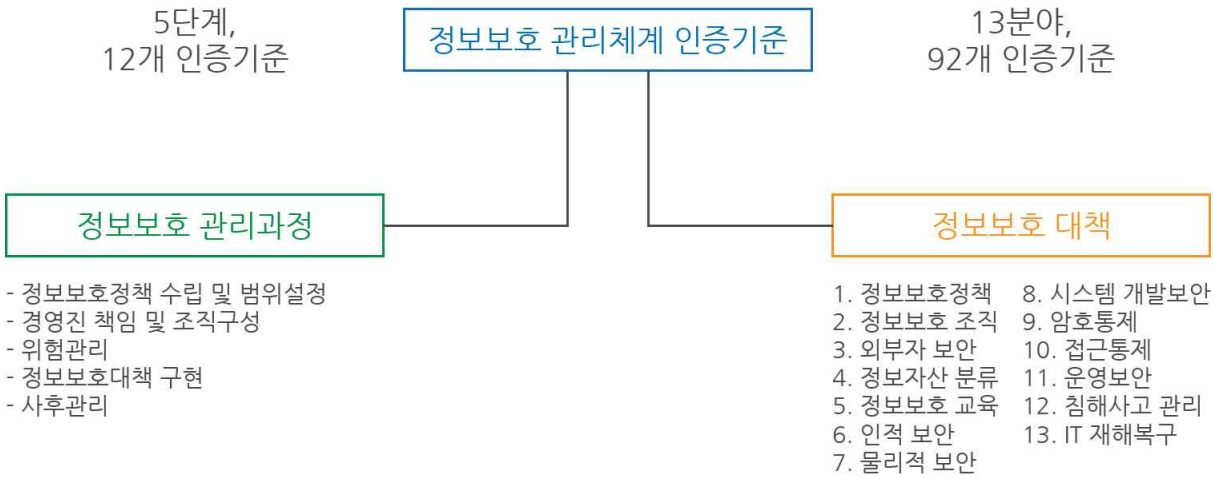
(2) 정보보안 요소

- 기밀성(Confidentiality)
  - 인가된 사용자만 정보 자산에 접근할 수 있도록 한다.
  - 방화벽, 암호 등
- 무결성(Integrity)
  - 적절한 권한을 가진 사용자가 인가된 방법으로만 정보를 변경할 수 있도록 접근 통제한다.
  - 시스템 내의 정보는 오직 인가된 사용자만 수정할 수 있어야 한다.
- 가용성(Availability)
  - 원하는 시점에 언제든 정보 자산에 접근이 가능하도록 한다.
- 인증(Authentication)
  - 접속한 사용자가 허가받은 사용자인지 확인하는 것
  - 전송된 메시지가 변조되지 않았는지 확인하는 것
- 부인방지(Non-repudiation)
  - 정보를 보낸 사람이 나중에 정보를 보냈다는 것을 발뺌(부인)하지 못하도록 하는 것

(3) 인증제도

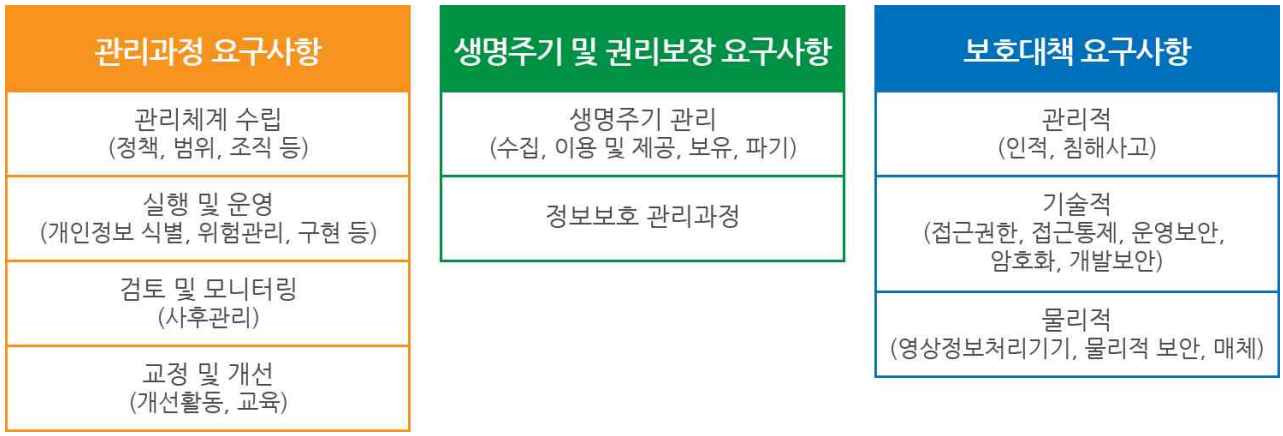
① ISMS(정보보호 관리체계 인증)

- 정보통신망의 안전성 확보를 위하여 수립하는 기술적, 물리적, 관리적 보호조치 등 종합적인 정보보호 관리체계에 대한 인증제도
- 기업 및 조직이 보유하고 있는 기업정보, 산업기밀, 개인정보 등의 중요한 정보자산이 안전하고 신뢰성 있게 관리되고 있음을 국가로부터 인증 받는 국가공인 제도
- 정보보호 관리체계 인증 구성 요소



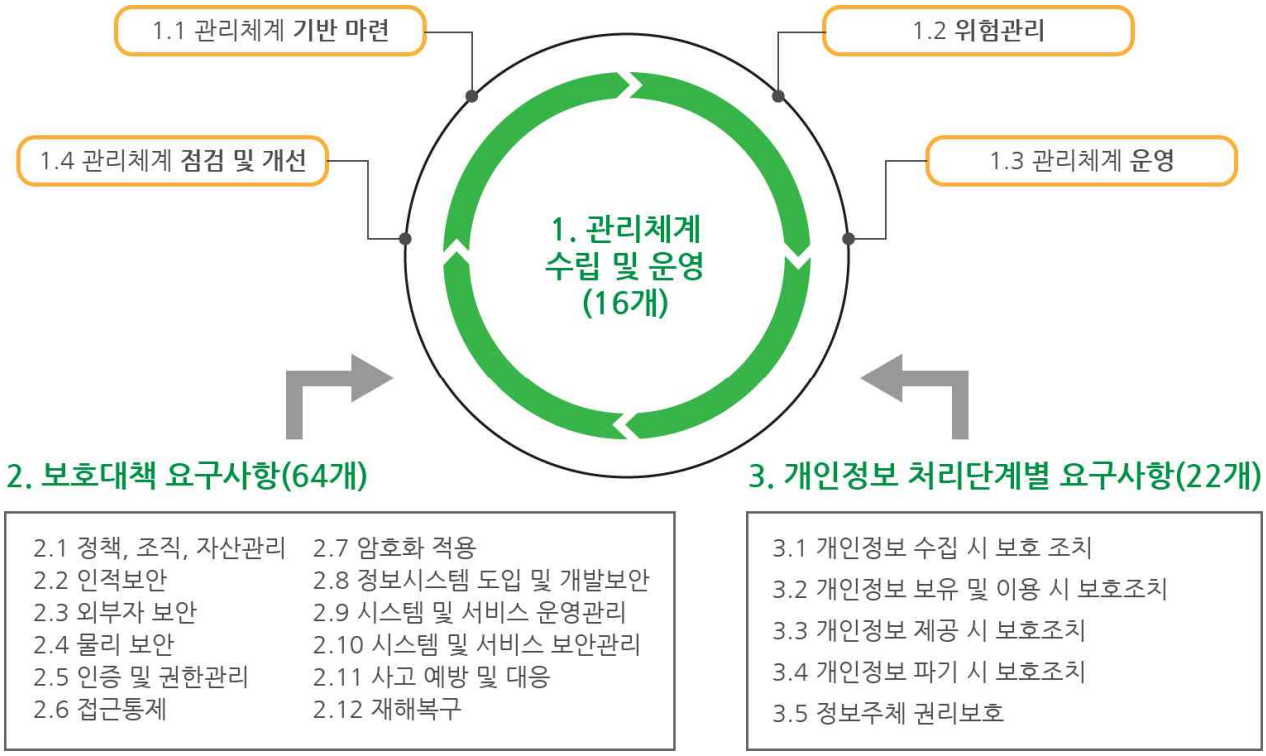
② PIMS(개인정보보호 관리체계 인증)

- 기관 및 기업이 개인정보보호 관리체계를 갖추고 체계적 · 지속적으로 보호 업무를 수행하는지에 대해 객관적으로 심사하여 기준 만족 시 인증 부여
- PIMS 구성요소



③ ISMS-P(정보보호 및 개인정보보호 관리체계 인증)

- 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도
- 인증기준



2. Secure SDLC(Software Development Life Cycle)

(1) Secure SDLC 의 개념

- 보안상 안전한 소프트웨어를 개발하기 위해 SDLC(Software Development Life Cycle)에 보안 강화를 위한 프로세스를 포함한 것
- 소프트웨어의 유지보수 단계에서 보안 이슈를 해결하기 위해 소모되는 비용을 최소화하기 위해 등장했다.
- 분석, 설계, 구현, 테스트, 유지보수 등 SDLC 전 단계에 걸쳐 수행되어야 할 보안 활동들을 제시한다.

