1. SW 개발 보안의 3대 요소 : 기무가 ( 기밀성, 무결성, 가용성 ) ( Confidentiality, Integrity, Availability )
2. SW 개발 보안 용어 : 자위취위 ( 자산, 위협, 취약점, 위험 ) ( Assets, Threat, Vulnerability )
3. Dos 공격 종류 : SYN 플러링 ( SYN Flooding ), UDP 플러링 ( UDP Flooding ), 스머프 ( Smurf ) / 스머핑 ( Smurfing ), 죽음의 핑 ( PoD : Ping of Death ), 랜드 어택 ( Land Attack ), 티어 드롭 ( Tear Drop ), 봉크 ( Bonk ), 보잉크 ( Boink )
4. DDoS 공격 구성요소 : HAMAD ( Handler, Agent, Master, Attacker, Daemon )
5. 세션 하이재킹 : 케빈 미트닉 TCP의 세션 관리 취약점을 이용
6. 네트워크 공격 : 스니핑, 네트워크 스캐너/스니퍼, 패스워드 크래킹, IP 스푸핑, ARP 스푸핑, ICMP Redirect 공격, 트로이 목마 ( Sniffing, Scanner/Sniffer, Password Cracking, IP Spoofing, ARP Spoofing, ICMP Redirect, Troian Horses )
7. 인증 기술의 유형 : 지소생특 ( 지식 기반, 소지 기반, 생체 기반, 특징 기반 인증 )
8. 접근 통제 보호 모델 : 벨기비무 ( 벨-라파듈라-기밀성, 비바 모델 – 무결성 )
9. 3A : 인증, 권한 부여, 계정 관리 ( Authentication, Authorization, Accounting )
10. 인증 관리 기술 : SSO, 커버로스, OAuth
11. 암호 알고리즘 방식

* 대칭 키 암호방식 : DES, AES, SEED, RC4
* 비대칭 키 암호 방식 : RSA ( 현재 비대칭 키 암호방식 중 가장 널리 쓰이고 있음 ), 디피-헬만 ( 암호키를 교환하는 방법 )

1. 대칭 키 암호 방식

* DES : 1975년 IBM에서 개발
* SEED : 1999년 한국 인터넷 진흥원 KISA 이 개발
* AES : 2001년 미국 표준 기술 연구소 NIST 에서 발표한 블록 암호화 알고리즘 3 DES 극복
* ARIA : 2004년 국가 정보원과 산학연구협회가 개발
* IDEA : DES를 대체하기 위해 스위스 연방기술 기관 개발
* LFSR : 시프트 레지스터의 일종
* Skipjack : NSA 에서 개발

1. 비대칭 키 암호화 알고리즘

* 디피-헬만 : 초최의 공개키 알고리즘으로 W.Diffie와 M.Hellman 이 1976년에 고안한 알고리즘
* RSA : 1977년 3명의 MIT 수학교수가 고안한 큰 인수의 곱을 소인수 분해
* ECC : 1985년 코블리치와 밀러가 RSA 암호 방식에 대한 대안으로 제안
* EIGamal : 1984년 제안

1. 해시 암호화 알고리즘

* MD5 : 1991년 R.rivest 가 MD4를 개선한 암호화 알고리즘
* SHA-1 : 1993년 NSA에서 미 정부 표준 지정 DSA 에서 사용
* SHA-256, 384, 512 : SHA 알고리즘의 한종류 256비트 해시값 생성
* HAS-160 : 국내 표준 서명 알고리즘 KCDSA를 위하여 개발된 해시 함수
* HAVAL : 메시지를 1024bits 블록으로 나눈다

1. 데이터베이스 암호화 기법 유형 : 애플티하 ( API 방식, Plug-In 방식, TDE 방식, Hybrid 방식 )
2. IPSec : 기밀성, 비 연결형 무결성, 인증, 재전송 공격 방지, 접근 제어

AH, ESP, IKE 프로토콜 ( 인증, 암호화, 키 관리 )