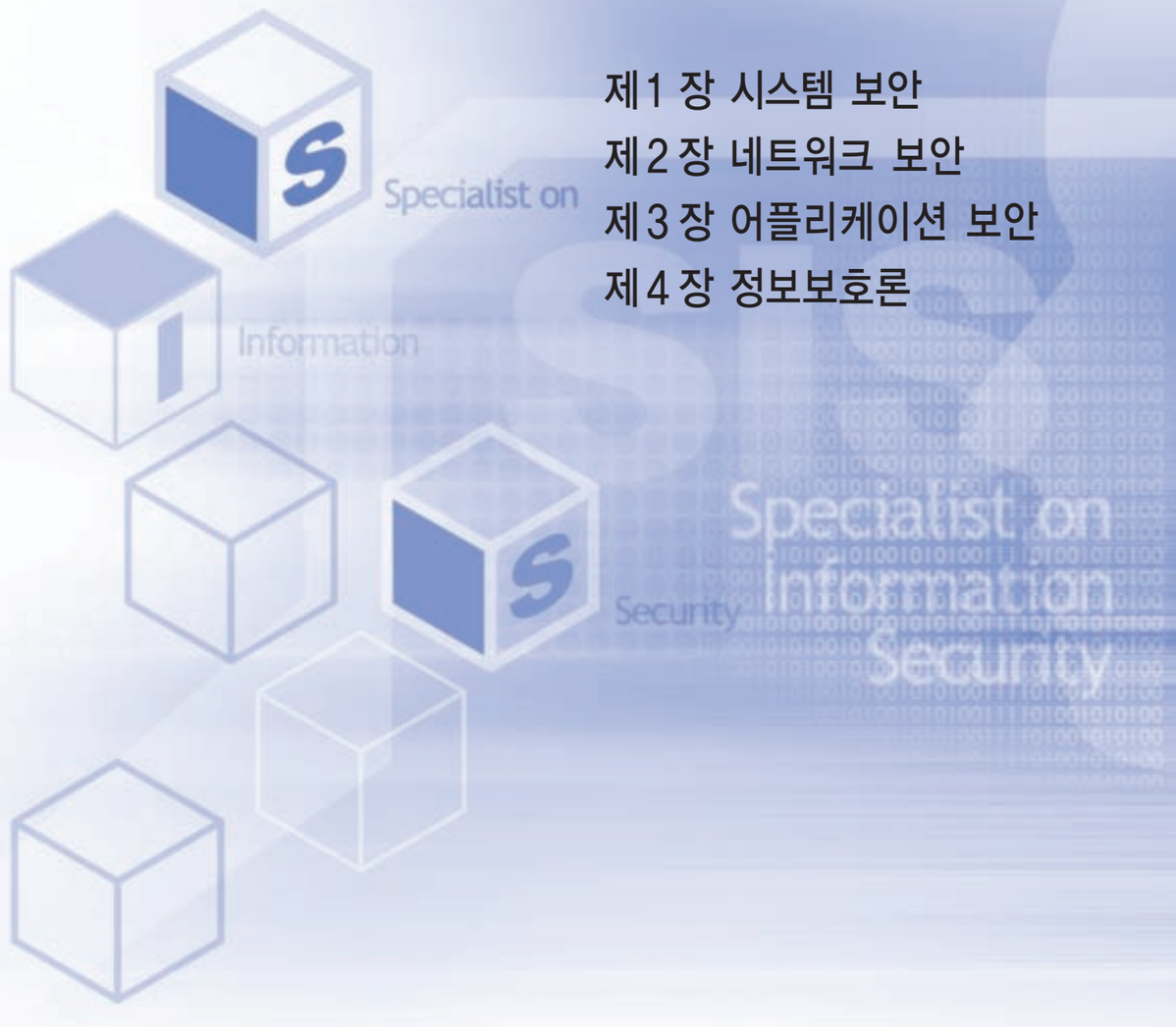
SIS 합격생 취업현황

지난해 SIS 합격생들의 취업현황을 조사한 결과, 약 86% 정도의 취업률을 기록했습니다. 이 수치는 연락이 되지 않은 사람을 포함한 것으로, 실제로는 대부분의 합격생이 취업을 한것으로 추정됩니다. 합격생들의 근무처를 살펴보면, 삼성전자, LG CNS, MS, KRNIC, 한국후지쯔, 국민은행, 중앙선관위 등 국내 유수한 기업에서 일하고 있는 것으로 나타났습니다.

2편 출제범위 및 예상문제



제1장 시스템 보안
제2장 네트워크 보안
제3장 어플리케이션 보안
제4장 정보보호론

제1장 시스템 보안

1절. 운영체제 (1급 : 10%, 2급 : 30%)

1. 운영체제 개요

시스템 프로그램으로서 운영체제가 가져야 하는 주요 기능에는 어떤 것들이 있는지 학습한다. 아울러 운영체제가 공통적으로 구축되는 공통 구조를 이해하고, 지금까지 운영체제들이 기술적인 측면에서 어떻게 발전해왔는지 이해한다.

가. 운영체제의 주요 기능

- ▶ 운영체제의 목적
  - 시스템 자원 활용도 극대화
  - 사용자 편의성 증대
- ▶ 운영체제의 기능
  - 프로그램 수행
  - 입출력 동작
  - 화일 시스템 조작
  - 통신
  - 오류 탐지
  - 계정 관리

나. 운영체제의 구조

- ▶ 커널과 유틸리티
  - 시스템 호출
- ▶ 이중 모드(dual mode) 구조
  - 일반 모드(사용자 모드)
  - 관리 모드(모니터 모드)
- ▶ 프로세스 관리
- ▶ 주기억 장치 관리
- ▶ 보조기억 장치 관리
- ▶ 입출력 시스템 관리
  - 장치 구동기(device driver)
  - 인터럽트 방식과 DMA 방식
  - 버퍼링과 스풀링
- ▶ 파일 관리
- ▶ 인터럽트
  - 인터럽트의 개념
  - 인터럽트의 종류
- ▶ 기타 관련 용어

다. 운영체제의 기술 발전 흐름

- ▶ 초기 운영체제
  - 단순 모니터
  - 상주 모니터
  - 작업 제어 언어(JCL)
- ▶ 일괄처리와 대화식
- ▶ 오프라인과 온라인
- ▶ 단일 사용자용과 다중 사용자용
- ▶ 다중 프로그래밍 운영체제
- ▶ 시분할 운영체제
  - 타임 슬라이스(time slice)
- ▶ 분산 운영체제
- ▶ 다중 처리기용 운영체제
  - 대칭형과 비대칭형

2. 운영체제의 주요 구성 기술

운영체제를 구성하는 주요 구성 기술 가운데서 프로세스 관리 기술, 기억장치 관리 기술, 파일 시스템 관리 기술을 중심으로 학습한다. 네트워크 기반으로 동작하는 분산 시스템을 지원하기 위하여 운영체제가 어떤 기능을 추가적으로 제공해야 하는지 이해한다.

가. 프로세스 관리

- ▶ 프로세스의 개념
  - 프로세스 상태
  - 프로세스 제어 블록
- ▶ 병행 처리와 프로세스
  - 프로세스 생성과 종료
  - 프로세스들간의 관계
  - 쓰레드(thread)와 태스크(task)
- ▶ 프로세스 스케줄링
  - 다중 프로그래밍과 스케줄링
  - 프로세스 큐
  - 스와핑(swapping)
- ▶ 스케줄링 알고리즘
  - 사용되는 기준
  - 선입 선처리(FCFS, FIFO) 스케줄링
  - 최소작업(SJF, shortest-job-first) 스케줄링
  - 최소잔여시간(SRT, shortest remaining time) 스케줄링
  - 우선순위(priority) 스케줄링
  - 순환 할당(RR, round-robin) 스케줄링
  - 다단계 큐(multi-level queue) 스케줄링
  - 다중 프로세서 스케줄링
- ▶ 프로세스간 협조
  - 생산자-소비자 모델
  - 경쟁조건(race condition)
  - 임계영역(critical section) 문제
  - 동기화 하드웨어(test-and-set)
  - 세마포(semaphore)
  - 프로세스간 통신(IPC)
- ▶ 교착상태
  - 교착상태(deadlock) 발생 조건
  - 자원할당 그래프
  - 교착상태의 예방, 회피, 탐지, 회복

나. 기억장치 관리

- ▶ 계층적 기억장치 구조
- ▶ 메모리 할당 기법
  - 최초 적격(first-fit)
  - 최상 적격(best-fit)
  - 최악 적격(worst-fit)
- ▶ 메모리 단편화 문제
  - 단편화의 원인
  - 압축을 통한 단편화 제거
- ▶ 페이지 기법
  - 페이징 하드웨어
  - 페이지 테이블
  - 공유 페이지
  - 메모리 교체(swapping)
  - 메모리 보호(protection)
- ▶ 세그먼테이션 기법
  - 세그먼테이션 하드웨어
  - 세그먼크 테이블
  - 세그먼트 페이징 기법
- ▶ 가상기억장치(virtual memory)
  - 가상기억장치의 개요 및 특징
  - 요구 페이징 기법
  - 페이지 교체(replacement) 알고리즘
    - · 선입선출(FIFO) 알고리즘
    - · 최적 페이지 교체(optimal) 알고리즘
    - · LRU 알고리즘
    - · LRU 근접 알고리즘
    - · 기타 알고리즘
  - 다중 프로그래밍과 스래싱(thrashing)
  - 작업 설정(work set) 모델
- ▶ 디스크와 디스크 스케줄링
  - 디스크의 구조
  - 가용 공간 관리 기법
  - 할당 방법 : 연속할당, 연결할당, 색인할당
  - 디스크 스케줄링 알고리즘
    - · 선입선처리(FIFO) 스케줄링
    - · 최소 탐색 우선(SSTF) 스케줄링
    - · 스캔(SCAN) 스케줄링
    - · LOOK 스케줄링

다. 파일 시스템 관리

- ▶ 파일과 디렉토리
  - 파일 조작 : 생성, 기록, 판독, 재설정, 삭제 등
- ▶ 디렉토리 구조
  - 다단계(1,2단계) 디렉토리 구조
  - 트리 구조 디렉토리
  - 그래프 디렉토리
- ▶ 파일 접근 방법
  - 순차 접근
  - 직접 접근

라. 분산 시스템

- ▶ 네트워크 운영체제(NOS)
- ▶ 분산 운영체제의 주요 특징
  - 자료이동
  - 연산 이동
  - 프로세스 이동
- ▶ 분산 시스템에서의 운영체제 기술
  - 사건 순서화(event ordering)
  - 상호 배제(mutual exclusion)
  - 교착 상태의 예방과 탐지
  - 선출(election) 알고리즘
- ▶ 분산 파일 시스템
  - 명칭 부여 구조(naming scheme)
  - 원격 프로시저 호출(RPC)
  - 캐시 기법
  - 파일 중복(replication) 기술

3. 운영체제 사례별 특징과 주요 기능

현존하는 운영체제 가운데서 가장 보편적으로 사용되고 있는 유닉스 및 윈도우 계열 운영체제의 특징과 주요 기능을 이해하고 구체적인 활용을 위한 주요 명령과 유틸리티를 학습한다. 전통적인 유닉스에서 출발하였으나 나름대로의 사용자층을 보유하고 있는 리눅스에 대해서도 이해한다.

가. 유닉스

▶ 유닉스의 특징과 주요 계보
- 운영체제로서의 유닉스 특징
- SVR과 BSD
- AIX, SunOS(Solaris), IRIX, DEC UNIX, HP UX

▶ 유닉스 쉘
- 쉘(shell)의 기능과 종류: sh, csh, ksh
- 간단한 쉘 프로그래밍

▶ 일반 사용자를 위한 유닉스 활용법
- 일반사용자용 주요 유닉스 명령
- 주요 유틸리티

▶ 유닉스 시스템 관리법
- 유닉스 시스템의 내부 구조
- 시스템 관리자용 주요 유닉스 명령

나. 윈도우

▶ 윈도우의 특징과 주요 계보
- 운영체제로서의 윈도우 특징
- 윈도우 9x 계열과 윈도우 NT 계열

▶ 윈도우 종류별 주요 활용법

다. 리눅스

▶ 리눅스의 특징과 주요 배포판
- 유닉스의 차별화된 특징
- X-윈도우 시스템
- 터보리눅스, 레드햇, 데비안, 수세, 칼데라, 맨드레이크, 슬랙웨어, FreeBSD 등

▶ 리눅스 쉘
- 쉘(shell)의 기능과 종류 : bash
- 간단한 쉘 프로그래밍

▶ 리눅스 시스템 관리법
- 시스템 설치 및 장치 설정
- 사용자 관리
- 네트워크 환경 설정
- 웹서버 설치 : Apache, PHP, MySQL

예제문제

(1) PCB(프로세스 제어 블록)은 프로세스에 대한 여러 가지 중요한 정보를 보유하고 있다. PCB에 들어가는 일반적인 정보로 보기 힘든 것은?
① 프로세스의 우선 순위
② 부모 프로세스
③ 프로세스의 현재 상태
④ 프로세스에 할당된 자원을 가리키는 포인터
⑤ 프로세스의 종료 예상 시각

[정답] ⑤
[난이도] 하
[해설] 프로세스의 종료 예상 시각을 기록하기 위해서는 상당한 오버헤드를 감수해야 한다. 따라서 SRT와 같은 일부 스케줄링 알고리즘에서는 이를 감수하면서도 활용하기는 하지만 프로세스 제어 블록에 저장되는 일반적인 정보는 아니다.

(2) 세마포(S, Semaphore)와 관련된 두 연산으로 P(S)와 V(S)를 꼽는다. 다음 빈칸에 들어갈 표현을 모두 적절하게 나열한 것은?
- 연산 P(S) : IF S 〉 0 THEN S ← (가) ELSE (S를 기다림)
- 연산 V(S) : IF (1개 이상의 프로세스가 S를 대기중) THEN (그 중 1개의 프로세스만 진행) ELSE S ← (나)

① 가. S − 1 나. S − 1
② 가. S + 1 나. S + 1
③ 가. S + 1 나. S − 1
④ 가. S − 1 나. S + 1
⑤ 가. 1 나. 0

[정답] ④
[난이도] 상
[해설] P(S)는 상호배제를 위한 임계 영역에 들어가는 작업으로서 세마포 값을 감소하게 되며, V(S)는 임계영역을 빠져나오며 P(S)와 반대의 역할을 한다.

(3) 윈도우 운영체제에서 사용할 수 있는 네트워크 관련 명령들을 가운데서, 현재 PC의 IP 주소와 DNS 서버 정보 등을 출력해볼 수 있을 뿐 만 아니라, DHCP 서비스 중일 경우 새로운 IP 주소를 얻을 수 있는 명령은?
① winipcfg
② tracert
③ netstat
④ ping
⑤ nbtstat

[정답] ①
[난이도] 중
[해설] tracert는 원격 컴퓨터로의 라우팅 정보를 검사한다. netstat는 현재의 TCP/IP 접속 상태와 통계를 표시한다. ping은 하나 이사의 원격 컴퓨터에 대한 접속 상태를 확인하여 준다. nbtstat은 NetBIOS의 접속상태를 검사하여 등록된 이름과 영역 ID의 상태를 결정한다.

2절. 클라이언트 보안 (1급 : 20%, 2급 : 50%)

1. 윈도우 보안

마이크로소프트사의 윈도우 운영체제(9x, NT, 2000, XP)에 대하여 클라이언트 측면에서의 주요 시스템 관리 기능을 학습한다. 특히, 보안 측면에서 중요한 공유자료 관리, 레지스트리 활용과 악성코드 대처 방법을 이해한다.

가. 설치 및 관리

▶ 윈도우 운영체제별 설치 및 업데이트

▶ 윈도우 운영체제 활용
- 제어판 활용
- 시스템 도구와 통신 활용

나. 공유자료 관리

▶ 파일시스템 이해 : NTFS

▶ 네트워크 드라이브의 이해

▶ 공유폴더 보안
- 사용권한 설정
- 폴더 옵션 활용

다. 바이러스와 백신

▶ 악성코드에 대한 이해
- 컴퓨터 바이러스
- 트로이목마
- 인터넷 웜
- 메일 폭탄
- 스파이웨어

▶ 컴퓨터 바이러스 종류별 명명법과 주요 특징 이해

▶ 안티바이러스의 종류와 활용법
- V3, Virobot, Norton AV, PC-cillin, McAfree VirusScan 등

라. 레지스트리 활용

▶ 윈도우 레지스트리의 기본 개념과 활용
- 레지스트리의 기본 개념과 구조
- 레지스트리의 백업과 복원
- 관련 파일 : SYSTEM.DAT, USER.DAT, SYSTEM.INI, WIN.INI

▶ 레지스트리의 편집과 활용
- Regedit를 통한 레지스트리의 편집
- 트로이목마 서버 S/W 사례별 발견과 제거

2. 인터넷 활용 보안

다양한 인터넷 서비스를 안전하게 받기 위하여 각각의 인터넷 서비스들과 관련된 보안 문제점과 해결책을 학습한 후 이를 시행하는 실무 과정을 이해한다.

가. 웹브라우저 보안

▶ 인터넷 익스플로러의 도구 메뉴의 인터넷 옵션
- 보안
- 개인정보
- 내용 : 내용관리자(인터넷 내용등급 서비스), 인증서 활용
- 연결 : VPN 설정

▶ 웹브라우저의 보안 취약성 갱신
▶ 웹브라우저 활용시의 오류 메시지 대처

나. 메일 S/W 보안

▶ Outlook 및 Outlook Express 보안
- Outlook의 주요 공격 대상 : 주소록, 메일 폴더, Visual Basic 파일
- 메일 필터링 기법
- 첨부 파일 보안
- PGP 활용

▶ 웹기반 메일 서비스 보안
- 웹기반 메일 서비스의 보안 취약성
- 코드 기반 공격
- SSL 활용
- PGP 활용

다. 기타 인터넷 S/W 보안

▶ ICQ, IRC의 보안 취약성과 대처방법
▶ 메일 서버 스캐너의 주요 기능과 사례
- Procmail과 Sanitizer
- Inflex 등

3. 공개 해킹도구에 대한 이해와 대응

클라이언트 컴퓨터에 대한 정보 보호 침해를 일으키는 공개 해킹도구들을 특징에 따라 몇 가지로 분류하고 이들 중 대표적인 소프트웨어에 대한 이해 및 대응 방법을 학습한다.

가. 트로이목마 S/W

▶ 트로이목마의 개요
▶ 트로이목마 S/W 사례별 이해
- NetBus
- Back Orifice
- School Bus 등

나. 크래킹 S/W

▶ 크래킹의 개요
▶ 크래킹 S/W 사례별 이해
- WWWhack
- Golden Eye 등

다. 포트 스캐닝 S/W

▶ 포트 스캐닝의 개요
▶ 포트 스캐닝 S/W 사례별 이해
- Aat4xx
- Super Scan 등

라. 키로그 S/W

▶ 키로그의 개요
▶ 키로그 S/W 사례별 이해
- Winhawk
- Keylog25 등

마. 기타 S/W

▶ 누킹 S/W : Vconnect, Cgsioob 등
▶ 폭탄 메일 S/W : QuickFyre, Avalanche, Anonymail, eremove 등

4. 도구활용 보안관리

클라이언트 PC에 대한 정보 보호 수준을 높이기 위한 적극적인 방법으로 전문적인 보안도구를 활용하는 것이 필요해지는데 이러한 PC용 보안도구들을 이해한 후 실무에서 운영하는 방법을 학습한다. 아울러 다수의 클라이언트용 PC들을 효율적으로 관리하며 높은 수준의 보안 상태를 유지하기 위한 전문 보안도구에 대해서도 익힌다.

가. PC용 보안도구 활용

▶ 공개해킹도구에 대한 대응 S/W
- BlackICE
- BO2K Server Sniper
- BO Remover, NoBo
- NoNuke
- Visual Route 등

나. PC용 방화벽 운영

▶ PC용 방화벽의 기본 개념과 용어
- 블로킹(blocking) : 포트, IP 주소
- 접근 제어 목록(ACL)
- 실행 제어 목록(ECL)
- 침입 탐지 기능
- False Positive

▶ PC용 방화벽의 종류와 활용법
- TIS-FWTK
- MR. Flux
- ZoneAlarm
- BlackICE Defender
- eSafe 등

다. PC실 관리 및 보안

▶ PC 실습실 관리 기능 이해
▶ PC 실습실 관리용 S/W 사례별 활용 이해
▶ PC 실습실 관리용 H/W 사례별 활용 이해
- 하드디스크 보안관
- 리본카드

예제문제

(1) 웹브라우저로 특정 사이트를 검색하고자 URL 입력하여 검색을 시작하자, 다음과 같이 "HTTP 404 오류"가 발생하였다. 이 오류에 대한 올바른 처리방법은?

① DNS에 해당 URL의 웹서버가 등록되도록 DNS 관리자에게 연락한다.
② 해당 웹서버에 지정한 웹페이지가 존재하지 않으므로 URL이 올바른지 확인하거나, URL 소유자에게 웹페이지 제공 여부를 문의한다.
③ 통신량이 적은 시간대에 다시 접근해본다.
④ URL의 웹서버 이름이 표기법상 잘못 기술되어 있으므로 구두점을 비롯하여 URL 이름과 관련된 맞춤법의 정확성을 검토한다.
⑤ 메일 서버와 뉴스 서버에 관한 환경을 다시 설정한다.

[정답] ②
[난이도] 하
[해설] 웹브라우저를 활용할 때 접하는 404 오류는 존재하지 않는 파일을 요청한 경우에 발생한다.

(2) 윈도우 바이러스가 처음 실행되는 영역과 나중에 후킹하고자 하는 대상 영역은?
① Ring 0 – Ring 3
② Ring 1 – Ring 0
③ Ring 0 – Ring 1
④ Ring 3 – Ring 0
⑤ Ring 0 – Ring 0

[정답] ④
[난이도] 중
[해설] 윈도우 운영체제에서 일반 프로그램이 실행되는 영역인 Ring 3에서 바이러스가 감염된 프로그램이 실행된 후, 시스템 영역인 Ring 0를 후킹(hooking)하게 된다.

