오리엔테이션
(교과목 개요 및 수업 방향 소개)

박종혁

서울과학기술대학교 컴퓨터공학과

jhpark1@seoultech.ac.kr

1. 교과목 개요

1.1 담당교수 소개

박종혁교수 (Jong Hyuk Park)

- 최종학위: 공학박사 (전공-컴퓨터보안)
- 주 연구분야: 컴퓨터보안, 블록체인, IoT 및 클라우드 보안
- 연구실: 미래관 325호
- 홈페이지: http://www.parkjonghyuk.net

- 대표 약력

연도(부터 ~ 까지)	기관명	업무	직위
2009.9 ~ 현재	서울과학기술대학교 컴퓨터공학과	교육 및 연구	교수
2002.12 ~ 2007.7	한화에스앤씨㈜ 기술연구소	선임연구원	연구
2011.1 ~ 현재	국제 HCIS 논문지 (SCIE, 세계 상위 15%)	총괄편집위원장	편집위원장
2009.9 ~ 현재	한국정보처리학회	국제 및 저널 총괄	부회장

1.2 교과목 소개

교과목 명	컴퓨터보안 (Computer Security)
교과 구분	전공 선택 (3학점)
강의 시간	월 2,3,4 교시
강의 구성	이론 (3)
강의 방법	대면

1.3 교과목 개요

- 본 교과목에서는 컴퓨터보안의 이론, 응용, 실무에 대해서 소개함
- 접근제어, 악성 소프트웨어, 서비스거부공격 등 컴퓨터 보안 기본개념에 대해 학습함
- 컴퓨터 및 모바일 보안위협 관련 응용에 대해서도 학습함
- 최근응용분야인 사이버범죄 및 수사 관련 디지털 포렌식에 대하여 보다 심도있는 학습을 진행함

1.4 학습 목표

I. 컴퓨터보안의 실무분야의 이론, 응용, 실무에 대해 학습한다.

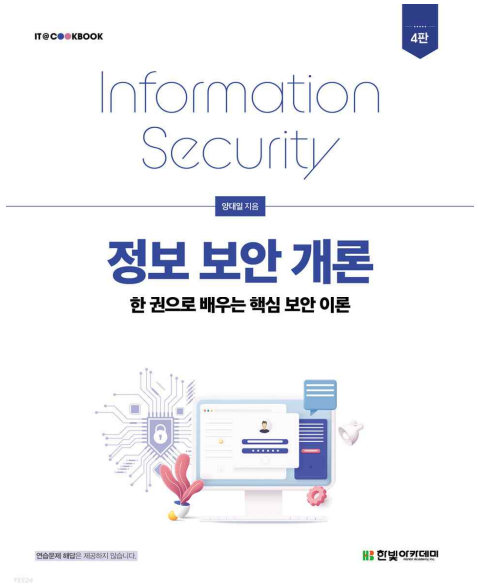
II. 컴퓨터보안의 실무분야인 디지털 포렌식에 대한 개념을 이해한다.

III. 최근 관련연구 분야에 대한 조사, 분석, 발표를 통해 복합적인 이론과 실무능력을 증진시킨다.

1.5 학습 교재

- **주교재**

  컴퓨터 보안, William Stallings 저,
  한영욱외 8인 역,
  한티미디어, 2016



- **보조교재**

- 정보보안 개론 (개정4판), 양대일 저, 한빛 출판네트워크, 2021

2.1 학습평가 방법

2.2 과제 설명

2.1 학습평가 방법

- **출석 (10%), 과제물 (20%), 중간고사 (30%), 기말고사 (30%), 기타(10%)**

- **기타**
  - 특별 발표
  - 비정기 퀴즈
  - 비정기 과제 등

2.2 과제 설명

과제 #1

- 컴퓨터 보안 관련 최근 연구 동향 보고서를 작성하여 기한 내 eClass에 업로드 한다.

  (8주차, 중간고사 당일 23시 까지)

과제 #2 :

- 개인과제 #1을 기반으로 "컴퓨터 보안에 대한 아이디어 제안"를 제작하여 기한 내 eClass에 업로드 한다.

  (14주차, 기말고사 전일 23시 까지)

기타 발표 (14주차-줌수업 시)

* 희망자 선착순 10명
  - 개인과제# 2 발표 (10분) ← 기타 점수 추가점 부여!!
  - 희망자는 조교선생님한테 9/10일까지 메일을 보내세요

    (조교: 진호천 석박사통합과정, chahot@seoultech.ac.kr)