(2) Secure SDLC 방법론

① CLASP(Comprehensive, Lightweight Application Security Process)

- SDLC의 초기 단계에서 보안을 강화하기 위해 개발된 방법론
- 활동 중심, 역할 기반의 프로세스로 구성되어 있음
- 현재 운용중인 시스템에 적용하기에 적합함

② MS-SDL

- MS사에서 안전한 소프트웨어 개발을 위해 기존의 SDLC를 개선한 방법론

③ Seven Touchpoints

- 소프트웨어 보안의 모범사례를 SDLC에 통합한 방법론
- 설계, 개발 과정의 모든 산출물에 대해 위험 분석 및 테스트를 수행한다.
- SDLC의 각 단계에 관련된 7개의 보안 강화 활동을 수행한다.

(3) 단계별 보안 활동

- 요구사항 분석 단계
  - 보안 항목에 해당하는 요구사항을 식별하는 작업을 수행
  - 조직의 정보보호 관련 보안 정책을 참고하여 소프트웨어 개발에 적용할 수 있는 보안 정책 문서화
- 설계단계
  - 식별된 보안 요구사항들을 소프트웨어 설계서에 반영하고, 보안 설계서를 작성
  - 네트워크, 서버, 물리적 보안, 개발 프로그램 등 환경에 대한 보안통제 기준을 수립하여 설계에 반영
- 구현 단계
  - 표준 코딩 정의서, 소프트웨어 개발 보안 가이드를 준수하며, 설계서에 따라 보안 요구사항들을 구현
  - 코드 점검, 소스코드 진단 작업을 통해 안정성을 확보한다.
- 테스트 단계
  - 설계 단계에서 작성한 보안 설계서를 바탕으로 보안 사항들이 정확히 반영되고 동작되는지 점검한다.
  - 보안 위협들과 취약점들을 점검할 수 있도록 테스트 계획을 수립하고 시행한다.
- 유지보수 단계
  - 발생할 수 있는 보안사고들을 식별하고, 사고 발생 시 이를 해결하고 보안 패치를 실시한다.

3. 시큐어 코딩(Secure Coding)

(1) OWASP(The Open Web Application Security Project)

- 오픈소스 웹 애플리케이션 보안 프로젝트
- 주로 웹에 관한 정보 노출, 악성 파일 및 스크립트 보안 취약점 등을 연구하며 10대 취약점을 발표했다.
- OWASP Top 10
  - 웹 애플리케이션 취약점 중 빈도가 많이 발생하고, 보안상 영향을 줄 수 있는 10가지를 선정하여 발표

(2) 시큐어 코딩 가이드

① 입력 데이터 검증 및 표현

- 프로그램 입력값에 대한 검증 누락 또는 부적절한 검증, 데이터형식을 잘못 지정하여 발생하는 보안 약점
- 보안 약점 종류

종류	설명
SQL Injection	- SQL문을 삽입하여 DB로부터 정보를 열람 및 조작할 수 있는 공격
XSS (크로스 사이트 스크립트)	- 악의적인 스크립트를 포함해 사용자 측에서 실행되게 유도하는 공격
자원 삽입	- 외부 입력값이 시스템 자원 접근 경로 또는 자원 제어에 사용되는 공격
위험한 형식 파일 업로드	- 서버측에서 실행될 수 있는 스크립트파일을 업로드 하여 공격
명령 삽입	- 운영체제 명령어 삽입 - XQuery 삽입 - XPath 삽입 - LDAP 삽입
메모리 버퍼 오버프로	- 입력받는 값이 버퍼를 가득 채우다 못해 넘쳐흘러 버퍼 이후의 공간을 침범하는 공격

② 보안기능

- 보안 기능을 부적절하게 구현하는 경우 발생할 수 있는 보안 약점
- 보안 약점 종류

종류	설명
적절한 인증 없이 중요기능 허용	- 적절한 인증과정이 없이 중요정보(계좌, 개인정보 등)를 열람 할 때 발생하는 보안 약점
부적절한 인가	- 적절한 접근 제어 없이 외부 입력값을 포함한 문자열로 중요 자원에 접근할 수 있는 보안약점
취약한 암호화 알고리즘 사용	- DES, MD5 등 안전하지 않은 알고리즘 사용
하드코딩된 패스워드	- 소스 코드 내에 비밀번호가 하드코딩되어 있어 소스코드 유출시 노출되는 보안 약점
패스워드 평문 저장	- 계정 정보 탈취 시 패스워드 노출
취약한 패스워드 허용	- 비밀번호 조합규칙(영문, 숫자, 특수문자 등)이 미흡하거나 길이가 충분하지 않아 노출될 수 있는 보안약점

③ 시간 및 상태

- 동시 수행을 지원하는 병렬 시스템이나 하나 이상의 프로세스가 동작하는 환경에서 시간 및 상태를 부적절하게 관리하여 발생할 수 있는 보안 약점
- 보안 약점 종류

종류	설명
경쟁 조건	- 동일 자원에 대한 검사 시점과 사용 시점이 상이하여 동기화 오류, 교착 상태를 유발
종료되지 않는 반복문 또는 재귀 함수	- 종료 조건이 없어 무한 루프에 빠져 자원 고갈을 유발

④ 에러 처리

- 에러를 처리하지 않거나 불충분하게 처리하여 에러 정보에 중요 정보가 포함될 때 발생할 수 있는 보안 약점
- 보안 약점 종류

종류	설명
오류 메시지 정보 노출	- 응용 프로그램의 민감 정보가 오류 메시지를 통해 노출됨 - 오류 메시지는 사용자가 필요한 최소한의 정보만을 노출해야 한다.
오류 상황 대응 부재	- 예외처리 미구현
부적절한 예외 처리	- 프로그램 수행 중 발생한 예외 조건을 적절히 검사하지 않음

⑤ 코드 오류

- 개발자가 범할 수 있는 코딩 오류로 인해 유발되는 보안 약점
- 보안 약점 종류

종류	설명
널 포인터 역참조	- 널 값을 고려하지 않은 코드에서 발생
부적절한 자원 해제	- 자원을 할당받아 사용한 뒤 반환하기 않는 코드에서 발생
해제된 자원 사용	- 해제한 메모리를 참조하는 코드에서 발생
초기화되지 않은 변수 사용	- 지역변수를 초기화하지 않고 사용하는 코드에서 발생

⑥ 캡슐화

- 중요한 데이터 또는 기능성을 불충분하게 캡슐화하거나 잘못 사용해 발생하는 보안 약점
- 보안 약점 종류

종류	설명
잘못된 세션에 의한 정보 노출	- 멀티 스레드 환경에서 서로 다른 세션 간 데이터가 공유될 수 있음
제거되지 않은 디버그 코드	- 배포 단계에 디버그 코드가 남아 있는 경우 민감 정보가 노출될 수 있음
시스템 정보 노출	- 시스템 내부 데이터가 노출될 수 있음
잘못된 접근 지정자	- private, public 잘못된 접근지정자 사용으로 민감 정보 노출될 수 있음

⑦ API 오용

- 의도된 사용에 반하는 방법으로 API를 사용하거나 보안에 취약한 API를 사용하여 발생할 수 있는 보안 약점
- 보안 약점 종류

종류	설명
DNS에 의존한 보안 결정	- 공격자가 DNS 정보를 변조하여 보안 결정을 우회 가능함
취약한 API 사용	- 금지되거나 안전하지 않은 함수를 사용함