(3) 백오리피스(BO)를 트로이목마형태로 변화시키는데 사용하는 프로그램은?
① AdAware
② inflex
③ SaranWrap
④ OptOut
⑤ Ultra-Edit 32

[정답] ③
[난이도] 상
[해설] AdAware와 OptOut은 스파이웨어를 제거하는 프로그램이다. Ultra-Edit 32는 2진수로 된 파일을 16진수로 변환하여 보여주는 프로그램이다. inflex는 바이러스 메일을 걸러주는 메일 서버 스캐너 프로그램이다.

3절. 서버 보안 (1급:70%, 2급:20%)

서버를 운영함에 있어서 필요한 보안 요구사항과 그에 대한 관리 방법에 대하여 학습한다. 특히 인증과 접근통제 기법, 보안 관리 측면에서의 요구 사항, 운영체제 및 서버 보안용 소프트웨어의 설치와 운영 시에 필요한 사항을 주요 내용으로 하고 있다.

1. 인증과 접근 통제

서버 운영에 있어서 인증 및 접근통제는 보안 관리를 위한 필수적인 요소이다. 유닉스 계열이나 윈도우즈 계열에서 계정과 패스워드를 운영하고 있으나, 패스워드에 대한 보호 정책에 일반 사람들은 무관심한 상태이다. 또한, 파일 시스템이나 운영체제를 보호하기 위한 방법으로 접근통제 및 여러 가지 환경 설정 방법을 운영할 수 있다. 인증과 접근통제 부분에서는 이러한 내용을 다룬다.

가. 계정과 패스워드 보호

▶ 시스템에서 사용하는 기본적인 접근 통제 방법
- 사용자 계정은 하나의 시스템을 여러 사람이 이용할 때 그들을 구분하는 역할
- 패스워드는 각 계정 사용자를 확인하기 위하여 사용
- 그룹은 목적을 같이하는 사용자들을 묶은 것으로써 그룹에 대한 권한 및 허가를 설정하고 관리

▶ 계정 및 패스워드 보호 정책
- 효과적인 계정 관리 기법 사용
  - · 사용자별 권한 그룹을 지정하여 관리
  - · root 권한에 대한 사용을 제한
  - · guest, anonymity 등의 특정 공개용 계정의 사용을 제한
- 안전한 패스워드 관리 기법 사용
  - · 예측하기 쉬운 패스워드를 사용하지 않음
  - · 패스워드 파일을 암호화하여 보관하고 무결성을 위해 이미지 파일 보관
- 여러 운영체제에 따라 적용하는 패스워드 방식
  - · 윈도우즈 NT에서 사용하는 계정과 패스워드 관리 기법
  - · 유닉스 계열에서 사용하는 계정과 패스워드 관리 기법
- 여러 가지 패스워드 방식
  - · OTP(One Time Password) 방식, PAM(Pluggable Authentication Modules)을 통한 인증 방법, SSH를 사용한 암호화 통신 등

나. 파일 시스템 보호

▶ 유닉스에서의 파일 시스템 구성 내용
- 유닉스 시스템에서는 각 파일마다 한 명의 소유자가 존재함
- 유닉스에서 파일은 그 파일의 소유자와 root만 변경 가능함
- mount 명령을 통하여 여러 파일 시스템을 연결하여 사용함
- SUID와 SGID를 이용하여 권한 밖의 자원에 대한 접근을 허용함

▶ 윈도우즈 NT에서의 파일 시스템 구성 내용
- 윈도우즈 NT의 파일 시스템 형식 : NTFS, FAT 등
- administrator 계정의 사용 권한 관리 방법
- 목적에 따른 계정 그룹의 사용 방법

▶ 파일 시스템 보호 정책
- 파일 시스템 백업(backup) 및 복구 방법
- 무결성 도구를 이용한 파일 시스템의 무결성 검사
- 파일 및 디렉토리 관리 기법

다. 시스템 파일 설정과 관리

▶ 유닉스에서의 시스템 파일 설정
- mount 테이블을 이용한 파일 시스템 관리
- 호스트에 대한 접근통제 내용의 설정 방법
- 네트워크 서비스에 대한 내용의 설정 방법
  - · ftp, telnet, http, rlogin, ssh, scp, samba 등
- X 윈도우 사용을 위한 환경 설정 및 관리 기법
- 시스템 로그 파일의 기록을 위한 환경 설정 및 관리 기법

▶ 윈도우즈 NT에서의 시스템 파일 설정
- NTFS에 대한 접근통제 수행 방법
- SAM을 통한 인증 서비스 수행 방법
- 관리용 공유 폴더의 유지 및 관리 기법
- 윈도우즈 환경의 레지스터리에 대한 보존 및 관리 기법

라. 시스템 접근통제 기술

▶ 주체와 객체간의 관계를 지정하고 접근을 제한하는 방법
- 접근통제 리스트 및 여러 가지 접근통제 관리 기법

▶ 접근통제 기술 분류 방법
- 강제적 접근통제 정책(MAC), 임의적 접근통제 정책(DAC), 역할기반 접근통제 정책(RBAC)등

▶ 접근통제 도구
- drawbridge, IPACL(IP ACcess List), IP packet filter for SunOS, Permissions, Screend, Tcp Wrapper 등

▶ 유닉스 계열의 접근통제
- 계정과 그룹에 대한 허가권 설정 및 변경 방법
- 패스워드 및 그룹 파일의 유지 및 관리 방법

2. 보안 측면의 관리

보안 측면의 관리에서는 시스템을 운영함에 있어서 필요한 보안 요소와 시스템 해킹으로부터 서버를 안전하게 보호하기 위한 서버 관리자의 임무에 대하여 이야기 한다. 운영체제를 설치하고 시스템 최적화 및 시스템 로그 관리를 수행하는 방법을 주요 내용으로 하고 있다.

가. 시스템 보안 등급

▶ 시스템 보안 평가 기준
- 정보 시스템 보안 평가 등급 기준
  - · 국가별 정보보호 시스템 평가 기준 : TCSEC, ITSEC, CTCPEC 등
  - · 국제 공통 평가 기준 표준 : CC
  - · 국내 평가 기준 : CC와 유사한 기준 제시 (침입차단 시스템, 침입탐지 시스템)
- 각 등급별 보안 요구사항

나. 운영체제 설치

▶ 시스템 파티션과 마운트
- 작업 용도에 따른 시스템의 파티션 분리
  - · 커널 파티션, 데이터 파티션, 소프트웨어 파티션 등
- 여러 가지 저장 매체를 사용가능 하도록 마운트

▶ 운영체제 커널과 소프트웨어 설치
- 유닉스 계열의 운영체제 커널 설치
  - · 운영체제 커널과 그에 맞는 소프트웨어 설치
  - · 커널 재구성 : HP-UX, Solaris, AIX, Linux 등
- 윈도우즈 계열의 운영체제 설치

다. 시스템 최적화

▶ 자원 관리의 최적화
- 메모리 관리
  - · 동적 메모리 관리, 스택/힙 영역 관리
- 프로세스 및 CPU 관리
  - · 좀비 프로세스 관리, 프로세스 우선 순위 관리 등

▶ 사용자 및 파일 관리
- 사용자별 사용 제한 설정
- 사용자별 홈 디렉토리 설정 및 접근 제어 기능

▶ 최소권한(least privilege)
- 보안에 대한 취약요소를 줄이기 위한 최소 권한의 프로세스 수행

라. 시스템 로그 설정과 관리

▶ 시스템 로그(syslog)
- 운영체제 제어 하에 시스템 관련 중요 이벤트에 대한 로그
  - · syslog, klog, 윈도우즈 이벤트 로그 등.

▶ 응용프로그램 로그
- 트렌젝션 로그
  - · 응용 트랜잭션 로그, 데이터베이스 로그, 운영체제 로그, 접근통제 로그, 통신 로그, 메일 로그, 웹 서버 로그 등
- 에러 로그
  - · 응용프로그램의 수행 도중 에러가 발생하였을때 생성되는 로그

마. 서버 해킹 원리 이해

▶ 시스템 해킹은 정보 시스템의 결함으로 생기는 보안 허점을 활용

▶ 직접 대입 공격
- 무차별 공격(brute force)
- 사전 공격(dictionary attack)

▶ 네트워크 공격

- 스푸핑(Spoofing)
  IP 주소 등의 정보를 속임으로써 권한을 획득하고 중요 정보를 가로채고 서비스 방해까지 행하는 공격
  · Session Hijacking, IP Spoofing, DNS Spoofing, ARP Spoofing, Mail Spoofing 등
- 스니핑(Sniffing)
  네트워크 패킷이나 버스를 통해 전달되는 중요 정보를 엿보고 가로채는 공격 행위
  · packet sniffer, spyware, keystroke monitoring 등
- 서비스 거부 공격(Denial of Service)
  대량의 패킷을 이용하여 네트워크를 마비시키거나 특정 서비스의 수행을 방해하는 공격
  · DOS, DDOS, 시스템 DOS 등

▶ 시스템 오류를 이용한 공격
- 버퍼 오버플로우(buffer overflow) 공격
  · 시스템의 스택과 같은 버퍼에 저장 가능한 용량 이상의 데이터를 보냄으로써 버퍼 영역 밖의 시스템 영역에 해커가 특정 데이터를 기록함으로써 권한을 획득하고자 하는 공격
  · eject, xinetd, fdformat 등
- 경쟁 상태(race condition) 공격
  두 가지 이상의 명령이 실행되는 동안 시간 차이나 임의로 생성된 파일을 이용한 공격
  · ffbconfig, ps, amountd 등

▶ 사회공학적 방법

바. 서버 관리자의 의무

▶ 시스템 시작과 종료
- 시작(booting)
  · 새로운 장치 설치, 시스템 사용환경 설정, 시스템의 초기화 등
- 종료
  · shutdown, halt, reboot 등의 명령을 통하여 시스템의 종료 수행

▶ 사용자 계정 관리
- 패스워드, 그룹 파일 관리
  · /etc/passwd, /etc/group, /etc/shadow 등의 사용자 계정관련 파일 관리

▶ 자원 관리
- 프로세스 관리
  · ps, kill, wait, su 등을 사용한 프로세스 관리
- 메일, 디스크, 메모리 등의 자원 관리
  · 사용자 메일 사용량, 디스크 사용량, 메모리 및 프로세스 사용량에 대한 제한을 설정하여 자원 관리

▶ 네트워크 관리
- 네트워크 연결 관리
  · IP 주소, DNS, 라우터, 네트워크 서비스에 대한 설정을 관리
- 네트워크 상태 관리
  · 네트워크 자원 사용량 측정 및 로드 분산

3. 서버 보안용 S/W 설치 및 운영

서버 보안을 위한 소프트웨어를 설치하고 운영하는 방법에 대하여 이야기 한다. 시스템 취약점 점검 도구, 침입탐지 시스템, 무결성 검정 도구, 감사로그 등과 같은 보안 소프트웨어의 종류, 특성, 사용 방법 및 결과 분석을 주요 내용으로 하고 있다.

가. 시스템 취약점 점검 도구

▶ 보안 취약성 및 위협
- 모든 정보 시스템은 취약성이 존재하며 완벽하게 안전한 시스템은 존재하지 않음
- 보안 취약성
  · 물리적 취약성, 자연적 취약성, 환경적 취약성, 하드웨어 취약성, 소프트웨어 취약성, 매체 취약성, 전자파 취약성, 통신 취약성, 인적 취약성 등으로 구분
- 보안 위협
  · 자연에 의한 위협, 인간에 의한 비의도적 위협, 인간에 의한 의도적 위협 등으로 구분

▶ 취약점 점검 도구
- SAINT, SATAN, COPS, ISS, K-COPS, nessus, gabriel 등

나. 시스템 침입 탐지 시스템

▶ 침입탐지 시스템의 특징
- 침입탐지 시스템은 정보 수집, 가공, 침입탐지 처리, 보고 등으로 구성
  · 정보 수집 : 감사 로그나 네트워크 패킷 정보를 수집
  · 정보 가공 : 침입탐지 시스템이나 침입대응 시스템에서 이용하기 편리하도록 정보를 가공하여 보관
  · 침입탐지 처리 : 이벤트 정보와 프로파일이나 공격관련 규칙을 비교하여 침입탐지 수행
  · 침입 보고 : 탐지된 행위에 대하여 보안 관리자 등에게 침입행위를 알림
- 침입탐지 시스템의 원리
  · 오용 기반 침입탐지 : 알려진 취약점을 기반으로 탐지 규칙을 작성하여 침입행위를 판단
  · 비정상행위 탐지 : 사용자나 시스템의 정상행위에 대하여 프로파일링을 수행한 후에 실제 발생한 이벤트의 정상유무를 판단

▶ 네트워크 모니터링
- 네트워크 모니터링 및 침입탐지 도구
  · Snort, Shadow 등
- 방화벽
  · TCP-Wrapper, IPCHAIN 등

▶ 침입대응 방법
- 가볍게 침입행위를 소리나 시스템 메시지로 알리는 대응부터 공격자의 세션을 끊고 공격자에 대한 정보를 수집하는 대응까지 다양한 방법이 사용됨

다. 무결성 점검 도구

▶ 시스템 무결성 검증
- 시스템 커널의 이미지를 복사하고 백업 보관하여 시스템 자체의 무결성을 검증
- 컴퓨터 포렌식스 용도로 사용하기 위한 시스템의 이미지 사본 저장

▶ 파일 무결성 점검
- 시스템 전체보다 중요한 파일이나 디렉토리에 관련된 정보를 보관한 후 불법적인 변조나 삭제가 있었는지를 점검함
  · tripwire, MD5 등

라. 접근통제 및 로깅 도구

▶ 유닉스 환경의 접근통제
- 그룹 영역을 설정하여 사용자별 그룹 관리
  · 객체에 대한 소유권을 부여하여 소유자 이외에는 접근이 어렵게 함
  · 비슷한 일을 수행하는 사용자에 대한 그룹을 부여하여 그룹별 접근통제 수행
- 파일이나 디렉토리에 대한 퍼미션 적용
  · 읽기/쓰기/실행 퍼미션을 적용하여 파일에 대한 접근통제 관리
  · sticky bit, set user id bit, set group id bit의 설정으로 융통성있는 접근통제 관리
- 접근통제 관련 로깅 도구
  · 유닉스 환경에서는 syslogd를 통하여 여러 가지 접근통제 위반 내용 및 허가권 변경 사항을 메시지로 기록할 수 있게 함

▶ 윈도우즈 환경의 접근통제
- administrator 권한의 수행
- 사용자 및 그룹별 접근 통제 수행
- 윈도우즈 NT 이상 시스템에서는 시스템 이벤트 로그 정보 기록

마. 스캔 탐지 도구

▶ 스캔 공격
- 알려진 취약점 점검 도구를 통한 공격
  · SATAN, SAINT, COPS, nessus, nmap 등
- 취약점을 찾기위한 공격용 도구
  · mscan, sscan 등

▶ 스캔 탐지 방법
- 네트워크 스캔 공격은 일반적으로 여러 포트의 존재 여부를 검사함
- 실시간 스캔 탐지 도구의 활용

바. 로깅 및 로그 분석 도구

▶ 로깅 정보
- 감사 증적(audit trail), 감사(auditing), 감사로그(audit log)
  · 감사 정보는 그 정보의 변조가 없다는 가정하에 법적 증거로써 사용 가능함
  · 따라서 감사로그의 보호 및 백업 방법이 필요함
- 감사로그 분석
  · 사후 감사로그 분석 : 일반적으로 많이 사용되었던 방식으로 사건 발생 후에 감사로그를 모아 놓고 집중적으로 분석 수행
  · 주기적 감사로그 분석 : 주기적으로 감사로그를 분석하여 시스템 침해가 있었는 지를 검사
  · 실시간 감사로그 분석 : 감사로그 파일을 실시간 탐지 시스템에 연결하여 시스템 침해가

발생하는 것을 실시간으로 탐지하고 대응함

▶ 로그 분석 도구
- 감사로그는 그 크기가 엄청날 수 있기 때문에 감사로그에 대한 축약 방법 및 백업 방법이 중요함
- 감사로그의 불법적인 변조나 삭제가 발생하였을 경우 감사로그의 증거로써 활용 가능성이 떨어지기 때문에 감사로그에 대한 변화를 탐지하는 방법이 필요함
- 감사로그를 이용하여 공격이 있었는지를 탐지하는 도구가 필요함

예제문제

(1) 다음은 계정 보안 방법에 관한 설명이다. 틀린 것은?
① 사용자 패스워드에 대한 암호화를 위해 MD5를 사용한다.
② SSL, PGP와 같은 암호화 프로토콜 사용한다.
③ 시스템관리의 편의를 위해 계정과 패스워드를 일치시킨다.
④ PAM 모듈을 이용하여 특정 그룹 및 계정의 접속을 제한한다.
⑤ 시스템에서 기본적으로 사용하지 않는 계정은 삭제한다.

[정답] ③
[난이도] 하
[해설] 서버를 운영함에 있어서 계정과 패스워드에 대한 보안은 중요하다. 사용자 계정에 대한 패스워드는 다른 사람이 이용하는 것을 방지하기 위해 암호화 하여 저장하며 네트워크 통신에서도 암호화 프로토콜을 사용하여 전달하여야 한다. 또한, 불필요한 계정은 삭제하고 접근통제 방법을 적용하여 객체에 대한 접근권한을 달리하는 것이 필요하다. 그리고, 패스워드는 쉽게 추측할 수 없도록 특수문자를 섞어서 사용하여야 하고, 연속적인 시스템의 침해를 예방하기 위하여 여러 시스템의 동일 계정에 대한 패스워드는 서로 다르게 하는 것이 좋다.

(2) 네트워크에서 쓰지 않는 컴퓨터 자원을 찾아 취약점을 확인하고 작은 세그먼트 내에서 그 프로그램을 실행하는 것을 무엇이라고 하는가?
① 컴퓨터 바이러스(Computer Viruses)
② 트로이 목마(Trojan Horses)
③ 비동기 공격(Asynchronous Attack)
④ 인터넷 웜(Internet Worms)
⑤ 서비스 거부 공격(Denial of Service)

[정답] ④
[난이도] 하
[해설] 위의 설명은 웜에 대한 설명이다. 컴퓨터 바이러스는 자체를 복제하고 다른 프로그램에 그것을 삽입함으로써 번식한다. 트로이 목마는 정상처럼 보이지만 해로운 프로그램 코드를 포함하고 있는 프로그램이다. 비동기 공격은 프로그램이 쉬고 있을 때 합법적인 데이터나 코드를 변경하는 간접적인 공격으로 실행된 후에 목적 프로그램이 변경되도록 한다. 서비스 거부 공격은 네트워크 포트로 대량의 패킷을 보냄으로써 네트워크 서비스를 수행할 수 없도록 하는 것이다.

(3) NTFS 보안 기능의 하나이며, 컴퓨터의 선택된 자원에 대한 접근을 추적할 수 있는 기능은 무엇인가?
① 소유권(Ownership)
② 감사(Auditing)
③ 허가권(Permissions)
④ 접근통제 리스트(Access Control List)
⑤ 트랜잭션 기록(Transaction Logging)

[정답] ②
[난이도] 중
[해설] NTFS는 윈도우즈 NT에서 관리하는 파일 시스템의 한 형식이다. 이 시스템에서는 소유권에 대한 접근통제 등을 수행할 수 있으며 자원에 대한 접근 내역을 추적할 수 있다. 감사(auditing)는 이러한 자원에 대한 감사 추적을 수행하는 기능을 말한다.

(4) 시스템 환경 설정 관리의 주요 목적은 무엇인가?
① 시스템 유지보수(system maintenance)
② 시스템 안정화(system stability)
③ 시스템 운영(system operations)
④ 시스템 추적(system tracking)
⑤ 시스템 감사(system auditing)

[정답] ②
[난이도] 중
[해설] 시스템 환경 설정 관리의 주요 목적은 시스템 기능, 특징, 동작이 바람직한 방향으로 제어되고 전체 시스템이 안정적으로 수행되는 것을 보장하는 것이다.

(5) 임의적 접근제어(DAC)에 대한 설명으로 틀린 것은?
① 트로이 목마 공격에 대해 취약하다.
② 자율적 정책이라고도 한다.
③ 신분에 근거하여 데이터에 대한 접근을 제한한다.
④ 데이터 의미에 대한 지식이 없다.
⑤ 낮은 등급으로의 정보 노출이 쉽다.

정답] ⑤
[난이도] 상
[해설] 임의적 접근제어는 자율적 정책이라고도 하며 신분에 근거하여 데이터에 대한 접근을 제한하는 방법이다. 임의적 접근제어 정책은 허가된 주체에 의하여 변경 가능한 하나의 주체와 객체간의 관계를 정의한다. 임의적 접근제어는 주체의 신분에 근거하기 때문에 데이터의 의미에 대한 지식이 없으며 트로이 목마 공격에 취약점이 있다. 또한, 하나의 주체와 객체에 대한 관계를 정의하므로 객체를 복사하는 경우에도 객체의 접근통제 정보가 전파되지는 않는다.

(6) 컴퓨터를 이용한 정보 시스템을 운영하는 위험 요소를 제어하는 데 가장 중요한 것은 다음 중에서 무엇인가?
① 위협을 유발하는 취약점
② 자산 평가
③ 위협의 확인
④ 공인과 인가
⑤ 취약점 분석

[정답] ①
[난이도] 상
[해설] 정보 시스템의 운영상 위험을 제어하기 위하여 관리자와 사용자는 시스템의 취약성과 알려진 위협에 대하여 알 필요가 있다. 위협 환경에 대한 지식은 시스템 관리자가 보안관리 측면에서 가장 용 효과적이다. 자산 평가는 본질적인 가치를 측정하는 것이며 시스템 침해의 결과에 영향을 받는다. 위협은 시스템에 잠재적 손해를 나타내는 것이다. 공인(certification)은 보호 장치와 제어기능이 시스템에 적합한지를 기술적으로 검증하는 것이고, 인가(accreditation)는 특정 행위에 대한 작업, 보안 수정, 또는 중지를 위한 공식적인 권한을 말한다. 취약성은 보호 장치의 유무를 분석하는데 가끔 사용되며 보안 절차상의 조건에 해당된다.