컴퓨터보안의 필요성

- 보안사고 영상

대법원·국방부·국토부 홈페이지 맘만 먹으면 해킹..."직접 뚫어 봤습니다!" / YTN
https://youtu.be/oHRFGv_ljyo

'트위터 계정 해킹'...역사상 최악의 보안사고 / C채널방송
https://www.youtube.com/watch?v=TPxOtILDs2U

- 사이버 보안기술 영상

스스로 형태 바꿔 방어" 신개념 사이버 보안기술 등장 / YTN
https://www.youtube.com/watch?v=j67RZmqZvO8

컴퓨터보안의 필요성

- 정보 자산에 대한 중요성 증가에 따른 사이버 위협의 증가
- 비대면 사회 활동 증가에 따른 사이버 활동의 신뢰성 이슈
- 개인의 프라이버시 이슈 증가
- IT기술 발달로 인한 컴퓨터의 사회적 영향력 증가
  → 해킹, 인터넷 사기 등 사이버 공격 및 범죄 이슈 증가

→ 이러한 이슈들을 해결하기 위한
컴퓨터 보안 (정보보호)의 필요성 대두

컴퓨터보안의 정의

◆ **좁은 의미**

컴퓨팅(Computing) 의미? 계산하다

Computer Security

계산능력을 갖는 정보 시스템 내의 자원(하드웨어, 소프트웨어, 데이터, 통신 등)들의 무결성, 가용성, 기밀성을 보존하기 위해 제공되는 보안(보호)

◆ **넓은 의미**

컴퓨터보안 = 정보보호 (정보보안)

정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적, 정책적 수단, 또는 그러한 수단으로 이루어지는 행위

컴퓨터보안의 종류

- 악성 소프트웨어
- 시스템 보안
- 네트워크 보안
- 웹 보안 / 모바일 보안
- 운영체제 보안
- 데이터베이스 보안
- 보안 관리/보안정책

- ICT 융합 보안 (IoT, 클라우드, AI 등)
- 블록체인
- 디지털 포렌식

주차 별 강의 내용 간략 소개

-컴퓨터보안 개요

-보안위협

-최근 ICT 서비스 보안 위협

-사용자 인증 개요

-비밀번호 기반 인증

-토큰 기반 인증

-생체 인식 인증

-원격 사용자 인증

-인증 보안 이슈

-CAPTCHA

-접근제어 원리

-주체, 객체, 접근권한

-임의 접근제어

-역할 기반 접근제어

-속성 기반 접근제어

-자격 기반 접근제어

-신원, 신용장, 접근 관리

-실무 접근제어 솔루션 및 사례

4장 데이터베이스와 클라우드 보안

-데이터베이스 보안의 필요성

-데이터베이스 관리 시스템(DBMS)

-SQL 주입 공격

-데이터베이스 접근 제어

-추론

-데이터베이스 암호화

-클라우드 컴퓨팅

-클라우드 보안 위험과 대응

-클라우드 데이터 보호

-서비스로서 클라우드 보안

-기타 클라우드 보안 이슈

-악성 소프트웨어의 유형

-지능형 지속 위협 (APT)

-전파: 손상된 내용, 바이러스

-전파: 사회 공학, 스팸 전자메일,트로이 목마

-페이로드: 시스템 파괴

-페이로드: 공격 에이전트, 좀비,봇

-페이로드: 정보 도용, 키로거, 피싱, 스파이웨어

-페이로드: 은신, 백도어, 루트킷

-대비책

-네트워크의 이해

-네트워크 공격과 보안

-무선 네트워크 공격과 보안

-방화벽

-침입 탐지 시스템

-침입 방지 시스템

7장 디지털 포렌식 개관

-디지털 포렌식 개요

- 등장 배경
- 디지털 포렌식 흐름
- 디지털 포렌식 연구분야

-디지털 포렌식 조사의 일반 원칙

-디지털 포렌식 수행 과정

-디지털 증거

- 디지털 증거의 종류
- 디지털 저장 매체
- 디지털 증거의 특징

-디지털 증거의 개념 및 특성

-디지털 증거의 법적 허용성

-위법수집증거배제의 원칙

- 전문법칙 (傳聞法則, Hearsay Rule)

-디지털 증거의 법적 허용성 요건

- 디지털 증거의 증거 능력을 보장하기 위한 특성
- 디지털 증거의 법적 허용성 보장을 위한 장치
- 디지털 데이터의 증거 능력 관련 판례

9장 디지털 포렌식 수행 절차

-디지털 포렌식 조사 모델 정의

-디지털 포렌식 조사 모델 비교

-디지털 포렌식 조사 모델

- 조사 준비
- 현장 도착 시 대응
- 증거 확보 및 수집
- 운반 및 확인
- 조사 및 분석
- 보고 및 증언

10장 디지털 증거 수집 기술 및 분석 기술

-디지털 증거 수집 장비 및 SW

-활성 시스템 조사

-디스크 이미징

-임베디드 시스템 증거 확보

-디스크 브라우징 기술

-검색 기술

-타임라인 분석

-로그 분석

-시각화 기술

-안티포렌식 대응 기술

-파일시스템의 이해

-정보 보안 거버넌스

-보안 프레임워크

-보안조직

-보안 정책과 절차

-보안 인증

-개인 정보 보호

-ISMS-P 소개

Q & A

27