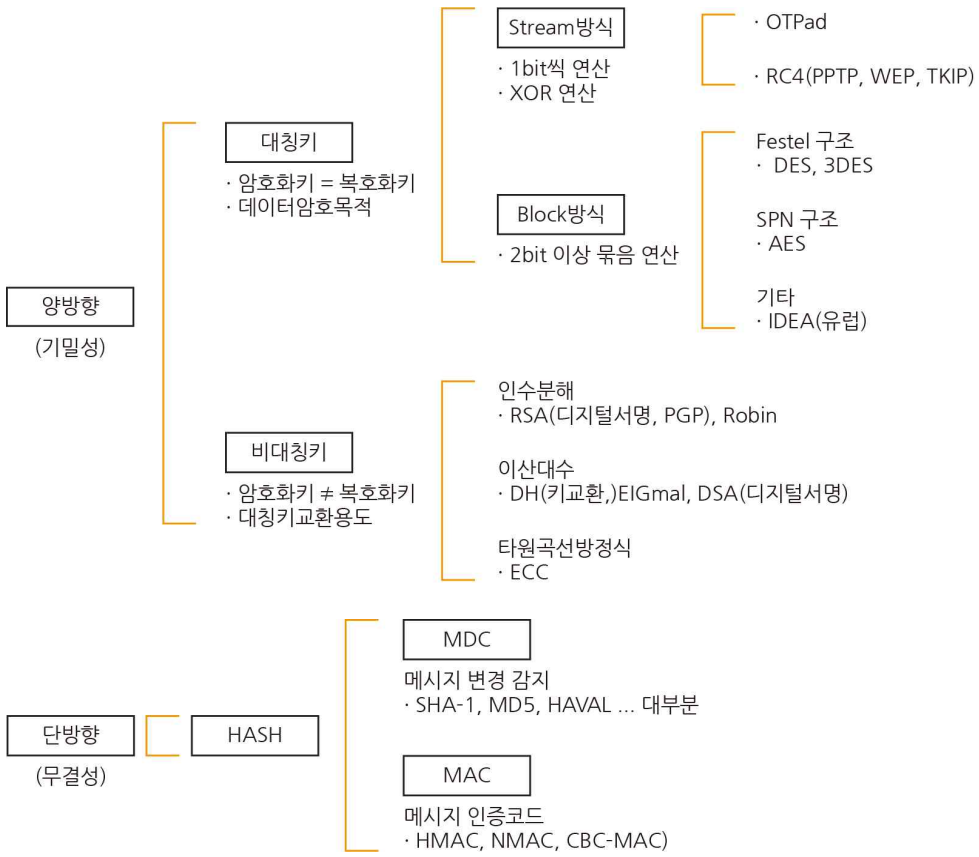
Section 2. SW개발 보안 구현

1. 암호 알고리즘

(1) 암호 알고리즘 용어

- 평문(Plaintext)
  - 해독 가능한 형태의 메시지(암호화전 메시지)
- 암호문(Cipertext)
  - 해독 불가능한 형태의 메시지(암호화된 메시지)
- 암호화(Encryption)
  - 평문을 암호문으로 변환하는 과정
- 복호화(Decryption)
  - 암호문을 평문으로 변환하는 과정
- 전자서명
  - 송신자는 개인키로 메시지를 서명하여 전달
  - 수신자는 송신자의 공개키를 이용하여 서명값 검증
- 양방향암호화
  - 평문을 암호문으로 암호문을 평문으로 변경할 수 있는 암호화
- 단방향암호화
  - 해싱을 이용하여 암호화하고, 평문으로 복호화는 불가능한 암호화

(2) 암호 방식에 따른 분류



⑶ 대칭키 암호(Symmetric key)

① 대칭키 암호 개념

- 암호화할 때의 키와 복호화할 때의 키가 동일한 암호 시스템
- 대칭키 암호는 혼돈과 확산의 성질을 이용하여 평문을 암호화 한다.

② 장/단점

장점	- 암호화방식에 속도가 빠르다. - 대용량 Data 암호화에 적합하다.
단점	- 키를 교환해야 하는 문제가 존재한다. - 사람이 증가할수록 키 관리가 어려워진다. - 키의 개수 : n(n-1)/2

③ 블록암호 알고리즘

알고리즘	설명
DES	- 64bit 블록, 56bit 암호화 키 사용 - 평문을 32bit 로 나눠 각 블록에 치환과 전치를 16Round 반복하여 암호화 - Feistel 암호 방식을 사용한다.
3-DES	- 암호화 키 2개를 사용하여 암호화→복호화→암호화 순으로 암호화
AES	- 128bit 평문을 128/192/256bit로 암호화 - 키 크기에 따라 10/12/14회 Round 수행 - 1997년 NIST에 의해 제정 - 레인달(Rijndael)에 기반한 암호화 방식 - SPN 암호 방식을 사용한다.
SEED	- 순수 국내기술로 개발한 128비트 및 256비트 대칭 키 블록의 암호 알고리즘
ARIA	- 국가 보안 기술 연구소(NSRI) 필두로 학계, 국가 정보원 등의 암호 기술 전문가들이 개발한 국가 암호화 알고리즘 - AES 알고리즘과 똑같이 128/192/256비트 암호화키를 지원한다.
IDEA	- 1990년 스위스에서 만들어진 PES를 개량하여 만들어진 블록 암호 알고리즘 - 키길이가 128bit, 블록길이가 64bit - Feistel 방식과 SPN의 중간형태 구조

④ 스트림암호 알고리즘

알고리즘	설명
LFSR	- LFSR은 현재 상태에서 선형 연산을 통해 다음 상태를 생성하는 레지스터 - 스트림 암호의 난수를 생성하는 용도로 많이 사용한다. - 블록암호에 비해 경량 및 고속 동작이 용이하다.
RC4	- 로널드 라이베스트가 만들었다. - 각 단계에서 키스트림 한 바이트를 생성한다. - LFSR의 구조를 가지지 않으며 옥텟 단위를 기반으로 한다. - 비트 단위의 암호화 보다 실행속도가 빠르다.
A5	- 시프트 레지스터를 기반으로 사용 - GSM 휴대폰 체계에 사용

(4) 비대칭키 암호

① 비대칭키 암호 개념

- 암호화와 복호화에 이용하는 키가 다른 방식
- 공개 키 암호 방식이라고도 한다.

② 키의 종류

- 공개키(Public key) : 대중에게 공개된 키
- 개인키(Private key) : 개인이 가지고 있으면서 관리하는 키

③ 장/단점

장점	- 키 분배/관리가 용이하다. - 사용자 증가에 따라 관리할 키의 개수가 상대적으로 적다. - 기밀성, 인증, 무결성을 지원하고, 부인방지 기능을 제공한다.
단점	- 키의 길이가 길고, 연산속도가 느리다. - 암호화 할 수 있는 평문의 길이에 제한이 있다.

④ 비대칭키 알고리즘

구분		설명
소인수 분해 기반	RSA	- 대표적인 공개키 암호 알고리즘
	Robin	- 1979년 Robin이 개발, RSA보다 빠르다.
이산대수 기반	Diffie-Hellman	- 키관리 센터 없이 공개키 전달 가능
	DSA	- 미국의 전자서명 표준
	ELGamal	- 같은 평문에서 다른 암호문의 생성이 가능
타원 곡선	ECC	- 타원 곡선상의 이산대수를 이용

(5) 단방향 암호화

① 단방향 암호화 개념

- Hash를 이용하여 암호화하는 과정
- 평문을 암호화 할 순 있지만, 복호화는 불가능하다.
- 암호화만 가능하기 때문에 단방향 암호화라 한다.

② 해시 함수 특성

특성	설명
역상 저항성	- 해시 값이 주어졌을 때, 그 해시 값을 생성하는 입력값을 알아내기가 불가능하다는 특성
제 2역상 저항성	- 어떤 입력 값과 동일한 해시 값(결과 값)을 가지는 다른 입력 값을 찾을 수 없어야 한다는 특성
충돌 저항성	- 해시 값(결과 값)이 같은 두 개를 찾을 수 없다는 특성

③ 해시 함수 종류

종류	설명
MD5	- 128 비트 암호학 해시 함수이다. - 1991년에 MD4를 대체하기 위해 고안되었다. - 1996년에 암호화 결함이 발견되었고 2008년에 결함을 이용해 SSL 인증서를 변조하는 것이 가능하다고 발표되었다.
SHA	- 미국 국가안보국(NSA)가 설계 했으며 미국 국가 표준으로 지정되어있다. - SHA-0, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512

④ 암호학적 해시 함수의 결점

- 무차별 대입 공격(Brute-force attack)
  - 공개키(Public key) : 해시 함수는 빠르기 때문에 무차별적 데이터를 넣다보면 암호화가 깨질 수 있다.
- Rainbow table 공격
  - 사용자의 암호유형을 정의한 Rainbow table을 만들어 하나씩 대입해 보면서 암호를 발견해 낼 수 있다.

⑤ 암호학적 해시 함수의 보완

- 키 스트레칭(Key Stretching)
  - 해시 암호화를 여러 번 반복하여서 암호학적 문제가 발생하는 점을 줄일 수 있다.
  - 무차별 대입 공격 을 방지하는 효과가 있다.
- 솔팅(Salting)
  - 데이터 앞/뒤에 임의의 값을 넣어 해시값을 만든다.
  - Rainbow Table 공격을 방지하는 효과가 있다.

2. 코드 오류

(1) 코드의 유형

- 순차 코드 (Sequence Code)
  - 자료의 발생순, 크기순 등 코드화 대상 항목을 일정한 순서에 의해 일련 번호를 부여하는 코드
  - 예) 교실내의 학생들의 번호
- 블록 코드 (Block Code)
  - 코드화 할 대상이 갖는 공통 특징을 중심으로 항목들을 별도의 집단으로 분류하고, 한 집단 안에서 순서대로 코드를 부여
  - 예) 시/군/구
- 10진 코드 (Decimal Code)
  - 10진수 형태로 표현한 코드
  - 예) 8104
- 그룹 분류 코드 (Group Classification Code)
  - 대상 항목에 대한 분류 기준에 따라 대분류, 중분류, 소분류 등 각 분류별로 번호를 순서적으로 부여하는 코드
  - 예) 대분류코드-중분류코드-소분류코드
- 연상 코드 (Mnemonic Code)
  - 코드 대상의 명칭과 관계있는 문자, 숫자, 약어를 코드의 일부로 사용하여 어떤 대상을 의미하는지 쉽게 파악할 수 있게 만든 코드
  - 예) TV_2021_04
- 표의 숫자 코드 (Significant Digit Code)
  - 코드화 대상 항목의 중량, 면적, 용량 등의 물리적 수치를 이용하여 만든 코드
  - 예) 30-50-120 (길이, 너비, 용량)
- 합성 코드 (Combined Code)
  - 두 개 이상의 코드를 조합하여 만든 코드 방식