제2장 네트워크 보안

1절. 네트워크 일반 (1급:10%, 2급:20%)

네트워크 보안에 대한 이해를 하기 위해서는 네트워크에 대한 일반적인 지식이 선행되어야 한다. OSI 7 layer와 인터넷의 근간이 되는 TCP/IP에서부터 TCP, UDP 등 각종 인터넷 프로토콜, 그리고 이러한 이론을 근간으로 한 Unix/Windows 계열의 응용 서비스에 대해 이해정도를 평가하도록 한다.

1. OSI 7 layer

OSI는 통신 네트워크로 구성된 컴퓨터가 어떻게 데이터를 전송할 것인가에 대한 표준규약 또는 참조 모델이다. OSI의 주된 개념은 통신 네트워크로 구성된 두개의 종단 이용자 사이에서, 통신 처리를 각 계층이 가지고 있는 특별한 기능을 가지고 계층별로 나눌 수 있도록 하는 것이다. 각 계층별 역할과 특징 등에 대해 평가한다.

가. 각 계층의 역할

▶ 물리층(Physical Layer)
- 물리층의 기능 이해
- 인터페이스와 매체의 물리적 특성
- 비트위 표현, 데이터 속도 및 비트의 동기화 등
- 화선구성, 물리적인 접속형태, 전송 모드 등
- 물리층에 해당하는 장비들에 대한 종류와 기능 이해

▶ 데이터 링크층(데이터-link Layer)
- 데이터 링크층의 데이터 전송 기능 이해
- 물리적 주소지정, 네트워크 토폴로지, 회선 사용 규칙, 오류 검출, 프레임 전달 그리고 흐름 제어 등에 관한 이해

▶ 네트워크층(Network Layer)
- 다른 장소에 위치한 두 시스템간에 연결성과 경로 선택 기능 이해(논리적 주소지정)
- 라우팅 프로토콜의 최적 경로를 선택과 선택된 경로를 따라 정보 전달기능 이해

▶ 전송층(Transport Layer)
- 서비스 지점 주소지정
- 데이터 전송 서비스를 제공기능 이해
- 분할과 재조립 및 신뢰성 있는 데이터 전송 검증 방법 이해
- 가상 회로의 구축, 유지 및 종료, 전송 오류 검출 및 복구 그리고 정보 흐름 제어의 절차이해 등

▶ 세션층(Session Layer)
- 애플리케이션간에 세션을 구축하고 관리하며 종료 기능 이해(대화제어)
- 프리젠테이션 층 사이의 대화를 동기 시키며 데이터 교환을 관리 기능 이해

▶ 표현층(Presentation Layer)
- 데이터 변환
- 암호화
- 압축 등 이해

▶ 애플리케이션층(Application Layer)
- 응용계층의 구체적인 기능 등 이해
- 네트워크 가상터미널, 파일접근, 전송 및 관리
- 우편 서비스, 디렉토리 서비스 등

나. 각 계층별 네트워크 장비의 정의 등

▶ 각 계층의 기능을 수행하는 장비들에 대해 학습
- 즉, 네트워크층에 해당하는 장비로는 라우터와 멀티 레이어 스위치가 해당
- 데이터링크층에 해당하는 장비로는 브리지와 스위치
- 물리층에 해당하는 장비로는 허브와 케이블과 커넥터 등

2. TCP/IP 일반

자주 사용하면서도 쉽게 지나칠 수 있는 TCP/IP의 주소체계와 서브넷, 포트 주소 등과 관련한 정의 및 일반적인 내용에 대해 평가하도록 한다. 그리고 서브넷팅 등을 직접 계산하는 방법에 대해서도 평가한다.

가. IP Addressing

▶ IP 주소의 기본 개념
- IP 어드래싱
- IP 네이밍(IP Naming)

▶ IP 주소지정
- 주소할당 방식
- IP 주소의 구조
- 주소 클래스

▶ 차세대 인터넷 프로토콜(IPv6)
- IPv6의 특징
- IPv6의 주소공간 할당 및 범주
- 유니캐스트 규칙
- 에니캐스트 규칙
- 멀티캐스트 규칙

나. 서브넷팅

▶ 서브넷(subnet)의 개념
▶ 서브넷 마스크 활용 및 장단점
▶ 각 클래스(A,B,C)의 서브넷팅 방법

다. CIDR 및 VLSM

▶ CIDR와 VLSM의 개요
▶ CIDR의 VLSM의 활용 및 장단점

라. Client-Server Model

▶ Client/Server 모델 개요
▶ 반복/병렬 서버의 특징 등을 학습

마. 데이터 캡슐화

▶ OSI 모델의 각 레이어에서 프로토콜 정보와 함께 데이터가 캡슐화
- 각 레이어는 수신 장비의 대응되는 레이어와 통신
- PDU(Protocol Data Unit) 사용
- 레이어 상의 데이터에 부과된 제어정보
- 전송장비에서 데이터를 캡슐화 하는 방법 등을 학습
  (1) 사용자 정보는 데이터로 변경되어 네트워크에서 전송된다.
  (2) 데이터는 세그먼트로 변경되고 연결은 전송 및 수신 호스트에서 이루어진다.
  (3) 세그먼트는 패킷이나 데이터그램으로 변경되며 논리적 어드레스는 헤더에 위치하고 패킷은 인터네트워크를 통하여 라우팅 된다.
  (4) 패킷 또는 데이터그램은 로컬 네트워크에 전송하기 위한 프레임으로 변환된다. 하드웨어 주소를 사용 로컬네트워크 세그먼트에서 호스트의 어드레스를 식별하는데 사용된다.
  (5) 프레임은 비트로 변경되고 디지털 인코딩과 동기화기법이 사용된다.

바. 포트주소의 의미와 할당원칙

▶ 포트의 개요
▶ 포트번호와 소켓
- 포트 사용 규칙 이해
- 포트 번호 체계 및 활용

사. IP, ARP, IGMP, UDP, TCP 등 각 프로토콜의 원리 및 이해

▶ ARP(Address Resolution Protocol)
- IP 네트워크 상에서 IP 주소를 물리적 네트워크 주소로 대응 원리 이해
- 물리적 네트워크 주소 이해(이더넷, 48bit 카드 주소 등)

▶ IGMP(Internet Group-Membership Protocol)
- IP 멀티캐스트의 기본적인 구성 요소
- 멀티캐스트 그룹 생성을 위해 D 클래스의 IP 주소를 사용
- IGMP는 D 클래스 주소를 가지는 멀티캐스트 그룹에 있는 각 호스트를 동적으로 등록하는데 사용
- 호스트는 IGMP 메시지를 전송하여 그룹 구성원 식별과 랜에서 활성 또는 비활성된 그룹을 발견 원리 이해

▶ UDP(User Datagram Protocol)
- UDP의 특징과 활용 학습
- TCP와 UDP의 비교

▶ TCP(Transmission Control Protocol)
- TCP 서비스 이해
- 다중화 역다중화 이해
- 분할 조립 기능 이해
- 흐름 조절, 에러검사 및 재전송 기능 이해

아. Broadcast 및 Multicast의 이해

▶ 인터넷의 전송 방식의 특징과 장단점 이해
- 유니캐스트 : 하나의 송신자가 다른 하나의 수신자로 데이터를 전송하는 방식
- 브로드캐스트(Broadcast) : 하나의 송신자가 같은 서브네트워크 상의 모든 수신자에게 데이터를 전송하는 방식
- 멀티캐스트(Multicast) : 하나 이상의 송신자들이 특정한 하나 이상의 수신자들에게 데이터를 전송하는 방식

3. Unix/Windows 네트워크 서비스

네트워크 서비스는 TCP/IP의 응용계층에 해당하는 프로토콜들의 기능에 해당하는 것으로 OSI 모델의 세션, 표현, 그리고 응용계층에 해당한다. 이에 해당하는 각종 프로토콜들에 대한 원리와 역할 등과 관련하여 평가한다.

가. DNS, DHCP, SNMP, telnet, ftp, smtp 등 각종 서비스의 원리 및 이해

- ▶ DNS 서비스
  - DNS 제공하는 서비스 이해
  - DNS의 동작 원리 이해
  - DNS 레코드 구성 이해
  - DNS 메시지 등 이해
- ▶ DHCP 서비스
  - BOOTP를 대체하는 프로토콜이다.
  - DHCP 동작 절차 이해
  - 패킷 형식 등 이해
- ▶ SNMP 서비스
  - SNMP의 개념 이해
  - SMI와 MIB 프로토콜과의 관계 이해
  - SNMP의 메시지 이해 등
- ▶ Telnet 서비스
  - 네트워크 가상 터미널 이해
  - 옵션과 옵션 협상 이해
  - 운영 모드 이해
  - rlogin과의 비교 등
- ▶ 기타 Rlogin, FTP, TFTP, SMTP 등 유닉스/Windows에서 제공하는 각종 네트워크 서비스에 대한 기본 개념과 기능에 대한 이해

나. Workgroup과 DOMAIN

- ▶ 디렉토리 데이터베이스(Directory database)
  - 디렉토리 데이터베이스의 역할 이해
  - domain controller의 역할 이해
  - Active Directory의 역할 이해
- ▶ Windows 2000 Workgroup 방식
  - 컴퓨터의 논리적 그룹 이해
  - 컴퓨터는 전용서버(Dedicated Server)와 Client의 교번 가능 이해
  - 보안 관리의 분산 이해

다. 터미널 서비스 등 각종 원격관리 서비스

- ▶ 터미널 서비스 구성 요소
  - 가상 데스크톱 컴퓨터 사용 장치의 활용 이해
  - Windows 2000 기반 서버의 원격 관리의 원리 이해
  - 터미널 서비스 클라이언트 소프트웨어의 특징 이해

라. 인터넷 공유 및 NAT 원리, 활용

- ▶ NAT 원리
  - IP 주소를 변환과 장단점 이해
- ▶ NAT의 활용
  - NAT의 테이블의 구성 요소와 역할 이해
  - IP 주소 정의 방법 이해

예제문제

(1) 라우터는 OSI 레이어 중 어디에 속하는가?
① 물리적 레이어
② 트랜스포트 레이어
③ 데이터 링크 레이어
④ 네트워크 레이어
⑤ 어플리케이션 레이어

[정답] ④
[해설] 라우터는 OSI의 네트워크 레이어에 정의된다.

(2) 하드웨어 어드레스는 몇 개의 비트로 정의되나?
① 6비트
② 16비트
③ 24비트
④ 46비트
⑤ 48비트

[정답] ⑤
[해설] 하드웨어 어드레스의 길이는 48비트(6바이트)이다.

(3) IP 어드레스가 172.16.10.22이고 넷마스크 255.255.255.240일 경우 유효한 호스트 범위는?
① 172.16.10.20부터 172.16.10.22까지
② 172.16.10.1부터 172.16.10.255까지
③ 172.16.10.16부터 172.16.10.23까지
④ 172.16.10.17부터 172.16.10.31까지
⑤ 172.16.10.17부터 172.16.10.30까지

[정답] ⑤
[해설] 우선 256마스크를 사용한다. 여기서는 256-240=16이다. 첫 번째 서브넷은 16, 두 번째 서브넷은 32이다. 이 호스트는 16 서브넷 안에 있어야 하고 브로드캐스트 어드레스는 31이며 유효한 호스트 범위는 17부터 30이다.

2절. 네트워크 활용 (1급 : 30%, 2급 : 30%)

앞의 네트워크 이론을 기반으로 실제 어떻게 활용되는지 알아보도록 한다. 라우터 및 스위치 등의 네트워크 장비의 활용법에 대해 알아보고 이러한 장비를 이용한 IP Routing, VLAN 등에 대해 알아본다. 그리고 네트워크 기반 프로그램인 ping, traceroute와 netstat, tcpdump 등의 활용방안에 대해 평가한다.

1. IP Routing

라우팅은 네트워크로부터 패킷을 수신하여 다른 네트워크로 전달하는 기능을 말한다. 보통 라우터는 여러 네트워크에 연결되는데 라우팅의 종류와 라우팅 알고리즘의 특징 등에 대해서 평가한다.

가. IP 라우팅의 종류

- ▶ Static Route 및 Dynamic Route
  - 라우팅 테이블의 역할 이해
  - 가상회선의 이해
- ▶ 라우팅 알고리즘
  - 링크상태 라우팅 알고리즘
  - 거리벡터 라우팅 알고리즘
  - 기타 라우팅 알고리즘 등
- ▶ default route
  - IP Network Address에 대한 route가 없을 때의 라우팅

2. 네트워크 장비 이해

가장 기본적인 네트워크 장비인 랜카드부터 허브, 스위치 및 라우터까지 각각의 네트워크 장비가 어떠한 기능을 가지고 있으며 각각의 차이점은 무엇인지 이해하고 있는지에 대해 평가한다. 아울러 장비가 제공하고 있는 메뉴나 명령어를 이용하여 원하는 설정을 조작할 수 있는지에 대해서도 평가한다.

가. 랜카드

- ▶ Half/Full-duplex 이해
- ▶ 커넥터 및 캐이블링 이해

나. 허브, 스위치 및 브리지

- ▶ 허브(Hub)
  - 허브의 기능 이해
  - 허브의 종류별 특징 이해
- ▶ 스위치(Switch)
  - 스위치의 기능 이해
  - 스위치의 종류별 특징 이해
- ▶ 브리지(Bridge)
  - 브리지의 기능 이해
  - 브리지의 종류별 특징 이해

다. VLAN

- ▶ VLAN(virtual LAN)
  - VLAN의 개념
  - VLAN의 표준 이해

라. 라우터 구성 명령어의 이해

- ▶ CISCO 라우터 구성 모드
- ▶ CISCO 라우터 명령어 이해
- ▶ 라우터에서 각종 암호를 설정하는 방법 이해

마. 네트워크 장비를 이용한 네트워크 구성

- ▶ 각각의 인터페이스에 적당한 IP 주소를 설정
- ▶ 네트워크를 구성
- ▶ 어떠한 라우팅 프로토콜이 필요한지 이해

바. 네트워크 토폴로지 이해

▶ 토폴로지의 일반적인 의미 이해
▶ 네트워크의 배열이나 구성을 개념적인 그림으로 표현
▶ 네트워크 토폴로지들 이해 (star형, 망형, 버스형, 환형, 나무형 등)

사. 각종 네트워크 응용 프로그램의 작동 원리와 활용

▶ 기타 다른 네트워크 응용 프로그램의 작동원리 및 활용방안에 대해 이해

3. 무선통신

WAP(Wireless Application Protocol)은 무선 응용 통신규약으로서 셀룰러폰이나 무선호출기 등과 같은 무선장치들이 전자우편, 웹, 뉴스그룹 및 IRC 등의 인터넷 액세스에 사용될 수 있는 방법을 표준화하기 위한 통신 프로토콜들의 규격 등에 대해서 학습한다.

가. 이동통신(PDA, WAP) 등

▶ Wireless Application Environment(WAE) 이해
▶ Wireless Session Layer(WSL) 이해
▶ Wireless Transport Layer Security(WTLS) 이해
▶ Wireless Transport Layer(WTP) 이해

나. 이동/무선통신 보안

▶ 보안정책
– 조직이나 업체가 무선랜을 도입하여 강화된 보안 정책 수립
▶ 보안 기능 제공 여부
– 하드웨어의 분실, 부적절한 엑세스포인트의 활용 이해
– 해커의 공격에 보안위협을 최소화할 수 있는 보안기능 방안 이해
– 상호인증을 위한 WEP키 활용 이해
– 중앙집중 제어방식의 보안을 관리하는 방안 이해 등

4. 네트워크 기반 프로그램 이해 및 활용

네트워크와 관련된 프로그램중 가장 기본적인 Ping이나 Traceroute등의 사용법 및 작동원리에 대해 이해하고 아울러 Netstat, Tcpdump 등의 프로그램을 활용하여 패킷분석을 통해 문제 해결 방법에 대해 이해하고 있는지에 대해 평가한다.

가. Ping, Traceroute등 네트워크 기반 프로그램의 활용

▶ Ping
– Ping의 기능 이해
– Ping의 옵션 활용 및 동작 원리 이해 등
▶ Traceroute
– Traceroute의 기능 이해
– Traceroute의 활용 및 동작 원리 이해

나. Netstat, Tcpdump 등 활용

▶ Netstat
– Netstat의 기능 이해
– Netstat의 동작 원리와 옵션 활용 이해

다. 네트워크 패킷/로그분석 및 이해

▶ Tcpdump
– Tcpdump의 기능 이해
– Tcpdump의 동작 원리 이해
– Linux나 BSD 등의 시스템의 로그파일 이해

라. 네트워크 문제의 원인분석과 장애처리 방안

▶ 다양한 네트워크 구조에서의 문제발생시 문제 발생 원인 분석
▶ 어떻게 장애처리를 하여야 하는지 다양한 해결 방안 이해

예제문제

(1) 다음중 VLAN의 역할은?
① Collision 도메인을 분리한다.
② Routing 도메인을 분리한다.
③ Broadcast 도메인을 분리한다.
④ Fragmentation Segment를 제공한다.
⑤ QoS를 제공한다.

[정답] ③
[해설] VLAN은 스위치 네트워크에서 Broadcast 도메인을 분리한다.

(2) CISCO 라우터의 RAM 환경설정파일을 TFTP호스트로 복사하기 위해서는 어떤 명령어를 사용하여야 하는가?
① config netw
② config mem
③ config term
④ copy run tftp
⑤ copy start tftp

[정답] ④
[해설] RAM에 저장된 config는 running-config이므로 RAM에서 TFTP호스트로 라우터의 장치구성을 복사하기 위해서는 copy running-config tftp 명령어를 사용한다.

3절. 네트워크 기반 공격의 이해 (1급 : 20%, 2급 : 30%)

실제 네트워크에 기반한 공격의 형태는 어떠한 것들이 있으며 이러한 각각의 공격이 사용하는 원리와 인지방법, 대처 요령에 대해서도 평가하도록 한다.

1. 서비스 거부(DoS) 공격

Dos 공격이란 공격자가 시스템의 하드웨어나 소프트웨어 등을 무력하게 만들어 시스템이 정상적인 수행을 하는데 문제를 일으키는 모든 행위들 뜻한다. 여러 가지 DoS 공격의 작동원리에 대해 이해하고 각각의 공격에 대해 어떻게 대처할 수 있는지에 대해 평가한다.

가. Land Attack 등 각종 DoS의 원리와 대처요령

▶ Land Attack
– Land Attack의 원리 이해
– Land Attack의 대응 방안
▶ Targa/NewTear/Nestea 공격
– Targa/NewTear/Nestea 공격의 원리 이해
– Targa/NewTear/Nestea 공격 대응 방안
▶ Ping of Death 공격
– Ping of Death 공격의 원리 이해
– Ping of Death 공격 대응 방안
▶ Inconsistent Fragmentation 공격
– Inconsistent Fragmentation 공격의 원리 이해
– Inconsistent Fragmentation 공격 대응 방안

나. Syn Flooding, Smurf 등 각종 Flooding 공격의 원리와 대응 방안

▶ Syn Flooding 공격
– Syn Flooding 공격의 원리 이해
– Syn Flooding 공격 대응 방안
▶ 스머프 공격
– 스머프 공격의 원리 이해
– 스머프 공격 대응 방안
▶ UDP Flood 공격
– UDP Flood 공격의 원리 이해
– UDP Flood 공격 대응 방안

2. 분산 서비스 거부 공격

DDoS 공격이란 네트워크로 연결되어 있는 많은 수의 호스트들에 패킷을 범람시킬 수 있는 DoS용 프로그램을 분산 설치하여 이들이 서로 통합된 형태로 한 대의 공격대상 시스템에 대해 성능저하 및 시스템 마비를 일으키는 기법이다. 이와 관련되어 최근까지 알려진 DDoS 공격의 작동원리 및 방식에 대해 이해하고 어떻게 대처할 수 있는지에 대해 평가한다.

가. Trinoo, TFN, Stacheldraht 등

▶ 트리누 공격
– 트리누 공격의 원리 이해
– 트리누 공격 대응 방안
▶ TFN 공격
– TNF 공격의 원리 이해

- TNF 공격 대응 방안

▶ Stacheldraht 공격
- Stacheldraht 공격의 원리 이해
- Stacheldraht 공격 대응 방안

▶ TFN2K 공격
- TFN2K 공격의 원리 이해
- TFN2K 공격 대응 방안

3. 네트워크 스캐닝

원격지의 OS나 열린포트, 버전정보 등에 대한 스캐닝은 본격적인 공격을 예고하는 것이라 할 수 있다. 각종 스캐닝이 어떻게 작동하는지 원리에 대해 이해하고 실제로 대응방안에 대해서도 평가하도록 한다.

가. Remote Finger Printing

▶ 원격지의 OS 등을 판별 방법 이해
- TCP/IP Fingerprinting의 특성을 이용 원리 이해

나. IP 스캔, 포트스캔

▶ PORT Scan Attack
- PORT Scan Attack의 원리 이해
- PORT Scan Attack 대응 방안

다. Third Party Effect 등

▶ Third Party Effect(제3자 현상)의 이해
▶ Third Party Effect와 각종 DoS 공격과의 관계 이해

4. IP Spoofing, Session Hijacking

IP Spoofing이란 IP를 속여서 공격하는 기법을 의미하며 Session Hijacking이란 TCP/IP 프로토콜 자체의 취약성을 이용하여 이미 사용중인 사용자의 세션을 가로채는 것을 뜻한다.
이러한 공격방식의 원리와 실제 환경에서 각각 어떻게 작동하는지에 대해 평가한다.

