<2016년도 2학기>

1. 강의개요

학습과정명	암호프로토콜	학점	3	교강사명		교강사 전화번호	
강의시간	3	강의실	학습과정 현황 참조	수강대상	정보보호	E-mail	

2. 교육과정 수업목표

- 암호화, 해시함수, 전자서명을 포함하는 네트워크 보안 응용에 사용되는 암호 알고리즘과 프로토콜에 대해 학습한다.
- 네트워크와 인터넷의 보안을 위한 암호 알고리즘과 보안 프로토콜 사용에 대해 학습한다.
- 네트워크 보안의 대표 기술인 SSL/TLS, IPSEC을 이해하고 S/MIME, PGP등의 전자 메일 보안 등을 학습하며 나아가 무선 네트워크 보안도 학습한다.

3. 교재 및 참고문헌

주교재	네트워크 보안 에센셜 4판	저자	William Stallings	출판사	생능	출판년도	2013
부교재(참고문헌)	Open SSL을 이용한 컴퓨터 시스템 보안 2판	저자	최태영	출판사	카오스북	출판년도	2013

4. 주차별 강의(실습·실기·실험) 내용

주별	차시	강의(실습·실기·실험) 내용	과제 및 기타 참고사항
제 1 주	1 2 3	[1] 강의주제 : 정보보호의 개념 [2] 강의목표 : 보안 구조와 관련 서비스 [3] 강의세부내용 : ① OSI 보안 구조 ② 보안 공격 ③ 보안 서비스 ④ 보안 메커니즘 [4] 수업방법 : 강의 및 질의응답	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.30-59 강의교안
제 2 주	1 2 3	[1] 강의주제 : 대칭 암호 [2] 강의목표 : 대칭 암호화 메시지 기밀성 [3] 강의세부내용 : ① 대칭 암호 원리 ② 대칭 암호 알고리즘 (DES, 3DES, AES) ③ 의사랜덤넘버 ④ 암호 블록 운용 모드 [4] 수업방법 : 강의 및 질의응답	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.63-99 부:P.44-75 강의교안
제 3 주	1 2 3	[1] 강의주제 : 공개키 암호 [2] 강의목표 : 공개키 암호와 메시지 인증 [3] 강의세부내용 : ① 메시지 인증 방법 ② 안전 해시함수 ③ 공개키 암호 원리 ④ 디지털 서명 [4] 수업방법 : 강의 및 질의응답	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.109-148 부:P.81-106 강의교안
제 4 주	1	[1] 강의주제 : 네트워크 보안 응용 1 [2] 강의목표 : 키 분배와 사용자 인증	기자재: 실습용PC, 빔 프로젝터

		[3] 강의세부내용 : ① 대칭키 분배 ② KERBEROS Version 4/5 ③ 비대칭 암호를 이용한 키 분배 ④ X.509 인증서 및 공개키 기반 구조 [4] 수업방법 : 강의 및 질의응답	스크린, 화이트보드 학습자료 : 주:P.158-196 부:P.110-181, P.278-285 강의교안 **과제 : OpenSSL을 통한 공개키 암호화**
제 5 주	1 2 3	[1] 강의주제 : 네트워크 보안 응용 2 [2] 강의목표 : 전송 레벨 보안 [3] 강의세부내용 : ① 웹보안 ② 전송 계층 보안 ③ SSL ④ SSH [4] 수업방법 : 강의 및 발표	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.217-258 부:P.278-314 강의교안
제 6 주	1 2 3	[1] 강의주제 : 네트워크 보안 응용 3 [2] 강의목표 : HTTP와 HTTPS [3] 강의세부내용 : ① HTTP 프로토콜의 이해 ② HTTPS 프로토콜 ③ 연결 개시 ④ 연결 종료 [4] 수업방법 : 강의 및 질의응답	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.243-244 부:P.278-314 강의교안
제 7 주	1 2 3	[1] 강의주제 : 네트워크 보안 응용 4 [2] 강의목표 : 무선 네트워크 보안 [3] 강의세부내용 : ① IEEE 802.11 무선 LAN ② 무선 응용 프로토콜 (WAP) ③ 무선 전송층 보안(WTLS) [4] 수업방법 : 강의 및 질의응답	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.265-312 부:P.286-291 강의교안
제 8 주	1 2 3	중 간 고 사	
제 9 주	1 2 3	[1] 강의주제 : 전자메일 보안 [2] 강의목표 : Pretty Good Privacy [3] 강의세부내용 : ① 동작 과정 ② 암호 키와 키 관리 ③ 공개키 관리 [4] 수업방법 : 강의 및 질의응답	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.325-350 부:P.91-94, P.110-134 강의교안
제 10 주	1 2 3	[1] 강의주제 : 전자메일 보안 [2] 강의목표 : S/MIME [3] 강의세부내용 : ① RFC 5322 ② MIME ③ S/MIME 기능 ④ S/MIME 인증서 처리 [4] 수업방법 : 강의 및 질의응답	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.351-372 부:P.91-94, P.110-134 강의교안
제 11 주	1	[1] 강의주제 : IP보안 [2] 강의목표 : IPSec	기자재: 실습용PC, 빔 프로젝터

	2 3	[3] 강의세부내용 : ① IPSec의 이해 ② IPSec 서비스 ③ 전송 모드와 터널 모드 ④ IP 보안 연관 정책 [4] 수업방법 : 강의 및 질의응답	스크린, 화이트보드 학습자료 : 주:P.391-405 강의교안 **수시평가**
제 12 주	1 2 3	[1] 강의주제 : IP보안 [2] 강의목표 : 캡슐화와 키교환 [3] 강의세부내용 : ① ESP 형식 ② 암호화 및 인증 알고리즘 ③ 전송 모드와 터널 모드 ④ 키 결정 프로토콜 [4] 수업방법: 강의 및 질의응답	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.406-434 강의교안
제 13 주	1 2 3	[1] 강의주제 : 시스템 보안 [2] 강의목표 : 침입 탐지 [3] 강의세부내용 : ① 감사기록 ② 침입탐지 방법 ③ 허니팟 ④ 침입탐지 교환 형식 [4] 수업방법 : 강의 및 질의응답	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.439-488 강의교안
제 14 주	1 2 3	[1] 강의주제 : 악성소프트웨어 [2] 강의목표 : 바이러스와 웜 [3] 강의세부내용 : ① 바이러스 유형 ② 안티바이러스 방법 ③ 웜 유형 ④ 웜 대응 방안 ⑤ 분산서비스거부 공격과 방어 [4] 수업방법 : 강의 및 질의응답	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.439-528 부:P.316-333 강의교안
제 15 주	1 2 3	기 말 고 사	

5. 성적평가 방법

중간고사	기말고사	과 제 물	출 결	기 타	합 계	비 고
30%	30%	10%	20%	10%	100%	

6. 수업 방법(강의, 토론, 실습 등)

- 강의, 발표, 질의응답

7. 수업에 특별히 참고하여야 할 사항

8. 문제해결 방법(실험·실습 등의 학습과정의 경우에 작성)