⑵ 코드의 오류 발생 형태

- 생략 오류 (omission error)
  - 입력 시 한 자리를 빼놓고 기록한 경우
  - 예) 1234 → 123
- 필사 오류 (Transcription error)
  - 입력 시 임의의 한 자리를 잘못 기록한 경우
  - 예) 1234 → 1235
- 전위 오류 (Transposition error)
  - 입력 시 좌우 자리를 바꾸어 기록한 경우
  - 예) 1234 → 1243
- 이중 오류 (Double Transposition error)
  - 전위 오류가 두 가지 이상 발생한 경우
  - 예) 1234-> 2143
- 추가 오류 (Addition error)
  - 입력 시 한 자리 추가로 기록한 경우
  - 예) 1234-> 12345
- 임의 오류 (Random error)
  - 위의 오류가 두 가지 이상 결합하여 발생한 경우
  - 예) 1234-> 12367

Section 3. 인증과 접근통제

1. 인증과 인가

(1) 인증(Authentication)

① 인증의 개념

- 로그인을 요청한 사용자의 정보를 확인하고 접근 권한을 검증하는 보안 절차

② 인증 유형

- 지식 기반 인증
  - 사용자가 기억하고 있는 정보를 기반으로 인증을 수행한다.
  - 아이디/패스워드, 아이핀 등
- 소유 기반 인증
  - 사용자가 소유하고 있는 것을 기반으로 인증을 수행한다.
  - 신분증, OTP(One Time Password) 등
- 생체기반 인증
  - 사용자의 고유한 신체적 또는 행동적 특징을 기반으로 인증을 수행한다.
  - 지문, 홍채, 음성 등
- 행위기반 인증
  - 사용자의 행동 정보를 이용해 인증을 수행한다.
  - 서명, 동작 등
- 위치기반 인증
  - 인증을 시도하는 위치를 기반으로 인증을 수행한다.
  - GPS, IP 주소 등

(2) 인가(Authorization)

- 로그인 후, 인증된 사용자에게 권한을 부여한다.
- 권한에 따라 사용 가능한 기능이 제한된다.

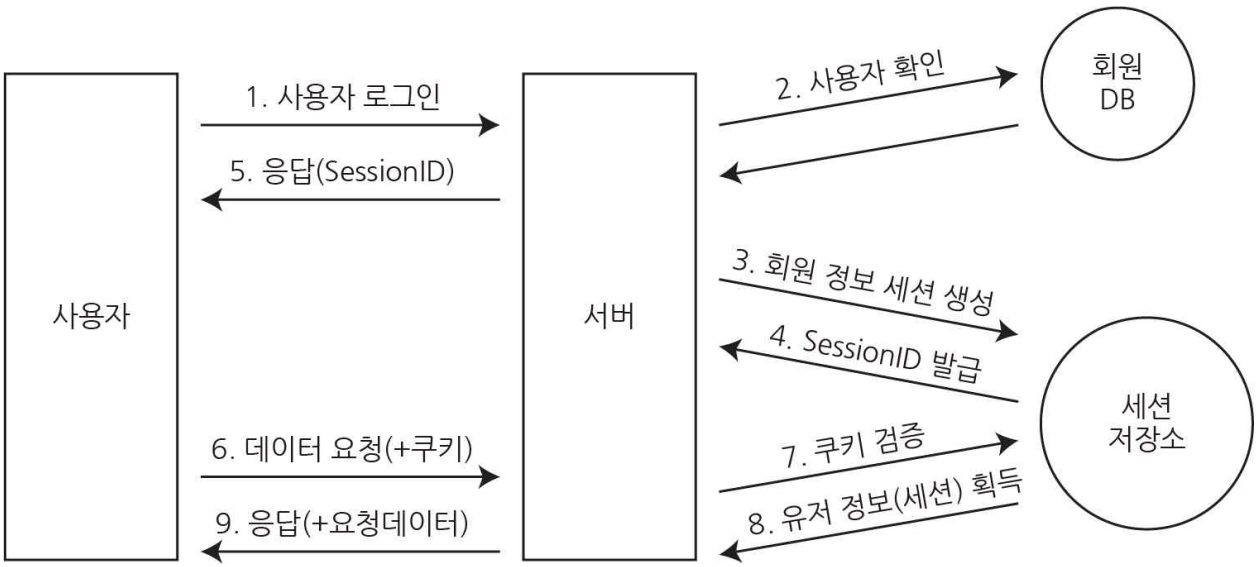
⑶ 인증방식

① 계정 정보를 요청 헤더에 넣는 방식

- 가장 보안이 낮은 방식이다.
- HTTP 요청에 인증할 수단을 넣어서 전송하는 방식이다.

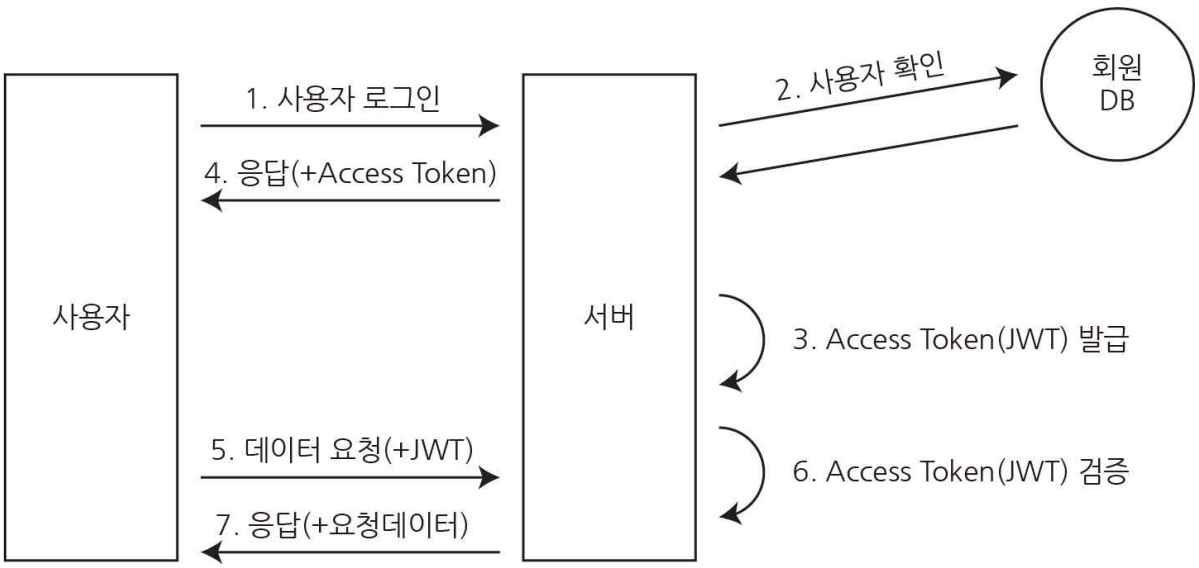
② Cookie/Session 방식

- 세션 기반인증을 위해 Session 과 Cookie 가 사용된다.
- 절차



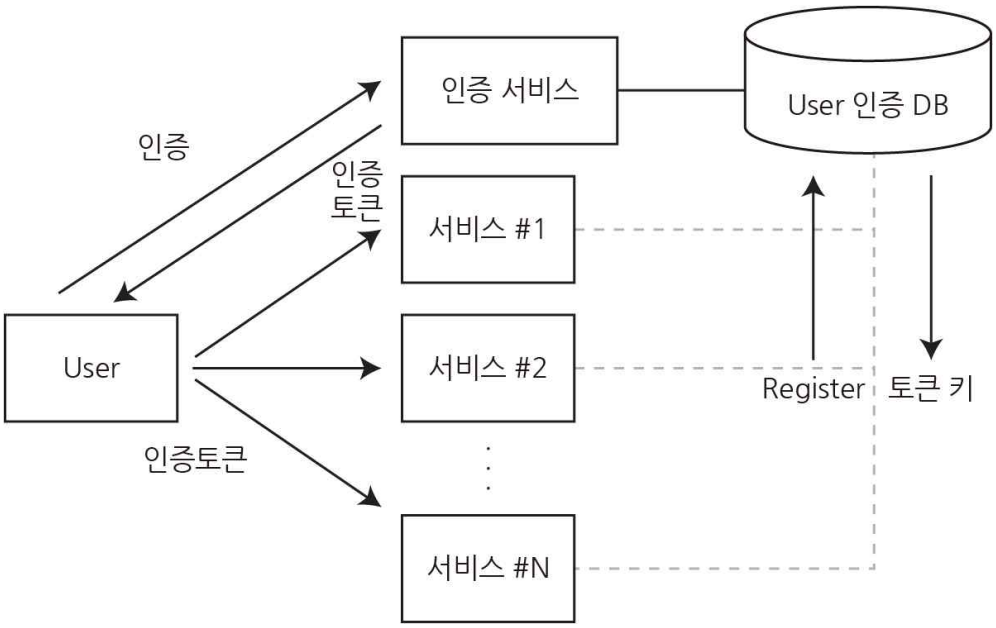
③ 토큰 기반 인증 방식(JSON Web Token, jwt)

- 인증을 위해 사용되는 암호화된 문자열을 이용한다.
- 절차



④ SSO(Single Sign-On)

- 하나의 로그인 인증 정보를 사용해 여러 어플리케이션을 접근할 수 있는 인증 서비스이다.
- 절차



2. 접근 통제

(1) 접근 통제 개념

- 정당한 사용자에게는 권한을 부여하고 그 외의 다른 사용자는 거부하는 것
- 시스템 및 네트워크에 대한 접근 제어의 가장 기본적인 수단은 IP와 서비스 포트로 볼 수 있다.
- 네트워크 장비에서 수행하는 IP에 대한 접근 제어로는 관리 인터페이스의 접근제어와 ACL(Access Control List) 등이 있다.