가. IP Spoofing과 Session Hijacking의 원리 및 실제

▶ IP Spoofing의 공격원리 이해
▶ 공격 종류와 특징 이해
- 순서제어번호 추측(Sequence Number Guessing)
- 반(Half) 접속시도 공격(SYN Flooding)
- 접속 가로채기 (Connection Hijacking)
- RST를 이용한 접속끊기(Connection Killing by RST)
- FIN을 이용한 접속끊기(Connection Killing by FIN)
- SYN/RST패킷 생성공격(SYN/RST Generation)
- 네트워크 데몬 정지(Killing the INETD)
- TCP 윈도우 위장(TCP Window Spoofing)

▶ 대응방안 이해
▶ Session Hijacking
- Session Hijacking의 공격 원리 이해
- Session Hijacking 공격의 대응 방안

5. 스니핑 및 암호화 프로토콜

스니핑이란 스니퍼등의 프로그램를 이용하여 네트워크상의 데이터를 도청하는 행위를 뜻한다. 스니핑이 어떠한 원리를 이용하여 가능한 것인지 그리고 이로 인한 피해를 최소화하거나 대처하기 위한 조처는 어떠한 것이 있는지에 대해 평가한다.

가. 스니핑 공격의 이해

▶ 스니핑 공격의 동작 원리 이해
▶ 스니핑 공격 대응 방안

6. 각종 Remote Attack

Remote Attack이란 타겟 호스트로의 접근 권한을 갖지 않고 있을 경우, root나 일반사용자 등 접근 가능한 계정권한을 획득하는 것을 의미하는데, 각각의 공격을 인지하는 방법과 각각의 공격에 대해 대처하는 방법에 대하여 평가한다.

가. 각종 공격의 인지 및 이해

▶ Local Attack과 Remote Attack의 비교
▶ named, imapd, smbp, mountd 등의 버그를 이용한 공격 이해

7. 각종 Trojan 및 Exploit 이해

시스템 및 네트워크를 운영하면서 접할 수 있는 각종 Trojan이나 Exploit에 대해 각각 어떻게 식별하고 대처할 수 있는지에 대해 평가한다.

가. Trojan, Exploit 등

▶ Trojan, Exploit 식별 요령
▶ Trojan, Exploit 대처 요령

예제문제

(1) 가장 대중적인 스캐닝 프로그램인 nmap은 많은 스캔 옵션을 제공한다. 이 중 아래는 TCP SYN 스캔에 대한 설명인데, ( )에 공통적으로 들어가는 용어는 무엇인가?
"SYN 스캔은 Full TCP 접속을 하지 않으므로 'half-open' 스캐닝이라 한다. 하나의 SYN 패킷을 보내어 SYN|ACK 응답이 오면 그 포트는 리슨하고 있는 상태이고, ( ) 응답이 오면 리슨하지 않는 것을 나타낸다. 이 기술은 하나의 패킷을 보내어 SYN|ACK 응답을 받으면 그 즉시 ( ) 패킷을 보내서 접속을 끊어버린다."
① SYN
② ACK
③ RST
④ FIN
⑤ PSH

[정답] ③
[해설] TCP의 접속을 끊는 tcp flag는 Reset(RST)이다.

(2) 다음은 어떤 공격에 대한 패킷로그를 검출할 것을 보여주고 있다. 어떠한 공격인가?
Source : 85.85.85.85
Destination : 85.85.85.85
Protocol : 6
Src Port : 21845
DST Port : 21845
① Land Attack
② Syn Flooding Attack
③ Smurf Attack
④ Ping of Death Attack
⑤ UDP Flood Attack

[정답] ①
[해설] Land Attack 는 소스IP와 목적지IP, 소스포트와 목적지포트가 같도록 위조한 패킷을 전송하는 공격형태이다. 따라서 답은 Land Attack이다.

4절. 각종 네트워크 장비를 이용한 보안기술 (1급 : 30%, 2급 : 20%)

침입탐지시스템, 침입차단시스템, VPN, 라우터 등 각종 네트워크에 기반한 보안장비 활용 방안에 대해 이해한다. 그리고 이러한 장비에서의 보안설정과 보안설정을 통한 효과에 대해서도 이해하도록 하며 장비에서의 로그나 패킷분석을 통하여 공격방식에 대해 이해하고 이에 대한 대처방법에 대해서 학습한다.

1. 침입탐지시스템(IDS)의 이해

IDS(Intrusion Detection System)는 단순한 제어기능을 넘어서서 침입의 Pattern Database와 Expert System을 사용해 네트워크나 시스템의 사용을 실시간 모니터링하고 침입을 탐지하는 시스템이다. IDS의 여러 특징에 대해 이해하고 나아가 IDS운영중 접하게 될 수 있는 False Positive나 False Negative에 대해서도 평가한다.

가. 원리, 종류, 작동방식, 특징, 구성, 실제 활용 등

▶ IDS(Intrusion Detection System)의 원리
▶ IDS의 종류 및 특징
▶ IDS의 작동 원리 이해
▶ IDS의 구성과 활용 이해

나. False Positive, False Negative 등

▶ IDS의 침입 판정 원리 이해
▶ False Positive/False Negative 판정 이해

2. 침입차단시스템(Firewall)의 이해

방화벽은 라우터 프로그램과 밀접하게 동작함으로써 모든 네트워크 패킷들을 그들의 수신처로 전달할 것인지를 결정하기 위해 검사하고 여과한다. 또한 방화벽은 워크스테이션 사용자 대신 네트워크에 요청을 해주는 proxy 서버의 기능을 아예 포함하기도 한다. 방화벽은 네트워크의 다른 부분들과는 별개로, 특별히 지정된 컴퓨터에 설치되는 경우가 많은데, 이는 들어오는 요구가 사설 네트워크 자원으로 곧바로 전달되지 않도록 하기 위한 것이다. 이러한 방화벽의 종류와 기능 등에 대해 평가한다.

가. 원리, 종류, 작동방식, 특징, 구성, 실제 활용 등

- ▶ 방화벽의 종류 이해
  - – 스크린라우터
  - – 베스천호스트
  - – 프락시(proxy) 서버 등
- ▶ 패킷필터링 기능
  - – 데이터의 흐름 필터링 원리 이해
  - – 통과 허용/차단 원리 이해
  - – 상태추적 등 최근 관련 기술 이해

3. 가상사설망(VPN)의 이해

VPN(Virtual Private Networks)은 고급 암호화 및 터널링 기술을 사용하여, 기업 환경에서 인터넷이나 엑스트라넷처럼 서드파티 네트워크로 안전한 엔드-투-엔드 사설 네트워크 연결을 구현할 수 있게 한다. 이러한 VPN의 동작 원리와 기능 등에 대해서 학습한다.

가. 원리, 작동방식, 특징, 구성, 실제 활용 등

- ▶ VPN의 동작원리 이해
- ▶ VPN의 구성과 활용 이해

4. 라우터의 이해

네트워크의 가장 앞단에 있는 장비인 라우터의 보안은 매우 중요하다. 라우터의 암호 설정 등 라우터 자체의 보안뿐만이 아니라 라우터를 이용하여 어떻게 내부 네트워크 보안을 구현할 수 있는지, 각종 공격에 대해 어떻게 대처할 수 있는지에 대해 평가한다.

가. 라우터 자체 보안설정

- ▶ 라우터 자체 보안 설정 이해

나. 라우터를 이용한 네트워크 보안설정

- ▶ 라우터를 이용한 네트워크 보안 설정 이해
- ▶ 소스라우트 원리와 기능 이해
- ▶ 라우팅 프로토콜 보안

다. Reflexive Access-list, NBAR를 통한 보안설정

- ▶ Reflexive Access-list를 이용하여 상태추적이 가능한 Access-list를 설정 이해
- ▶ 웜 형태의 공격을 라우터에서 차단할 수 있는 방법 이해
- ▶ NBAR의 분류기능 이해

라. 라우터의 리소스 점검

- ▶ CLI에서의 show process cpu, show process mem으로 CPU나 메모리 상태를 모니터링 이해

마. 인증 서버를 통한 보안

- ▶ Cisco에서 제공하는 AAA(Authentication, Authorization, Accounting) 모델에 대해 이해

바. CAR를 이용한 보안설정

- ▶ CAR(Committed Access Rate) 기술 이해
- ▶ ICMP나 SYN 패킷량을 제한하는 기능 이해

사. 각종 응용 프로그램을 이용한 라우터 보안

- ▶ Solarwinds 등 라우터 관련 응용 프로그램을 이용하여 라우터의 보안을 강화하는 방안에 대해 이해

5. 각종 네트워크 기반 보안 프로그램 활용 방안

이외 다른 네트워크 보안 관련 프로그램을 활용하여 어떻게 보안을 강화할 수 있는지에 대해 평가한다.

가. 기타 네트워크 기반 보안 프로그램의 활용

각 프로그램의 작동원리 및 활용방안에 대해 이해한다.

6. 각 장비의 로그 및 패킷 분석을 통한 공격방식의 이해 및 대처요령

로그 및 패킷분석은 문제 확인과 해결등에 반드시 필요하다. 로그와 패킷 분석을 통해 공격을 인지하는 방법과 이러한 공격에 대해 어떻게 대처할 지에 대해 평가한다.

가. 호스트 및 IDS, 방화벽, 라우터 등 각종 네트워크 장비의 로그 및 패킷분석

- ▶ 각종 네트워크 기반의 장비 또는 프로그램의 로그나 패킷을 분석
- ▶ 네트워크의 activity 이해
- ▶ 공격여부를 감지하는 방법 이해
- ▶ 이에 대해 대처할 수 있는 방법에 대해 이해

예제문제

(1) 다음 중 standard access-list에서 사용되는 access-list 번호는?
① 1-10
② 1-99
③ 10-99
④ 100-199
⑤ 1000-19999

[정답] ②
[해설] standard access-list는 1-99까지 사용한다.

(2) 196.15.7.0 네트워크로 www 트래픽만을 허용하는 엑세스 리스트는 다음 중 무엇인가?
① access-list 100 permit tcp any 196.15.7.0 0.0.0.255 eq www
② access-list 10 deny tcp any 196.15.7.0 eq www
③ access-list 100 permit 196.15.7.0 0.0.0.255 eq www
④ access-list 110 permit ip any 196.15.7.0 0.0.0.255
⑤ access-list 110 permit www 196.15.7.0 0.0.0.255

[정답] ①
[해설] 이와 같은 질문에서 먼저 점검해야 할 것은 엑세스리스트 번호이다. 그렇다면 ②는 틀렸다는 것을 알 수 있다. standard access-list 번호를 사용하였기 때문이다. 두 번째 살펴보아야 할 것은 프로토콜이다. 상위 레이어 프로토콜에 의해서 필터링하려면 UDP나 TCP중의 하나를 사용해야 한다. 여기에서 ④를 제외시킬 수 있다. ③과 ⑤는 문법이 틀렸다.

5절. 최근 경향 및 추세 (1급 : 10%, 2급 : 0%)

최근 새로운 양상으로 펼쳐지고 있는 각종 침해사고의 유형과 공격 원리 등에 대해 이해하고 아울러 새롭게 출시되거나 각광받고 있는 최신 보안 솔루션이나 새로운 보안기법에 대해 평가한다.

1. 최근 네트워크 기반 침해사고에 대한 이해

최근에 알려지고 있는 새로운 공격방식의 유형과 어떠한 특징을 가지고 있는지에 대해 평가한다. 아울러 이러한 공격유형을 어떻게 인지하고 어떠한 방식으로 대응할지에 대해서도 평가한다.

가. 분산반사 서비스 거부 공격(DRDoS), 기타 새로운 공격방식

- ▶ DRDoS 공격의 원리 이해
- ▶ DRDoS 공격 대응 방안
- ▶ 기타 새로운 공격방식에 대한 이해

2. 최근 보안솔루션에 대한 이해

공격이 다양해질수록 이에 대한 보안 솔루션도 하루가 다르게 많은 제품이 소개되고 있다. 이러한 보안 솔루션들은 어떠한 것이 있고 또 어떠한 특징을 가지고 있는지에 대하여 평가한다.

제3장 어플리케이션 보안

가. 역추적 시스템, 보안관제, 취약성 점검, ESM 등

▶ 역추적 시스템
- 원천지 주소 추적 기법 이해
- 로그 분석 방법 이해
- 보안 장치간 연동 기법 이해

▶ ESM
- ESM의 개념 이해
- ESM 제품들의 특징

▶ 취약성 점검 프로그램
- 네트워크 기반
- 호스트 기반 프로그램

(1) 시스템 환경 설정 점검 : 시스템에서 중요한 환경 파일의 설정을 검사한다.
(2) 사용자 환경설정 점검 : 사용자의 부주의로 잘못 설정된 환경설정에 대해 검사한다.
(3) 파일 무결성 점검 : 시스템 내부의 중요한 파일에 대해 변조나 삭제 유무를 정확히 파악한다.
(4) 파일 퍼미션 점검: 시스템 내부의 중요한 파일에 대해 퍼미션을 점검한다.
(5) 패스워드 점검 : 각각의 사용자에 대해 취약한 패스워드를 점검한다.
(6) 데몬 버전 점검 : 취약한 프로그램이나 데몬의 버전을 점검한다.

예제문제

(1) 다음은 모 신문 기사중 일부이다.

"지난 1월 미국에서 처음 발견된 이 공격은 기존 공격에 비해 해커들이 사용하기 쉽고 공격을 당한 사이트들은 복구가 어렵다는 점에서 그 심각성이 높아지고 있다. 업계 전문가들은 국내에서 아직까지 이 공격에 의한 피해 사례가 보고되지 않았으나 이 공격방법이 해커들 사이에서 급속히 확산되고 있어 조만간 국내 웹사이트들도 주요 공격대상이 될 가능성이 있다고 지적했다. 또한 국내는 이 공격을 당해도 기존 공격과 구별할 방법이 없어 피해를 입어도 뚜렷한 대안이 없는 상태다."

아래는 이 공격에 대한 작동원리에 대해 분석한 내용이다.

공격 시스템의 list.txt에는 540,985개의 80/tcp 포트가 제공되는 IP 목록이 있다.

```
[root@ server /tmp]# cat list.txt
64.xx.0.2:80
64.xx.0.3:80
...
205.xxx.83.66:80
205.xxx.83.67:80
```

공격자는 앞서 가진 목록의 서버에 공격목표시스템에서 보낸 것처럼 패킷을 위조해서 syn패킷을 보낸다.

목표시스템은 거의 54만여개의 서버로부터 ack/syn 패킷을 받아 네트워크 bandwidth를 다 소모하게 된다.

위의 두 글에서 공통적으로 이야기하는 '이공격'의 정확한 이름은 무엇인가?
① Fragmentation 공격
② UDP Flooding 공격
③ SYN Flooding 공격
④ 분산 서비스 거부 공격
⑤ 분산반사서비스거부 공격

[정답] ⑤
[해설] DRDoS(분산반사서비스거부)-Distributed Reflection DOS 에 대한 설명이다.

(2) 다음 글을 읽고 물음에 답하라.
(　　) 은 해커를 취약성을 가진 서버에 침입하도록 유도한 뒤 해킹 수법이나 해킹 경로 등을 관찰함으로써 해커의 기술수준과 공격 의도를 파악할 수 있도록 하는 차세대 인터넷보안 기술로서 해커 몰래 실시간 모니터링 및 침입 기록 등을 감시하는 능동적인 보안 기술로, 추적자나 시스템 관리자들은 이를 이용해 분석된 자료를 기반으로 해커가 어떠한 과정을 통해 해당 서버로 접근했으며 어떠한 취약점을 공격했는지 알아낼 수 있다.
최근 이와 관련된 프로젝트가 보안관련 조직이나 단체에서 많이 수행되고 있는데, 여기에서 (　　) 에 들어갈 적당한 용어는 무엇인가?
① 싱글 사인 온
② ESM
③ EAM
④ 허니팟
⑤ 침입방지시스템
[정답] ④
[해설] 허니팟(HoneyPot)

1절. 인터넷 응용 보안 (1급 : 50%, 2급 : 70%)

응용계층에서 보안을 제공하는 기술이란 FTP(File Transfer Protocol), Mail, HTTP, Telnet 등의 프로토콜을 이용하여 전송되는 데이터를 보호하는 것을 말하며, 이것은 네트워크 특성상 상호운용성(Interoperability)이 요구되기 때문에 표준화 경향으로 가고 있다.

1. FTP 보안

ftp는 파일전송을 위하여 많이 활용되고 있는 인터넷 어플리케이션이다. ftp보안에 있어서는 먼저 ftp 프로토콜의 개념을 이해하고, 기본적인 ftp 서비스 운영 실무기술을 습득하여야 하며, ftp서비스 운영에 있어서 주의해야할 공격유형에 대해서 이해하고 각 공격에 대한 대책을 숙지하여야 한다.

가. ftp 개념

ftp프로토콜의 개념을 학습함에 있어서 가장 중요한 것은 제어연결과 데이터연결의 차이점을 이해하는 것이며, 특히 데이터연결에서의 액티브모드와 패시브모드의 차이점은 ftp서비스와 방화벽과의 연관 설계에 있어서 매우 중요하다.

(1) ftp 프로토콜 개념

▶ ftp에서는 두 개의 connection이 있음
- 클라이언트에서의 서버로의 명령과 서버의 응답을 위한 제어연결
- 파일이 전송될 때 생성되는 데이터연결

▶ ftp의 명령어와 동작과정
- ABOR, LIST, PASS, PORT, QUIT, RETR, STOR, SYST, TYPE, USER, PASS 명령
- ftp 연결 동작과정

▶ 클라이언트에서 서버로 파일 전송 동작
▶ 서버에서 클라이언트로 파일 전송 동작
▶ 서버에서 클라이언트로 파일 또는 디렉토리 목록 전송 동작
▶ ftp 데이터 연결의 액티브 모드와 패시브 모드
- ftp 액티브 연결
- ftp 패시브 연결
▶ 방화벽과 ftp 데이터 연결의 tunning

나. ftp 서비스 운영

ftp서비스를 실제로 운영함에 있어서는 각 플랫폼별 ftp 어플리케이션의 설치 및 운영 지식을 다양한 실무 경험을 통해 익히는 것이 필요하다.

(1) ftp 서버 설치 및 운영

▶ UNIX 환경에서의 ftp 서버 설치 및 운영
- anonftp 설치 및 운영
- proftp 설치 및 운영
- wuftp 설치 및 운영
- /etc/ftpusers 파일 설정을 이용한 ftp접속자 제한
- /etc/ftphosts 파일 설정을 이용한 접속 제한

▶ 윈도우NT 환경에서의 ftp 서버 설치 및 운영
- ftp 로그온 구성
- ftp 서버 프로그램 설치 및 폴더 구성

다. ftp 공격 유형

ftp서비스를 운영함에 있어 주의해야할 공격유형 bounce ataack, tftp 공격, anonymous ftp 공격, ftp서버 자체 취약점 공격 등이 있으며, 특히 ftp서버 자체 취약점에 대한 공격은 최신 해킹 경향에 따라 끊임없이 새로운 공격기법이 발견되므로, 항상 최신 보안 경향에 관심을 갖고 있어야 한다.

(1) bounce attack

▶ bounce attack의 공격 개념의 이해

(2) tftp 공격

▶ TFTP 프로토콜을 이용한 긴 파일네임전송 공격
▶ TFTP는 인증 절차를 요구하지 않으므로, 설정이 잘못 되어 있을 경우 누구나 그 호스트에 접근하여 불필요한 정보유출 가능. 대표적으로 /etc/passwd를 예로 들 수가 있음

(3) anonymous ftp

▶ anonymous ftp 설치에 있어서의 파일과 디렉토리 권한 설정이 매우 중요함.
▶ anonymous ftp 설정 잘못을 이용한 파일 유출 공격 기법

(4) ftp 서버 자체 취약점

▶ wuftp 포맷스트링 취약점 등

라. ftp 보안대책

ftp에 대한 공격을 방어할 수 있는 보안대책에 대하여 숙지하여야 하며, 일반적인 ftp 보안대책 이외에도 최신 취약점을 방어할 수 있는 보안 경향에도 관심을 기울여야 한다.

(1) ftp 서비스 보안 대책

▶ anonymous ftp 보안대책
  - Anonymous 사용자의 루트디렉토리, bin, etc pub 디렉토리의 소유주와 퍼미션을 정확히 해야함.
  - $root/etc/passwd 파일에서 anonymous ftp에 불필요한 항목 제거
▶ tftp 보안대책
  - tftp가 불필요한 경우 제거
  - tftp가 필요한 경우 secure mode로 운영
▶ 최신 ftd 서버 프로그램 사용 및 주기적인 패치

예제문제

(1) ftp 패시브 연결에 대한 설명이 틀린 것은?
① 파일리스트 출력결과나 파일전송할 때에만 관계된다.
② FTP server쪽에서 client가 data 전송을 위해 Server에 접속할 port N을 client에게 알려주게 된다.
③ 이 경우 port N은 일반적으로 1~1023 사이이다.
④ FTP client는 자신의 1023이상의 비사용 중인 port로부터 Server가 알려준 port N을 향해 접속을 시도한다.
⑤ connection을 맺은 후 data를 전송한다.

[정답] ③
[난이도] 중

(2) 리눅스 시스템에서 TFTP는 Trivial-FTP의 약어로서 초기 개발취지는 TFTP가 제공되는 서버를 "부팅서버"로서 사용을 위한 것이었다. 또한 TFTP는 패스워드 없이 접속하여 파일을 가져올 수 있기 때문에 이로 인한 해킹 사고를 방지할 수 있도록 설정에 신경을 써야 한다. 아래에서 보여주는 내용은 /etc/inetd.conf 파일의 tftp에 대한 설정을 보여주고 있다. 이에 대한 설명으로 옳지 않은 것은?

tftp dgram udp wait root /usr/sbin/in.tftpd – s /tftpboot

① 시스템에서 tftp를 사용하지 않는다면 inetd.conf 파일내에서 주석처리 혹은 아예 이 행을 지워 버리는 것을 권장한다.
② 설정되어 있는 내용으로 보아 해당 시스템으로 tftp접속을 할 경우 /home/kisa 디렉토리 아래뿐만 아니라 /(root)아래 모든 정보를 다 가져올 수 있다.
③ -s옵션을 설정한 것은 chroot( ) 기능을 이용해 보안상의 문제를 해결하기 위해서이다
④ 시스템에서 tftp를 사용하지 않고 만약 리눅스 시스템이 inetd대신에 xinetd를 사용한다면 /etc/xinetd.d/tftp파일을 삭제하면 된다.
⑤ tftp는 udp datagram을 사용하는 것임을 알 수 있다.

