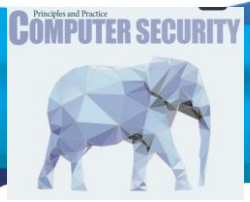
서울과학기술대학교

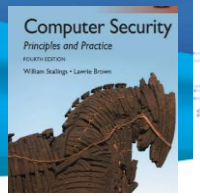
[2025년 2학기]
컴퓨터 보안 (Computer Security)

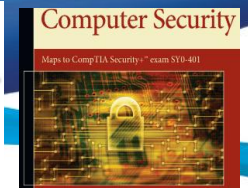
오리엔테이션
(교과목 개요 및 수업 방향)

2025. 9

박종혁 (Jong Hyuk Park) 교수
서울과학기술대학교 컴퓨터공학과
jhpark1@seoultech.ac.kr





목 차

1. 교과목 개요

1.1 담당교수 소개

박종혁교수 (Jong Hyuk Park)

- 최종학위: 박사1(정보보호), 박사2(Human Science)
- 주 연구분야: 컴퓨터보안, 블록체인, IoT 및 클라우드 보안, 양자정보기술, AI보안
- 연구실: 미래관 325호
- 홈페이지: http://www.parkjonghyuk.net
- 연구실: UCS Lab, https://ucs.seoultech.ac.kr/index.do
  연구실소개 자료 CLICK
- GQAS 연구소 부소장, https://gqas.seoultech.ac.kr

- 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

- 컴퓨터보안 개념 (정보보안 기초, 네트워크 보안, 보안 정책 등)의 이론, 응용, 실무에 대해서 학습함

- 인증, 접근제어 등 기본 필수 보안 및 악성 소프트웨어, 보안공격, 모바일 및 IoT 보안, 인공지능 보안, 양자 보안 등 응용보안에 대해 학습함

- 컴퓨터보안 사이버 범죄 수사관련 응용 분야인 디지털 포렌식에 대해 학습함

1.4 학습 목표

I. 컴퓨터보안의 실무분야를 위한 기본 이론, 응용, 실무 적용 등에 대한 필수 지식 습득

II. 컴퓨터 보안 개념이 적용된 최근 관련 응용 연구 분야 조사, 분석 및 신규 아이디어 제안을 통한 컴퓨터보안 지식의 창의성 및 활용성 능력을 배양함

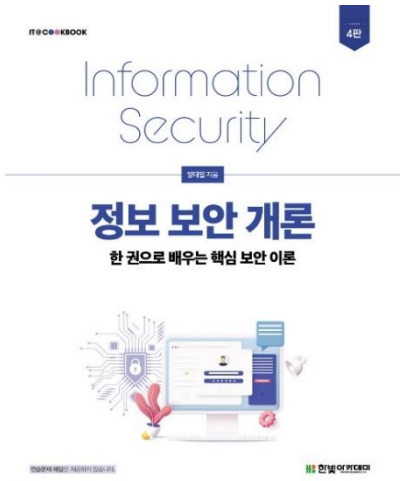
1.5 학습 교재

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

1.5 학습 교재

- **보조교재**

- 정보보안 개론 (개정4판), 양대일 저, 한빛 출판네트워크, 2021
- 네트워크 해킹과 보안(4판), 양대일 , 홍성혁 저, 한빛 아카데미, 2023
- 인터넷 해킹과 보안(4판), 김경곤 저, 한빛 아카데미, 2022



1.6 주차별 강의 운용 계획

주별	날짜	강의내용	수업방식	비고	보강 날짜
1	9/1	OT 및 교과목 개요	대면		
2	9/8	보안 위협요소와 백신	대면		
3	9/15	사용자 인증	대면		
4	9/22	접근제어	대면		
5	9/29	데이터베이스와 클라우드 보안	대면		
6	10/6	악성 소프트웨어	휴강	추석 연휴	온라인 영상 수업
7	10/13	네트워크 보안 (1)	대면	과제 1차 제출	
8	10/20	중간고사	대면		
9	10/27	네트워크 보안 (2)	대면		
10	11/3	디지털포렌식 (1)	대면		
11	11/10	디지털 증거	대면		
12	11/17	디지털포렌식(2-1)	휴강	논술고사일	온라인 영상 수업
13	11/24	디지털 포렌식 (2-2), 보안관리	휴강	국제 학술회의 참석	온라인 영상 수업
14	12/1	최신 ICT 보안 기술 및 과제 발표	대면	과제 2차 제출	
15	12/8	기말고사	대면		

2. 평가 방법

2.1 학습평가 방법

2.2 과제 설명

2.1 학습평가 방법

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

- **기타**
  - 과제 발표 (14주차)
  - 비정기 과제

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 보안 응용 기술 또는 서비스에 대한 신규 아이디어 제안"을 작성하여 기한 내 eClass에 업로드 한다.