(2) 접근 통제 과정

① 식별(Identification)

- 사용자 ID를 확인하는 과정

② 인증(Authentication)

- 패스워드가 정확한지 확인

③ 인가(Authorization)

- 읽고, 쓰고, 실행시키는 권한을 부여

(3) 접근 통제 원칙

- 최소 권한의 원칙
  - 최소한의 권한만을 허용하여 권한의 남용을 방지
- 직무분리
  - 업무의 발생, 승인, 변경, 확인, 배포 등이 한 사람에 의해 처리되지 않도록 직무를 분리

(4) 접근 통제 정책

① 강제적 접근통제(MAC, Mandatory Access Control)

- 자원의 보안 레벨과 사용자의 보안 취급인자를 비교하여 접근 제어한다.
- 보안 등급, 규칙 등은 관리자만 수정할 수 있다.
- 기밀성이 강조되는 조직에서 사용된다.
- 대표적인 모델 : BLP(벨라파듈라)모델, Biba 모델, 클락-윌슨 모델, 만리장성 모델

② 임의적 접근통제(DAC, Discretionary Access Control)

- 주체가 속해 있는 그룹의 신원에 근거하여 객체에 대한 접근을 제한한다.
- 자원의 소유권을 가진 사람이, 다른 사람의 접근을 허용하거나 제한 할 수 있다.
- 특정 객체에 대해 특정 주체가 다른 주체에 대해 임의적으로 접근 제어가 가능하여 매우 유연한 접근 제어 서비스를 제공할 수 있다.

③ 역할기반 접근통제(RBAC,Role Based Access Control)

- 사용자의 역할에 기반을 두고 접근을 통제하는 모델이다.
- 정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내 개인 역할에 따라 허용 여부를 결정하는 모델이다.

④ 정책별 내용

정책	MAC	DAC	RBAC
권한부여	시스템	데이터 소유자	중앙관리자
접근결정	보안등급(Label)	신분(Identity)	역할(Role)
정책변경	고정적(변경 어려움)	변경 용이	변경 용이
장점	안정적, 중앙 집중적	구현 용이, 유연함	관리 용이

(5) 접근 통제 모델

① 벨-라파둘라 모델(BLP, Bell-LaPadula Confidentiality Model)

- 미 국방부 지원 모델로 기밀성을 강조한 모델이다.
- 정보가 높은 레벨에서 낮은 레벨로 퍼지는 것을 방지한다.
- No Read Up, No Write Down

② 비바 모델(Biba Integrity Model)

- 무결성을 위한 상업용 모델이다.
- 무결성의 3가지 목표 중 비인가자의 데이터 수정 방지 가능
- No Read Down, No Write Up

③ 클락-윌슨 모델(Clark-Wilson Integrity Model)

- 무결성 중심의 상업용 모델이다.
- 상용 응용 보안 요구사항을 다루고 있다.

④ 만리장성 모델(Chinese Wall Model, Breswer-Nash Model)

- 충돌을 야기하는 어떠한 정보의 흐름도 차단해야 한다는 모델로 이익 충돌 회피를 위한 모델
- 금융 서비스 제공 회사가 이해 충돌의 발생을 막기 위한 내부 규칙

Section 4. 시스템 보안 구현

1. 취약점 분석

(1) 보안 취약점

- 정보시스템에 불법적인 사용자의 접근을 허용할 수 있는 위협
- 정보시스템의 정상적인 서비스를 방해하는 위협
- 정보시스템에서 관리하는 중요 데이터의 유출, 변조, 삭제에 대한 위협

(2) 보안 취약점 점검 분류

① 관리적 관점

- 정보보호 관리체계 보안 통제에 근거하여 취약점 점검
- 운영적 취약성
- 정보보호 관리 취약성
- 인적 관리 취약성

② 기술적 관점

- 서버, 네트워크, PC 보안점검 등을 통한 취약점 점검
- 컴퓨터/통신 관련
- 정보보호 시스템 관련(방화벽, IPS, IDS)
- 시스템 개발 관련

③ 물리적 관점

- 문서 검토, 체크리스트, 실사를 통하여 취약점 점검
- 출입 통제 관리 시스템 관련
- 화재, 침수, 항온, 항습 관련

(3) 취약점 평가 수행 절차

- 취약점 분석/평가 계획 수립
- 취약점 분삭/평가 대상 선별
- 취약점 분석 수행
- 취약점 평가 수행

2. 보안관제

(1) 보안관제 개념

- 24시간 정보자산을 지키기 위해 모니터링하고, 외부의 공격자가 전달하는 패킷을 관측한다.
- 고가의 보안 장비들을 도입하지만 더욱 다양화되고, 지능화된 사이버 위협은 점차 증가
- 법적으로 보안관제인력은 필수적으로 구성되어야 한다.
- 실제 침해사고 시 CERT(Computer Emergency Response Team)팀이 대응함

(2) 통합로그 분석 장비

- ESM(Enterprise Security Management)
- SIM(Security Information and event Management)
- SOAR

3. 보안 운영체제(Secure-OS), 신뢰성 운영체제(Trusted OS)

(1) 보안 운영체제 개념

- 컴퓨터 운영체제 상에 내재된 보안상의 결함으로 인하여 발생할 수 있는 각종 해킹으로부터 시스템을 보호하기 위하여 기존의 운영체제 내에 보안 기능을 추가한 운영체제
- 컴퓨터 사용자에 대한 식별 및 인증, 강제적 접근 통제, 임의적 접근 통제, 재사용 방지, 침입 탐지 등의 보안 기능 요소를 갖추어진 운영체제

(2) 보안 운영체제 목적

① 안정성

- 중단 없는 안정적인 서비스를 지원함

② 신뢰성

- 중요 정보의 안전한 보호를 통한 신뢰성 확보

③ 보안성

- 주요 서버에 대한 침입차단 및 통합 보안관리
- 버퍼오버 플로우, 인터넷 웜 등 다양해지는 해킹 공격을 효과적으로 방어할 수 있는 서버 운영환경 구축

(3) 보안 운영체제 기능

- 식별 및 인증, 계정관리
- 강제적 접근통제
- 임의적 접근통제
- 객체 재사용 방지
- 모든 접근경로에 대한 완전한 통제
- 보안커널 변경 방지
- 해킹 방지

4. 보안 솔루션

(1) 방화벽(firewall)

- 기업이나 조직 내부의 네트워크와 인터넷 간에 전송되는 정보를 선별하여, 수용/거부/수정하는 기능을 가진 침입차단 시스템
- 외부에서 내부로 들어오는 패킷만 체크하여 인증된 패킷만 통과시키며, 내부에서 외부로 나가는 패킷은 그대로 통과시킴

(2) 웹방화벽(Web Firewall)

- SQL 삽입공격, Cross-Site Scripting(XSS) 등의 웹기반 공격을 방어할 목적으로 만들어진 웹서버 특화 방화벽

(3) 침입탐지시스템(IDS; Intrusion Detection System)

- 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 "실시간"으로 탐지하는 시스템
- 방화벽의 기능을 보완한다.
- 침입탐지 방식에 따른 분류
  - 오용탐지 : 미리 입력해 둔 공격 패턴이 감지되면 이를 알려준다.
  - 이상탐지 : 평균적인 시스템의 상태를 기준으로 비정상적인 행위나 자원의 사용이 감지되면 알려준다.
- 침입탐지 대상에 따른 분류
  - 네트워크 기반 IDS(NIDS) : 네트워크 패킷을 분석하여 침입을 탐지한다.
  - 호스트 기반 IDS(HIDS) : 로그 분석과 프로세스 모니터링을 통한 침입을 탐지한다.