[정답] ②
[난이도] 하

2. MAIL 보안

mail서비스는 인터넷 환경에서 필수불가결한 응용서비스이면서 많은 보안상의 과제를 파생시키는 분야이다. mail보안에 있어서는 먼저 mail 서비스를 구성하는 핵심 프로토콜인 smtp프로토콜의 개념을 이해하고, 사용자 기반의 메일 서비스를 위한 pop, imap프로토콜의 개념을 이해해야 한다. 이러한 기본 개념 하에서 각 응용서비스를 실제 운용할 수 있는 mail서버와 pop서버의 설치 및 운영 실무지식이 필요하다. 이를 바탕으로 mail서비스 운영에 있어서 주의해야할 보안상 문제에 대해서 이해하고 각 문제들을 해결할 수 있는 대책을 숙지하여야 한다.

가. mail 개념

mail서비스를 구성하는 핵심 프로토콜에는 MTA간의 직접 메일 전송과 전달과정을 제어하는 smtp프로토콜과 MTA와 MUA간의 사용자 기반의 메일 서비스를 위한 pop, imap프로토콜이 있다.

(1) smtp 프로토콜 개념

▶ Simple Message Transfer Protocol로서 전자우편을 보내고 받는데 사용되는 기본 TCP/IP 프로토콜
▶ MTA, MDA, MUA의 개념
▶ 메일 헤더 구조
▶ MX Records의 이해
▶ smtp 명령어의 이해
▶ 메일 전송 과정

(2) pop 프로토콜 개념

▶ Post Office Protocol로서 메일서버가 사용자를 위해 전자우편을 수신하고 그 내용을 보관하기 위해 사용되는 클라이언트/서버 프로토콜
▶ 클라이언트에서 POP3 데몬을 이용하여 메일을 직접 내려 받아 읽어옴
▶ POP3 데몬 포트 : 110번 포트
▶ POP3를 이용해 메일 서버에서 가져온 메일은 더 이상 서버의 메일 박스에 남아 있지 않으므로 사용자가 고정적인 위치에서 메일을 받는 경우에 유리

(3) imap 프로토콜 개념

▶ Internet Message Access Protocol로서 메일서버를 이용하여 전자우편을 수신하고 보관하는 클라이언트/서버형 프로토콜
▶ IMAP의 경우 143번포트 사용, IMPA3의 경우 220번포트 사용
▶ 메일을 해당 사용자에게 보내는 역할은 pop3와 같지만 메일을 보내는 방법 차이
▶ IMAP로 접속하여 메일을 읽으면 메일 서버에는 메일이 계속 존재(메일 헤더만 보고 읽을 수 있으며, 읽은 메일은 읽지 않은 메일과 구분되어 표시)
▶ POP3는 '보관하고 전달하는' 서비스라고 비유할 수 있으며, IMAP은 원격지 파일서버라고 비유할 수 있음

나. mail 서비스 운영

mail서비스를 실제로 운영함에 있어서는 각 플랫폼별 mail서버 어플리케이션(MTA 및 pop서버)의 설치 및 운영 지식을 다양한 실무 경험을 통해 익히는 것이 필요하다.

(1) mail서버 설치 및 운영

▶ sendmail 설치 및 운영
▶ qmail 설치 및 운영
▶ MS exchange 설치 및 운영
▶ 메일 로그 설정
▶ 메일 용량 제한

(2) pop서버 설치 및 운영

▶ qpopper 설치 및 운영 및 운영

다. mail 서비스 공격유형

mail서비스에 있어서 공격유형은 크게 메일 사용자 클라이언트의 취약점을 이용한 사용자 컴퓨터 공격과 메일서버(MTA)의 취약점을 이용한 메일서버 공격으로 나뉜다. mail서비스 관련 공격은 최신 해킹 경향에 따라 끊임없이 새로운 공격기법이 발견되므로, 항상 최신 보안 경향에 관심을 갖고 있어야 한다.

(1) 최신 mail서비스 공격 유형

▶ 메일 클라이언트(outlook 등) 최신 취약점을 이용한 공격
  - 메일 클라이언트 취약점을 이용한 인터넷 바이러스공격
▶ 메일 서버(sendmail 등) 취약점을 이용한 메일서버 공격기법

라. spam 대책

mail서비스에 관련된 중요한 자원관리 문제로서 spam메일에 대한 대책은 매우 중요하다. 사용자 관점에서 클라이언트 어플리케이션을 이용한 spam대책과 mail서버 관리자 관점에서의 spam relay차단 대책으로 나눌 수 있다.

(1) 사용자 관점의 spam 메일 대책

▶ 메일 클라이언트 프로그램(outlook 등)을 이용한 메일 필터링
▶ spam 대응 조치 요령

(2) mail서버 관리자 관점의 spam relay 대책

▶ 메일서버(MTA)에서의 spam 릴레이 허용 불허 설정
- sendmail에서의 anti-spam기능과 AcessDB를 이용한 스팸 릴레이 차단
- MS exchange에서의 기능설정 또는 레지스트리 설정을 통한 스팸 릴레이 차단
- EMWAC 메일서버에서의 스팸 릴레이 차단

마. 악성 메일 대책

최근 급증하고 있는 email을 이용한 바이러스 등의 악성코드가 탑재된 악성 메일에 의한 피해가 급증하고 있으며, 이를 차단하기 위한 대책은 매우 시급하고 중요한 보안문제이다. 특히 메일 클라이언트 응용프로그램을 목표로 하는 최신 해킹 경향에 따라 끊임없이 새로운 악성메일이 발견되므로, 항상 최신 보안 경향에 관심을 갖고 있어야 한다.

(1) 악성메일 및 웜 대책

▶ 라우터에서의 악성메일 및 웜 차단
- class-map 이용을 차단
- Policy map을 이용한 차단

▶ 메일서버 프로그램(MTA)에서의 패턴매칭에 의한 차단
▶ virus wall을 이용한 차단

바. mail 보안 기술

전자우편은 모든 분산환경에서 가장 많이 사용하는 네트워크기반 응용이며, 모든 시스템 구조와 제품에서 광범위하게 사용되는 분산 응용이기도 하다. 전자우편의 폭발적인 증가 추세를 볼 때, 인증과 비밀성 서비스에 대한 요구가 증가하고 있으며, 현재 PGP(Pretty Good Privacy)와 S/MIME(Secure/Multipurpose Internet Mail Extension)이 많이 사용되고 있다.

(1) PGP(Pretty Good Privacy)

▶ PGP의 구성요소
- 암호화 기술
- 인증 받은 메시지와 파일에 대한 전자 서명 생성과 확인 작업 지원
- RSA와 Diffie-Hellman등 공개키 생성 지원
- 공개키 분배 및 취득

▶ PGP의 주요기능
- 인증(Authentication)
- 비밀성(Confidentiality)
- 압축(Compression)
- 전자우편 호환성(E-mail Compatibility)
- 단편화와 재조립(Segmentation and Reassembly)

▶ 암호화와 키 연결관계
- 세션키 생성
- 키 식별자(Key Identifier)
- 키 링(Key Ring)

▶ 공개키 관리
- 공개키 관리의 접근법
- 신뢰의 사용
- 공개키 철회(Revoking Public Key)

(2) S/MIME(Secure/Multipurpose Internet Mail Extension)

▶ MIME(Multipurpose Internet Mail Extension)
- MIME 내용타입
- MIME 전송 부호화

▶ S/MIME의 구성요소
- RSA, DSA, Diffie-Hellman 공개키 암호화
- Triple DES, RC4, IDEA, DES, RC2 대칭 암호화
- X.509 버전3 인증서 지원
- DER 및 PEM으로 인코딩된 인증서 파일 프로세싱 기능 지원

▶ S/MIME의 주요 기능
- 봉인된 데이터(Enveloped data)
- 서명 데이터(Signed data)
- 순수한 서명(Clear-signed data)
- 서명과 봉인된 데이터(Signed and enveloped data)

예제문제

(1) 사용자의 PC가 VBScript 웜에 감염되었을 때, 다음 중 가능한 감염경로가 아닌 것은?
① 아웃룩 메일프로그램으로 메일의 첨부파일을 열었을 때
② 인터넷 써핑 중 'Click accept ActiveX' 메시지가 팝업되어 Yes 버튼을 눌렀을 때
③ 채팅 도중 상대에게 전송받은 파일을 실행시킬 때
④ 네트워크에 읽기쓰기 권한의 폴더를 접근 패스워드 설정하여 공유시켰을 때

[정답] ④

(2) 스팸메일 방지를 위한 보안대책으로 Sendmail 8.9.0으로 버전이 높아지면서 새롭게 추가된 기능이 anti-spam과 관련된 기능으로 볼 수 있는데, 이에 대한 설명으로 옳지 않은 것은? 또한 아래 보이는 것은 /etc/mail/access 파일의 내부 형식을 보여주고 있다.

spam@hacker.com	REJECT
useful.org	OK
211.252.150.	RELAY

① /etc/mail/access 파일에서 첫 번째 필드는 e-mail Address, Domain Name, Network IP Address가 올 수 있고, 두 번째 필드는 메일에 대한 처리를 결정한다.
② Access DB는 /etc/mail/access란 이름으로 파일 시스템에 저장되고 makemap 명령을 실행하게 되면 access.dir과 access.pag라는 이름으로 DB가 생성된다.
③ access의 파일 구조는 텍스트 파일이며, Sendmail이 인식할 수 있는 DB형태로 만들어 주기 위해 makemap이란 프로그램을 사용한다.
④ 이미 Access DB가 만들어져 있다면, 다른 메일 정책이 /etc/mail/access 파일에 추가되더라도 makemap을 사용할 필요가 없다.
⑤ sendmail외의 다른 MTA에도 anti-spam 기능이 있다.

[정답] ④
[난이도] 상

(3) 다음과 같이 sendmail.cf를 설정하는 것은 다음중 어떤 공격을 방어하기 위함인가?
HContent-Type: $)check_nv
D{ATTACK}"Your message may contain the malicious code"
Scheck_nv
Rboundary="
====_ABC1234567890DEF_====" $#error
$: 550 ${ATTACK}

① back oriffice
② codered worm
③ 멜리사 바이러스
④ Mircpack 바이러스
⑤ nimda 바이러스

[정답] ⑤
[난이도] 하

3. Web 보안

인터넷 서비스 환경이 World Wide Web환경으로 통합되어 가고 있다. Web서비스는 다양한 아키텍쳐에 의하여 구동되며, 이에 따른 많은 보안상의 과제를 파생시키는 분야이다. web보안에 있어서는 먼저 web 서비스를 구성하는 핵심 프로토콜인 http 프로토콜의 개념과 그 구조를 이해하고, 강화된 웹 프로토콜인 SSL과 TLS에 대하여도 개념을 잘 이해하여야 한다. 이러한 기본 개념하에서 웹서버의 설치 및 운영 실무 지식을 통해 응용서비스를 실제 운용할 수 있어야 한다.
이를 바탕으로 최근 급속도로 증가하고 있는 웹서버에 대한 공격 유형을 이해하고 이에 대한 대책을 숙지하여야 한다. 또한 XML환경으로 발전해가는 추세에 맞추어서 XML기반의 웹보안 기술에 대한 학습 또한 중요하다.

가. web 개념

웹 어플케이션의 아키텍쳐는 주요 전송 매개체인 Hyper Text Transfer Protocol을 사용하여 웹서버와 웹클라이언트 사이의 서비스 요청과 응답을 처리하게 된다. 웹서버에서는 다양한 구조의 웹 어플리케이션 서비스를 제공하게 되며 가장 대표적인 것이 웹서버와 데이터베이스를 연동하여 정보서비스를 제공을 하는 것이다. 보안 측면에서 보다 향상된 웹서비스를 제공하게 위하여

SSL과 TLS 프로토콜 등이 사용된다.

(1) http 프로토콜 개념

▶ 웹 어플리케이션 아키텍쳐
▶ 웹서버와 웹 어플리케이션
▶ 웹서버와 데이터베이스

(2) SSL, TLS, https 프로토콜 개념

▶ SSL 프로토콜
  - SSL Handshake
  - SSL 2.0과 3.0의 비교
▶ TLS
  - TLS 레코드 프로토콜
  - TLS 핸드셰이크 프로토콜

나. web 서비스 운영

실제 웹서비스를 운영하게 될 때에 가장 대표적으로 사용하는 웹서버 어플리케이션은 apache와 IIS이다.

(1) apache 웹서버 설치 및 운영

▶ apache 웹서버 설치
▶ apache 웹서버 운영

(2) IIS 웹서버 설치 및 운영

▶ IIS 웹서버 설치
▶ IIS 웹서버 운영

다. web 로그보안

웹서비스는 웹서버와 웹클라이언트 사이의 많은 개개의 서비스요청과 서비스응답으로 이루어지게 되므로, 웹서버의 로그관리를 철저히 하여 보안문제 발생시 이를 잘 분석하여 활용할수 있어야 한다.

(1) apache서버 로그관리 및 분석

▶ 로그파일 위치 및 로그관련 설정
▶ 로그형식 및 로그내용의 분석
  - 접속한 클라이언트의 IP 주소, 혹은 도메인
  - 클라이언트(사용자 브라우저)의 접속시간정보 (httpd 접속시간)
  - 클라이언트(사용자 브라우저) 요청종류 (GET, POST)
  - 클라이언트가 요청한 홈페이지 URL 주소(요청한 자료 & 자료위치)
  - 상태코드(예. 200 정상처리)
▶ 보안 관점의 로그분석
  - 홈페이지 취약점 공격시 로그 패턴 분석

(2) IIS 서버 로그관리 및 분석

▶ 로그파일 위치 및 로그관련 설정
▶ 로그형식 및 로그내용의 분석
  - Host, AuthUser, Time, Service, ServerIP, Status, Request, Filename 등
▶ 보안 관점의 로그분석
  - 홈페이지 취약점 공격시 로그 패턴 분석
  - codered 공격시 IIS 패턴 등

라. web 서비스 공격 유형

web 서비스에 있어서 공격유형은 크게 web 사용자 클라이언트의 취약점을 이용한 사용자 컴퓨터 공격과 웹서버의 취약점을 이용한 웹서버 공격으로 나뉜다.
특히 웹서버에 대한 공격은 해당 네트웍의 방화벽의 필터링을 관통하여 내부네트웍을 공격하는 시작지점이 되므로 특히 주의하여야 한다.
웹 서비스 관련 공격은 최신 해킹 경향에 따라 끊임없이 새로운 공격기법이 발견되므로, 항상 최신 보안 경향에 관심을 갖고 있어야 한다.

(1) web 서버 자체 버그
▶ apache 서버에 존재하는 최신 취약점들
▶ IIS 서버에 존재하는 최신 취약점들
  - IIS공격을 응용한 인터넷 웜 공격기법 (codered 등)

(2) 파일 업로드 공격
▶ 게시판에서 파일 업로드를 허용할 경우 게시판 개발 언어와 동종의 script파일을 업로드 한 후에 다시 이를 Server Side Interpreter 특성을 이용하여 실행시킴으로서 웹서버 내부명령어를 실행하는 공격임

(3) 쿠키/세션 위조
▶ 클라이언트에 전달된 쿠키분석
▶ 각 인증에 사용되는 웹페이지 분석
▶ 매번 접속할 경우 변하는 쿠키부분과 변하지 않는 쿠키부분 분석
▶ 쿠키의 이름을 보고 내용 유추
▶ GET방식과 POST방식을 이용하여 위조된 쿠키로 인증통과 기법

(4) sql injection 공격
▶ 입력확인 기법을 통한 웹 어플리케이션 데이터베이스 에러 발생 기법
▶ 잠재적인 SQL구문의 구조 확인후 적절히 실행되는 문자들의 결합을 찾을 때까지 입력조작 기법
▶ 조작된 SQL질의를 통하여 공격자가 원하는 SQL구문 실행 기법

마. 웹 보안 개발

웹서버에 대한 공격은 정형화된 취약점을 정형화된 공격툴로 공격하는 것이 아니기 때문에 정형화된 점검툴로는 각 사이트별로 특정적으로 존재하는 취약점에 대하여 완전한 점검이 일반적으로 불가능하다. 따라서 각 사이트별로 웹 환경을 개발할때에 보안에 입각하여 개발을 하는 것이 중요하다.

(1) 웹 보안 프로그래밍

▶ 파일 업로드 공격 방지 개발 방법
  - cgi를 통해 시스템 호출함수를 사용할 수 없도록 코딩
  - 업로딩 디렉토리에 해당소스의 실행권한을 삭제 등

바. XML기반 웹 보안

XML은 웹 상에서 구조화된 문서를 전송 가능하도록 설계된 표준화된 텍스트 형식이다. 이는 인터넷에서 기존에 사용하던 HTML의 한계를 극복하고 SGML의 복잡함을 해결하는 방안으로써 HTML에 사용자가 새로운 태그(tag)를 정의할 수 있는 기능이 추가되었다. 또한, XML은 SGML의 실용적인 기능만을 모은 부분집합(subset)이라 할 수 있으며, 어떤 플랫폼에서나 읽을 수 있는 포맷을 제공하는 범용성을 갖는다.

(1) UDDI(Universal Description, Discovery and Integration)

▶ UDDI의 특징
  - General 메타 데이터를 제공
  - 벤더의 보장(Commitment) 제공
  - 여러 방식의 프로토콜 적용가능
  - 개방성이 없음
  - RDB(Relational Database Management) 쿼리 인터페이스가 없음
▶ UDDI의 주요 기능
  - 레지스트리 운영자(Registry Operator)
  - 비즈니스 제공자
  - 택사노미 제공자(Taxonomy Provider)
  - 정보 수집자(Information Aggregator)
  - 정보 확인자(Information validator)
▶ UDDI의 데이터 구조
  - 비즈니스 엔티티(businessEntity)
  - 비즈니스 서비스(businessService)
  - 바인딩 템플릿(bindingTemplate)
  - tModel

(2) SOAP(Simple Object Access Protocol)

▶ SOAP의 구성요소
  - SOAP envelope
  - SOAP encoding rules
  - SOAP RPC(Remote Procedure Call) 표현
  - SOAP binding
▶ SOAP의 특징
  - 프로토콜 독립성
  - 언어 독립성
  - 플랫폼 및 운영 체제 독립성
  - SOAP XML 메시지 첨부 지원(다중 MIME 구조 사용)

(3) WSDL(Web Service Description Language)

▶ WSDL의 구성요소
  - 공개적으로 사용할 수 있는 기능들의 정보
  - XML 메시지를 위한 데이터 타입 정보
  - 사용된 전송 프로토콜에 관한 바인딩 정보
  - 특정한 서비스 위치에 관한 주소 정보
▶ WSDL의 특징

- 추상적인 구문과 메시지
- WSDL 파일에는 포트 정보를 제공할 필요가 없음
- WSDL 스키마는 상위 레벨 혹은 언어상의 주된 element들을 정의

▶ WSDL의 문서 구조
- 문서 명명 및 연결
- 언어 확장성 및 바인딩
- 설명서

▶ WSDL의 웹 서비스 명세
- portType
- message
- types
- binding
- port
- service

(4) XML 보안

▶ XML Encryption
- XML 암호에 대한 구문과 처리규칙
- XML 암호에 대한 수행 규칙
- 3DES, RSA-v1.5, base64 알고리즘 지원
- XMS 암호의 적용 대상(일반 XML 문서, 일반 2진 형식 데이터)

▶ XML Signature
- XML 전자서명에 대한 구문과 처리규칙
- 무결성, 메시지 및 서명자 인증, 부인방지
- 어떤 디지털 컨텐츠에도 적용 가능

예제문제

(1) Apache 웹서버에 대한 리모트 스캔시 웹서버의 버전이 보이지 않도록 설정하기 위해서는 httpd.conf 파일에서 설정해야 한다. 다음 중 추가해야 하는 내용을 고르면?
① ServerTokens Minimal
② ServerTokens OS
③ ServerTokens ProductOnly
④ ServerTokens Full
⑤ ServerTokens Any

[정답] ③
[난이도] 중

(2) 다음 중 IIS 서버를 관리하는데 있어서 주의해야 할 점이 아닌 것은?
① Adminstrator나 guest 같은 기본 계정을 삭제하거나 변경한다
② 웹 서버에 포함되어 있는 견본 프로그램을 참고하며 서버를 운영한다
③ 불필요한 서비스는 사용하지 않는다
④ IPSec 등을 이용하여 포트 공격 등을 차단한다
⑤ IIS에 대한 로그관리를 철저히 해야한다.

[정답] ②
[난이도] 하

(3) 다음은 아파치 웹서버 로그 파일에서 볼 수 있는 상태코드로 HTTP/1.1에서 정의한 내용이다. 짝지어진 내용 중 틀린 것은?
① 200 - OK
② 400 - Forbidden
③ 404 - Not Found
④ 500 - Internal Server Error
⑤ 302 - Found

[정답] ②
[난이도] 상

(4) 웹서버의 로그에 아래와 같은 내용이 반복되어 남은 것을 발견하였다. 아래 로그를 분석한 결과로 맞는 것은?

[04/Aug/2001:20:36:54 +0900] "GET /default.ida?
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0" 404 292

① 시스템 관리자의 IIS 설정 오류로 인한 로그이다
② Code Red 웜에 감염된 시스템에서의 공격이다
③ root.exe 파일을 다운로드받아 설치해서 패치하도록 한다
④ 위의 로그가 다시 발생하지 않게 하려면 tcp 21번 포트 접근제한 설정을 해야 한다
⑤ apache 웹서버가 파일업로드 공격에 의해 침입당한 것으로 보인다.

[정답] ②
[난이도] 중

4. DB 보안

정보조직에서 가장 중요한 정보자산가치를 갖는 것이 바로 데이터베이스이다. 현실 세계에서의 정보보안의 근본적인 보호대상이 바로 데이터베이스에 수록되어 있는 중요 정보자산이라 할 수 있을 것이다. 이러한 데이터베이스 보안에는 크게 DB데이터 보안과 DB관리자권한 보안으로 나뉠수 있으며, 이를 토대로 효율적인 DBMS 보안운영이 가능할 것이다.

