정보보호

주요 개념 (1)

- 보안위협(Threat)
- 취약성(Vulnerability)
- 위험(Risk)
- 공격
  - 중단(interruption)
  - 가로챔(interception)
  - 변조(modification)
  - 가공(fabrication)
- Active & passive attacks
- 정보보호 3요소
  - 기밀성(Confidentiality)
  - 무결성(Integrity)
  - 가용성(Availability)
  - + 부인방지 (nonrepudiation)

주요개념 (2)

- 식별(Identification)
- 인증(Authentication)
- 권한부여(Authorization)
  - 최소권한 원칙
- 단일사용승인(SSO : Single Sign On)
- 접근통제 모델
  - Access Control Matrix
  - ACL(Access Control List)
  - 강제적 접근통제
  - 자율적 접근통제
  - 역할기반 접근통제
- 위험관리(Risk Management)
  - 위험 분석
  - 위험 평가
- 정보보호시스템 평가 기준

주요개념 (3)

- 암호화
  - 대칭키 방식
  - 공개키 방식
- 키관리
- 해쉬함수
- 사용자 인증
- 메시지 인증
- 전자서명
- 공개키 기반 구조 (PKI)
- 인증서

주요 개념 (4)

- 해킹
- 백도어
- 트랩 도어
- 트로이목마
- 웜
- 바이러스
- 서비스거부(DoS)
- DDoS
- 경주상황(Race Condition)
- 버퍼 오버플로우 공격
- 스니핑
- 스푸핑
- 플러딩

주요 개념 (5)

- 침입탐지시스템
- SSL(Secure Socket Layer)/TLS(Transfer Layer Security)
- IPSec
  - AH(Authentication Header)
  - ESP(Encapsulation Security Payload)
- 침입차단시스템
- 가상사설망(VPN)
- 소프트웨어 역공학
- 디지털 권한 관리(DRM)
- 소프트웨어 개발 과정의 비보안성

정보보호의 의미

- 사용자
  - 보안에 대한 문제의식
- 개발자
  - 개발과정의 문제점
- 관리자
  - 시스템/망 관리자
  - 정보 관리자
  - 보안전문가