교과목 개요

1. 정보보호론

이 과목은 정보보호에 대한 전반적인 내용을 포괄적으로 다룬다.
전반1부에는 정보보호관련 개론, Usable Security, 암호학 등을 다룬다. 전반 2부는 운영체제의 공격에 대한 일반적인 소개와 이들로부터 운영체제를 보호하는 기법을 파악한다. 후반1부에서는 네트워크 공격 및 보안에 관련한 내용 등을 다룬다. 후반 2부에서는 소프트웨어에 대한 공격 및 보안을 다룬다.

2. 정보보호실습

본 과목에서는 다양한 보안이론에 대한 실험실습을 중심으로 암호, 시스템 방어, 소프트웨어 공격, 네트워크 공격 및 방어 등의 기술을 학습한다.

3. 시스템보안개론

공격으로부터 안전한 시스템을 디자인 할 수 있는 기초적인 역량을 배양하기 위하여 시스템이 공격당하는 원인과 이를 방어하기 위한 기법들을 학습한다. 또한, 고신뢰 시스템을 설계하기 위해 많이 이용되는 커널 감시 기법들와 신뢰 실행 환경들에 대해 학습한다.

4. 해킹의 이해

본 강좌는 정보 보호를 이해하는데 있어서 기본이 되는 시스템에 대한 공격에 대하여 살펴보고자 한다. 다양한 시스템에 대한 다양한 공격 방식에 대한 학습을 통하여 새로운 공격을 찾는 방법을 습득하여 향후에는 안전한 시스템의 설계에 운용할 수 있는 기초를 닦고자 한다.

5. 컴퓨터 구조와 보안

본 과목은 컴퓨터 보안에 필수적인 컴퓨터 시스템의 구조를 이해하도록 하는데 목적이 있으며 기본적인 컴퓨터 구조와 시스템 보안에 관련된 토픽을 다룬다. 첫 번째로 컴퓨터 구조의 기본이 되는 프로세서 구조, 캐쉬 및 메모리 시스템, 가상 메모리 및 시스템 가상화 지원, I/O 시스템을 이해하도록 한다. 두 번째로 하드웨어 기반의 보안 기술에 대해 다루도록 한다.

6. 정보보호 정책 및 경영

본 과목에서는 정보보호에 관한 국가적 정책에 관련된 이슈 및 대응체계와 한 기업이나 공공기관이 정보보호를 이룩하기 위한 다양한 관리적 대응방안들과 정보보호 산업에 대해 다룬다.

7. 컴퓨터 보안을 위한 머신러닝

이 과목은 기계 학습의 기본 이론과 이와 관련된 여러 기술들과 알고리즘들을 소개한다. Percepton 이론에서 부터 최근의 Boosting, SVM 그리고 Bayesian networks 이론에 대해서 설명한다. 또한, 대부분의 알고리즘에서 사용되는 통계적 추론을 기본으로 수업이 진행된다.

8. 보안을 위한 정보이론

정보이론은 보안시스템 또는 보안 시스템을 이루고 있는 요소기술들의 성능을 분석하는 도구로서 중요한 역할을 한다. 본 과목에서, 보안 시스템을 분석할 때 필요한 정보이론의 기초와 정보이론 기반의 보안 과목을 수강하기위한 기초 지식을 습득할 수 있다.

9. 네트워크 보안

이 과목에서는 네트워크 보안과 관련된 기본적인 이론 및 기술에 대해서 강의 합니다. OSI 7 layer를 기준으로 각 layer에서 발생할 수 있는 기본적인 보안 이슈와 이를 해결하는 방법에 대해서 강의 합니다.

10. 무선이동인터넷과 보안

무선이동인터넷과 관련 보안기술을 이해하고자하는 대학원생을 위한 과목으로, 개념, 기술, 최근 동향 및 open issues를 다루고자한다. 다루는 주제로는 이동인터넷을 위한 네트워크 (IEEE 802.11, 애드호크 네트워크, 무선매쉬 네트워크 등)와 서비스(VoIP, Video streaming, Location based services 등)에 관한 프로토콜, 정보보호, 표준화 등이다.