가. DB데이터 보안

DB데이터보안에서는 크게 DB보안 요구사항, DB보안통제, DB백업과 복구로 나뉠수 있다.

▶ DB보안 요구사항
- 부적절한 접근방지
- 추론방지
- 데이터 무결성
- 감사기능
- 사용자 인증

▶ DB 보안통제
- 흐름통제
- 추론통제
- 접근통제

▶ DB 백업과 복구
- 장애유형
  · 사용자오류
  · 명령문 장애 : 유효한 SQL구성이 아닌 경우와 같이 명령문을 처리할 때 발생하는 논리적 상태. 명령문에 장애가 발생하면 명령문의 실행 결과가 자동으로 무효화되고 제어가 사용자에게로 돌아감
  · 프로세스 장애
  비정상적인 접속 해제나 프로세스 종료와 같이 DB를 액세스하는 사용자 프로세스에 발생하는 장애.
  · 인스턴스 실패
  인스턴스(시스템 글로벌 영역과 백그라운드 프로세스)가 계속 작업을 수행할 수 없게 되었을 때 발생함.
  · 매체고장
- 복구에 사용되는 기술
  · redo로그
  · 제어파일
  · 롤백

나. DB 관리자 권한 보안

데이터베이스 관리자들은 특별한 operations을 수행해야 하므로 데이터베이스 관리자 username은 보다 안전한 인증 schema을 필요로 한다.

▶ Operation system에 의한 인증
▶ Network 인증 서비스(kerberos 등)에 의한 인증

다. DBMS 운영

실제의 DBMS시스템을 운영함에 있어서 각 DBMS 플랫폼별로 주어진 보안기능을 적절히 활용하여 안정성있는 DB보안관리를 해야한다.

▶ oracle 보안운영
▶ informix 보안운영
▶ MS sql 보안운영
▶ my sql 보안운영

라. DB 보안 개발

데이터베이스에 접근할 수 있는 데이터베이스 어플리케이션에 보안상 문제점이 있을 경우 이를 이용하여 DB정보에 주어진 권한을 넘어 접근할 수가 있게된다. 특히 최근엔 웹서버와 데이터베이스 서버간에 연동이 되어 정보서비스를 구축하는 웹-DB 연동 어플리케이션 개발 과정에서 보안을 고려한 개발이 더욱 요구된다.

(1) DB 어플리케이션 보안 프로그래밍

▶ 웹을 통한 sql injection 공격 방지 개발 방법
- 원시 ODBC에러를 사용자가 볼수 없도록 코딩
- 테이터베이스 어플리케이션의 최소 권한으로의 구동
- 데이터베이스 내장 프로시저 사용
- 테이블 이름, 칼럼 이름, sql구조 등이 외부 HTML에 포함되어 나타나서는 안됨

예제문제

(1) Mysql 실행시 다음과 같이 아이디와 패스워드를 입력하고 실행중일 때 나타나는 문제점을 고르면?

mysql -u〈UID〉 -p〈Password〉 〈DB name〉

① mysqldump를 실행할 수 없다
② mysql 서버에 부하가 걸린다
③ 다른 사용자가 DB의 내용을 볼 수 있다
④ 다른 사용자가 ps -ef 했을 때 패스워드를 볼 수 있다
⑤ mysql 데이터와 다른 DBMS간의 데이터 변환이 불가능하게 된다.

[정답] ④
[난이도] 중

(2) 다음중 오라클 DB서버를 운용할때에 보안상 적절히 않은 것은?
① 오라클 DBMS를 설치시 필요요소가 명확치 않다면 일단 Typical installation을 선택하여 설치한다.
② 디폴트 사용자 ID를 lock시키고 기간만료시켜야 한다
③ 모든 사용자가 Data Dictionary를 사용하게 할 필요는 없다.
④ public 사용자 그룹에서 불필요한 권한을 회수하여야 한다
⑤ 오라클 DB보안과 DB서버의 OS패치는 무관하다

[정답] ⑤
[난이도] 하

2절. 전자상거래 보안 (1급 : 30%, 2급 : 30%)

전자상거래는 소비자와 기업이 컴퓨터라는 매체를 통하여 이루어지는 거래이기 때문에 일반 상거래와는 달리 신원확인의 어려움, 대금결제, 프라이버시 침해, 그리고 전자상거래와 관련한 보안문제들이 발생할 수 있다. 전자상거래에 있어서 보안문제는 수많은 고객들이 인터넷을 이용한 전자상거래를 하고자 하는 경우에 많은 제약으로 작용하기 때문에 이러한 보안상의 문제가 중요한 문제로 부각되고 있다.

1. 전자상거래 기술

인터넷의 상업적 이용이 급증하면서 수많은 기업들은 인터넷을 단순히 정보만을 제공하는 것이 아니라 온라인으로 제품을 구입하고 판매하는 등 기업경영 전반에 걸쳐 적극적으로 활용하고 있다. 기업경영전반에 걸친 인터넷의 활용은 네트워크보안 및 거래보안과 관련한 제반 문제가 발생됨으로써 보안기술에 대한 중요성이 크게 증가하고 있다.

가. 암호 시스템

▶ 대칭키 암호방식
- DES, IDEA 암호 알고리즘

▶ 공개키 암호방식
- RSA, Rabin, Knapsack, ECC(Elliptic Curve Cryptography) 암호 알고리즘

나. 전자서명

▶ 전자서명의 기능
- 무결성 확보(Integrity)
- 신뢰성(Authenticity)
- 부인봉쇄(Non-repudiation)
- 신뢰확보
- 서면 및 서명요건의 충족

다. 공개키 기반구조

▶ 공개키 기반구조의 구성요소
- CA(Certificate Authority)
- RA(Registration Authority)
- 인증서 관리 프로토콜 (Certificate Management Protocol)
- 인증서 폐기(Certification Revocation)
- 인증서 저장소(Certificate Repositories)

▶ 공개키 기반구조의 구성 방법
- 계층 구조
- 네트워크 구조
- 혼합형 구조

2. 전자상거래 프로토콜

전자상거래가 웹에서 이루어지는 방법들은 반드시 그 자체의 안전성이 보장되어야 한다. 현 시점에서, 전자상거래 보안은 지불 방식에 중점을 두고 있으며, 다양한 보안 지불 프로토콜이 제안되고 있다.

가. 전자지불/화폐 프로토콜

▶ 전자화폐의 개념 및 특성
▶ 전자화폐의 분류
- IC카드형
- Network형

▶ 전자화폐의 문제점
▶ 전자화폐의 안전성 요구사항
- 익명성
- 오프라인성
- 양도성
- 분할성
- 독립성 (완전 정보화)
- 복사 및 위조방지
- 익명성 취소기능

▶ SET 프로토콜
- SET 암호기술

▶ 전자지불시스템 기술요건
- 거래당사자 확인
- 거래정보보호
- 거래부인 방지
- 거래 정보에 대한 접근 통제

▶ 전자지불시스템 위협요소
- 위조
- 국가통화관리
- 이중사용
- 위장

▶ 안전한 전자지불 서비스를 위한 보안 메커니즘
- 불추적성
- 분할성
- 익명성 제어

▶ Secure 전자지불서비스 모델
- B2B 전자지불 서비스 모델
- 신용카드 기반 전자지불 시스템
- IC카드형 전자화폐 시스템
- 네트워크형 전자화폐 시스템

나. 전자입찰 프로토콜

다. 전자투표 프로토콜

▶ 전자투표시스템 요구사항
- 완전성
- 익명성
- 이중투표방지
- 정당성
- 투표자격제한
- 검증 가능

3. 무선 플랫폼에서의 전자상거래 보안

무선 전자상거래(m-commerce)는 이동통신 네트워크 기술과 무선단말기를 기반으로 하여 언제 어디서나 필요한 시점에 행할 수 있는 상거래를 의미한다. 즉, 모바일 폰(hand-held phone), PDA, 노트북 등 무선단말기를 이용하여 B2B, B2C를 비롯하여 컨텐츠, 정보제공, 오락, 게임 등을 포함하는 모든 유료화된 상거래를 의미한다.

▶ 무선 전자상거래의 주요 특징
- 편재성
- 도달성
- 보안
- 편리성
- 위치성
- 즉시접속
- 개인화

▶ 무선 전자상거래 서비스
- 커뮤니케이션 서비스 (Communication service)

- 정보 서비스(Information service)
- 엔터테인먼트 서비스(Entertainment service)
- 거래 서비스(Transaction service)

▶ 무선컨텐츠 지불 서비스 모델
- B2B 결제
- 신용카드 기반 전자 지불
- IC 카드형 전자 화폐
- 네트워크형 전자 화폐

4. 전자상거래 응용보안

전자상거래 기반 기술을 토대로 특정한 응용분야 기술들이 개발되고 있는데 그 중에 하나가 ebXML(electronic business XML)이다. 이는 인터넷 표준 브라우저만으로 장소에 구애 없이 어디서나 전자상거래를 할 수 있으며 저렴한 구현 비용, 개방된 네트워크로 전자거래 교환을 위한 국제 표준을 제공한다. 기존의 EDI(Electronic Data Interchange)와는 달리 XML에 기반하고 있어 각각의 시스템을 가진 다양한 업종의 회사들간에 무수한 형태의 계약을 전자상거래로 처리할 수 있다.

가. e-business를 위한 ebXML 보안

▶ ebXML 구성
- ebXML은 트랜잭션의 개념 제공
- 약결합(loosely coupled), 메시지 중심적
- 비즈니스 프로세스와 모델을 정의
  (예 : Rose ttanet의 PIP와 유사한 개념)
- 비즈니스 프로세스와 정보 모델을 레지스터
- 파트너 비즈니스 프로세스
- 서비스 인터페이스
- 비즈니스 메시지
- 구성 정보(trans-port, security, encoding)를 discover / retrieve

▶ ebXML의 특징적 요소
- 글로벌한 광고 가능
- 분산된 형태의 아키텍처
- 리치 쿼리 기능이 가능
- 믿을 수 있는 SOAP을 이용
- 보다 특화된 그룹에 신경을 씀
- 벤더 독립적
- 비즈니스 프로세스에도 신경 쓰는 표준
- ACID 개념이 전혀 없음
- spec뿐이기에 벤더 보장, commitment가 없음

3절. 기타 어플리케이션 보안 기술 (1급 : 20%, 2급 : 0%)

1. 응용프로그램 보안개발 방법

많은 OS응용프로그램에서는 이른바 bug라 불리우는 보안 취약점이 포함되어 있어서 이를 patch를 통해 제거하기 전에는 이 취약점에 의해 시스템이 심각한 피해를 입기도 한다. 따라서 응용프로그램을 개발함에 있어서 이러한 보안 취약점을 남기지 않는 보안 프로그래밍을 하는 것이 중요하며, 특히 최근 많이 등장하는 버퍼오버플로우와 포맷스트링 버그를 방지할 수 있는 프로그래밍 기술을 익히는 것이 중요하다.

가. 취약점 및 버그방지 개발방법

▶ SUID/EUID 보안 프로그래밍
- UID와 GID를 가능한 제한
- exec를 호출하기 전에 effective UID와 GID를 재설정
- exec를 호출하기 전에 모든 파일 기술자를 닫음

▶ 새로운 프로세스의 생성 보안
- system(), popen() 함수를 사용하지 않음
- 모든 파일 기술자를 닫았는지 꼭 확인
- 프로그램을 실행할 때 전체 경로 이름을 사용하는지 확인
- 자식 프로세스에 전달된 환경변수를 확인

▶ 안전한 임시 파일 사용 보안
- 알려진 임시 디렉토리 안에 임시 파일을 생성하지 않음
- 임시파일을 생성하는 인터페이스를 제공하는 시스템을 사용
- 임시 파일의 이름을 예측할 수 있는 이름으로 생성하지 말고 랜덤하게 생성

▶ 버퍼오버플로 방지 프로그래밍
- 안전한 함수 사용

2. 보안 신기술

인터넷에서는 언제나 약점은 있고, 재미를 위해서 혹은 이익을 위해서 항상 문제를 만들어내는 사람도 존재하기 때문에 인터넷을 완전하게 보안한다는 것은 불가능한 일이다. 절대적인 보안이 가능한 어느 곳에서든 현재의 상황을 향상시키기 위한 작업으로부터 분리시키려는 것은 불가능한 목표라는 사실을 인식해야 한다. 따라서 수많은 불가능한 단계들이 보다 안전한 환경을 위한 인터넷의 일부분으로써 발전하도록 형성해 가는 작업이 필요하다.

가. 암호 알고리즘의 성능 향상과 새로운 암호 알고리즘

▶ 암호 알고리즘의 안전성 강화
- 새로운 수학적 문제에 기반한 암호 알고리즘 개발

▶ 암호 알고리즘의 고속화
- RSA암호 알고리즘의 고속화
- 타원곡선 알고리즘의 응용

▶ 구현의 용이성

나. 새로운 인증 기술

▶ 생체인증 기반의 전자서명
- 전자펜으로 입력된 서명의 진위를 판별하는 기술
- 영상 인식 기술

▶ 타기술과 PKI의 접목을 통한 인증 방법의 강화
- 생체인증과 PKI
  · 공인인증서와 생체정보를 결합한 편리하고 완벽한 사용자 인증 기능 지원
  · 단순한 지문 이미지가 아닌 생체정보를 이용한 알고리즘
  · 암호화기술에 의한 안전한 생체정보의 전달 및 관리기능
- 주요 서비스 분야
  · 인터넷 뱅킹
  · 사이버 증권
  · 쇼핑몰에서 상품주문 및 지불결제
  · 인터넷 유료 컨텐츠 이용
  · 무선 인터넷

▶ 차세대 네트워크를 위한 PKI
- 무선 PKI 기술
  · 무선 PKI 구축 기술
  · 무선 단말의 제한된 리소스에 따른 암호 알고리즘
  · 유·무선 PKI의 통합 기술
  · 차세대 네트워크 신기술과 PKI의 통합

다. DRM(Digital Rights Management)

▶ DRM의 주요 특징
- 용이한 사용자 최적화 및 연동성 제공
- 유동적인 서버 운용 및 CA관리 가능
- 판매 방식의 다양한 지원, CRM(Customer Resource Management) 서비스 제공
- 최고의 안전성을 가지는 국제 표준 암호 알고리즘 제공
- 대용량 전송 네트워크 지원
- 실시간 라이센스 키 다운로드 지원
- 다양한 멀티미디어 컨텐츠 지원
- 컨텐츠 복사 방지, 사용 횟수 제한 (Copy Control)가능

▶ DRM의 적용 분야
- AOD(Audio on Demand) 서비스
- VOD(Video on Demand) 서비스
- 웹 캐스팅 서비스 및 광고서비스
- 온라인 교육 컨텐츠 서비스
- e-book 관련 컨텐츠 서비스
- 온라인 뱅킹 서비스

예제문제

(1) 버퍼 오버플로우를 예방하는 방법 중 프로그래머가 코딩시 입력버퍼의 경계값을 검사하는 안전한 함수를 사용하는 방법이 있다.
다음 중 여기에 해당하지 않는 함수는?
① strncpy()
② snprintf()
③ fget()
④ getopt()
⑤ getwd()

[정답] ④
[난이도] 상

제4장 정보보호론

1절 암호학 (1급 : 30%, 2급 : 40%)

정보보호시스템을 설계, 개발, 관리, 유지보수를 위하여 필요한 암호학에 관한 전반적인 이론을 다룬다. 기본적인 암호 알고리즘, 전자서명과 더불어 암호 응용 프로토콜, 키관리를 포함한다.

1. 암호 알고리즘

암호 관련 용어 및 기초 개념을 다루며 공격 방법에 기본 개념에 대한 이해가 요구된다. 또한 관용 암호, 공개키 암호 등에 대한 이해와 활용 방법에 대한 충분한 이해를 요구한다.

가. 암호 관련 용어

- ▶ 암호시스템 개념
  - 평문, 암호문, 키, 암호 알고리즘
  - 공격자
- ▶ 정보보호서비스 개념
  - 기밀성, 무결성, 부인방지, 접근제어

나. 암호 공격 방식

- ▶ 각종 공격 방식
  - 암호문 단독 공격, 기지 평문 공격, 선택 평문 공격, 선택 암호문 공격
  - 수동 공격, 능동 공격
- ▶ 안전성 개념
  - 무조건적 안전성
  - 계산량적 안전성

다. 정보 이론

- ▶ 엔트로피 이론
  - 엔트로피 개념
  - 엔트로피 특성과 암호의 안전성 관련 이론
- ▶ 키 결정 거리

라. 스트림 암호

- ▶ 스트림 암호의 정의
  - 동기식, 비동기식에 대한 개념
- ▶ 스트림 암호 구성 원리
  - LFSR, FCSR 관련 이론
  - 결합 논리, 시각 제어 논리
- ▶ 안전성 개념
  - 선형복잡도, 주기
  - 랜덤 특성
  - 상관관계 공격

마. 블록 암호

- ▶ 블록 암호의 구조
  - SPN, Feistel
  - 라운드 함수, 키스케줄
- ▶ 블록 암호의 예
  - DES, AES, IDEA, SKIPJACK, SEED
- ▶ 블록 암호 운영 모드
  - ECB, CFB, CBC, CFB, Counter mode

바. 블록 암호 공격

- ▶ 기본 사항
  - 설계 원리, 키사이즈, 블록 사이즈
  - 취약키, 보수 특성, 중간일치공격 등
- ▶ 차분 공격
- ▶ 선형 공격
- ▶ 기타 공격

사. 인수분해 기반 공개키 암호

- ▶ RSA 공개키 암호의 시스템 변수 선정 방법
- ▶ RSA, Rabin
- ▶ 이차잉여류문제

아. 이산로그 기반 공개키 암호

- ▶ ElGamal 공개키 암호의 시스템 변수 선정 방법
- ▶ 타원곡선 공개키 암호

자. 확률적 공개키 암호

- ▶ 공개키 암호의 안전성 개념
  - Semantic Secure, Non-malleable
- ▶ RSA-OAEP
- ▶ 그 외의 확률적 공개키 암호
  - BBS, Goldwasser-Micali 등

2. 해쉬 함수와 디지털 서명

해쉬 함수와 MAC에 관한 이론을 다룬다. 디지털 서명에 사용하기 위해 필요한 암호학적 특성, 블록 암호를 이용하여 설계하는 방법, 전용 해쉬 함수 등을 다루고, 데이터 무결성과 메시지 인증 기법을 다룬다. 또한 각종 디지털 서명 기법을 다루고 시스템 설정에 따른 제반 문제점을 논한다. 또한 특수 서명 기법에 기반하여 응용 프로토콜에 대한 개념을 다룬다.

가. 해쉬 함수 일반

- ▶ 암호학적 요구 특성
  - 역상 저항성, 두 번째 역상 저항성, 충돌 저항성
- ▶ 생일 역설과 안전성 개념
- ▶ 데이터 인증

나. 블록 암호 이용 방식

- ▶ 각종 해쉬 함수 모드
  - Matyas-Meyer-Oseas, Davies-Meyer, MDC-2, MDC-4
- ▶ CBC-MAC, 3GPP-MAC, HMAC

다. 전용 해쉬 함수

- ▶ MD4, MD5, SHA, HAS, RIPE-MD

라. 해쉬 함수 설계 원리

- ▶ 암축함수와 패딩 기법
- ▶ MD-method
- ▶ Universal One-way Hash Function
- ▶ 해쉬 함수를 이용하여 MAC을 설계하는 방법

마. 디지털 서명 일반

- ▶ 수기 서명과 디지털 서명의 차이점
- ▶ PKI 개념
- ▶ 서명 위조와 안전성 개념
- ▶ 메시지 복원형과 메시지 부가형

바. 디지털 서명 예

- ▶ RSA 디지털 서명
- ▶ ElGamal 디지털 서명
- ▶ Schnorr, DSA, KCDSA, ECDSA

사. 특수 서명

- ▶ 은닉 서명과 응용 프로토콜
- ▶ 위임 서명과 응용 프로토콜
- ▶ Undeniable Signature
- ▶ Fail-Stop Signature

3. 인증 및 키 분배

개인 식별, 메시지 인증, 키 분배 기법을 다룬다. 나아가서 암호학에서 요구되는 안전성을 만족하면서 보안 서비스를 제공하기 위한 각종 정보보호 프로토콜을 다룬다.

가. 사용자 인증

- ▶ 패스워드 기반 개인 식별
  - 사전 공격
  - 패스워드 생성 및 관리 방법
- ▶ 시도 응답 프로토콜
- ▶ 영지식 기반 개인 식별
  - Fiat-Shamir
  - Schnorr

나. 메시지 인증

- ▶ 데이터 원본 인증, 거래 인증
- ▶ 무결성 달성 방법
  - CRC, MAC, MDC 등을 이용한 방법

다. 키 분배 프로토콜

- ▶ Kerboros
- ▶ Diffie-Hellman
- ▶ 키 로밍

라. 영지식 증명

▶ 영지식 증명 개념
- 계산 이론
- 대화형 증명

▶ 영지식 증명 프로토콜의 예

▶ 영지식 비대화형 증명

예제문제

(1) 다음은 암호 시스템을 사용하는 일반적인 원칙이다. 올바르지 않은 것은 무엇인가?
① 암호 시스템에서 키를 제외한 모든 부분은 공개되어 있다고 고려한다.
② 암호 알고리즘은 안전성을 좌우하는 중요한 요소이기 때문에 비공개가 원칙이다.
③ 여러 가지 공격 방법을 고려하여 될 수 있는 한 키를 자주 변경해야 한다.
④ 암호 알고리즘은 충분한 안전성을 확보하기 위하여 주기적인 재평가가 이루어져야 한다.
⑤ 평문을 암호화할 때에는 먼저 압축한 후에 암호화하는 것이 바람직하다.

