Course Description

IS511 Information Security

This lecture covers a wide variety of information security issues. Its first part includes general issues like threats and vulnerabilities, information security management systems, risk analyse and information classification. Second part provides introductions of technical methods like access control, cryptographic control, system and network security control. Final part discusses social and legal issues like digital forensic, law, industrial espionage, privacy and Internet ethics.

IS521 Information Security Laboratory

This course covers a broad range of security topics including cryptography, OS defenses, software exploitation, network attacks and defenses. Students will gain extensive hands-on experience on various topics in security.

IS522 Introduction to Systems Security

The main purpose of this course is to explore systems exploitations and defenses techniques with the goal of cultivating the cability to design a robust system against attacks. The class also introduces kernel reference monitors and trusted execution environments, which can be employed in designing secure systems.

IS523 Hacking Exposed

Every scientific research starts from finding new problems. Likewise, the most important step in security research is to discover new attacks. Today, media is filled with attacks on various systems: Web servers, DNS, Internet banking, e-voting systems, cellular networks, social networks, mobile phones, nuclear power plants, and implantable medical devices. These attacks are originated from various vulnerabilities, such as user interface design, ignorance or security by obscurity, deployment mistakes, and physical exposure. The main objective of this course is to learn how to think like an adversary. In other words, we will look at various ingenuous attacks and discuss why and how such attacks were possible. This is first crucial step to design and deploy systems robust against various attacks.

IS531 Computer Architecture and Security

This course covers the computer architecture essential for system security, addressing the basic understanding of computer organization, and the advanced issues for hardware security. For the basic computer architecture, this course covers processor architecture, cache and memory organization, virtual memory and hardware support for virtualization, and I/O subsystems. This course also addresses hardware-rooted security techniques.

IS532 Information Security policy and management

In this lecture, we will discuss national cyber security issues and policies, various managerial issues and methods related to information security in an organization, and information security business strategy.

IS534 Machine learning for computer security

This course introduces students the fundamental concepts and intuition behind modern machine learning techniques and algorithms, beginning with topics such as perceptron to more recent topics such as boosting, support vector machines and Bayesian networks. Statistical inference will be the foundation for most of the algorithms covered in the course.

IS537 Information Theory for Security

Information theory plays an essential tool to evaluate secrecy systems and sub-systems. This lecture is a prerequisite to information theoretic security and also provides students with solid grasp of fundamental theories.

IS539 Network Security

In this coursework, students will learn about basic network security theories and issues. Based on OSI-7 layer, we will investigate network security issues and solutions in each layer. In addition, students will learn some basic network attacks, such as worm and DDoS.

IS541 Wireless Mobile Internet and Security

This course is intended for graduate students who want to understand Wireless Mobile Internet and related security issues. It provides a comprehensive technical guide covering introductory concepts, fundamental techniques, recent advances and open issues in IEEE 802.11, ad hoc networks and wireless mesh networks with their security matters. The course consists of lectures, exams and term project.

IS551 User-Centric Security

Despite continuous effort to develop user-centric security mechanisms, bridging the chasm between security and usability is still a core scientific challenge. Regardless of the level of protection that a security system can provide, its security guarantee is bounded by the humans who operate the system. Hence, usability and security must be considered concurrently. This course introduces a variety of usability issues related to security and current research efforts in this area. Students also get an opportunity to conduct a research project to analyze and improve a variety of usability issues in the current security systems.

IS561 Binary Code Analysis and Secure Software Systems

This course provides an in-depth study of attacks and defenses in software. The major themes this course will teach include memory safety vulnerabilities, control-flow hijacking, malicious software, web attacks, program analysis techniques, and software model checking. We will offer significant hands-on experience on each topic.

IS571 Advanced Cyber Security Practice

The goal of the course is raising up the ability of security vulnerability analysis. We will practice debugging and exploitation of the vulnerability examples. Each student will analyze, exploit and present assigned vulnerabilities which are patched vulnerabilities of the web browsers.

IS572 Embedded Systems Security

Embedded systems are just everywhere around us. All we have smart phones, and we are surrounded by IoT devices, network appliances, military systems, vehicular devices, and/or industrial control devices. Recently, media covers the security problems in deploying such embedded systems almost everyday. This course aims to raise the ability of security analysis in view of offensive manner so that students also can design any defense measures around this area.

IS593 Introductory Special Topics in Security and Privacy

Area of security and privacy has been changed rapidly. News areas are showing up every year and a lot of convergence with different field is happening. To address these, this course covers topics of interest in security and privacy at the graduate level. The course content is specifically designed by the instructor.

IS631 Kernel System Security

Operating system kernel is the most critical component in the system as it provides the basic functionalities and the secure environment in which applications run and operate. In this course, the fundamentals of OS kernel and system programming, principles and operation of the open-source Linux operating system are taught with an emphasis on security aspect, so that students can acquire a comprehensive understanding of operating system kernel, analysis methods and countermeasures against various rootkit malware that compromise and manipulate operating system.

IS632 Hypervisor System Security

Hypervisor is a software platform that virtualizes computer hardware to support multiple instances of operating system running concurrently on a shared hardware system. Hypervisors are also widely used for cloud-based hosting service. This hypervisor platform can be utilized for higher degree of isolation for computer security monitoring and analysis. It provides an adequate environment for building kernel integrity monitors. This course will provide the fundamentals and inner-workings of hypervisors in the context of designing new security, monitoring, and analysis tools

IS639 Advanced Network Security

In this class, students will learn about recent and emerging networking technology and related security issues through research papers. In addition, students will learn how to realize the covered techniques by implementing real network security applications.

IS681 Content Security

In this course, multimedia data protection and related security issue will be studied for privacy and commercial property protection. Particulary, image video, and related media protection mechanism will be focused including the digital watermarking, fingerprinting, etc.

IS711 Advanced Theory for Information Security Technology Convergence

A study for advanced information security theory including technology, policy and manager and cyber hacking response process, Future information security technology. Case study for Real cyber hacking incident and proposal for cyber hacking response measure

IS893 Special Topics in Security and Privacy

Area of security and privacy has been changed rapidly. News areas are showing up every year and a lot of convergence with different field is happening. To address these, this course covers topics of interest in security and privacy at the graduate level. The course content is specifically designed by the instructor.

IS960 M.S. Thesis Research

IS966 Seminar (M.S.)

IS980 Ph.D. Dissertation Research

IS986 Seminar (Ph.D.)