  (14주차 수업 전일 23시 까지)

** 과제 양식을 꼭 사용하여 작성할것 (다른 양식 사용시 감점) **

** Copy Killer 검사 결과 꼭 제출할것 **

기타 발표 (14주차)

* 희망자 선착순 10명
  - 개인과제# 2 발표 (10분) ← 기타 점수 추가점 부여!!
  - 희망자는 조교선생님한테 9/22 18:00까지 메일을 보내세요

    (조교: 이태환, fgds8@seoultech.ac.kr)

과제 제출관련 중요사항

도서관 표절 검사기 (Copykiller) 활용

- 각 과제 보고서를 도서관의 표절검사기로 유사율을 검사하여 함께 제출 해야 함 (유사율이 높을 경우, 표절로 판정함)

Copy Killer CAMPUS 서울과학기술대학교 https://seoultech.copykiller.com

- 최근 전세계적으로 문서(레포트, 논문 등)에 관한 유사도를 확인하고있며, 연구 윤리 측면에서 심각한 문제로 대두됨
- 우리 수업에서도 **표절률** 이용 감산제를 적용함

- 유사도 검사 결과 표절율이 **30% 이상**인 학생에게 패널티를 부여함
  - 과제점수 * 표절율 감점 적용

- 예) 과제점수 7점, 표절율 40%
  - 패널티 점수 =3점
  - 과제점수 (7) * 표절율 (40%) = 2.8 (3점 적용)
  - 최종 과제 점수 = 기본점수 (7) – 패널티 점수 (3점) = 4점

- 표절률이 **60%** 이상인 보고서는 완전 표절로 판단 **"0점"**을 부여함

3. 컴퓨터보안의 필요성

- 보안사고 뉴스 영상

얼굴 사진 넣으면 10초 만에 딥페이크 뚝딱 / MBN 뉴스7
https://www.youtube.com/watch?v=Mx9Lfnpdwi U

보안 취약 업체 노렸나..한 곳 뚫린 뒤 줄줄이 해킹 / MBC
https://www.youtube.com/watch?v=iQDLDOzy3R8

보안 뚫린 北 서버 보니 줄줄이 쏟아진 건... / YTN
https://www.youtube.com/watch?v=PR1BjTyiwBg

- 사이버 보안기술

당신의 사이버 보디가드, AI기반 사이버 보안 플랫폼을 만나다 / 매일경제TV
https://www.youtube.com/watch?v=6MHqFQQsB78

AI 후속 테마는 AI 연관 산업"...사이버보안 주목/한국경제TV뉴스
https://www.youtube.com/watch?v=9zjov3_5ZzU

[STCON 2024] 최신 보안 기술 컨퍼런스
https://www.youtube.com/watch?v=K_oYhAZQP4E

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

4. 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) = 사이버 보안

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

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

5. 강의 내용

주차 별 강의 내용 간략 소개

-컴퓨터보안 개요

-보안위협

-최근 ICT 서비스 보안 위협

2장 사용자 인증

-사용자 인증 개요

-비밀번호 기반 인증

-토큰 기반 인증

-생체 인식 인증

-원격 사용자 인증

-인증 보안 이슈

-CAPTCHA

3장 접근제어

-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

5장 악성 소프트웨어

-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

6장 네트워크 보안

-네트워크의 이해

-네트워크 공격과 보안

-무선 네트워크 공격과 보안

-방화벽

-침입 탐지 시스템

-침입 방지 시스템

7장 디지털 포렌식 (1) - 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

8장 디지털 증거

-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 (2-1) - 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