[정답] ②
[난이도] 하
[해설] 암호시스템에서 암호 알고리즘을 비공개로 하는 경우도 있지만 이론적인 관점에서는 키를 제외한 모든 부분이 공개되어 있다고 가정하고 이러한 가정하에서 주어진 암호 시스템이 안전해야 한다. 암호 알고리즘의 비공개는 공격자에게 공격하는데 어려움이 주는 요소이지만 절대적인 것은 아니며 공개적인 검증 절차를 통하여 안전성이 확인된 암호 알고리즘을 사용하는 것이 바람직하다.

(2) 다음은 암호 공격 환경에 대한 설명이다. 틀리게 설명한 것은 무엇인가?
① 암호문만을 가지고 키나 평문을 알아내고자 하는 방식을 암호문 단독 공격(Ciphertext Only Attack)이라 한다.
② 공격자가 사전에 동일한 키로 암호화된 여러 개의 암호문과 대응하는 평문 쌍을 획득한 후 주어진 암호문에 대응하는 평문 또는 키를 알아내고자 하는 방식을 기지 평문 공격(Known Plaintext Attack)이라 한다.
③ 공격자가 임의의 평문을 선택하면 대응하는 암호문을 획득할 수 있는 능력을 보유하고서 주어진 암호문에 대응하는 평문이나 키를 알아내고자 하는 방식을 선택평문공격(Chosen Plaintext Attack)이라 한다.
④ 공격자가 임의의 암호문을 선택하면 대응하는 평문을 획득할 수 있는 능력을 보유하고서 주어진 암호문에 대응하는 평문이나 키를 알아내고자 하는 방식을 선택암호문공격(Chosen Ciphertext Attack)이라 한다.
⑤ 선택 평문 공격에서 공격자가 주어진 암호문을 본 후에 평문을 선택하여 암호문을 획득하고 다시 평문을 선택하여 암호문을 선택하는 과정을 반복적으로 행하는 경우를 능동 선택 평문 공격(Adaptive Chosen Plaintext Attack)이라 한다.

[정답] ④
[난이도] 중
[해설] 암호 공격 방식을 간략히 설명한 것으로 선택 암호문 공격에서 공격자는 해독하고자 하는 암호문을 제외한 모든 암호문에 대해 평문을 획득할 수 있는 능력이 있다고 본다.

(3) 블록 암호의 사용 방식 중 데이터 암호용으로 적합하지 않은 모드는?
① ECB 모드
② CBC 모드
③ CFB 모드
④ OFB 모드
⑤ Couter 모드

[정답] ①
[난이도] 중
[해설] 미연방 표준으로 되어 있는 블록 암호의 운영 모드 중에서 ECB 방식은 각 암호문 블록이 대응하는 평문 블록에만 의존하여 생성되기 때문에 동일한 암호문 블록이 발견되면 동일한 평문 블록이 암호화되었다는 정보가 노출되며, 키 전수조사를 위한 평문, 암호문 블록을 직접적으로 획득할 수 있어 데이터 암호용으로 권고되지 않으며 보통 난수 발생용으로 사용된다.

(4) 다음은 RSA 공개키 암호의 시스템 변수 선택에 관한 내용이다. 올바른 것은?
① 공개키 e와 개인키 d는 $d \equiv 1 mod \phi(n)$의 관계식이 만족하도록 선택된다.
② 공개키 e는 암호화 속도를 증가시키기 위해 보통 3으로 고정된다.
③ 스마트카드와 같은 환경에서는 복호화 속도를 높이기 위해 개인키 d를 $n^{1/4}$를 보다 작은 값으로 선택한다.
④ 공개키 n의 두 약수 p, q의 차는 충분히 크게 선택한다.
⑤ 공개키 n의 두 약수 p, q는 Strong Prime의 조건을 만족해야 한다.

[정답] ④
[난이도] 상
[해설] e와 d는 효율성을 위해 $ed \equiv 1 mod \lambda(n)$의 관계식을 만족하도록 선택하며, 암호화 속도를 증가시키기 위해 e를 작게 선택하지만 3으로 택하면 취약점이 발견되기 때문에 사용되지 않는다. d 역시 복호화 속도를 증가시키기 위해 작은 값으로 선택할 수 있지만 너무 작게 선택하면 d가 노출될 위험성이 있다. 현재는 타원곡선 인수분해 방법 등에 의하여 굳이 Strong Prime일 필요는 없다.

(5) 다음의 전자 서명에서 부분군을 사용하지 않은 것은?
① Schnorr 전자 서명
② KCDSA
③ DSA
④ Nyberg-Rueppel 전자 서명
⑤ ElGamal 전자 서명

[정답] ⑤
[난이도] 하
[해설] 위의 전자 서명은 모두 이산로그의 어려움에 기반한 방식이다. 또한 ElGamal 전자 서명을 제외하면 모두 서명 생성의 효율성을 위해 부분군을 사용한다.

2절 정보보호관리 (1급 : 50%, 2급 : 40%)

정보보호관리를 위해서는 우선 정보보호의 의미를 정확하게 파악해야 한다. 즉 정보보호는 조직의 임무와 목표를 달성하기 위해 정보자산의 기밀성, 무결성, 가용성을 적절한 수준에서 보장하기 위한 활동이다. 정보보호는 일상적인 관리활동으로서 정보보호 정책 및 조직 수립, 위험분석, 위험평가, 정보보호대책 선정 및 계획수립, 구현 및 운영 등의 프로세스로 구성되어 있다. 또한 재난으로 인한 업무중단을 최소화하기 위한 업무연속성관리도 정보보호관리의 중요한 영역으로 최근 인식되고 있다. 정보보호관리 활동을 위해서는 관련 국제 표준/지침 및 현안 이슈에 대해서도 인식이 필요하다.

1. 정보보호관리의 개념

정보보호는 그 자체로서의 의미보다는 비즈니스의 목적을 달성하기 위해 존재하는 것이라는 사실이 중요하다. 따라서 경영환경의 변화와 이와 관련한 정보보호의 필요성, 목적, 발전과정 등을 이해하는 것이 매우 중요하다. 또한 비즈니스에서 정보보호를 달성하기 위한 정보보호관리 활동에 대해 전반적인 프로세스와 성공요인을 파악하는 것이 필요하다.

가. 정보보호의 목적 및 특성

▶ 경영환경의 변화와 정보보호의 필요성
▶ 정보보호의 정의
▶ 정보보호의 목적인 비밀성, 무결성, 가용성에 대한 이해
▶ 정보보호의 특성
▶ 정보보호의 발전 과정

나. 정보보호와 비즈니스

▶ 비즈니스에서의 정보보호의 위상 변화
▶ 컴퓨터 범죄 증가와 정보보호의 필요성
▶ 정보보호의 시스템 모델

다. 정보보호관리의 개념

▶ 정보보호관리의 정의 및 기능
▶ 정보보호관리 과정
▶ 정보보호관리의 성공요인

라. 정보보호관리와 타 관리기능간의 관계

▶ 구성관리, 성능관리, 계정관리, 문제관리, 서비스 수준관리 등 관리 기능과 정보보호관리 기능과의 관계
▶ 통합정보보호관리의 의미와 접근방법

2. 정보보호 정책 및 조직

정보보호 정책은 조직의 정보보호에 대한 방향과 전략 그리고 정보보호 프로그램의 근거를 제시하는 매우 중요한 문서이다. 따라서 정책의 의미, 유형, 수립과정, 포함될 내용을 이해하여야 한다. 또한 정보보호 프로그램이 조직 내에서 효과적으로 수행되기 위해서는 정보보호에 대한 책임과 역할이 명확히 규명되어야 하고 이것이 조직 체계로서 구현되어야 한다. 따라서 정보보호를 위한 조직의 유형과 역할, 구성 등에 대한 이해가 필요하다.

가. 정보보호 정책의 의미 및 유형

- ▶ 정보보호 정책의 중요성
- ▶ 정보보호 정책의 유형
  - – 정보보호 정책, 지침/표준, 절차의 차이

나. 정보보호 정책 수립과정 및 내용

- ▶ 정보보호 정책 수립과정
- ▶ 정보보호 정책에 포함되어야 할 내용

다. 조직 체계와 역할/책임

- ▶ 정보보호조직 체계
  - – 정보보호위원회, 정보보호관리자의 조직상 위상
  - – 위원회의 구성 및 정보보호관리자의 자격
- ▶ 역할 및 책임
  - – 정보보호위원회, 정보보호관리자, 기타 경영층과 일반사용자의 역할 및 책임

라. 예산 수립과 정당화 방법

- ▶ 예산 수립시 고려해야 할 사항
- ▶ 정보보호 예산/투자에 대한 정당화 기법
  - – ROSI(return on security investment), TCO(total cost of ownership), Risk Analysis 등에 대한 이해

3. 위험관리

정보보호의 목적 달성을 위해서는 조직이 당면하고 있는 위험을 인식하고 이를 조직에 적절한 수준으로 통제하는 것이 위험관리이다. 즉 위험관리란 측정된 위험과 보안대책의 비용 및 효과와 비교하여, 조직의 정보보호 정책과 목적에 일치하는 구현전략과 정보보호 대책을 도출하는 과정을 말한다. 이 과정에는 다양한 종류의 보호대책이 고려되어야 하며, 그들의 비용과 효과에 대한 분석이 수행되어야 한다. 보호대책은 위험의 잠재적 영향 정도와 조직에서 감당할 수 있는 위험 수준을 고려하여 선정하여야 한다.

가. 위험관리 전략 및 계획수립

- ▶ 위험관리의 필요성
- ▶ 위험관리 전략
  - – 상세위험분석
  - – 기본통제 접근방법
- ▶ 위험관리 계획 수립시 고려사항
  - – 위험관리팀 구성, 위험분석 자동화도구 선정 기준 등

나. 위험분석

- ▶ 자산식별 및 가치 산정 방식
  - – 자산가치 산정 방식
- ▶ 위협 및 취약성 분석 방식
  - – 위협의 정의 및 유형
  - – 취약성의 정의 및 유형
  - – 위협 및 취약성 분석 방식
- ▶ 영향평가 방식
  - – 영향의 의미
  - – 영향 산정 방식
- ▶ 위험산출 방식
  - – 정량적 위험산정 방식
  - – 정성적 위험산정 방식

다. 정보보호대책 선정 및 계획서 작성

- ▶ 정보보호대책 선정시 고려사항
  - – 제약조건, 비용효과 분석
- ▶ 목표위험수준의 설정 방법
  - – DoA(Degree of Assurance)
- ▶ 정보보호계획서에 포함될 내용

4. 대책 구현 및 운영

정보보호대책 유형과 구현시 고려사항을 이해해야 하며 이 과정에서 특히 교육과 훈련의 중요성을 인식해야 한다. 정보보호대책은 기술적, 관리적, 물리적 대책을 모두 고려해서 시스템적인 접근방법을 통해 구축해야 한다. 또한 시스템, 네트워크 운영시 정보보호 측면에서 수행해야 하는 기법 등을 숙지해야 하며 비즈니스 및 기술환경의 변경 등을 반영할 수 있는 변경관리 절차, 운영과정의 모니터, 보안사고대응절차, 내부감사의 방법 등에 대한 이해가 요구된다.

가. 정보보호 대책 구현

- ▶ 정보보호대책 유형
  - – 기술적, 관리적, 물리적 대책
  - – 위험회피, 위험전가, 위험감소 대책
  - – 예방, 탐지, 교정 대책
- ▶ 정보보호대책 구현시 고려사항
  - – 프로젝트 관리

나. 정보보호 교육 및 훈련

- ▶ 교육 및 훈련의 중요성
- ▶ 교육 및 훈련 프로그램 수립
- ▶ 인식제고 방법

다. 운영

- ▶ 컴퓨터 운영
  - – 관리 기능, 로그 관리
- ▶ 네트워크 운영
  - – 관리 기능, 로그 관리, 네트워크 장비 관리 절차
- ▶ 매체관리
  - – 매체 보관, 폐기 등 관리 절차

라. 사후관리

- ▶ 모니터링
- ▶ 사고대응
  - – 대응절차, 역할 및 책임
- ▶ 변경관리
  - – 변경절차, 승인
- ▶ 내부감사
  - – 내부감사 계획, 절차

5. 업무연속성관리

정보시스템에 대한 의존도가 높아짐에 따라 일상적인 위험관리외에 자연재해나 인위적/기술적 재난으로 인한 비상사태시에도 조직의 주요 업무를 지속적으로 영위하기 위한 업무연속성계획 수립이 필요하다. 이는 과거의 정보기술 중심의 비상대책 및 재해복구대책을 확장한 개념으로 사용되고 있으며 일상적인 관리 활동으로 인식되고 있다. 따라서 업무연속성관리 과정, 업무영향평가 방식, 업무연속성을 위한 전략, 계획의 유형, 시험전략, 및 유지보수에 대한 이해가 필요하다.

가. 업무연속성관리 체계

- ▶ 업무연속성관리 과정
- ▶ 업무연속성계획 프레임워크
  - – 위험감소대책, 긴급조치 및 대응, 백업대체처리, 복구절차
- ▶ 업무연속성관리와 정보보호관리와의 관계

나. 업무연속성계획 수립

- ▶ 업무영향평가 방법 및 결과
  - – 복구시간목표
  - – 복구대상목표
- ▶ 백업처리 유형과 각각의 장단점
  - – Hot site, Cold site, Mirror site, 상호협정 등
- ▶ 데이터 백업 방식과 각각의 장단점

다. 업무연속성계획 유지관리

- ▶ 시험
  - – 시험 방법, 유형
- ▶ 유지관리
  - – 교육/훈련, 변경관리

6. 관련 표준 및 지침

정보보호 프로그램을 효과적으로 설계하고 운영하기 위해서는 정보보호에 대한 국내외 표준 및 동향에 대한 이해가 필요하며 이를 적극적으로 반영할 수 있어야 한다. 특히 최근 ISO, OECD와 같은 국제기구에서 정보보호 관련 정책/지침이나 국제표준이 계속적으로 발표되고 있으며, 미국을 위시한 주요국에서는 사이버공간 보안을 위한 국가전략을 수립하고 이를 구체적으로 실행하고 있다. 또한 정보보호 제품이나 관리체계에 대한 제3자 인증체계에 대한 이슈도 파악해야 한다.

가. 국제/국가표준

▶ 국제협정 및 표준
- OECD 정보보호 가이드라인 : 9원칙
- 미국의 사이버공간 보안을 위한 국가전략

▶ 정보보호관리 표준/지침
- GMITS, ISO 17799, BS7799 등

▶ 정보보호제품 관련 표준/지침
- CC

나. 인증체계

▶ 정보보호관리체계 인증
- KISA의 ISMS 인증체계
- KAB의 ISMS 인증체계

▶ 정보보호제품 인증
- 국내 정보보호제품 인증체계

예제문제

(1) 다음은 위험분석의 의미와 특징에 관한 설명이다. 틀린 것은?
① 위험분석은 정보보호 대책 구현에 선행되어 수행되어야 한다.
② 효과적 정보보안 프로그램의 초석으로서 의미를 가지고 있다.
③ 정량적 분석방법이 정성적 분석방법보다 정확한 위험수준을 결정할 수 있다
④ 자산식별, 위협분석, 취약성 평가, 영향 평가, 대책선정, 권고안 작성 순으로 진행
⑤ 조직의 특수 상황을 고려한 정보보호 대책을 선정할 수 있다.

[정답] ③
[난이도] 하
[해설] 위험분석은 정보보호 프로그램의 초석과 같은 역할을 수행한다. 즉 정보보호 대책 구현에 앞서 해당 시스템이 가지고 있는 위험을 분석함으로써 효과적인 대책을 선정할 수 있기 때문이다. 즉, 위험분석은 해당 시스템의 정보자산 식별 및 가치 산정과 시스템에 대한 위협과 취약성을 분석하여 위험을 계산하고 이에 따라 적절한 대책을 선정할 수 있기 때문에 조직의 특수한 상황을 고려한 정보보호 대책을 선정할 수 있다. 위험분석방법은 크게 정량적, 정성적 방법으로 구분할 수 있는데 어느 방법이 더 우월하냐는 상황에 따라 다를 수 있다. 즉 정확한 데이터와 과거 기록이있다면 정량적 방법이 더 좋을 수 있으나 다른 경우에는 정성적 방법이 더 적절할 것이다.

(2) 업무지속성을 위한 백업처리능력 대안으로서 Hot site, Mirror site, Warm site가 있는데 이중 가장 빠르게 백업을 제공하는 순서를 기술한 것은?
① Hot site, Warm site, Mirror site
② Hot site, Mirror site, Warm site
③ Mirror site, Warm site, Hot site
④ Warm site, Hot site, Mirror site
⑤ Mirror site, Hot site, Warm site

[정답] ⑤
[난이도] 중
[해설] 백업처리 방식으로서 많이 언급되는 것이 Mirror site, Hot site, Warm site이다. Mirror site는 메인센터와 동일한 구성의 백업센터를 구축하고 메인센터와 백업센터간 실시간 데이터 동기화를 유지하여 메인센터 재해 발생시 즉시 백업센터에서 업무대행을 실시간으로 처리할 수 있다. Hot site는 메인센터와 동일한 H/W, S/W, 부대설비를 준비하고 실시간 DB Log 전송 및 DB Image Backup을 준비하여 메인센터 재해 발생시 데이터 복구작업을 실시 하여 약 24시간 이내에 재개할 수 있다. Warm site는 메인센터 장비 일부 및 Data 백업만을 준비하여 재해 발생시 주요 업무 데이터만 복구하는 시설로 필요시 Hot Site로 전환 가능하다.

(3) 다음에서 정보보호 관리자의 역할에 대한 설명으로 틀린 것은?
① 조직의 전략 및 계획에 부응되는 정보보호 계획 수립
② 정보보호 대책의 구현과 운영
③ 정보보호 인식제고 프로그램을 개발
④ 정보보호 목적, 전략 및 정책을 결정
⑤ 전사적인 정보보호 활동의 조정 및 감시

[정답] ②
[난이도] 상
[해설] 정보보호 관리자는 조직의 정보보호 프로그램을 기획, 관리하는 자로서 매우 중요한 역할을 수행한다. 우선 조직의 임무 및 전략을 반영한 정보보호 목적, 전략 및 정책을 개발하고 이에 따른 구체적인 정보보호 계획을 수립하여 이를 실현시켜야 한다. 이에는 인식제고 및 교육 훈련 프로그램도 포함되어야 한다. 또한 조직내 정보보호 활동을 모니터링하고 변경사항을 조정하는 역할을 수행한다. 실제로 정보보호대책(예 : 침입탐지시스템)을 운영하는 자는 해당 부서의 직원(예 : 전산운영 담당자)이 하는 것이고 운영자료의 분석 결과를 통한 조치는 정보보호 관리자의 책임이라고 할 수 있다.

3절 관련법규 (1급 : 20%, 2급 : 20%)

정보보호(IT 보안)과 관련하여서는 1990년대 중반 정보화촉진기본법이 제정됨으로써 비로소 제도화가 이루어지기 시작하였다. 이후 1998년에는 정보통신망보급및이용촉진에관한법률에서 정보통신서비스제공자의 개인정보보호와 정보보호 의무를 일반적으로 규정하였고, 1999년에는 전자서명법이 제정되어 전자서명의 이용에 관한 법률적 근거를 마련하였다. 2000년대에 들어 정보화가 더욱 촉진되면서 사회 전분야의 정보시스템에 대한 의존이 높아지고 또 정보시스템이 상호연결되어 이용됨에 따라 정보통신인프라는 정보사회의 중요한 사회인프라로 인식되게 되었다. 따라서 사회의 안정과 번영을 위하여는 이들 정보통신인프라를 각종 위협으로부터 보호하는 것이 국가의 중대한 과제로 인식됨에 따라 이에 대한 대책을 수립하고 그 법률적 근거로서 2001년 정보통신기반보호법을 제정하였다. 이외에 각 분야에서 정보기술의 도입이 활발해짐에 따라 관련법률에서 개별적으로 정보보호에 대한 규정을 마련하는 경우가 많아지고 있다.

1. 정보화촉진기본법

가. 정보보호의 정의

▶ "정보보호"라 함은 정보의 수집 · 가공 · 저장 · 검색 · 송신 · 수신중에 정보의 훼손 · 변조 · 유출 등을 방지하기 위한 관리적 · 기술적 수단(이하 "정보보호시스템"이라 한다)을 강구하는 것을 말한다.(제2조 4호)

나. 정보화시책의 기본원칙

▶ 정보화시책의 기본원칙에 개인의 사생활 보호와 각종 정보자료의 안전성 유지 등 정보보호 포함(제3조 5호)

다. 정보화촉진기본계획과 정보보호

▶ 정보화촉진기본계획에 행정, 산업, 재정 · 금융, 교육 · 연구 · 과학기술 · 환경, 지역 · 문화 · 생활 기타 분야별 정보보호와 개인정보보호에 관한 사항 포함(제5조 제3항 7호 및 9호)

라. 정보보호시책 강구

▶ 정부는 정보보호시책을 강구할 책무를 짐(제14조 제1항)
- 제14조(정보보호 등) ①정부는 정보의 안전한 유통을 위하여 정보보호에 필요한 시책을 강구하여야 한다.

▶ 정부는 암호기술의 개발 · 이용을 촉진하고 암호기술을 이용한 정보통신서비스 안전조치를 강구할 책무를 짐(제14조 제2항)
- 제14조(정보보호 등) ②정부는 암호기술의 개발과 이용을 촉진하고 암호기술을 이용하여 정보통신서비스의 안전을 도모할 수 있는 조치를 강구하여야 한다.