(4) 침입방지시스템(IPS; Intrusion Prevention System)

- 방화벽과 침입탐지시스템을 결합한 것
- 탐지 후 방화벽 가동

(5) 데이터유출방지(DLP; Data Leakage/Loss Prevention)

- 내부 정보의 외부 유출을 방지하기 위한 보안솔루션

(6) VPN(Virtual Private Network, 가상 사설 통신망)

- 인터넷 등 통신 사업자의 공중 네트워크에 암호화 기술을 이용하여 사용자가 마치 자신의 전용 회선을 사용하는 것처럼 해주는 보안솔루션

(7) NAC(Network Access Control)

- 네트워크에 접속하는 내부PC의 MAC주소(고유랜카드주소)를 IP관리 시스템에 등록한 후 일관된 보안관리 기능을 제공하는 보안솔루션
- 내부PC의 소프트웨어 사용현황을 관리하여 불법적인 소프트웨어 설치를 방지

(8) ESM(Enterprise Security Management)

- 다양한 장비에서 발생하는 로그 및 보안 이벤트(방화벽, IDS, IPS, 웹방화벽, VPN 등)를 통합관리 하는 보안 솔루션
- 종합적인 보완관리체계 수립

5. 방화벽(firewall)

(1) 구현방식에 따른 유형

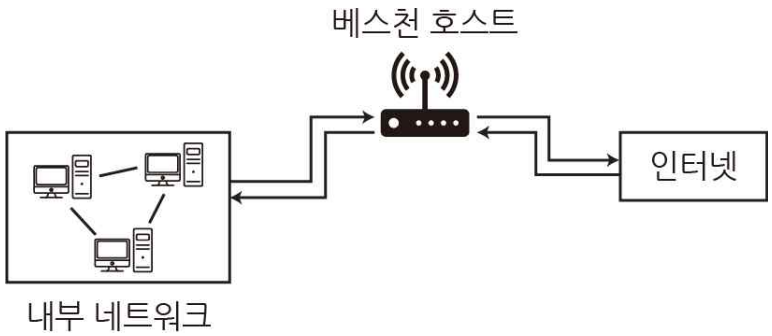
유형	설명
패킷 필터링 (Packet Filtering)	- 네트워크 계층과 전송 계층에서 동작한다. - IP주소, Port주소 등의 데이터를 바탕으로 방화벽 정책을 세워 패킷을 필터링 한다. - 다른 방화벽에 비해 속도가 빠르다.
애플리케이션 게이트웨이 (Application Gateway)	- 응용계층에서 동작한다. - 로그에서 다양한 정보를 얻어 여러 기능을 추가할 수 있다.
회선 게이트웨이 (Circuit Gateway)	- 응용계층과 세션 계층 사이에서 동작한다.
상태 기반 패킷 검사 (Stateful Packet Inspection)	- OSI 의 모든 계층에서 패킷을 분석하여 차단하는 기능 - 방화벽 중 가장 강력하다.
혼합형 타입 (Hybrid Type)	- 서비스 종류에 따라 복합적으로 구성한다.

(2) 방화벽 시스템 구축 유형

① 스크리닝 라우터(Screening Router)

- IP, TCP, UPD의 헤더 부분에 포함된 내용만 분석하여 동작한다.
- 내부 네트워크와 외부 네트워크 사이의 패킷을 허용/거부하는 라우터이다.
- 비용이 적게 들지만, 패킷 내의 데이터는 차단 및 관리 어렵다.

② 베스천 호스트(Bastion Host)

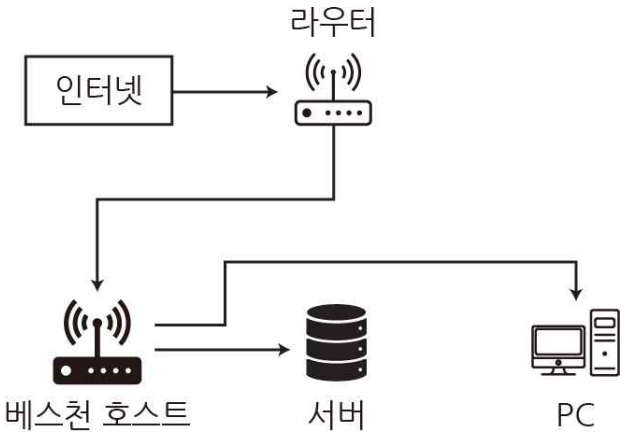


- 내부 네트워크로 진입하기 전에 베스천 호스트를 두어 내부 네트워크를 전체적으로 보호한다.
- 접근 제어를 기본으로 프록시 기능을 사용하며, 인증, 로깅 등의 여러 작업을 수행한다.
- 스크린 라우터보다 안전하고, 로그 생성 관리가 용이하다.
- 베스천 호스트 손상 시 내부망이 손상된다.

③ 듀얼 홈드 호스트(Dual-Homed Host)

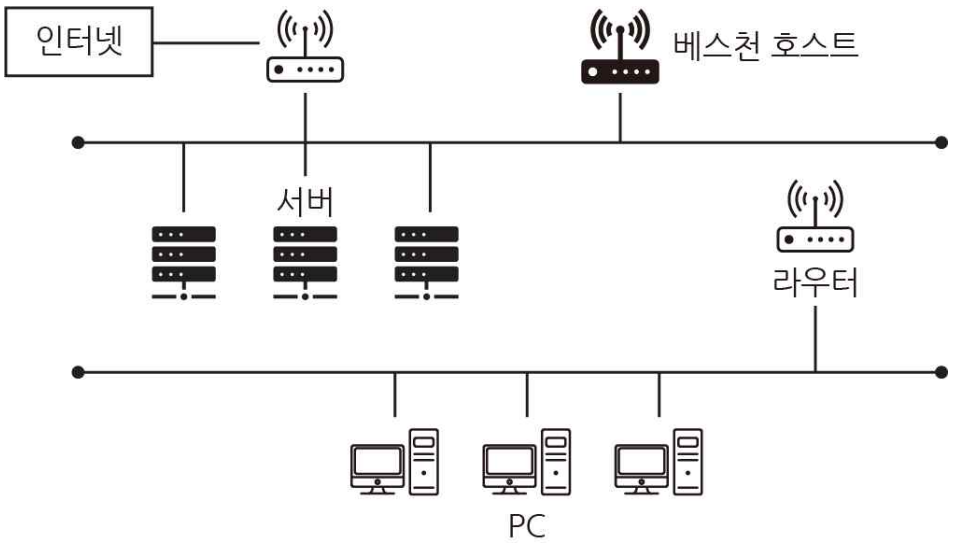
- 2개의 인터페이스를 가진 베스천 호스트로, 하나의 NIC은 내부 네트워크 연결, 다른 NIC는 외부 네트워크와 연결한다.
- 정보 지향적인 공격 방어가 가능하고, 로깅과 정보 생성 관리가 편리하다.
- 방화벽에서 보안 위반이 초래될 수 있고, 서비스가 늘어날수록 관리가 힘들어진다.

④ 스크린드 호스트(Screened Host)



- 패킷 필터 라우터와 베스천 호스트로 구성되어 있다.
- 패킷 필터 라우터는 내/외부 패킷을 통과시킬 것인지 결정한다.
- 베스천 호스트는 내/외부 네트워크 시스템에 대한 인증을 담당한다.
- 네트워크 계층과 응용계층의 2단계 방어로 안전하다.
- 스크리닝 라우터의 정보가 변경되면 방어가 불가능하고, 구축 비용이 많이 든다.

⑤ 스크린드 서브넷(Screened Subnet)



- 스크린드 호스트의 보안성 문제점을 해결한 것이다.
- 외부 네트워크와 내부 네트워크 사이에 하나 이상의 경계 네트워크를 두고, 내/외부 네트워크를 분리하기 위한 구조이다.
- 두 개의 스크리닝 라우터와 한 개의 베스천 호스트로 구성되어 있다.
- 스크린드 호스트의 장점을 유지하고 매우 안전한 구조이다.
- 설치 및 관리가 어렵고 구축비용이 높으며, 서비스 속도가 느려질 수 있다.

6. 보안 프로토콜

(1) SSH(Secure Shell Protocol)

- 원격 호스트에 접속하기 위해 사용되는 보안 프로토콜
- 기존 원격 접속은 '텔넷(Telnet)'이라는 방식을 사용했는데, 암호화를 제공하지 않기 때문에 보안상 취약하다는 단점이 있다.
- 안전하지 못한 네트워크에서 안전하게 통신할 수 있는 기능과 강력한 인증방법을 제공한다.
- 문자를 암호화하여 IP Spoofing, DNS Spoofing으로부터 보호할 수 있다.
- 22번 포트를 사용한다.

(2) SSL(Secure Socket Layer)

- 웹 브라우저와 웹 서버 간에 데이터를 안전하게 주고 받기 위한 업계 표준 프로토콜
- SSL이 적용된 웹 페이지는 URL이 https 로 시작되며, 443번 포트를 사용한다.(http는 80포트)

(3) TLS(Transport Layer Security)

- 전송계층을 기반으로 개발 되었다.
- 데이터의 정보 보호와 무결성을 제공하기 위해 만들어졌다.

(4) IPSec

① IPSec 개념

- IP계층(네트워크 계층)을 안전하게 보호하기 위한 기법
- 패킷에 대한 보안을 제공한다.

② 동작모드

- 전송 모드(Transport Mode)
  - IP 헤더를 제외한 IP 패킷의 페이로드(Payload)만을 보호한다.
  - IP 헤더는 암호화 하지 않으므로 트래픽 경로는 노출된다.
- 터널 모드(Tunneling Mode)
  - IP 패킷 전체를 보호한다.

③ 프로토콜

- AH(Authentication Header)
  - 메세지 인증 코드(MAC)를 이용하며 무결성(Data Integrity)과 인증(Authentication) 기능 제공
  - 암호화는 제공되지 않는다.
- ESP(Encapsulating Security Payload)
  - AH가 가진 무결성과, 인증도 제공하고 추가적으로 대칭키 암호화를 통해 기밀성(Confidentiality) 제공
- IKE(Internet key Exchange)
  - IPSec에서 키 교환에 사용되는 프로토콜

(5) S-HTTP (Secure HTTP)

- 웹상에서 네트워크 트래픽을 암호화하는 주요 방법 중 하나이다.
- 웹상의 파일들이 안전하게 교환될 수 있도록 해주는 HTTP의 확장판이다.