9장 디지털 포렌식 (2-2) -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

10장 보안관리

-정보 보안 거버넌스

-보안 프레임워크

-보안조직

-보안 정책과 절차

-보안 인증

-개인 정보 보호

-ISMS-P 소개

11장 최신 ICT 보안기술

-양자 정보기술 (보안)

-Zero Trust

-AI 보안 등

6. 컴퓨터보안 전망

◆ 전망: 현정부 – 대통령 공약

o 디지털경제 패권국가' 도약을 위한 실천과제: **사이버보안 10만 인재 양성**

- 신규 인력공급
- 재직자 역량 강화

정규 과정 (1.0만명)

[고급] 대학원(0.1만명)
- (확대)융합보안대학원 확대 (8개교 → 12개교, 석사 → 석·박사)

[중급] 대학(0.4만명)
- (확대)정보보호특성화대 확대(3개교→10개교)

[초급] 특성화고·전문대학(0.4만명)
- (신규)사이버부사관 특화 정보보호 전문대학

특화 교육 (3.9만명)

[고급] 최정예 우수 인력 확보(0.1만명)
- (신규)최정예 보안제품 개발과정 'S-개발자'(50명)
- 정예 화이트해커(Best of Best, BoB) 양성(200명)

[중급] 실무형 인재 양성(3.6만명)
- (확대)구직자 대상 K-Shield Jr.(300명→1000명)
- (신규)중급 화이트해커(화이트햇 스쿨) 양성(300명)
- (신규)시큐리티 아카데미 도입(200명)

[초급] 보안관리 인력 공급 확대(0.2만명)
- (확대)ICT 융합 보안교육 확대(400명→600명)

사이버 훈련장 (2.5만명)

'디지털 실전형 사이버훈련장' 구축(2.5만명)
- [고급] 실전형 사이버 공격·방어 훈련 실시
- [중급] 침해사고 대응 등 해킹방어 기본기술 습득
- [초급] 동영상 강의, 실습 등 기초역량 교육

지역 교육 (2.6만명)

'지역 정보보호교육센터' 설립(2.6만명)
- [중·고급] 악성코드 분석·탐지 등 실무형 교육
- [초급] 사이버보안 소양, 보안제품 실습 등 기초 직무 교육

◆ 전망: 현정부 – 보안투자 확대

O 2023년 우리나라 정부의 정보 보호 정책 사업 예산(출처: 과학기술정보통신부)

구분	세부 사업	예산(전년 대비 증가율)
사이버보안 인재 양성	보안 핵심 인재 육성	67억 6000만 원(17.4%)
	정보 보호 전문 인력 육성	162억 8000만 원(68.2%)
	지역 정보 보호 교육 지원	23억 8000만 원 (36.6%)
	실전형 사이버 훈련장 구축	20억 원(신규)
정보 보호 산업 육성	정보 보호 산업 경쟁력 강화	74억 2000만 원(3.4%)
	정보 보호 시스템 평가 및 인증 기반 강화	21억 8000만 원(9.9%)
	전자 서명 인증	45억 원(116.4%)
사이버 보안 기술 개발	암호화 사이버 위협 대응 기술	30억 원(신규)
	국방 드론 사이버 보안 기술 개발	17억 7000만 원(신규)
	데이터 프라이버시 기술 R&D	56억 원(30.2%)
	무인 서비스 물리 보안 플랫폼 개발	40억 원(33.3%)
	사이버 보안 챌린지	33억 원(41.9%)
사이버 침해 사고 대응	해킹, 바이러스 대응 체계 고도화	641억 4000만 원(1.2%)

학교

◆ 정보보호산업의 글로벌 경쟁력 확보 전략

○ 2027년까지 정보보호산업 시장규모 30조원 달성, 보안유니콘 육성 등을 목표로 4대 전략과 13개 과제를 추진 (출처: 과학기술정보통신부)

참고문헌

1. 尹 정부, 사이버보안 인재 10만명 키운다, 2022, https://zdnet.co.kr/view/?no=20220713103021
2. 2023년 정부 정보보호 정책 사업에 약 3000억원이 투입된다. 올해보다 4.5% 늘어난다.,2022, 전자신문, https://www.etnews.com/20220905000100
3. 정보보호 산업규모 2027년 30조원 목표... 예산 1조 1천억 투입, 보안뉴스, 2023, https://www.boannews.com/media/view.asp?idx=121642

Q & A

36