마. 정보보호시스템 평가, 인증

▶ 정보통신부장관이 정보보호시스템의 성능과 신뢰도에 관한 기준을 고시하고, 정보보호시스템을 제조하거나 수입하는 자에게 이 기준의 준수를 권고(제15조 제1항)

▶ 정보통신부장관은 정보보호시스템을 제조하거나 수입하고자 하는 자의 요청이 있는 경우 유통중인 정보보호시스템이 성능과 신뢰도에 관한 기준에 합치하는지 여부를 평가하여 기준에 미치지 못할 경우에 정보보호시스템의 보완 기타 필요한 사항을 권고할 수 있음(제15조제2항)
- 정보통신부장관은 한국정보보호진흥원의 장으로 하여금 당해 정보보호시스템을 조사 또는 시험·평가하게 할 수 있음(시행령 제16조제2항)

▶ 관련 법률조항 : 제15조(정보보호시스템에 관한 기준고시등)

2. 정보통신망이용촉진및정보보호등에관한법률

가. 용어의 정의

▶ 개인정보
- "개인정보"라 함은 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.(제2조 제1항 6호)

▶ 용어정의 준용
- 정보통신망이용촉진및정보보호등에관한법률에서 사용하는 용어의 정의는 동법에서 정하는 것을 제외하고는 정보화촉진기본법이 정하는 바에 의함(제2조 제2항)
  · 따라서 "정보보호"의 정의는 정보통신망이용촉진및정보보호등에관한법률에서도 준용됨

나. 정보통신망 정보보호 등 시책 강구

▶ 정보통신부장관의 책무
- 정보통신부장관은 정보통신망의 안정적 관리·운영과 이용자의 개인정보의 보호 등을 통하여 정보사회의 기반을 조성하기 위한 시책을 마련할 책무를 가짐(제4조 제1항)
- 정부는 정보통신서비스제공자단체 또는 이용자단체의 개인정보보호 및 정보통신망에서의 청소년보호 등을 위한 활동을 지원할 수 있음(제3조제3항)

▶ 관련 법률조항
- 제4조(정보통신망이용촉진및정보보호등에관한시책의강구) 3항
- 제3조(정보통신서비스제공자 및 이용자의 책무)

▶ 시책의 내용
- 정보통신부장관이 정보통신망의 안정적 관리·운영과 이용자의 개인정보의 보호 등을 통하여 정보사회의 기반을 조성하기 위해 마련하는 시책에 포함되는 정보보호 관련사항(제4조 제2항)
  · 정보통신망을 통하여 수집·처리·보관·이용되는 개인정보의 보호
  · 정보통신망의 안전성 및 신뢰성 제고
  · 정보통신망에 관련된 기술의 개발·보급
  · 정보통신망의 표준화

▶ 정보화촉진기본계획과의 연계
- 정보통신부장관은 정보보호 시책을 수립함에 있어서 정보화촉진기본계획과 연계되도록 하여야 함(제4조 제3항)

다. 정보통신망법과 타법률과의 관계

▶ 정보보호와 관련하여 정보통신망이용촉진및정보보호등에관한법률은 다른 법률과의 관계에서 일반법의 지위를 가짐
- 제5조(다른 법률과의 관계) 정보통신망이용촉진및정보보호등에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법이 정하는 바에 의한다.

라. 개인정보보호

▶ 개인정보의 수집과 관련한 정보통신서비스제공자의 의무와 수집제한
- 정보통신서비스제공자가 이용자의 개인정보를 수집하는 경우 원칙적으로 당해 이용자의 동의를 얻어야 함. 다만, 다음 세 가지 경우에는 예외 인정(제22조 제1항)
  · 정보통신서비스 이용계약의 이행을 위하여 필요한 경우
  · 정보통신서비스 제공에 따른 요금정산을 위하여 필요한 경우
  · 이 법 또는 다른 법률에 특별한 규정이 있는 경우

▶ 동의를 얻고자 하는 경우의 고지사항과 고지방법(제22조 제2항)
- 제22조(개인정보의 수집)
  ②정보통신서비스제공자는 제1항의 규정에 의한 동의를 얻고자 하는 경우에는 미리 다음 각호의 사항을 이용자에게 고지하거나 정보통신서비스 이용약관에 명시하여야 한다.

  1. 개인정보관리책임자의 성명·소속부서·직위 및 전화번호 기타 연락처
  2. 개인정보의 수집목적 및 이용목적
  3. 개인정보를 제3자에게 제공하는 경우의 제공받는 자, 제공목적 및 제공할 정보의 내용
  4. 제30조 제1항·제2항 및 제31조 제2항의 규정에 의한 이용자 및 법정대리인의 권리 및 그 행사방법
  5. 그 밖에 개인정보 보호를 위하여 필요한 사항으로서 대통령령이 정하는 사항
- 개인정보의 수집제한(제23조)

▶ 개인정보의 이용 및 제공과 관련한 정보통신서비스제공자의 의무
- 개인정보의 이용 및 제공과 관련한 제한(제24조)
- 개인정보처리 위탁시 고지의무와 손해배상에 관한 특칙(제25조)
- 영업양도, 합병 및 상속의 경우 통지의무(제26조)
- 개인정보관리책임자의 지정, 개인정보 보호조치, 개인정보의 파기(제27조 내지 제29조)

▶ 개인정보와 관련한 이용자의 권리
- 이용자는 동의를 언제든지 철회할 수 있는 권리, 개인정보를 열람하고 오류의 정정을 요구할 수 있는 권리를 가짐(제30조)
- 정보통신서비스제공자가 만 14세 미만의 아동으로부터 개인정보를 수집하거나 이용 또는 제3자에게 제공하고자 하는 경우에는 그 법정대리인의 동의를 얻어야 함(제31조)
- 손해배상청구권(제32조)

▶ 개인정보분쟁조정위원회
- 관련 법률조항
  · 제33조(개인정보분쟁조정위원회의 설치 및 구성) 제34조(위원의 신분보장) 위원은 자격정지 이
  · 상의 형의 선고를 받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직 또는 해촉되지 아니한다.
  · 제35조(위원의 제척·기피·회피)
  · 제36조(분쟁의 조정)
  · 제37조(자료요청 등)
  · 제38조(조정의 효력)
  · 제39조(조정의 거부 및 중지)
  · 제40조(조정절차 등)

▶ 개인정보관련 국제계약의 제한
- 정보통신서비스제공자는 이용자의 개인정보에 관하여 법규정을 위반하는 사항을 내용으로 하는 국제계약을 체결하여서는 아니된다.(제54조)

▶ 정보통신서비스제공자외의 자에 대한 준용
- 개인정보보호에 관한 규정중 일부(개인정보분쟁조정위원회 관련조항 제외)는 정보통신서비스제공자외의 자로서 대통령령이 정하는 재화 또는 용역 제공자에게도 적용(제58조)

마. 정보통신망의 안정성 확보

▶ 정보통신서비스제공자의 정보보호조치 의무
- 정보통신서비스제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치 의무를 짐(제45조 제1항)
  · 정보통신부장관은 보호조치의 구체적 내용을 정한 정보통신서비스의 정보보호에 관한 지침을 정하여 고시하고 정보통신서비스제공자에게 그 준수를 권고할 수 있다.(제45조 제2항)

▶ 집적정보통신시설 운영·관리자의 정보보호조치 의무
- 관련 법률조항
  · 제46조(집적된 정보통신시설의 보호)
  ①타인의 정보통신서비스제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자는 정보통신시설의 안정적 운영을 위하여 정보통신부령이 정하는 바에 의한 보호조치를 취하여야 한다.
  ②제1항의 규정에 의한 사업자는 집적된 정보통신시설의 멸실, 훼손 기타 운영장애로 인하여 발생한 피해의 보상을 위하여 정보통신부령이 정하는 바에 따라 보험에 가입하여야 한다.
  ③정보통신부장관은 제1항의 규정에 의한 보호조치를 취하지 아니한 사업자에게 상당한

기간을 정하여 시정조치를 명할 수 있다.

▶ 정보보호관리체계 인증
- 관련 법률조항
  · 제47조(정보보호관리체계의 인증)
  ①정보통신서비스제공자 및 정보통신서비스를 제공하기 위한 물리적 시설을 제공하는 자는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위하여 수립·운영하고 있는 기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호관리체계"라 한다)가 당해 서비스에 적합한 지에 관하여 제52조의 규정에 의한 한국정보보호진흥원으로부터 인증을 받을 수 있다.
  ②정보통신부장관은 제1항의 규정에 의한 인증에 관한 정보보호관리 기준 등 필요한 기준을 정하여 고시할 수 있다.
  ③제1항의 규정에 의하여 정보보호관리체계의 인증을 받은 자는 정보통신부령이 정하는 바에 의하여 인증의 내용을 표시하거나 홍보할 수 있다.
  ④제1항의 규정에 의한 인증의 방법·절차 및 수수료 기타 필요한 사항은 정보통신부령으로 정한다.

바. 정보통신망 침해행위 등의 금지

▶ 해킹, 컴퓨터바이러스 유포, 서비스거부공격의 금지(제48조)
▶ 타인정보의 훼손, 타인비밀의 침해·도용·누설 금지(제49조)
▶ 광고성 정보전송의 제한(제50조)
▶ 중요정보의 국외유출 제한(제51조)

사. 한국정보보호진흥원

▶ 관련 법률조항
- 제52조(한국정보보호진흥원)
- 제57조(비밀유지 등)

아. 벌칙

▶ 관련 법률조항
- 제61조 내지 제67조

3. 정보통신기반보호법

가. 용어의 정의

▶ "정보통신기반시설"(제2조 1호)
- 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망이용촉진및정보보호등에관한법률 제2조 제1항 제1호의 규정에 의한 정보통신망.

▶ "전자적 침해행위"(제2조 2호)
- 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고 출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위

▶ "침해사고"(제2조 3호)
- 전자적 침해행위로 인하여 발생한 사태

나. 주요정보통신기반시설 보호체계

▶ 정보통신기반보호위원회
- 국무총리 소속하에 정보통신기반보호위원회를 둠(제3조)
  · 위원장(국무총리)을 포함한 25인 이내의 위원으로 구성
  · 위원은 대통령령이 정하는 중앙행정기관의 장과 위원장이 위촉하는 자로 함
  · 위원회의 효율적인 운영을 위하여 위원회에 실무위원회를 둠

▶ 위원회의 기능(심의기능)(제4조)
- 주요정보통신기반시설 보호정책의 조정에 관한 사항
- 주요정보통신기반시설에 관한 보호계획의 종합·조정에 관한 사항
- 주요정보통신기반시설 보호와 관련된 제도의 개선에 관한 사항
- 그 밖의 주요정보통신기반시설 보호와 관련된 주요 정책사항으로서 위원장이 부의하는 사항

▶ 주요정보통신기반시설 관리기관의 장
- 주요정보통신기반시설 관리기관의 장은 취약점 분석·평가의 결과에 따라 소관 주요정보통신기반시설을 안전하게 보호하기 위한 물리적·기술적 대책을 포함한 관리대책(주요정보통신기반시설보호대책)을 수립·시행(제5조)
- 주요정보통신기반시설 관리기관의 장은 취주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(정보보호책임자)를 지정하여야 한다.
(제5조 제4항)

▶ 관계중앙행정기관의 장
- 관계중앙행정기관의 장은 관리기관의 장으로부터 제출받은 주요정보통신기반시설보호대책을 종합·조정하여 소관분야에 대한 주요정보통신기반시설에 관한 보호계획(주요정보통신기반시설보호계획)을 수립·시행(제6조)
- 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(정보보호책임관)를 지정하여야 한다.
(제6조 제4항)

▶ 주요정보통신기반시설 보호 지원기관의 장
- 지원기관의 장은 요청이 있는 경우 다음의 기술적 지원을 수행(제7조)
  · 주요정보통신기반시설보호대책의 수립
  · 주요정보통신기반시설의 침해사고 예방 및 복구

다. 주요정보통신기반시설의 지정과 취약점 분석·평가

▶ 주요정보통신기반시설의 지정
- 중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정 가능(제8조 제1항)
  · 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
  · 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
  · 다른 정보통신기반시설과의 상호연계성
  · 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
  · 침해사고의 발생가능성 또는 그 복구의 용이성
- 지정절차(제8조 제2항 내지 제6항)

▶ 주요정보통신기반시설의 취약점 분석·평가
- 관리기관의 장이 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가(제9조)
  · 취약점을 분석·평가하는 전담반 구성(한국정보보호진흥원, 정보공유·분석센터, 정보보호컨설팅 전문업체, 한국전자통신연구원에 의하는 경우 전담반을 구성하지 않을 수 있음)

라. 주요정보통신기반시설의 보호 및 침해사고의 대응

▶ 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당 분야의 관리기관의 장에게 이를 지키도록 권고할 수 있다.(제10조)
▶ 관계중앙행정기관의 장은 제출받은 주요정보통신기반시설보호대책을 분석하여 필요하다고 인정하는 때에는 해당 관리기관의 장에게 주요정보통신기반시설의 보호에 필요한 조치를 명령 또는 권고할 수 있다.(제11조)
- 정보통신부장관은 명령 또는 권고를 받은 해당 관리기관의 장이 보호조치를 시행하는데 필요한 기술적 지원을 수행 가능

▶ 금지되는 주요정보통신기반시설 침해행위(제12조)
▶ 관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는파괴된 사실을 인지한 때에는 관계행정기관, 수사기관 또는 보호진흥원에 그 사실을 통지하여야 한다. 이 경우 관계기관등은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취하여야 한다.(제13조)
▶ 관리기관의 장은 소관 주요정보통신기반시설에 대한 침해사고가 발생한 때에는 해당 정보통신기반시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다.(제14조)
▶ 위원회의 위원장은 주요정보통신기반시설에 대하여 침해사고가 광범위하게 발생한 경우 그에 필요한 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여 위원회에 정보통신기반침해사고대책본부를 둘 수 있다(제15조)
▶ 정보공유·분석센터(제16조)

마. 정보보호컨설팅 전문업체

▶ 지정기준 및 절차, 결격사유, 양도·합병 및 휴지·폐지·재개 등의 경우 절차, 지정취소, 기록 및 자료

의 보존에 관한 규정
▶ 관련 법률조항
– 제17조 내지 제23조

바. 비밀유지의무

▶ 취약점 분석 · 평가업무를 하는 기관, 침해사고의 통지 접수 및 복구조치와 관련한 업무를 하는 관계기관등 그리고 정보공유 · 분석센터에 종사하는 자 또는 종사하였던 자는 그 직무상 알게된 비밀을 누설하여서는 아니된다. 다만, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다.(제27조)

사. 벌칙

▶ 관련 법률조항
– 제28조 내지 제30조

4. 전자서명법

가. 용어의 정의

▶ 전자서명, 공인전자서명, 인증서, 공인인증서, 공인인증기관, 가입자, 서명자 등 전자서명법상 용어의 법률적 정의에 대한 기본적인 이해를 요함(제2조)

나. 전자서명의 효력

▶ 전자서명의 효력(제3조)
– 다른 법령에서 문서 또는 서면에 서명, 서명날인 또는 기명날인을 요하는 경우전자문서에 공인전자서명이 있는 때에는 이를 충족한 것으로 본다.
– 공인전자서명이 있는 경우에는 당해 전자서명이 서명자의 서명, 서명날인 또는 기명날인이고, 당해 전자문서가 전자서명된 후 그 내용이 변경되지 아니하였다고 추정한다.
– 공인전자서명외의 전자서명은 당사자간의 약정에 따른 서명, 서명날인 또는 기명날인으로서의 효력을 가진다

다. 공인인증기관의 지정과 감독

▶ 공인인증기관의 지정과 관련하여 지정기준 및 절차, 결격사유를 정확히 이해하는 것이 필요 (제4조 및 제5조)
▶ 공인인증기관은 인증업무를 개시하기 전에 다음 사항이 포함된 공인인증업무준칙을 작성하여 정보통신부장관에게 신고하여야 한다.(제6조)
– 인증업무의 종류
– 인증업무의 수행방법 및 절차
– 공인인증역무의 이용조건 및 이용요금
– 기타 인증업무의 수행에 관하여 필요한 사항
▶ 인증역무의 제공, 공인인증업무 수행, 인증업무의 양수 · 합병 및 유지 · 폐지 등, 시정명령, 업무정지, 지정취소 등 공인인증기관의 감독에 관한 규정내용 (제7조 내지 제14조)

라. 공인인증서

▶ 공인인증서의 발급, 효력소멸, 효력정지, 폐지 등 공인인증서에 관한 규정내용. 특히 공인인증서의 내용 및 법률효과에 유의(제15조 내지 제18조)
▶ 다른 법률에서 공인인증서를 이용하여 본인임을 확인하는 것을 제한 또는 배제하고 있지 아니한 경우에는 공인인증기관이 발급한 공인인증서에 의하여 본인임을 확인할 수 있다.(제18조의2)

마. 인증업무의 안전성 및 신뢰성 확보

▶ 인증업무의 안전성 및 신뢰성 확보를 위한 보호조치, 인증업무에 관한 시설 및 장비의 안전운영, 전자문서의 시점확인, 전자서명생성정보 및 개인정보보호에 관한 규정내용(제18조의3 내지 제25조)

바. 이용자의 준수사항, 특정공인인증서 요구 금지, 배상책임

▶ 이용자는 공인인증서 기재사항 등에 의하여 공인전자서명의 진위여부를 확인하기 위하여 다음 조치를 취하여야 한다.(제25조의2)
– 공인인증서의 유효 여부의 확인
– 공인인증서의 정지 또는 폐지 여부의 확인
– 공인인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항 및 가입자가 제3자를 위한 대리권 등을 갖는 경우 또는 직업상 자격등의 표시를 요청한 경우 이에 관한 사항의 확인

▶ 누구든지 공인인증서를 이용하여 전자서명을 확인하는 경우 정당한 이유없이 특정 공인인증기관의 공인인증서만을 요구하여서는 아니된다. (제25조의3)
▶ 공인인증기관은 인증업무 수행과 관련하여 가입자 또는 공인인증서를 신뢰한 이용자에게 손해를 입힌 때에는 그 손해를 배상하여야 한다. 다만, 그 손해가 불가항력으로 인하여 발생한 경우에는 그 배상책임이 경감 되고, 공인인증기관이 과실없음을 입증한 경우에는 그 배상책임이 면제된다.(제25조)

사. 전자서명인증정책 추진 등

▶ 전자서명의 안전성과 신뢰성을 확보하고 그 이용을 활성화하는 등 전자서명 및 인증업무의 발전을 위한 정부의 시책 수립 · 시행, 상호연동, 기술개발 및 인력양성, 시범사업 및 지원에 관한 규정내용 이해 (제26조의2 내지 제26조의6)

아. 벌칙

▶ 관련 법률조항
– 제31조 내지 제34조

5. 전자거래기본법

가. 전자서명

▶ 전자거래를 함에 있어서 전자서명에 관한 사항은 전자서명법이 정하는 바에 따른다.(제11조)

나. 정보보호

▶ 개인정보보 : 12조(개인정보보호)
▶ 영업비밀보호 : 제13조(영업비밀보호)

다. 암호제품의 사용

▶ 전자거래사업자는 전자거래의 안전성 및 신뢰성을 확보하기 위하여 암호제품을 사용할 수 있다. 다만, 정부는 국가안전보장을 위하여 필요하다고 인정하는 경우에는 암호제품의 사용을 제한하고, 암호화된 정보의 원문 또는 암호기술에의 접근에 필요한 조치를 할 수 있다.(제14조)

예제문제

(1) 현행법률의 정보보호에 관한 규정내용을 설명한 것이다. 옳은 것은 어느 것인가?
① 정보통신부장관은 5년마다 정보화촉진기본계획과 함께 정보보호기본계획을 작성하여야 한다.
② 악성프로그램을 전달 또는 유포하는 자가 정보보호조치를 침해하여 정보통신망에 침입하는 자보다 무거운 처벌을 받는다.
③ 정보통신서비스제공자가 정보보호조치 의무를 위반한 경우 3천만원 이하의 벌금에 처한다.
④ 정보보호에 대한 용어정의가 정보화촉진기본법과 정보통신망이용촉진및정보보호등에관한법률에서 각기 다르다.
⑤ 전자서명인증관리 업무에 종사하는 자 또는 종사하였던 자는 그 직무상 알게된 비밀을 타인에게 누설하거나 직무상 목적외에 이를 사용하여서는 아니된다.

[정답] ②
[난이도] 중
[해설] 악성프로그램을 전달 또는 유포하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에, 정보보호조치를 침해하여 정보통신망에 침입하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. ①정부가 5년마다 정보화촉진기본계획을 작성하며, 여기에 분야별 정보보호에 관한 사항이 포함된다. ③정보통신서비스제공자의 정보보호조치 의무위반에 대해서는 처벌규정이 없다. ④ 정보통신망이용촉진및정보보호등에관한법률은 정보화촉진기본법의 용어정의를 준용하고 있으므로 동일하다. ⑤ 비밀유지의무를 부담하는 자는 분쟁조정위원회의 분쟁조정 업무, 정보보호관리체계 인증 업무, 정보보호시스템의 평가 업무에 종사하는 자 또는 종사하였던 자이다 (정보통신망이용촉진및정보보호등에관한법률 제57조)

(2) 정보통신망이용촉진및정보보호등에관한법률상 개인정보보호와 관련하여 이용자에게 인정되는 권리가 아닌 것은?
① 동의철회권

② 개인정보 열람청구권
③ 개인정보 오류정정 청구권
④ 손해배상청구권
⑤ 자료요청권

[정답] ⑤
[난이도] 중
[해설] 자료요청권은 분쟁조정위원회가 분쟁조정을 위하여 분쟁당사자에게 필요한 자료의 제공을 요청할 수 있는 권리이다.(제37조)

(3) 다음은 전자서명에 관한 설명이다. 틀린 것은?
① 전자문서에 공인전자서명이 있는 때에는 다른 법령에서 문서 또는 서면에 서명, 서명날인 또는 기명날인을 요하는 경우 이를 충족한 것으로 본다.
② 공인인증기관으로 지정 받을 수 있는 자는 국가기관 · 지방자치단체 또는 법인에 한한다.
③ 지정이 취소된 후 2년이 경과되지 아니한 법인은 공인인증기관으로 지정받을 수 없다
④ 전자서명법은 디지털서명 방식만을 인정하고 있다.
⑤ 정보통신부장관은 공인인증기관이 사위 기타 부정한 방법으로 지정을 받은 경우는 지정을 취소할 수 있다.

[정답] ④
[난이도] 하
[해설] 전자서명법은 1999년 제정당시 디지털서명 방식만을 인정하였으나, 2001년 개정을 통하여 디지털서명 방식과 동일한 수준의 안전성 및 신뢰성을 갖춘 다른 기술방식도 인정하는 입장을 수용하였다(기술중립주의).