7. 스토리지

(1) 스토리지 개념

- 컴퓨터에 데이터를 저장하는 저장소의 역할을 수행하는 부품
- 컴퓨터의 하드디스크와 동일한 역할을 수행하는 부품이며, 스토리지를 직접 서버에 연결 할 수 있다.
- 대용량의 데이터를 저장하기 위해 별도의 스토리지용 네트워크를 구성할 수 있다.

(2) 스토리지 종류

① DAS(Direct Attachted Storage)

- PC나 서버에 직접 꽂아서 사용하는 스토리지
- 서버와 하드웨어를 1:1로 연결
- 각 서버가 직접 파일 시스템을 관리한다.
- 서버에 직접 외장저장장치를 연결하므로 속도는 빠르고 확장은 쉽지만, 연결 수에 한계가 있다.

② NAS(Networt Attached Storage)

- 서버와 저장장치가 이더넷등의 LAN방식의 네트워크에 연결된 방식
- DAS와 달리 PORT수 제한이 없어 확장성과 유연성이 뛰어나다.
- 접속증가시 성능저하, 전송속도 DAS보다 느리다.

③ SAN(Storage Area Network)

- 서버와 저장장치를 Fiber channel(광채널) switch로 연결한 고속데이터 네트워크
- 전용 파이버채널 스위치(광채널)를 둠으로써 빠른 속도의 연결을 유지한다.

(3) RAID(Redundant Array of Inexpensive Disks)

① RAID 개념

- 복수의 HDD를 하나의 드라이브와 같이 인식하고 표기한다.
- HDD의 신뢰성을 높여준다.
- 데이터를 분산하여 쓸 수 있어 고속화를 기대할 수 있다.

② RAID 구성

- 스트라이핑(Striping) : 논리적으로 연속된 데이터들이 물리적으로 여러 개의 디스크에 라운드로빈 방식으로 저장되는 형태
- 미러링(Mirroing) : 데이터를 그대로 복제하는 것으로 신뢰성 확보를 위해 사용됨

③ RAID 형태

- RAID-0
  - 빠른 데이터 입출력을 위해 스트라이핑을 사용하는 방식으로, 디스크의 모든 용량을 사용한다.
  - 하나의 디스크가 잘못되면 데이터를 잃어버릴 수 있다.
- RAID-1
  - 두 개 이상의 디스크를 미러링을 통해 하나의 디스크처럼 사용한다.
  - 완전히 동일하게 데이터를 복제하기 때문에 가용량이 절반이다.
  - 하나의 디스크에서 에러가 발생하면 미러링 된 디스크를 통해 복구가 가능하다.
- RAID-2
  - 오류 정정을 위한 해밍코드를 사용하는 방식
- RAID-3
  - 하나의 디스크를 패리티(Parity) 정보를 위해 사용하고 나머지 디스크에 데이터를 균등하게 분산 저장
  - 하나의 디스크에서 에러가 발생하면 패리티 디스크를 통해 복구할 수 있다.
- RAID-4
  - RAID-3 과 같이 패리티 정보를 독립된 디스크에 저장한다.
  - 블록(Block)단위로 분산 저장하는 차이가 있다.
- RAID-5
  - 3개 이상의 디스크를 붙여서 하나의 디스크처럼 사용하고 각각의 디스크에 패리티 정보를 가지고 있는 방식
  - 패리티 디스크를 별도로 사용하지 않음으로 병목현상이 발생하지 않는다.
- RAID-6
  - 하나의 패리티를 두 개의 디스크에 분산 저장하는 방식
  - 패리티를 이중으로 저장하기 때문에 두 개의 디스크에 에러가 발생해도 정상적으로 복구할 수 있다.

8. 고가용성(HA, High Availability)

- 서버와 네트워크, 프로그램 등의 정보 시스템이 오랜 기간 동안 지속적으로 정상 운영이 가능한 성질
- 가용성이 높다는 의미로 고장이 나지 않음을 의미한다.
- 고가용성을 제공하기 위해 주로 2개의 서버를 연결하는 방식을 사용한다.

Section 5. 서비스 공격 유형

1. DoS(Denial of Service) 공격

(1) DoS 공격의 개념

- 대상 시스템이 정상적인 서비스를 할 수 없도록 가용성을 떨어뜨리는 공격
- 대상 시스템에 과도한 트래픽을 보내거나, 트래픽 발생을 유도함으로써 정상적인 운영이나 서비스가 될 수 없게 하는 공격

(2) 공격 목표

- 물리적인 파괴 (디스크 및 시스템 파괴)
- 시스템 자원 공격 (CPU , Memory , Disk의 자원고갈)
- 네트워크 자원 공격 (대역폭 고갈)

(3) DoS 공격 유형

① Smurf Attack

- 여러 호스트들로 하여, 특정 대상에게 다량의 ICMP Echo Request 를 보내게 하는 공격 방법
- IP와 ICMP 의 특성을 이용한다.
- 공격자는 IP 주소를 공격 서버의 IP 주소로 위장하고, ICMP Request 패킷을 브로드캐스트를 통해 다수의 시스템에 전송한다. 이 때 브로드캐스트를 수신한 다수의 시스템은 ICMP Echo Reply 패킷을 공격자가 아닌 공격 대상의 서버로 전송하게 되면서 부하를 발생시킨다.

② Ping Of Death

- 규정 크기 이상의 ICMP 패킷으로 시스템을 마비시키는 공격 방법
- ICMP 패킷을 정상적인 크기보다 크게 만들어 공격 대상에게 전송하면, 사이즈가 크기 때문에 패킷을 나눠서 보내게 된다. 공격대상은 쪼개진 패킷을 조립하는 과정에서 많은 부하가 발생하고, 재조합 버퍼의 오버플로우가 발생하여 정상적인 서비스가 불가능해진다.
- 반복적으로 들어오는 일정 수 이상의 ICMP 패킷을 무시하는 방법으로 대응한다.

③ Land Attack

- 출발지 IP와 목적지 IP가 같은 패킷을 만들어 보내는 공격 방법
- 수신자가 응답을 보낼 때, 목적지 주소가 자기 자신이므로 SYN 신호가 계속 자신의 서버를 돌게 되어 서버의 자원을 고갈 시켜 가용성을 파괴한다.
- 방화벽에서 출발지와 목적지가 같은 패킷은 모두 제거하여 대응한다.

④ Teardrop Attack

- 재조합을 할 수 있는 fragment number를 위조하는 공격 방법
- 데이터를 보낼 때, 데이터를 나누고, 재조립 할 수 있는 fragment number를 부여 하는데, fragment number를 위조하여 재조합이 안 되어 다운되게 하는 공격

⑤ SYN Flooding

- TCP의 연결과정(3Way Handshaking)의 취약점을 이용한 공격 방법
- 공격자가 SYN 신호만 전달하고, ACK 응답을 받지 않아, Backlog queue에 연결 정보를 계속 쌓게 하여 정상적인 서비스 제공이 불가능하게 만드는 공격

⑥ UDP Flooding

- 다량의 UDP 패킷을 전송하여 네트워크 자원을 고갈시키는 공격

⑦ Ping Flooding

- 특정 사이트에 매우 많은 ICMP Echo를 보내면, 이에 대한 응답(Respond)을 하기 위해 시스템 자원을 모두 사용해버려 시스템이 정상적으로 동작하지 못하도록 하는 공격 방법

2. DDoS(Distributed Denial of Service attack) 공격

(1) DDoS 공격의 개념

- 특정 서버(컴퓨터)나 네트워크 장비를 대상으로 많은 데이터를 발생시켜 장애를 일으키는 대표적인 서비스 거부 공격
- 분산된 다수의 좀비 PC를 이용하여 공격 대상 시스템의 서비스를 마비시키는 공격 형태

(2) DDoS 공격 구성

① 공격자(Attacker)

- 해커의 시스템
- 좀비 PC를 만들고, C&C에 명령을 전달한다.

② 명령 제어(C&C:Command and Control)

- 공격자로부터 공격 명령을 전달 받는 시스템
- 전달 받은 내용을 좀비 PC에게 전달하는 역할을 한다.

③ 좀비(Zombie) PC

- C&C의 명령을 받고 실제 공격을 수행하는 다수의 PC
- 봇(Bot), 슬레이브(Slave), 에이전트(Agent)라고 부르기도 한다.

④ 공격 대상(Target)

- 좀비 PC의 공격을 받는 대상 시스템

(3) DDoS 공격 순서

- 관리자가 관리할 수 없는 곳에 계정을 획득하여 스니핑(Sniffing)이나 버퍼 오버플로우 등의 공격으로 설치권한이나 루트 권한 획득
- 공격대상을 파악하기 위해 취약한 서비스를 제공하는 서버 파악
- 취약한 시스템의 리스트를 확인하고, 실제 공격을 위한 Exploit(공격자의 의도된 명령/프로그램 등) 작성
- 권한을 획득한 시스템에 침투하여 Exploit을 컴파일하여 설치
- 설치한 Exploit 으로 공격 시작

(4) DDoS 공격 툴의 종류

① Trinoo(트리누)

- Master/Agent 로 구성되어 있으며 Master의 명령으로 Agent가 작업을 수행하는 DDos 공격 도구
- UDP Flooding 공격을 수행한다.
- 목표 시스템에 대량의 UDP 패킷이 전송되어 시스템을 다운 시킨다.