11. 사용자중심적 보안

보안시스템의 개발은 활발히 이루어지고 있으나 유용성을 높이기 위해서는 아직 많은 연구가 필요합니다. 이 과목은 보안시스템의 여러가지의 유용성 관련 문제점과 제안된 해결방안을 소개, 분석하며 학생들은 이 과목을 통하여 사용자를 중심으로 하는 보안시스템에 대하여 연구할 수 있는 기회를 얻게 될 것입니다.

12. 바이너리코드 분석과 소프트웨어 보안

본 강의에서는 소프트웨어의 해킹과 보안에 대한 이론과 기술에 대해 학습한다. 메모리 취약점, 익스플로잇, 악성코드, 웹 공격, 그리고 프로그램 분석에 이르는 다양한 소프트웨어 보안의 테마에 대하여 공부하며, 해킹공격과 방어에 대한 다양한 실습을 진행한다.

13. 커널 시스템 보안

운영체제의 커널은 시스템의 기본적인 기능들을 제공하며 어플리케이션들이 동작할 수 있는 환경을 제공하는 시스템의 가장 핵심적인 소프트웨어이다. 본 과목에서는 시스템의 핵심인 운영체제 커널의 동작방식에 대한 개념과 원리를 보안과 관련된 부분에 중점을 두고 공부하여, 학생들은 오픈소스 운영체제인 리눅스의 동작 원리를 익히고, 운영체제 커널 레벨 프로그래밍을 통해 커널에 대한 이해도를 높여, 이러한 운영체제 커널을 공격하는 악성코드인 루트킷을 분석하고 이를 탐지 차단 하는 방법을 디자인 할 수 있는 능력을 배양한다.

14. 가상화 시스템 보안

하이퍼바이저인 Xen 을 기반으로 하이퍼바이저의 상세한 작동원리를 학습하고 하이퍼바이저 레벨에서 OS 의 커널레벨 악성코드를 탐지 및 차단할 수 있는 방법에 대하여 이론적으로 학습한 뒤 실습을 통해 구현할 수 있는 능력을 배양한다.

15. 고급네트워크 보안 기술의 이해

이 과목에서는 네트워크 기술 및 보안과 관련된 고급 기술, 최신 동향, 이론 및 기술에 대해서 강의합니다. 교과서에서 미처 다루지 못하는 최신 네트워크 기술과 이에 대한 공격과 방어 기술을 다루며, 동시에 이런 방어 기술을 실제로 구현해 보도록 합니다. 또한, 수강 학생이 담당 교수의 지도하에 프로젝트를 수행하여 직접 최신 네트워크 보안 관련 연구를 수행해 보도록 합니다.

16. 디지털 콘텐츠 보안

본 교과목에서는 모바일 인터넷이나 웹을 이용한 각종 미디어 유통시 개인적인 미디어 데이터나 경제적 부가가치가 있는 멀티미디어 콘텐츠를 보호하기 위한 각종 보호/보안 기술과 이와 관련된 최신 연구 내용들을 공부한다. 특히 영상, 동영상, 오디오 등의 미디어 데이터를 보호하기 위한 기법들에 초점을 맞추어 관련 기법들을 공부한다.

17. 정보보호 신기술 융합 특론

- 정보보호기술, 정책 등을 포함한 정보보호 고급이론과 해킹사고 대응분석 결과 등 정보보호 실무기술 및 미래 정보보호 신기술을 학습
- 사이버 해킹사고에 대해 각 CASE별 분석 및 대응방법, 정책적인 방안 제시

18. 정보보호 특강

정보보호는 역사가 길지는 않으나 최근 폭발적으로 성장을 하고 있는 연구 분야이다. 매년 새로운 분야가 생겨나고 있으며 다양한 전공들과의 융합이 활발하게 일어나고 있는 분야라고 할 수 있다. 본 강좌는 이러한 융합의 시류를 반영하기 위하여 현재의 흐름을 파악할 수 있는 주제, 새로운 개념, 새로운 분야 등을 다룬다.