② TFN(Tribal Flood Network)

- Master와 Agent의 통신에는 ICMP ECHO-REPLY 메시지를 사용한다

③ Stacheldraht(슈타첼드라트)

- Trinoo의 네크워크 구조와 TFN의 다양한 공격방법, Communication 상의 encryption 기능을 포함한 공격도구

3. 기타 해킹 기법

- 웜(Worm)
  - 네트워크를 통해 자신을 복제하고 전파할 수 있는 악성 프로그램
- 바이러스(Virus)
  - 파일, 부트, 메모리 영역에서 스스로를 복사하는 악성프로그램으로 파일 속에 숨어 옮겨 다닌다.
- 트로이목마(Trojan)
  - 겉으로 보기에는 전혀 해를 끼치지 않을 것처럼 보이고 자기 복제 능력이 없지만 실제로는 바이러스 등의 위험인자를 포함하고 있는 프로그램
- 혹스(Hoax)
  - 남을 속이거나 장난을 친다는 뜻으로, 말 그대로 가짜 바이러스를 말한다.
- 포트 스캐닝(Port Scanning)
  - 서버에 열려있는 포트를 확인 후 해당 포트의 취약점을 이용한 공격
  - Nmap을 이용해 열린포트, 호스트, 버전 등을 탐지할 수 있다.
- 스니핑 공격(Sniffing Attack)
  - 네트워크로 전송되는 패킷을 훔쳐보는 공격
- Smishing(SMS phishing)
  - 문자메시지를 이용한 피싱
- Qshing
  - QR코드를 통해 악성 링크로 접속을 유도하거나 직접 악성코드를 심는 금융범죄 기법
- 세션 하이재킹(Session Hijacking)
  - 이미 인증을 받아 세션을 생성, 유지하고 있는 연결을 빼앗는 공격
  - 대책 : ACK Storm 탐지, 데이터 암호화, MAC 주소 고정, 비동기화 상태 탐지, 패킷의 유실 및 재전송 증가 탐지
- IP Spoofing
  - 자신의 IP 주소를 속여서 접속하는 공격
- ARP Spoofing
  - ARP 프로토콜의 허점을 이용하여 자신의 MAC(Media Access Control) 주소를 다른 컴퓨터의 MAC인 것처럼 속이는 공격
- DNS Spoofing
  - DNS 서버로 보내는 질문을 가로채서 변조된 결과를 보내주는 것으로 일종의 중간자 공격
- SQL injection
  - 코드 인젝션의 한 기법으로 클라이언트의 입력값을 조작하여 서버의 데이터베이스를 공격할 수 있는 공격

- Rainbow Table
  - 해시함수(MD-5, SHA-1, SHA-2 등)를 사용하여 만들어낼 수 있는 값들을 대량으로 저장한 테이블
- Backdoor
  - 정상적인 인증 절차를 거치지 않고, 응용프로그램 및 시스템에 접근할 수 있도록 만든 프로그램
  - 시스템의 취약점을 이용하거나, 정상적인 파일에 악성코드를 삽입하여 공격하는 기법
  - 탐지방법 : 현재 동작 중인 프로세스 및 열린 포트 확인, SetUID 파일 검사, 무결성 검사(tripwire), 로그분석 등
- Password Cracking
  - 시스템의 비밀번호를 각종 툴(프로그램)을 통해 알아내는 공격 기법
- Format String Attack
  - 문자열의 출력 포맷을 애매하게 설정할 때의 취약점을 포착하여, 메모리의 RET 위치에 악성코드 주소를 입력하여 공격하는 기법
- APT(Advanced Persistent Threat)
  - 지속적이고 지능적인 해킹 공격의 통칭
- CSRF(Cross-site requset forgery)
  - 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청하게 하는 해킹 공격
- XSS(Cross-Site Scripting)
  - 악의적인 사용자가 공격하려는 사이트에 스크립트를 넣는 기법
- Nucking
  - 특정 아이피에 대량의 패킷을 보내 인터넷 접속을 끊는 크래킹의 일종
- Buffer Overflow
  - 버그의 일종 또는 이를 이용한 공격 방법
  - 프로그램이 실행될 때 입력받는 값이 버퍼를 가득 채우다 못해 넘쳐흘러 버퍼 이후의 공간을 침범하는 현상
  - 방어기법

종류	설명
스택가드 (Stackguard)	- 메모리상에서 프로그램의 복귀 주소와 변수 사이에 특정 값을 저장해 두었다가 그 값이 변경되었을 경우 오버플로우 상태로 가정하여 프로그램 실행을 중단하는 기술
스택쉴드 (Stack Shield)	- 함수 종료 시 저장된 값과 스택의 RET값을 비교해 다를 경우 오버플로우로 간주하고 프로그램 실행을 중단하는 기술
ASLR (Address Space Layout Randomization)	- 메모리 공격을 방어하기 위해 주소 공간 배치를 난수화한다.

- 부채널 공격(side channel attack)
  - 암호 알고리즘을 대상으로 한 물리적 공격 기법
- Brute Force
  - 무차별 대입 공격
  - 조합 가능한 모든 문자열을 하나씩 대입해 공격

- Dictionary Attack
  - 암호화되어 저장된 패스워드를 알아내기 위한 공격 방법 중 하나
  - 많이 사용되는 날짜, 전화번호 등과 같은 패턴들을 사전(dictionary) 형태로 만들고 이들을 조합하는 방식으로 공격
- Key Logger Attack
  - 컴퓨터 사용자의 키보드 움직임을 탐지해 ID, 패스워드 등 개인의 중요한 정보를 몰래 빼가는 해킹 공격
- 스파이웨어(Spyware)
  - 스파이와 소프트웨어 합성어로, 광고나 마케팅을 목적으로 배포되는게 대부분이어서 애드웨어(Adware)라고도 한다.
- 랜섬웨어(Ransomware)
  - 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다.
- 제로데이 공격(Zero-Day Attack)
  - 컴퓨터 소프트웨어의 취약점(exploit)을 공격하는 기술적 위협으로, 해당 취약점에 대한 패치가 나오지 않은 시점에서 이루어지는 공격
- 사회공학(social engineering)
  - 기술적인 방법이 아닌 사람들 간의 기본적인 신뢰를 기반으로 사람을 속여 비밀정보를 획득하는 기법
- Evil Twin Attack
  - 소셜 네트워크에서 악의적인 사용자가 지인 또는 특정 유명인으로 가장하여 활동하는 공격 기법
  - 와이파이(WiFi) 무선 네트워크에서 공격자가 가짜 AP(Access Point)를 구축하고 강한 신호를 보내어 사용자가 가짜 AP에 접속하게 함으로써 사용자 정보를 중간에서 가로채는 기법
- Bluebug
  - 블루투스 장비간 취약한 연결관리를 이용한 공격
  - 한번 연결되면 이후에는 다시 연결해주지 않아도 자동으로 연결되는 인증 취약점 이용
- BlueSnarf
  - 블루투스 취약점을 이용하여 장비의 임의의 파일에 접근하는 공격
  - 인증없이 정보를 교환하는 OPP 기능을 사용하여 파일에 접근
- BluePrinting
  - 블루투스 공격장치의 검색 활동
- BlueJacking
  - 블루투스를 이용해 스팸처럼 명함을 익명으로 퍼뜨리는 것
  - 근처에 있는 다른 블루투스가 장착된 휴대폰에 메일처럼 퍼뜨리는 휴대폰 바이러스
- Switch Jamming
  - 위조된 매체 접근 제어(MAC) 주소를 지속적으로 네트워크로 흘려보내, 스위치 MAC 주소 테이블의 저장 기능을 혼란시켜 더미 허브(Dummy Hub)처럼 작동하게 하는 공격
- Honeypot
  - 비정상적인 접근의 탐지를 위해 의도적으로 설치해 둔 시스템
  - 침입자를 속여 실제 공격을 당하는 것처럼 보여줌으로써 크래커를 추적 및 공격기법의 정보를 수집하는 역할을 한다.
  - 쉽게 공격자에게 노출되어야 하며 쉽게 공격이 가능한 것처럼 취약해 보여야 한다.
- 스턱스넷(Stuxnet)
  - 대단히 정교한 컴퓨터 웜
  - 기존에 알려진 여러 가지 윈도우 제로데이 취약점을 이용해 컴퓨터를 감염시키고 확산된다

- 물리적인 피해를 입히는 목적으로, 핵무기와 원자로를 가동하는 농축 우라늄을 생산하는 데 아용되는 원심분리기를 타격한다

• 루팅(Rooting)
- 안드로이드 운영체제 에서 최상위 권한을 얻어 해당 기기의 제약을 해제하는 행위
- iOS 관련 용어인 탈옥(Jailbreaking)과 비슷하다